**JOINT COMMENTS OF
AIRLINES FOR AMERICA,
THE INTERNATIONAL AIR TRANSPORT ASSOCIATION,
THE REGIONAL AIRLINE ASSOCIATION, AND
THE NATIONAL AIR CARRIER ASSOCIATION**

Docket CDC-2020-0013

ATTACHMENTS PART 2

JOINT COMMENTS OF
AIRLINES FOR AMERICA,
THE INTERNATIONAL AIR TRANSPORT ASSOCIATION,
THE REGIONAL AIRLINE ASSOCIATION, AND
THE NATIONAL AIR CARRIER ASSOCIATION

Docket CDC-2020-0013

ATTACHMENT 17

Department of Health and Human Services
Centers for Disease Control and Prevention

OMB Control No.:0920-1180
Expiration date: 05/31/2020

ORDER OF THE CENTERS FOR DISEASE CONTROL AND PREVENTION, DEPARTMENT OF HEALTH AND HUMAN SERVICES UNDER 42 CFR 71.31 and 71.4

Attn: Each airline carrying a passenger who has departed from, or was otherwise present within, the People's Republic of China (excluding the special administrative regions of Hong Kong and Macau) within 14 days of the date of the passenger's entry or attempted entry into the United States via that airline's carriage.

In accordance with 42 CFR §§ 71.31(b) and 71.4(d), as authorized by 42 U.S.C. § 264:

1. Each airline is hereby ordered to collect and provide information about any passenger who has departed from, or was otherwise present within, the People's Republic of China (excluding the special administrative regions of Hong Kong and Macau) within 14 days of the date of the passenger's entry or attempted entry into the United States via that airline's carriage ("Designated Passengers").
2. Each airline must collect and provide the following information ("Designated Information") to the extent such information exists for any Designated Passenger carried by that airline:
    a. Full name (last, first, and, if available, middle or others);
    b. Primary contact phone number to include country code, at which a Designated Passenger can be contacted while in the United States;
    c. Secondary contact phone number to include country code;
    d. Address or addresses while a Designated Passenger is in the United States (number and street, city, State, and zip code), except that a U.S. citizen or a lawful permanent resident will provide address of permanent residence in the United States (number and street, city, State, and zip code); and
    e. Email address that a Designated Passenger will use for email communications while in the United States.
3. Each airline must produce, using existing data-sharing channels, the Designated Information to the Director of the CDC's Division of Global Migration and Quarantine ("DGMQ"), or his representative. If existing data-sharing channels become unavailable, within 12 hours, the affected airline or airlines must identify an alternate means of transmitting the required data in a manner acceptable to CDC.
4. Each airline must provide Designated Information within 2 hours of the departure of the flight carrying a Designated Passenger.
5. Before or immediately upon arrival in the United States, each airline must provide to CDC (the head of the arrival airport's Quarantine Station) the name of any Designated Passenger who had refused or was otherwise unable to provide all five fields of the Designated Information prior to departure.
6. Each airline must provide Designated Information for the duration of the January 31, 2020 Proclamation on Suspension of Entry as Immigrants and Nonimmigrants of Persons who Pose a Risk of Transmitting 2019 Coronavirus. This order will

An agency may not conduct or sponsor, and a person is not required to respond to a collection of information unless it displays a currently valid OMB Control Number. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to CDC/ATSDR Reports Clearance Officer, 1600 Clifton Road NE, MS D-74, Atlanta, Georgia 30333; ATTN: PRA 0920-1180 cease to be effective when the Interim Final Rule at Federal Register, Vol. 85, No. 29, ceases to be effective.

The CDC Director has determined that Designated Passengers may be at risk of exposure to COVID-19. CDC will use this information for the purposes of public health follow-up, such as health education, treatment, prophylaxis, or other appropriate public health interventions, including travel restrictions.

"Airline" as used in this order has the meaning provided at 42 CFR § 71.1(b).

Failure to comply with this order may result in the imposition of fines or other penalties as provided in 42 U.S.C. § 271 and 42 C.F.R. § 71.2, or as otherwise provided by law. CDC maintains information retrieved by personal identifier in accordance with federal law, including the Privacy Act of 1974 (5 U.S.C. § 552a). Identifiable information may be shared only for lawful purposes, including with authorized personnel of the U.S. Department of Health and Human Services, state and local public health departments, and other cooperating authorities. CDC will delete the Designated Information when no longer required for the purposes set forth above, in accordance with federal law, and request that State and local governments do the same.

CDC may modify this order by an updated publication in the Federal Register or by posting an advisory to follow at www.cdc.gov.

In testimony whereof, the Director, Centers for Disease Control and Prevention, U.S. Department for Health and Human Services, has hereunto set his hand at Atlanta, Georgia, this 18th day of February, 2020.

Robert R Redfield MD

Robert R. Redfield, M.D.
Director, Centers for Disease Control and Prevention

**JOINT COMMENTS OF
AIRLINES FOR AMERICA,
THE INTERNATIONAL AIR TRANSPORT ASSOCIATION,
THE REGIONAL AIRLINE ASSOCIATION, AND
THE NATIONAL AIR CARRIER ASSOCIATION**

Docket CDC-2020-0013

ATTACHMENT 18

GUIDELINES

ON

ADVANCE PASSENGER INFORMATION

(API)

WCO/IATA/ICAO

2014

GUIDELINES ON ADVANCE PASSENGER INFORMATION

TABLE OF CONTENTS

Appendices to the API Guidelines are published as separate downloadable files

*

* *

INTRODUCTION

1.1. In recent years there has been a dramatic growth in passenger numbers on scheduled and charter flights in all regions of the world. In spite of recent events there is every indication that this strong growth in passenger traffic will be sustained for the foreseeable future.

1.2. Customs and other Border Control Agencies (Immigration, Police, Quarantine, Health and Safety, Agriculture, etc.) are therefore being faced with a greatly increased workload. In normal conditions shouldering this increased burden would not pose insurmountable problems. However, two additional factors have combined with the increase in passenger numbers to make the task of the Border Control Agencies very difficult indeed. These factors are the increased compliance risk posed by the growth in, for example, trans-national organized crime and a manpower shortfall within the Border Control Agencies themselves.

1.3. While the demands on the Border Control Agencies continue to grow and the manpower resources within which they must operate tighten, a number of very valuable opportunities have arisen, which, if taken advantage of, could allow these Agencies to maintain or even enhance their effectiveness. These opportunities are mainly in the following fields:

- Information Technology,
- Greater co-operation between Border Control Agencies domestically,
- Greater international co-operation between Customs and with other Border Control Agencies,
- Greater co-operation between Border Control Agencies and carriers.

1.4. Co-operation, particularly in relation to intelligence exchange, is extremely important. As it is recognized that success in the enforcement of Customs and other laws relies more on carefully targeted efforts, based on high quality intelligence, than it does on random or systematic action, Border Control Agencies have been making significant efforts to ensure their resources are directed toward those areas where they are most likely to produce noteworthy results.

1.5. Having underlined the role of intelligence as a key ingredient in effective enforcement, it is also important to stress the benefits that can be gained from the efficient use of Information Technology (i.e. computerized passenger screening/clearance systems). The deployment of such systems, incorporating passenger selection criteria developed on the basis of high quality intelligence, can and do have a very positive effect on enforcement activities. Information Technology can be further harnessed to ensure that details of arriving passengers are received in advance of the arrival of the flight - thus allowing the Border Control Agencies adequate time to utilize their resources more efficiently. This advance notification to the Border Control Agencies by carriers (or other parties) using electronic data inter-change (EDI), is the topic of this Guideline. Advance Passenger Information (API) is already in use at a number of locations around the world and has brought benefits to all concerned (Border Control Agencies, Passengers, Airport Authorities, Carriers). These benefits are discussed in greater depth in Section 6 of this Guideline.

1.6. Although much of the content of this Guideline is focused on the discussion of the many issues which surround API, there is one part of the Guideline that is more in the nature of a joint recommendation of the World Customs Organization (WCO), International Air Transport Association (IATA) and the International Civil Aviation Organization (ICAO). That part concerns the data to be transmitted from the carrier in the airport of departure to the Border Control Agency(ies) in the country of departure, in countries where the flight will transit and in the country of final destination. The data requirements shown in that part of the Guideline should be the maximum required by a Border Control Agency in respect of an inbound or outbound flight. Further details may be found in Section 8.

1.7 Ultimately, the goal of this Guideline is to establish an agreed best practice, to which States and aircraft operators seeking to implement API systems can, to the greatest extent practicable, adhere. Non-standard API programme implementation may lead to operational and financial implications for both government and aircraft operators.

1.8. This document does not cover the provisioning of Passenger Name Record (PNR data to Border Control Agencies. PNR is explored in other WCO/IATA/ICAO instruments.

1.9. If the Guideline gives rise to any questions on the part of implementers, please do not hesitate to contact either the Secretariat of the WCO, IATA or the ICAO. Although this paper focuses on the use of API for air passengers, it is clear that the technique can also be used for passengers using other modes, particularly cruise liner traffic. The material in this Guideline also applies mutatis mutandis to the other modes of transport.

PROBLEM DEFINITION

Growth in passenger numbers

2.1. As mentioned in the introduction, there are a number of factors influencing the manner in which passengers are processed by Border Control Agencies at international airports around the world. Perhaps the principal factor is the sheer volume of passengers travelling on international flights. The rate of growth varies in the different regions of the world, between 5% and 7%. In a region with a 5% growth rate, passenger numbers will double in 14 years, while in regions with a 7% growth rate numbers will double in 10 years. In addition, the introduction of new very large aircraft, most notably in airports already operating at or at near capacity, will only further exacerbate congestion and the associated demand on inspection processes during peak arrival and departure times

Expanded airport facilities

2.2 This increase in passenger numbers is having a substantial effect on airport facilities. In order to cater for the growth in traffic, Airport Authorities in many parts of the world are being required to dramatically expand their facilities and supporting infrastructures. New runways and new terminals are being built, and in some cases, complete new airports are being constructed to cope with the growth in numbers. Apart from the enormous expense involved in these projects, there are frequently many environmental problems associated with such large-scale developments.

International terrorism and security

2.3. The threat posed by international terrorism is also one which must be faced not only by the Border Control Agencies, but also by the carriers and airport operators. Additional security checks/risk assessments on passengers prior to departure have added considerably to the time required for the check-in process. Checks by Border Control Agencies prior to departure have also had to be increased, or, in some cases, reinstated based on changing risk factors. Because of the threat from terrorism, the arrival processing of passengers by the Border Control Agencies has had to be intensified, with additional delays being experienced.

Threats from Serious Crime

2.4. Over the past decade or more, Border Control Agencies have been faced with a number of threats which, if not entirely new, have certainly been increasing in their intensity. The phenomenal growth in drug trafficking is one that is most in the public eye. Drug smuggling by passengers is a substantial part of the problem. Customs at international airports are a country's first line of defence against this type of activity and their responsibilities have increased as the drug problem has worsened. The increased compliance risk posed by passengers has meant that Border Control Agencies have had to be more vigilant and more intensive in their processing of this traffic. The result has shown an impact on the overall passenger clearance process.

Manpower resources

2.5. Manpower resources available to Border Control Agencies and carriers, assigned to deal with these additional responsibilities and threats have not been able to keep pace with the demand. In most countries, the recruitment of additional manpower to cope with the increased workload has simply not been an option. Indeed, in some countries the number of public servants and carrier's staff have been declining.

Inter-agency co-operation

2.6. There are a variety of Border Control Agencies in place at most international airports. These include Customs, Immigration, Police, Quarantine, Health and Safety, Agriculture etc. The level of co-operation between these Border Control Agencies varies from place to place. Different agencies frequently operate their own automated systems for passenger processing without any sharing of information. The strict division of responsibilities between the agencies means that passenger processing is often unnecessarily prolonged.

Penalties

2.7. Furthermore, carriers are also responsible for ensuring the passengers they are carrying are properly documented. Heavy financial penalties are frequently imposed on carriers who transport a passenger whose official travel documents are not valid for the country of destination. In addition, the carrier is usually required to repatriate any improperly documented passengers at carrier’s expense, and may also incur costs for any period during which the passenger is held in detention.

CURRENT PASSENGER PROCESSING TECHNIQUES

Selective approach to passenger clearance

3.1. The responses of the Border Control Agencies to the challenges explained in the previous section have been many and varied. In terms of Border Control Agency response, it became clear many years ago that the routine examination of all passengers and their possessions was no longer a suitable way of processing the ever increasing passenger numbers. The emphasis for Border Control Agency has turned from a high percentage of passenger examinations, to a more selective approach based on risk assessment, intelligence, behavioural patterns, etc., as well as randomly applied inspection processes. It is now well recognized that such an approach yields significantly better results, proportionate to the manpower employed, than purely random or intensive examination. So based on purely pragmatic considerations, Border Control Agency has already gone some considerable way towards greater facilitation of passengers.

Red/Green Channels

3.2. Another element in this change of approach by Customs has been the advent of the Red/Green channel system. This technique of passenger streaming, which is now in use at a large number of airports around the world, is recommended in the Convention on the Simplification and Harmonization of Customs Procedures (as amended) (otherwise known as the revised Kyoto Convention), adopted by the WCO in 1999. Choice of the Red or Green channel is deemed to be the equivalent to making a formal declaration to Customs as to the goods being brought into the country. In spite of the existence of this provision in the Kyoto Convention, it still remains the practice in some countries to require a written Customs Declaration from each individual passenger upon entering the country.

Pre-departure passenger clearance

3.3. Another approach to passenger facilitation on arrival is the transfer of the Border Control Agencies activities to the airport of departure. Flights arriving from that international point can then be treated as domestic, requiring no further processing. This process (pre-clearance of flights) alleviates some of the pressure at the arrival airport, and can conceivably eliminate the need for staff at small airports with little traffic. Although this approach has had some success, it is not in widespread use and presents some practical, financial and political issues.

Inter-Agency co-operation

3.4. Although the level of co-operation between the various Border Control Agencies has been variable in a number of countries, there are several examples of co-operative efforts taking place in order to rationalize procedures, save on manpower and other resources, and facilitate passengers. Such co-operation can result in the clearance process for passengers being reduced in complexity to the level where a single Border Control Officer will be able to process the vast majority of arriving passengers. The Officer, representing the various interested agencies, is tasked with conducting a primary inspection of each arriving passenger, and referring those requiring additional examination to the appropriate service. In addition, with increasing inter-agency co-operation, the case for the development of single inter-agency automated systems, serving the needs of two or more agencies becomes more compelling. The advent of the concept of a single Border Control Officer for all initial and simple controls has been a major passenger facilitation improvement, avoiding the complexity of a passenger queuing separately to pass multiple border inspections.

Passenger streaming

3.5. A number of other initiatives have been undertaken by the Border Control Agencies in order to facilitate arriving passengers. These mainly involve variations on the passenger-streaming concept.

For instance, citizens of the country of arrival may be separated from non-nationals, and streamed through a simplified immigration process. Citizens who travel frequently may be accorded a facilitated service if they agree to comply with certain conditions, and passengers on designated flights may be subject to either intensive or cursory examination depending on flight risk assessments developed by the Border Control Agencies.

Other facilitation initiatives

3.6. In addition to the use of automated systems, the Border Control Agencies generally, and Customs in particular, have instituted new techniques to help them identify potential or likely offenders. Training for Customs officials who process arriving passengers now routinely includes behavioural analysis.

Electronic Data Interchange (EDI)

3.7. While the use of all the above procedures and techniques have brought about considerable advances in the passenger clearance process, it is clear that there is always room for improvement - both from the facilitation point of view and from the compliance perspective. The recent upsurge of interest in EDI, and the capabilities it offers for transmission of passenger details to the point of destination well in advance of the passengers' arrival, is seen as a very positive step towards achieving both facilitation and compliance goals.

Advance Passenger Information (API)

3.8. Advance Passenger Information (API) involves the capture of a passenger's biographic data and other flight details by the carrier prior to departure and the transmission of the details by electronic means to the Border Control Agencies in the destination country. API can also act as a decision making tool that Border Control Agencies can employ before a passenger is permitted to board an aircraft. Once passengers are cleared for boarding, details are then sent to the Border Control Agencies for screening against additional databases and can identify passengers and crew of interest including those subject to United Nations Security Council sanctions lists and travel bans. While this technique is beginning to be used by more and more Border Control Agencies it has been used by a number of countries for some time. API has the potential to considerably reduce inconvenience and delays experienced by passengers as a result of necessary border processing. It also provides a system which carriers can use to comply with relevant legislation of the countries they fly to including legislation implementing travel bans against those on United Nations Security Council sanctions lists.

ORGANIZATIONAL POLICY

4.1. WCO policy

4.1.1. As an International Organization responsible for Customs matters, the WCO has, as its goals, the simplification/ harmonization of Customs formalities and the promotion of efficient means of Customs control. This covers passenger movements as well as movements of commercial cargo across international boundaries.

4.1.2. Due to the increased risk, such as trans-national organized crime and international terrorism, Customs have had to enhance their controls on passengers in order to apprehend offenders and to minimize the risk posed on global security.

4.1.3. The combined effect of the need to enhance controls together with the growth in passenger traffic has placed a severe strain on the resources of Customs and other Border Control Agencies. The result has been delays and increased pressure on airport facilities, many of which were designed to cater to much lower passenger volumes.

4.1.4. The interest of the WCO in API stems mainly from its responsibility to help its Members target their scarce resources, and at the same time, improve their service to the travelling public. The WCO sees its role as:

(a) Providing its Members with information concerning API programme development, and the benefits it can bring;

(b) Providing a forum in which the constraints on API can be discussed and hopefully resolved; and,

(c) Seeking to jointly agree standards with the Airline industry so that API does not develop and proliferate in an inconsistent or unstructured way.

4.1.5. The WCO sees API as a very useful technique to enhance border integrity[1], while maintaining facilitation for low risk passengers, which benefit Customs and other Border Control Agencies, Carriers, Airport Authorities (and other passenger facility operators) and Passengers themselves. The revised Kyoto Convention took this into account and API is now included in the Specific Annex J1 (Travellers) of the Convention as “Recommended Practice”. The technique has already been used with great successes and is likely to expand in the future. The WCO would like to see API develop in an orderly and disciplined manner, and to that end, would like to see standards and jointly agreed principles put in place so as to facilitate the development and spread of API.

4.1.6. Where countries identify the need for additional API elements, and these are agreed in accordance with the WCO’s Data Maintenance Request procedures, these Guidelines will be updated accordingly. Additionally, any necessary changes to the UN/EDIFACT passenger list message (PAXLST) structure must be developed concurrently and any amendments shall be submitted by the WCO to the appropriate UN body prior to adoption.

4.2. IATA policy

4.2.1. As the globally recognized representative of more than 240 scheduled carriers that account for approximately 83% of passengers transported by air worldwide, IATA's interest in API essentially focuses on enhancing and streamlining the control processes applied in respect of arriving and departing international passengers as they pass through Customs, Immigration and other border controls.

4.2.2. Like the WCO and ICAO, IATA has constantly sought to eliminate unnecessary forms and procedures in international air transport, and the abolition of the passenger manifest in paper formats has long been an important policy objective for the Association. Additionally, IATA – in cooperation with other interested stakeholders – has continued to look toward globally aligned processes which can assist in mitigating the impact that enhanced security requirements adopted in response to emerging threats can have on passenger processing at the border. As more States seek to automate border control processes, the concept of API and its potential to facilitate efficient border clearance processing remains a primary focus.

4.2.3. Collection of passenger details at the time the passenger checks in for the flight in question, presents a problem of additional workload for carriers at a point in the system where staff and facilities are frequently already stretched to maximum capacity. Consequently, carrier support for API depends heavily on there being truly realizable benefits for aircraft operators and for passengers who are departing the State, or upon arrival at the final destination, or both depending upon regulations in effect.

4.2.4. Furthermore, given the practical constraints and financial ramifications associated with data capture and transmission, IATA strongly supports the concept that required information should be limited to that which can be captured by automated means from an official travel document, and, where required under national legislation, from the transporting carrier’s own reservation and/or departure control systems. This passenger-specific information can then be augmented by basic flight details, also retrieved from the carrier’s systems by automated means. With this in mind, IATA sees particular benefit in co-operating with the WCO and ICAO to define the data and message sets for API systems under UN/EDIFACT PAXLST message standards that have been internationally

[1] Border Integrity is defined in Annex 9 of the Chicago Convention.

agreed and widely adopted by participating countries. IATA, through its Security and Travel Facilitation team and its Passenger Experience activities, is also committed to establishing mutually agreed principles, which can expand the benefits of automating and integrating all elements of the passenger process from origin to destination.

4.2.5. IATA believes the true value to this Guideline is derived from its focus on a harmonised approach to data collection and transmission to all interested Border Control Agencies via globally interoperable message structures and formats. In today's environment, Public Authorities in the country of origin, in transit countries and at the final destination may individually mandate provision of advance passenger information for a given flight, Failure to adopt a common globally recognised approach will result in unnecessary complexity for systems needed to support multiple data exchange process requirements.

4.2.6 The costs associated with developing and managing multiple applications may be unsustainable for many stakeholders involved in the process. IATA fears that the impact of these unaligned requirements on airport and airline operations is far greater than the benefits to any single party derived from implementing a program outside the confines of this Guideline.

4.2.7 The majority of proprietary systems developed by international airlines providing scheduled service continue to rely upon the use of UN/EDIFACT PAXLST messaging transmitted via existing airline communication networks to comply with API data provision requirements. Other entities, such as Charter Carriers, Air Taxi operators, and Executive Air Carriers operate using a differing business model, and may not have the technical infrastructure in place to support PAXLST message generation.

4.2.8 IATA fully endorses States' adoption of these Guidelines, including the use of the UN/EDIFACT PAXLST message format and transmission via existing airline communication networks, to support a common and globally aligned approach to national API data provision requirements. At the same time, IATA also urges States to recognize that, in addition to UN/EDIFACT PAXLST messaging, alternative methods for transmitting required passenger data will need to be considered as part of any national program implementation.

4.2.9 Ultimately, it is IATA's view that to achieve the greatest possible efficiency, passenger data exchange processes must evolve to the point where a common and globally agreed data set is collected one time from each person for whom it is required, transmitted once to all having the legal authority to request and view that data, and then used in the most efficient way possible based on clearly established risk analysis criteria and consistent with acceptable data privacy norms.

4.3. ICAO Policy

4.3.1 The International Civil Aviation Organization (ICAO) is an intergovernmental organization established by the Convention on International Civil Aviation (Chicago Convention) in 1944. A specialized agency of the United Nations, ICAO serves as the medium for establishment of standards and recommended practices by its 191 Contracting States, in the fields of safety, security, aviation environment protection and facilitation.

4.3.2 ICAO's interest in API systems stems from the Chicago Convention's mandates for Contracting States to prevent unnecessary delays by facilitating border clearance formalities and to adopt internationally standard Customs and immigration procedures. Moreover, national programmes of travel document issuance and security, and the efficacy of inspection systems in controlling smuggling and illegal migration, can have a significant effect on the security of civil aviation.

4.3.3 Equally, the application of technology and modern management science to control systems, in order to facilitate international traffic flow, is increasingly important in the present climate of intensified security controls. Increased congestion and lengthened processing times caused by the sudden imposition of unfamiliar procedures can be counterproductive to security, as the confusion and disorder that result can be exploited by those seeking to evade inspection.

4.3.4 In recent years, projects in the facilitation programme have aimed at a strengthened and more efficient system of border controls at airports, addressed at raising the level of general security and at the same time yielding measurable improvements in facilitation for the vast majority of travellers.

4.3.5 Consequently, the following specific recommendations are proposed for adoption by States, at the least:

(a) States should consider adoption of API in the context of a total system approach to border management, encompassing the issuance of machine readable passports and visas including electronic visas, migration to automated entry/exit records to replace embarkation/disembarkation cards, and interoperability among the API systems of other participating States.

(b) Future configurations of API-based border control systems should include the deployment of biometric technology to assist with the identification and identity confirmation of passengers.

API PROGRAM DIFFERENTIATION: BATCH OR INTERACTIVE API

5.1 Advance passenger information systems currently used by governments and those planned for future implementation can be placed in two distinct processes, each having unique features and delivering specific results.

Non-interactive Batch Style API Systems

5.2 Non-interactive batch style API data covering all passengers and, in many cases, all crew members on board a specific flight are gathered during the check-in process and then transmitted in a single manifest message at or immediately following flight reconciliation or departure. Typically non-interactive batch-style API is received by the requesting government well in advance of the flight's arrival, allowing the receiving government to perform adequate checks of all inbound passengers and crew. The primary benefit of this approach is an expedited inspection processes at the primary Immigration booth, for the majority of travellers. Advance information also affords Border Control Authorities the ability to identify legitimate travellers from travellers who may be of interest. As passenger data under a non-interactive batch style API system is normally transmitted at flight reconciliation or after departure of the flight in question, the ability to enhance aviation security is limited.

5.3 Non-interactive batch style API systems traditionally utilize airline based Type-B messaging protocols transmitted via existing airline communication networks. Message construction is based upon the UN/EDIFACT "PAXLST" message format (see Appendix IIA), which has been adopted as the globally interoperable message standard for API messages. Governments' ability to receive and process non-interactive batch style API passenger manifest data is specific to each individual government's system.

Interactive API Systems (i-API)

5.5 An alternative to the batch style approach to API is an interactive API (iAPI) system allowing two way communication, in near real-time, on a passenger-by-passenger or transaction by transaction basis, which is initiated during check-in. Such interactive systems may be developed by or at the direction of a Border Control Agency and may be proprietary. ..

5.6 Upon receipt of the transaction message, the receiving government can perform sufficient checks and return a response to the carrier which may indicate approval to board/do not board or where required, indicate further Border Control Agency checks required for the identified traveller. Timely evaluation and response to interactive API messages is critical to ensure the airline check-in processes are not negatively impacted. In many existing systems today, the goal for submission, evaluation and response to individual transmissions is 4 seconds or less per transaction.

5.7 The iAPI message exchange incorporates the use of both the UN/EDIFACT PAXLST and CUSRES standard messages. For the Message Implementation Guidelines for CUSRES message, please see Appendix IIB. Communication networks utilized do vary. However iAPI systems require a more robust network protocol than the non-interactive batch API message. Governments should establish best practices when working with individual carriers and service providers, to ensure adequate network protocols are available.

5.8 Adoption of an iAPI system can result in greater and more immediate benefits to both governments and carriers:

5.8.1 Persons known or believed to pose an unacceptable level of risk may be identified prior to a flight or even entry in to an airport sterile area, therefore directly enhancing Border -Integrity.

5.8.2 Persons who are known to be inadmissible may be identified prior to travel, thereby reducing the incidence of inadmissible arrivals.

.5.8.3 Carriers can expect to benefit through the identification of persons whom the receiving government may declare to be inadmissible and can be prevented from boarding at the point of departure. These benefits would be associated with cost avoidance for detention and return, in the case of inadmissibility, avoidance of possible fines for transporting persons with improper documents and avoidance of potential security-related incidents within airport facilities or in aircraft cabins.

5.8.4 Benefits for the passenger could be to prevent an unnecessary trip, loss of time and expenses when a determination of inadmissibility would be made upon arrival.

5.9 iAPI systems are far more complex than non-interactive batch style systems and therefore costs associated with their development; implementation and ongoing operation are significant for both governments and airline operators. Many airline operators have already established iAPI capabilities to meet current active iAPI systems. Timeframes for implementation of iAPI systems may require a significant amount of time for full implementation.

5.10 API systems need to be supported by best practise business process to realise the benefits to governments and carriers. This should include an identity check by aircraft operators, ensuring that individual travel document data reflects the data collected from the travel document and that the passenger's identity conforms with the passengers current document at the time of embarkation.

COSTS AND BENEFITS OF API

6.1. In deciding whether to adopt API, potential providers of the passenger data (the carriers) and potential users of the data (the Border Control Agencies), will need to examine and then determine if the benefits which this technique can provide can justify the costs involved both from a start-up viewpoint and for on-going operation.

6.2. The costs, which will be incurred by both carriers and Border Control Agencies, can be measured with some confidence. The benefits which API can bring are less easy to quantify. This section of the Guideline seeks to identify those areas where costs will likely be incurred, so that potential API users are aware of the cost implications of API and can measure these in their own company or administration.

6.3 The Guideline also identifies the potential benefits of API. Some of these benefits are tangible in nature; e.g. staff savings. However other benefits, such as "greater convenience for the travelling public", are more difficult to quantify in purely monetary terms but may be competitively very valuable.

COSTS

6.4. Border Control Agencies:

6.4.1 Where no single Border Control database currently exists, there will clearly be a significant cost involved in developing a working system. Ideally, establishing a single inter-agency database, for passenger clearance, would be most desirable. This is not only a more efficient means of processing passenger list data received by API, it is also more economical, since the development cost would be spread over a number of Border Control Agencies which could contribute in accordance with their projected use of the system.

6.4.2. Where a Border Control database already exists, yet only available to a single agency, there may be a cost incurred if the decision is made to share information with or between multiple agencies. It is technically feasible to have API data feeding one or more Border Control Agency systems independently. However, it seems prudent and cost efficient to adopt a co-ordinated approach to API amongst the Border Control Agencies, having the API data processed by one single system rather than simultaneously by several different systems.

6.4.3. Apart from the system related costs involving the development of new systems or the merging of existing systems, there will be costs incurred on the system development side associated with the electronic receipt of passenger data. Incoming data will need to be converted to a format that is compatible with and can be processed by the receiving system. There will be a cost involved in enhancing existing systems to perform this function. The system may also need to produce certain additional outputs associated with the processing of API passengers; e.g. lists of passengers for closer investigation, statistical reports, performance evaluations, etc.

6.4.4. Depending on decisions made by Border Control Agencies, there will be some costs incurred when connecting their system to one or more selected data networks used to receive passenger data electronically.

6.4.5. In some instances, the Border Control Agencies in the country of arrival have provided Machine Readable Passport readers to the carriers in the airport of departure. Where this is done, there will clearly be a cost involved that can be quite substantial.

6.4.6. As with all systems, costs will be incurred in respect of on-going maintenance and upgrading.

6.5 Carriers:

6.5.1 The principal costs for carriers are associated with system development/integration and capture of passenger details for transmission to the origin and/or destination country of a flight. Costs may be incurred in other areas as well; e.g. additional check-in staff to cope with the extended period of time required to complete check-in formalities, additional check-in desks, hardware acquisition, etc. Various techniques can be used to offset these costs to some degree; e.g. agreements with governments, as is the case in Australia, machine-readable passports, "up-stream" capture of passenger data at the time of booking, etc. These issues are examined further in Section 8.2.

6.5.2 The adaptation of carriers' automated reservation systems and/or departure control systems (DCS) to collect, convert, and transmit API data, and to respond to expanding data requirements will also give rise to significant cost.

.

6.5.3 On-going maintenance costs may also be incurred in respect of the above-mentioned systems.

6.5.4. Finally, there will be the recurring cost of data transmission in respect of the passenger data for each API flight.

6.6 Airport Authorities:

6.6.1 Depending on the current layout of the arrival and passenger processing area, there may be a requirement to re-structure this area to cater for API passengers; i.e. a special stream for API passengers with designated baggage carousels, etc.

BENEFITS

6.7 Passengers:

6.7.1 One of the main benefits of API, and one of the principal reasons for undertaking the advance transmission of passenger data, is the potential benefit to the travelling public. The time saved by the legitimate (non-targeted) passenger while undergoing normal arrival formalities will, of course, vary from airport to airport. However total clearance times should be significantly reduced, and in normal circumstances, should not exceed the ICAO goal of 45 minutes.

6.8 Carriers:

6.8.1 The additional passenger data captured at the time of check-in primarily through automated scanning of the passenger's official travel document could, in some instances, enhance carrier security and help to ensure that all passengers carry valid official travel documents required for admission to the destination country. This has the potential of reducing carrier exposure to penalties for transporting passengers that are not properly documented.

6.8.2 Where States have implemented interactive API programmes, and are able to provide "Board / Do Not Board" responses at time of check-in, carriers may be more readily able to avoid costs associated with the detention and/or removal of persons who might otherwise be determined, based on specific factors available to the Border Control Agencies, to be inadmissible upon arrival at the final destination.

6.9 Border Control Agencies:

6.9.1. One of the major benefits of API for the Border Control Agencies is the enhanced enforcement capability realised through advance notification of the arrival and departure of potential or known offenders or inadmissible persons. API permits a thorough and rigorous screening of inbound and outbound passengers to be accomplished, identifying those passengers that present the highest risk, and allowing for the faster throughput of low risk passengers.

6.9.2 The use of automated alert lists is particularly effective in taking preventive measures in case of travel by individuals against whom there are legally sanctioned UN travel restrictions or prohibitions. Border Control Authorities and Carriers may use publicly available lists of individuals who are subject to travel bans

6.9.3 Since passenger data will be provided in an electronic, readily processed format, there should be a data capture saving, as the Border Control official will not be required to perform a normal data entry operation when the passenger arrives at the entry or departure point.

6.9.4 API provides for more effective allocation of border control and law enforcement resources. In addition, the increased automation of passenger processing can result in reduced staff costs.

6.9.5 API has the potential to be a catalyst for greater interagency co-operation at both the national and international level.

6.10 Airport Authorities:

6.10.1. API also assists the growth in passenger traffic being accommodated through improved use of technology rather than additional infrastructure.

6.10.2 Consequently, there should be a reduced need to expand or upgrade current facilities in response to increased traffic, provided data capture can, for the most part, be accomplished through automated means

6.10.3 Greater passenger satisfaction with facilities, fewer complaints, etc.

6.10.4 Better public image nationally/internationally, good for tourism etc.

NATIONAL PASSENGER PROCESSING STRATEGY

7.1 In most countries, the responsibility for the implementation of national law regarding persons and goods entering or leaving a country rests with a number of different agencies. These agencies; include Customs, Immigration, Police, Quarantine, Health and Safety, Agriculture, Food and Drug and various combinations of these. Although Customs, Immigration and/or national Border Police are usually in the front line in respect of processing an arriving passenger into the country, representatives of the other agencies are sometimes present and may be available on a referral basis. In other cases, the functions of some of the other agencies may, in fact, be carried out by Customs.

7.2 Regardless of the arrangements that are in place, it is clear that there must be a high degree of co-ordination among all Border Control Agencies involved in passenger clearance in order to eliminate unnecessary process duplication and delays to the travelling public. The degree of co-ordination that already exists varies from country to country, and there are some excellent examples of inter-agency co-operation which result in a speedy service to passengers and savings for the taxpayer.

7.3 Inter-agency co-ordination and co-operation are sometimes difficult to achieve in the airport environment. Attempts to streamline the process may not be welcomed by agencies whose vested interests may not be served by a rationalization of current procedures. It will be necessary however, if there is to be progress in this area, to ensure that all agencies work together to bring about the type of passenger processing system which both serves the passenger and ensures compliance with national and international law.

7.4 One approach to successful co-operation among all the Border Control Agencies may be realized through the development of a plan that outlines a joint passenger processing strategy. This plan should be the blueprint for future activities and initiatives aimed at facilitating passengers and ensuring a higher degree of compliance.

7.5 Some considerable thought and effort should be devoted to the development of this plan and it should have the support of the senior management of all the agencies concerned during its development and implementation.

7.6 The following is a checklist of topics which should be covered in this plan :

7.6.1 A description of the current passenger processing environment must be agreed. This should contain a narrative and diagrammatic description of the current flow of passengers through the airport. It should identify any areas of difficulty and any actual or potential bottlenecks. Current times taken for passenger processing (Minimum, maximum and average) should be indicated.

7.6.2 The plan should describe the demands being placed on the Border Control Agencies and on carriers as well. These demands include the legislation that must currently be administered or observed and any future changes anticipated in such legislation. The demands should also include trends in the growth of such things as drug smuggling or illegal immigration and other similar threats. The plan should give statistics on passenger numbers - including peaks and troughs - and projections for future growth/decline in these numbers.

7.6.3 The constraints under which the Border Control Agencies and carriers operate should be fully identified. Constraints can exist in the areas of physical airport and/or systems infrastructure, manpower and/or material resources. Such limitations can often have an adverse effect on passenger clearance times.

7.6.4 Numerous opportunities exist which can help the Border Control Agencies to carry out their obligations in a more effective and efficient manner. The possibilities afforded by advanced information exchange capabilities can be used to help identify suspect passengers by checking passport details against data stored on enforcement databases. This has proven to be a major benefit to Border Control Agencies. A variety of technical aids are now available which can also prove to be very effective tools for these agencies. Improved training methods offer the possibility of enhancing the performance of existing staff. All of these should be considered and included in the plan.

7.6.5 Having described the overall situation, the plan should go on to analyze current practices. Are the Border Control Agencies properly fulfilling their obligations insofar as the application of the law is concerned? If not, what are the factors which prevent or inhibit the Border Control Agencies? Are passengers being facilitated to the greatest extent possible? If not, why is this so? The analysis should thoroughly explore all measures of performance, identify any shortcomings and pinpoint any deficiencies. This part of the plan should be an impartial assessment of the actual level of service provided by the Agencies concerned.

7.6.6 The plan should then seek to establish certain targets in respect of their activities. Obviously it is very difficult to set enforcement targets which specify numbers unauthorized travellers apprehended or number of seizures or quantities of illegal products/substances seized. Increases or decreases in seizures do not necessarily reflect success or failure of the enforcement effort. Increases in seizures could be an indication of increased illegal traffic and not a higher real success rate while decreases in seizures could simply mean a reduction in traffic and not a lower real success rate. One area where it is possible to set targets is in the time taken for passenger processing. ICAO has set a target of 45 minutes from disembarkation to final clearance. The plan should aim to at least conform to this recommendation, or if possible, to better it. Obviously, not all of the time spent between disembarkation and final clearance is attributable to the Border Control Agencies. Inefficient baggage handling systems can be the cause of considerable delay. There can also be substantial delays prior to disembarkation due to such factors as unavailability of jet-ways and ground transport. All of these factors should be considered when setting targets. It is prudent to set relatively ambitious targets. When some experience has been gained with the new procedures then the targets can be revised if appropriate.

7.7 Having described the current position, analyzed the existing practices, identified problems and opportunities and then set realistic targets, the plan should then outline the means necessary to attain those goals. This part of the plan should address the following areas:

7.7.1 Re-organization of passenger processing procedures. Where the analysis of current practices has identified delays in the process which could be rectified by a change of procedures, such changes should be described.

7.7.2. The introduction of API requires close collaboration amongst all the Border Control Agencies, including sharing of responsibilities and information. A description of how a joint passenger clearance process would operate should be agreed and implemented. The role and responsibility of each agency should be clearly identified.

7.7.3 Co-operation with carriers is clearly a key to API's success. In preparing and implementing the plan, the Border Control Agencies will need to have close contact with the carriers. The plan should describe the part to be played by the carriers in the clearance processes that would be implemented.

7.7.4 The Airport Authorities also have a critical role. There is a clear need to involve these authorities in all planning for revision of the passenger processing procedures, particularly with respect to physical infrastructure modifications that might be necessary.

7.7.5 The opportunities afforded by international co-operation with Border Control Agencies in other countries should be explored. Advance Passenger Information can originate from these agencies as well as from carriers. In addition, supplementary information to the basic passport details which are foreseen to be transmitted by API may also be provided by overseas counterparts. The mechanism for obtaining this information will need to be examined in the plan.

7.7.6 Finally, there should be a detailed description of the use of Information and Communication Technology in the processing of passengers. Here, it will be necessary to explore such matters as automated systems for passenger screening (e.g. computerized alert lists/suspect databases). The potential joint use of such systems is another area to be explored.

API DATA CAPTURE AND TRANSMISSION

8.1 Data to be captured and transmitted

8.1.1 For API to function successfully and on a widespread basis, it is essential that there be a limitation and a very high-degree of uniformity in relation to the data required by the Border Control Agencies which will receive and process that data. From the perspective of the Border Control Agencies, the limitation and harmonization of this data may be somewhat restrictive to their operations. However it is clear that for carriers to capture and transmit passenger data on a large scale to a large number of Border Control Agencies, this limitation and harmonization is essential.

8.1.2 The WCO, IATA and ICAO have jointly agreed on the maximum set of API data that should be incorporated in the PAXLST message to be used for the transmission of such data by the carriers to the Border Control Agencies. It is important to note that countries should limit their data requirements to the minimum necessary and according to national legislation. This data can be divided into two distinct categories:

(8.1.4) Data relating to the Flight (Header Data)

(8.1.5) Data relating to each individual passenger (Item Data).

(a) Core Data Elements as may be found in the Machine Readable Zone of the Official Travel Document

(b) Additional data as available in Airline systems.

(c) Additional data not normally found in Airline systems and which must be collected by, or on behalf of the Airline.

8.1.3 Details of the individual data items for each of these two categories are given below. It should be noted that the Flight data should already be available to carriers from their own automated systems. The passenger data corresponds to those items of data that currently appear on machine-readable passports, other official travel documents or those which may be available in the transporting carrier's reservation system. From the point of view of promoting the use of API, extending the required data element set beyond that limit would hinder carriers' operation and could potentially impact airport throughput and passenger capacity. The WCO, IATA and ICAO recommend to their members that the API data must not exceed that given in this guideline.

8.1.4 Data relating to the flight (Header data):

Flight Identification

(IATA Airline code and flight number[2])

Scheduled Departure Date

(Date of scheduled departure of aircraft (based on local time of departure location)

Scheduled Departure Time

(Time of scheduled departure of aircraft (based on local time of departure location)

Scheduled Arrival Date

(Date of scheduled arrival of aircraft (based on local time of arrival location)

Scheduled Arrival Time

[2] Where the aircraft operation is not represented by an IATA airline code (such as a private aircraft movement), then information to be provided for this element will be determined by the implementing authority.

(Time of scheduled arrival of aircraft (based on local time of arrival location)

Last Place/Port of Call of Aircraft

(Aircraft departed from this last foreign place/port of call to go to "place/port of aircraft initial arrival")

Place/Port of Aircraft Initial Arrival

(Place/port in the country of destination where the aircraft arrives from the "last place/port of call of aircraft")

Subsequent Place/Port of Call within the country

(Subsequent place/port of call within the country)

Number of Passengers

(Total number of passengers on the flight)

8.1.5 Data relating to each individual passenger:

Data relating to a passenger based on the following list of elements will not be available from a single source, and may instead require collection from several sources as detailed below:

(a) Core Data Elements as may be found in the Machine Readable Zone of the Official Travel Document

- **Official Travel Document Number**

(Passport or other official travel document number)

- **Issuing State or Organization of the Official Travel Document**

(Name of the State or Organization responsible for the issuance of the official travel document)

- **Official Travel Document Type**

(Indicator to identify type of official travel document)

- **Expiration Date of Official Travel Document**

(Expiration date of the official travel document)

- **Surname/Given Name(s)**

(Family name and given name(s) of the holder as it appears on the official travel document.)

- **Nationality**

(Nationality of the holder)

- **Date of Birth**

(Date of birth of the holder)

- **Gender**

(Gender of the holder)

(b) Additional Data elements normally found in Airline systems

- **Seating Information**

  (Specific seat assigned to the passenger for this flight)

- **Baggage Information**

  (Number of checked bags, and where required, the baggage tag numbers associated with each)

-
- **Traveller's Status**

(Passenger, Crew, In-transit)

- **Place/Port of Original Embarkation**

  (Place/port where traveller originates foreign travel, refer to 8.1.6)

- **Place/Port of Clearance**

(Place/port where the traveller is cleared by the Border Control Agencies)

- **Place/Port of Onward Foreign Destination**

  (Foreign place/port where traveller is transiting to, refer to 8.1.7)

- **Passenger Name Record Locator Number (or unique identifier)**
- (As available in the traveller's Passenger Name Record in the carrier's airline reservation system)

(c) Additional data not normally found in Airline systems and which must be collected by, or on behalf of the Airline

- **Visa Number**

(Number of the Visa issued)

- **Issue Date of the Visa**

(Date of the Visa issuance)

- **Place of Issuance of the Visa**

(Name of the place where the Visa was issued)

- **Other Document Number Used for Travel**

(The other document number used for travel when the official travel document is not required)

- **Type of Other Document used for Travel**

(Indicator to identify type of document used for travel)

- **Primary Residence**

- **Country of Primary Residence**

  (Country where the traveller resides for the most of the year)

- **Address**

  (Location identification such as street name and number.)

- **City**

  (City)

- **State/Province/County**

  (Name of the State, Province, County, as appropriate)

- **Postal code**

  (Postal code)

- **Destination Address**

  - **Address**

    (Location identification such as street name and number.)

  - **City**

    (City)

  - **State/Province/County**

    (Name of the State, Province, County, as appropriate)

  - **Postal code**

    (Postal code)

- **Place of Birth**

(Place of birth such as city and country)

8.1.6. It should be noted that API transmissions will contain data for passengers carried into a country (initial place/port of arrival) from the last place/port of call of that aircraft abroad. API transmissions may provide information of passengers' originating foreign port of embarkation based on the information contained in the transporting carrier's passenger reservation or departure control system. Where countries identify the need for additional API elements, please refer to paragraph 4.1.6.

8.1.7 The onward foreign destination port may be required for those passengers not intending to enter the territory of the country of transit.

8.1.8 Some countries may prefer to receive identifying passenger data elements from a machine-readable visa they have issued. In these situations that information should be collected in addition to the passport information. Countries seeking to obtain additional information for specific passengers may utilize internal linkage of government systems that is based upon data provided by the carrier.

8.1.9. Complete specifications of the data items mentioned in 8.1.5 (a) are contained in ICAO Doc 9303, Machine Readable Travel Documents. Parts 1, 2 and 3 of Doc 9303 set forth specifications for machine-readable passports, visas and official travel documents, respectively. Diagrams of the machine-readable zones of such documents are found in Appendix I to this Guideline.

8.1.10 It is recommended that standard message formats (such as UN/EDIFACT PAXLST and CUSRES) be used to avoid difficulties and significant additional costs that would be caused by the introduction and use of local national standards.

8.1.11 The UN/EDIFACT PAXLST message has been adopted specifically to handle airline passenger manifest transmissions to governments. Additionally, UN/EDIFACT CUSRES message has been adopted to facilitate governments' response. Implementation guides for both messages are included as Appendices to this Guideline. These Appendices will be amended regularly to reflect latest developments. Administrations and airlines should contact the WCO, IATA or ICAO to ensure they obtain the most up-to-date version of the API Guidelines.

8.2 Data capture methods:

8.2.1 Perhaps the most critical aspect of API is the means by which the data to be transmitted to the Border Control Agencies is captured. Manual data capture can be costly, time consuming, labour intensive and error prone. The capture of data concerning passengers at the airport of departure introduces a delay in the check in process that could, if not managed properly, offset the potential advantage to passengers provided by efficient API applications. If the check-in process in unduly prolonged, API will simply shift much of the delays and congestion, away from the arrival area, to the departure area.

8.2.2 Machine Readable Travel Documents

Machine Readable Travel Documents (MRTD) and Document Readers are an important component in API. The use of this technology for data capture at the airport can greatly reduce delays. It is estimated that manual keying of API data from an official travel document takes approximately 45 seconds per passenger. On a flight of 200 people, the total additional time for check-in formalities is estimated to be 150 minutes. Assuming that there are 5 check-in counters dedicated to that flight, it would take approximately 30 minutes longer overall to check-in all passengers. This means passengers reporting at the airport 30 minutes earlier than normal or the flight being delayed by 30 minutes.

8.2.3 In addition to the normal flight data provided in paragraph 8.1.4, it is essential that States limit their API programme requirements to those elements that can be captured by automated means from the MRTD. Additional data elements not contained in the Machine Readable Zone should normally be limited to data which the issuing authority has included in the MRTD's visible zone. Except where specified by the national legislation, States should normally avoid data elements that require airline personnel to question travellers and record their verbal responses.

8.2.4 Using an MRTD and document reader, integrated with the airport check-in process, minimizes disruption and the time required for data capture. Capture of data elements in Machine Readable Form is both quick and avoids manual input errors. The MRTD specifications have been adopted by ICAO and endorsed by the International Organization for Standardization (ISO) as ISO Standards 7501-1, 7501-2 and 7501-3. Travel Documents which do not conform to the ICAO specifications cannot be read by the document reading devices which are programmed to read MRTDs. (Note: Additional consideration will be required to ensure data collection and its accuracy when check-in is accomplished outside of the airport facility itself e.g. web check-in and tele-check-in.)

8.2.5 "Up-stream" data capture

Another mechanism which might be useful in reducing time spent on data capture at check-in and thus further facilitate the passengers would be to consider what use might be made of data captured when the reservation is made. Such data is still speculative and must be manually verified or even re-captured at check-in to prevent manipulation and avoid substitution and/or input error.

8.2.6 However, it should be noted that most countries requiring API hold the carrier transporting an individual to their territory responsible for the accuracy of API data transmitted, and may impose significant financial penalties for inaccuracies or omissions. Accordingly, many carriers are unable to make use of data captured at time of reservation or that which is captured by another carrier at point of origin.

8.3 Data transmission:

8.3.1 Since API uses Electronic Data Interchange (EDI) techniques, there will clearly be a need for participating carriers and Border Control Agencies to have their automated systems connected to one or more data transmission networks so that passenger details can be transmitted and received electronically. While alternative transmission methods (such as web-based applications) are being developed, many airlines are currently unable to support this mode of transmission.

8.3.2. API data can be sent or received utilizing a number of organizations capable of providing reliable and secure data transmission services. The choice of data network will ultimately be determined by cost and other considerations, such as existing business relationships with a data network provider.

8.3.3 Border Control Agencies should consider establishing systems, as secondary alternatives that are capable of receiving secure API data transmissions, as a means of reducing data transmission costs for carriers that do not operate with traditional reservation and/or departure control systems.

LEGAL ASPECTS OF API[3]

9.1 Generally speaking, API provides Border Control Agencies with data they could otherwise access upon the passenger's arrival and presentation at an immigration inspection desk. API data simply provides data at an earlier time and through different means with the aim of expediting the passengers' clearance.

9.2 However, airlines may collect, store and transmit passengers' API information to Border Control Agencies only in accordance with applicable national legislation.

9.3 Privacy and data protection legislation has been enacted in many countries in recent years in order to protect the individual's right to privacy and to allow individuals to exercise their rights relating to the use of their personal data. .

9.4 This legislation can vary from country to country. However, there is a large degree of commonality within the provisions of such legislation. Privacy and data protection legislation typically requires that personal data undergoing automated (computer) processing:

- should be obtained and processed fairly and lawfully;
- should be stored for legitimate purposes and not used in any way incompatible with those purposes;
- should be adequate, relevant and not excessive in relation to the purposes for which they are stored;
- should be accurate and, where necessary, kept up to date;
- should be preserved in a form which permits identification of the data subjects for no longer than is required for the purposes for which that data is stored.

9.5 Such legislation also incorporates provisions concerning the rights of individuals regarding their personal data. There may also be provisions regarding disclosure of personal data to other parties, and about transmission of such data across national borders and beyond the jurisdiction of the country in which it was collected.

9.6 It is clear from the above the existence of such legislation may well have an impact on a carrier's ability to capture personal details of passengers and to transmit this data to a foreign government. However, it is also clear the nature of API data (basic personal information that appears in an official document) and the use to which it is put, should conform to the national law of most countries. The long-term archiving of passenger manifests on computer media and the use of such data for purposes other than national security or passenger clearance may pose problems in certain countries.

9.7 Because of the differences in the provisions and interpretation of privacy and data protection laws from country to country, carriers required to participate in API should enquire on a case-by-case basis whether the capture, storage and transmission of the passenger details mentioned in this Guideline is in contravention of applicable national law. Where such contravention is determined, the country requiring the API data should, to the best of its abilities, seek to address and resolve those legal concerns.

[3] The EU reserves its position with regard to Section 9 on Legal aspects on API, in view of on-going discussions on the transfer of API data to third countries within the framework of the Article 29 Data Protection Working Party (gathering of national data protection authorities at EU level), in order not to jeopardize in any way the outcome of these discussions and a possible follow-up which the Commission may consider.

CONCLUSIONS

10.1 API is a technique that has the capability of bringing substantial advantages to all involved in the movement of passengers. The WCO, IATA and ICAO **fully support the effectiveness of API data exchange processes, where adopted in accordance with these guidelines.**

10.2 The cost-effective and efficient use of API depends on a common agreement by all concerned, Carriers and Border Control Agencies, to adopt and implement harmonized data standards, formats and transmission processes. To facilitate this objective, Appendices to this paper contain jointly agreed data and messaging standards that are recommended by the WCO, IATA and ICAO.

10.3 Through the efficient use of API data received from carriers and the close co-operation between multiple agencies concerned, API can be the catalyst for increased contact between these agencies and the development of common programmes which can be of benefit from the perspectives of compliance, facilitation and security. Agreement on a joint national passenger processing strategy, in which API plays a central role, is of critical importance.

JOINT COMMENTS OF
AIRLINES FOR AMERICA,
THE INTERNATIONAL AIR TRANSPORT ASSOCIATION,
THE REGIONAL AIRLINE ASSOCIATION, AND
THE NATIONAL AIR CARRIER ASSOCIATION

Docket CDC-2020-0013

ATTACHMENT 19

Data Protection and Privacy Legislation Worldwide

107 countries (of which 66 were developing or transition economies) have put in place legislation to secure the protection of data and privacy. In this area, Asia and Africa show a similar level of adoption, with less than 40 per cent of countries having a law in place.

Overview

E-transaction Laws

Cybercrime Laws

Consumer
Protection Laws

64%
COUNTRIES WITH
LEGISLATION

8%
COUNTRIES WITH
DRAFT LEGISLATION

18%
COUNTRIES WITH
NO LEGISLATION

11%
COUNTRIES WITH
NO DATA

Countries:

Regions:

Download:

Full Data

Created with Highcharts 7.1.1Data Protection and Privacy Legislation WorldwideZoom in+Zoom out-LegislationDraft LegislationNo LegislationNo DataSource: UNCTAD, 18/02/2020

DELEGATES PORTAL
CIVIL SOCIETY
JOURNALISTS
TECHNICAL COOPERATION
CAREERS

United Nations Conference on Trade and Development

Palais des Nations, 8-14,
Av. de la Paix, 1211 Geneva 10
Switzerland

T: +41 22 917 1234
F: +41 22 917 0057

Connect with us

Signup for our Newsletter

Enter Email... Subscribe

**JOINT COMMENTS OF
AIRLINES FOR AMERICA,
THE INTERNATIONAL AIR TRANSPORT ASSOCIATION,
THE REGIONAL AIRLINE ASSOCIATION, AND
THE NATIONAL AIR CARRIER ASSOCIATION**

Docket CDC-2020-0013

ATTACHMENT 20

AGREEMENT
BETWEEN THE UNITED STATES OF AMERICA
AND THE EUROPEAN UNION
ON THE USE AND TRANSFER OF PASSENGER NAME RECORDS
TO THE UNITED STATES DEPARTMENT OF HOMELAND SECURITY

THE UNITED STATES OF AMERICA,

hereinafter referred to also as "the United States", and

THE EUROPEAN UNION,

hereinafter referred to also as "the EU",

together hereinafter referred to as "the Parties",

DESIRING to prevent and combat terrorism and serious transnational crime effectively as a means of protecting their respective democratic societies and common values;

SEEKING to enhance and encourage cooperation between the Parties in the spirit of transatlantic partnership;

RECOGNIZING the right and responsibility of states to ensure the security of their citizens and protect their borders and mindful of the responsibility of all nations to protect the life and safety of the public including those using international transportation systems;

CONVINCED that information sharing is an essential component in the fight against terrorism and serious transnational crime and that in this context, the processing and use of Passenger Name Records (PNR) is a necessary tool that gives information that cannot be obtained by other means;

DETERMINED to prevent and combat terrorist offenses and transnational crime, while respecting fundamental rights and freedoms and recognizing the importance of privacy and the protection of personal data and information;

HAVING REGARD for international instruments, U.S. statutes and regulations requiring each air carrier operating passenger flights in foreign air transportation to or from the United States to make PNR available to the Department of Homeland Security (DHS) to the extent they are collected and contained in the air carrier's automated reservation/departure control systems, and comparable requirements that are or may be implemented in the EU;

NOTING that DHS processes and uses PNR for the purpose of preventing, detecting, investigating and prosecuting terrorist offenses and transnational crime in compliance with safeguards on privacy and the protection of personal data and information, as set out in this Agreement;

STRESSING the importance of sharing PNR and relevant and appropriate analytical information obtained from PNR by the United States with competent police and judicial authorities of Member States of the European Union, hereinafter "EU Member States", and Europol or Eurojust as a means to foster international police and judicial cooperation;

ACKNOWLEDGING both Parties' longstanding traditions of respect for individual privacy, as reflected in their laws and founding documents;

MINDFUL of the EU's commitments pursuant to Article 6 of the Treaty on European Union on respect for fundamental rights, the right to privacy with regard to the processing of personal data as stipulated in Article 16 of the Treaty on the Functioning of the European Union, the principles of proportionality and necessity concerning the right to private and family life, the respect for privacy, and the protection of personal data under Article 8 of the European Convention on the Protection of Human Rights and Fundamental Freedoms, Council of Europe Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data and its additional Protocol 181, and Articles 7 and 8 of the Charter of Fundamental Rights of the European Union;

MINDFUL that DHS currently employs robust processes to protect personal privacy and ensure data integrity, including physical security, access controls, data separation and encryption, audit capabilities and effective accountability measures;

RECOGNIZING the importance of ensuring data quality, accuracy, integrity, and security, and instituting appropriate accountability to ensure these principles are observed;

NOTING in particular the principle of transparency and the various means by which the United States ensures that passengers whose PNR is collected by DHS are made aware of the need for and use of their PNR;

FURTHER RECOGNIZING that the collection and analysis of PNR is necessary for DHS to carry out its border security mission, while ensuring that collection and use of PNR remains relevant and necessary for the purposes for which it is collected;

RECOGNIZING that, in consideration of this Agreement and its implementation, DHS shall be deemed to ensure an adequate level of data protection for the processing and use of PNR transferred to DHS;

MINDFUL that the United States and the European Union are committed to ensuring a high level of protection of personal information while fighting crime and terrorism, and are determined to reach, without delay, an agreement to protect personal information exchanged in the context of fighting crime and terrorism in a comprehensive manner that will advance our mutual goals;

ACKNOWLEDGING the successful Joint Reviews in 2005 and 2010 of the 2004 and 2007 Agreements between the Parties on the transfer of PNR;

NOTING the interest of the Parties, as well as EU Member States, in exchanging information regarding the method of transmission of PNR as well as the onward transfer of PNR as set forth in the relevant articles of this Agreement, and further noting the EU's interest in having this addressed in the context of the consultation and review mechanism set forth in this Agreement;

AFFIRMING that this Agreement does not constitute a precedent for any future arrangements between the Parties, or between either of the Parties and any other party, regarding the processing, use, or transfer of PNR or any other form of data, or regarding data protection;

RECOGNIZING the related principles of proportionality as well as relevance and necessity that guide this Agreement and its implementation by the European Union and the United States; and

HAVING REGARD to the possibility of the Parties to further discuss the transfer of PNR data in the maritime mode;

HEREBY AGREE:

CHAPTER 1

GENERAL PROVISIONS

ARTICLE 1

Purpose

1. The purpose of this Agreement is to ensure security and to protect the life and safety of the public.

2. For this purpose, this Agreement sets forth the responsibilities of the Parties with respect to the conditions under which PNR may be transferred, processed and used, and protected.

ARTICLE 2

Scope

1. PNR, as set forth in the Guidelines of the International Civil Aviation Organization, shall mean the record created by air carriers or their authorized agents for each journey booked by or on behalf of any passenger and contained in carriers' reservation systems, departure control systems, or equivalent systems providing similar functionality (collectively referred to in this Agreement as "reservation systems"). Specifically, as used in this Agreement, PNR consists of the data types set forth in the Annex to this Agreement ("Annex").

2. This Agreement shall apply to carriers operating passenger flights between the European Union and the United States.

3. This Agreement shall also apply to carriers incorporated or storing data in the European Union and operating passenger flights to or from the United States.

ARTICLE 3

Provision of PNR

The Parties agree that carriers shall provide PNR contained in their reservation systems to DHS as required by and in accordance with DHS standards and consistent with this Agreement. Should PNR transferred by carriers include data beyond those listed in the Annex, DHS shall delete such data upon receipt.

ARTICLE 4

Use of PNR

1. The United States collects, uses and processes PNR for the purposes of preventing, detecting, investigating, and prosecuting:

(a) Terrorist offenses and related crimes, including

(i) Conduct that –

1. involves a violent act or an act dangerous to human life, property, or infrastructure; and

2. appears to be intended to –

a. intimidate or coerce a civilian population;

b. influence the policy of a government by intimidation or coercion; or

c. affect the conduct of a government by mass destruction, assassination, kidnapping, or hostage-taking.

(ii) Activities constituting an offense within the scope of and as defined in applicable international conventions and protocols relating to terrorism;

(iii) Providing or collecting funds, by any means, directly or indirectly, with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the acts described in subparagraphs (i) or (ii);

(iv) Attempting to commit any of the acts described in subparagraphs (i), (ii), or (iii);

(v) Participating as an accomplice in the commission of any of the acts described in subparagraphs (i), (ii), or (iii);

(vi) Organizing or directing others to commit any of the acts described in subparagraphs (i), (ii), or (iii);

(vii) Contributing in any other way to the commission of any of the acts described in subparagraphs (i), (ii), or (iii);

(viii) Threatening to commit an act described in subparagraph (i) under circumstances which indicate that the threat is credible;

(b) Other crimes that are punishable by a sentence of imprisonment of three years or more and that are transnational in nature.

A crime is considered as transnational in nature in particular if:

(i) It is committed in more than one country;

(ii) It is committed in one country but a substantial part of its preparation, planning, direction or control takes place in another country;

(iii) It is committed in one country but involves an organized criminal group that engages in criminal activities in more than one country;

(iv) It is committed in one country but has substantial effects in another country; or

(v) It is committed in one country and the offender is in or intends to travel to another country.

2. PNR may be used and processed on a case-by-case basis where necessary in view of a serious threat and for the protection of vital interests of any individual or if ordered by a court.

3. PNR may be used and processed by DHS to identify persons who would be subject to closer questioning or examination upon arrival to or departure from the United States or who may require further examination.

4. Paragraphs 1, 2, and 3 shall be without prejudice to domestic law enforcement, judicial powers, or proceedings, where other violations of law or indications thereof are detected in the course of the use and processing of PNR.

CHAPTER II

SAFEGUARDS APPLICABLE TO THE USE OF PNR

ARTICLE 5

Data Security

1. DHS shall ensure that appropriate technical measures and organizational arrangements are implemented to protect personal data and personal information contained in PNR against accidental, unlawful or unauthorized destruction, loss, disclosure, alteration, access, processing or use.

2. DHS shall make appropriate use of technology to ensure data protection, security, confidentiality and integrity. In particular, DHS shall ensure that:

(a) encryption, authorization and documentation procedures recognized by competent authorities are applied. In particular, access to PNR shall be secured and limited to specifically authorized officials;

(b) PNR shall be held in a secure physical environment and protected with physical intrusion controls; and

(c) a mechanism exists to ensure that PNR queries are conducted consistent with Article 4.

3. In the event of a privacy incident (including unauthorized access or disclosure), DHS shall take reasonable measures to notify affected individuals as appropriate, to mitigate the risk of harm of unauthorized disclosures of personal data and information, and to institute remedial measures as may be technically practicable.

4. Within the scope of this Agreement, DHS shall inform without undue delay the relevant European authorities about cases of significant privacy incidents involving PNR of EU citizens or residents resulting from accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, or any unlawful forms of processing or use.

5. The United States confirms that effective administrative, civil, and criminal enforcement measures are available under U.S. law for privacy incidents. DHS may take disciplinary action against persons responsible for any such privacy incident, as appropriate, to include denial of system access, formal reprimands, suspension, demotion, or removal from duty.

6. All access to PNR, as well as its processing and use, shall be logged or documented by DHS. Logs or documentation shall be used only for oversight, auditing, and system maintenance purposes or as otherwise required by law.

ARTICLE 6

Sensitive Data

1. To the extent that PNR of a passenger as collected includes sensitive data (i.e., personal data and information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or data concerning the health or sex life of the individual), DHS shall employ automated systems to filter and mask out sensitive data from PNR. In addition, DHS shall not further process or use such data, except in accordance with paragraphs 3 and 4.

2. DHS shall provide to the European Commission within 90 days of the entry into force of this Agreement a list of codes and terms identifying sensitive data that shall be filtered out.

3. Access to, as well as processing and use of, sensitive data shall be permitted in exceptional circumstances where the life of an individual could be imperiled or seriously impaired. Such data may be exclusively accessed using restrictive processes on a case-by-case basis with the approval of a DHS senior manager.

4. Sensitive data shall be permanently deleted not later than 30 days from the last receipt of PNR containing such data by DHS. However, sensitive data may be retained for the time specified in U.S. law for the purpose of a specific investigation, prosecution or enforcement action.

ARTICLE 7

Automated Individual Decisions

The United States shall not make decisions that produce significant adverse actions affecting the legal interests of individuals based solely on automated processing and use of PNR.

ARTICLE 8

Retention of Data

1. DHS retains PNR in an active database for up to five years. After the initial six months of this period, PNR shall be depersonalized and masked in accordance with paragraph 2 of this Article. Access to this active database shall, unless otherwise permitted by this Agreement, be restricted to a limited number of specifically authorized officials.

2. To achieve depersonalization, personally identifiable information contained in the following PNR data types shall be masked out:

(a) name(s);

(b) other names on PNR;

(c) all available contact information (including originator information);

(d) General Remarks, including other supplementary information (OSI), special service information (SSI), and special service request (SSR); and

(e) any collected Advance Passenger Information System (APIS) information.

3. After this active period, PNR shall be transferred to a dormant database for a period of up to ten years. This dormant database shall be subject to additional controls, including a more restricted number of authorized personnel, as well as a higher level of supervisory approval required before access. In this dormant database, PNR shall not be repersonalized except in connection with law enforcement operations and then only in connection with an identifiable case, threat or risk. As regards the purposes as set out in Article 4(1)(b), PNR in this dormant database may only be repersonalized for a period of up to five years.

4. Following the dormant period, data retained must be rendered fully anonymized by deleting all data types which could serve to identify the passenger to whom PNR relate without the possibility of repersonalization.

5. Data that are related to a specific case or investigation may be retained in an active PNR database until the case or investigation is archived. This paragraph is without prejudice to data retention requirements for individual investigation or prosecution files.

6. The Parties agree that, within the framework of the evaluation as provided for in Article 23(1), the necessity of a 10-year dormant period of retention will be considered.

ARTICLE 9

Non-discrimination

The United States shall ensure that the safeguards applicable to processing and use of PNR under this Agreement apply to all passengers on an equal basis without unlawful discrimination.

ARTICLE 10

Transparency

1. DHS shall provide information to the traveling public regarding its use and processing of PNR through:

(a) publications in the Federal Register;

(b) publications on its website;

(c) notices that may be incorporated by the carriers into contracts of carriage;

(d) statutorily required reporting to Congress; and

(e) other appropriate measures as may be developed.

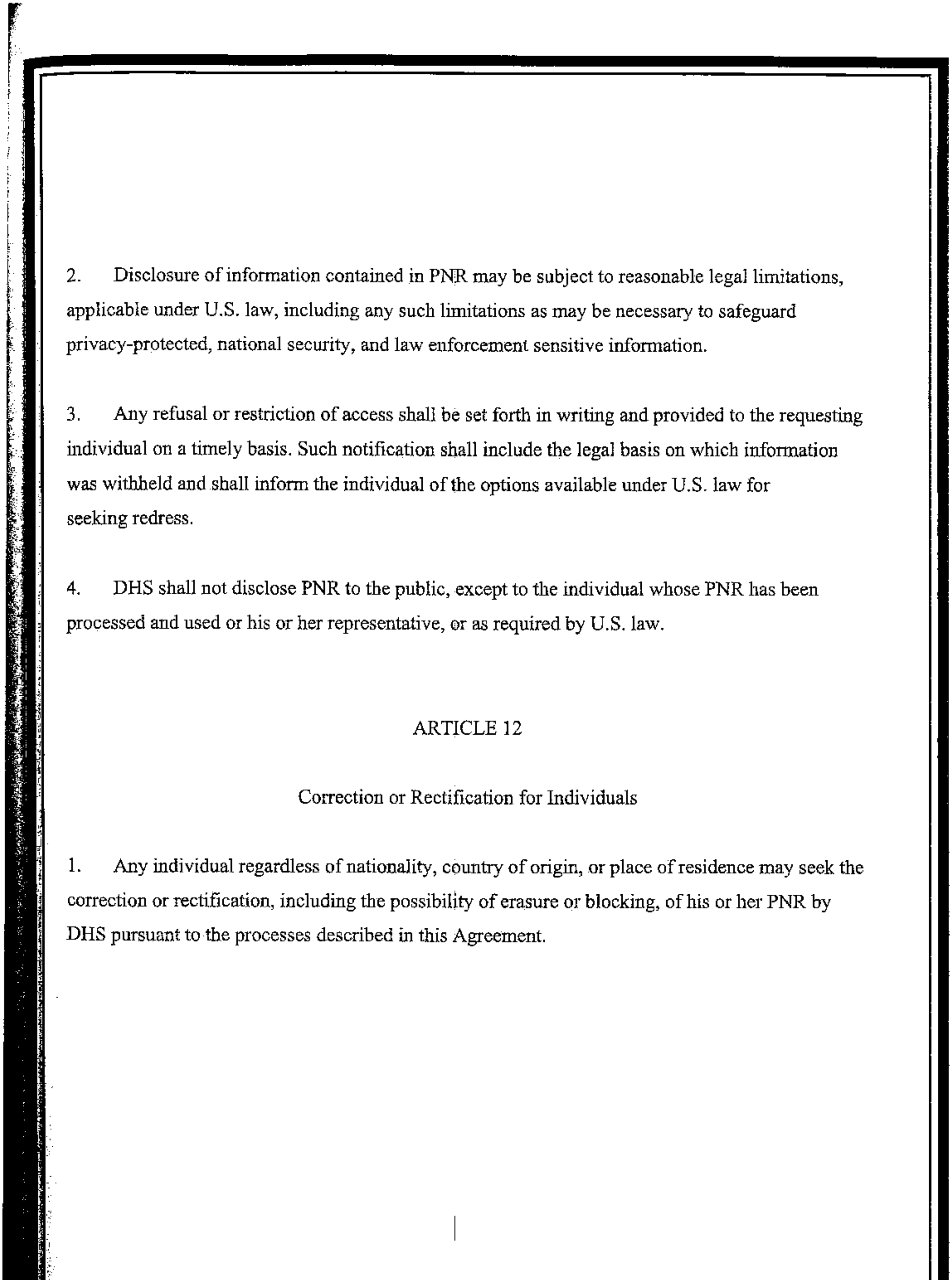
2. DHS shall publish and provide to the EU for possible publication its procedures and modalities regarding access, correction or rectification, and redress procedures.

3. The Parties shall work with the aviation industry to encourage greater visibility to passengers at the time of booking on the purpose of the collection, processing and use of PNR by DHS, and on how to request access, correction and redress.

ARTICLE 11

Access for Individuals

1. In accordance with the provisions of the Freedom of Information Act, any individual, regardless of nationality, country of origin, or place of residence is entitled to request his or her PNR from DHS. DHS shall timely provide such PNR subject to the provisions of paragraphs 2 and 3 of this Article.



2. Disclosure of information contained in PNR may be subject to reasonable legal limitations, applicable under U.S. law, including any such limitations as may be necessary to safeguard privacy-protected, national security, and law enforcement sensitive information.

3. Any refusal or restriction of access shall be set forth in writing and provided to the requesting individual on a timely basis. Such notification shall include the legal basis on which information was withheld and shall inform the individual of the options available under U.S. law for seeking redress.

4. DHS shall not disclose PNR to the public, except to the individual whose PNR has been processed and used or his or her representative, or as required by U.S. law.

ARTICLE 12

Correction or Rectification for Individuals

1. Any individual regardless of nationality, country of origin, or place of residence may seek the correction or rectification, including the possibility of erasure or blocking, of his or her PNR by DHS pursuant to the processes described in this Agreement.

2. DHS shall inform, without undue delay, the requesting individual in writing of its decision whether to correct or rectify the PNR at issue.

3. Any refusal or restriction of correction or rectification shall be set forth in writing and provided to the requesting individual on a timely basis. Such notification shall include the legal basis of such refusal or restriction and shall inform the individual of the options available under U.S. law for seeking redress.

ARTICLE 13

Redress for Individuals

1. Any individual regardless of nationality, country of origin, or place of residence whose personal data and personal information has been processed and used in a manner inconsistent with this Agreement may seek effective administrative and judicial redress in accordance with U.S. law.

2. Any individual is entitled to seek to administratively challenge DHS decisions related to the use and processing of PNR.

3. Under the provisions of the Administrative Procedure Act and other applicable law, any individual is entitled to petition for judicial review in U.S. federal court of any final agency action by DHS. Further, any individual is entitled to petition for judicial review in accordance with applicable law and relevant provisions of:

(a) the Freedom of Information Act;

(b) the Computer Fraud and Abuse Act;

(c) the Electronic Communications Privacy Act; and

(d) other applicable provisions of U.S. law.

4. In particular, DHS provides all individuals an administrative means (currently the DHS Traveler Redress Inquiry Program (DHS TRIP)) to resolve travel-related inquiries including those related to the use of PNR. DHS TRIP provides a redress process for individuals who believe they have been delayed or prohibited from boarding a commercial aircraft because they were wrongly identified as a threat. Pursuant to the Administrative Procedure Act and Title 49, United States Code, Section 46110, any such aggrieved individual is entitled to petition for judicial review in U.S. federal court from any final agency action by DHS relating to such concerns.

ARTICLE 14

Oversight

1. Compliance with the privacy safeguards in this Agreement shall be subject to independent review and oversight by Department Privacy Officers, such as the DHS Chief Privacy Officer, who:

(a) have a proven record of autonomy;

(b) exercise effective powers of oversight, investigation, intervention, and review; and

(c) have the power to refer violations of law related to this Agreement for prosecution or disciplinary action, when appropriate.

They shall, in particular, ensure that complaints relating to non-compliance with this Agreement are received, investigated, responded to, and appropriately redressed. These complaints may be brought by any individual, regardless of nationality, country of origin, or place of residence.

2. In addition, application of this Agreement by the United States shall be subject to independent review and oversight by one or more of the following entities:

(a) the DHS Office of Inspector General;

(b) the Government Accountability Office as established by Congress; and

(c) the U.S. Congress.

Such oversight may be manifested in the findings and recommendations of public reports, public hearings, and analyses.

CHAPTER III

MODALITIES OF TRANSFERS

ARTICLE 15

Method of PNR Transmission

1. For the purposes of this Agreement, carriers shall be required to transfer PNR to DHS using the "push" method, in furtherance of the need for accuracy, timeliness and completeness of PNR.

2. Carriers shall be required to transfer PNR to DHS by secure electronic means in compliance with the technical requirements of DHS.

3. Carriers shall be required to transfer PNR to DHS in accordance with paragraphs 1 and 2, initially at 96 hours before the scheduled flight departure and additionally either in real time or for a fixed number of routine and scheduled transfers as specified by DHS.

4. In any case, the Parties agree that all carriers shall be required to acquire the technical ability to use the "push" method not later than 24 months following entry into force of this Agreement.

5. DHS may, where necessary, on a case-by-case basis, require a carrier to provide PNR between or after the regular transfers described in paragraph 3. Wherever carriers are unable, for technical reasons, to respond timely to requests under this Article in accordance with DHS standards, or, in exceptional circumstances in order to respond to a specific, urgent, and serious threat, DHS may require carriers to otherwise provide access.

ARTICLE 16

Domestic Sharing

1. DHS may share PNR only pursuant to a careful assessment of the following safeguards:

(a) Exclusively as consistent with Article 4;

(b) Only with domestic government authorities when acting in furtherance of the uses outlined in Article 4;

(c) Receiving authorities shall afford to PNR equivalent or comparable safeguards as set out in this Agreement; and

(d) PNR shall be shared only in support of those cases under examination or investigation and pursuant to written understandings and U.S. law on the exchange of information between domestic government authorities.

2. When transferring analytical information obtained from PNR under this Agreement, the safeguards set forth in paragraph 1 of this Article shall be respected.

ARTICLE 17

Onward Transfer

1. The United States may transfer PNR to competent government authorities of third countries only under terms consistent with this Agreement and only upon ascertaining that the recipient's intended use is consistent with those terms.

2. Apart from emergency circumstances, any such transfer of data shall occur pursuant to express understandings that incorporate data privacy protections comparable to those applied to PNR by DHS as set out in this Agreement.

3. PNR shall be shared only in support of those cases under examination or investigation.

4. Where DHS is aware that PNR of a citizen or a resident of an EU Member State is transferred, the competent authorities of the concerned Member State shall be informed of the matter at the earliest appropriate opportunity.

5. When transferring analytical information obtained from PNR under this Agreement, the safeguards set forth in paragraphs 1 to 4 shall be respected.

ARTICLE 18

Police, Law Enforcement and Judicial Cooperation

1. Consistent with existing law enforcement or other information-sharing agreements or arrangements between the United States and any EU Member State or Europol and Eurojust, DHS shall provide to competent police, other specialized law enforcement or judicial authorities of the EU Member States and Europol and Eurojust within the remit of their respective mandates, as soon as practicable, relevant, and appropriate, analytical information obtained from PNR in those cases under examination or investigation to prevent, detect, investigate, or prosecute within the European Union terrorist offenses and related crimes or transnational crime as described in Article 4(1)(b).

2. A police or judicial authority of an EU Member State, or Europol or Eurojust, may request, within its mandate, access to PNR or relevant analytical information obtained from PNR that are necessary in a specific case to prevent, detect, investigate, or prosecute within the European Union terrorist offenses and related crimes or transnational crime as described in Article 4(1)(b). DHS shall, subject to the agreements and arrangements noted in paragraph 1 of this Article, provide such information.

3. Pursuant to paragraphs 1 and 2 of this Article, DHS shall share PNR only following a careful assessment of the following safeguards:

(a) Exclusively as consistent with Article 4;

(b) Only when acting in furtherance of the uses outlined in Article 4; and

(c) Receiving authorities shall afford to PNR equivalent or comparable safeguards as set out in this Agreement.

4. When transferring analytical information obtained from PNR under this Agreement, the safeguards set forth in paragraphs 1-3 of this Article shall be respected.

CHAPTER IV

IMPLEMENTING AND FINAL PROVISIONS

ARTICLE 19

Adequacy

In consideration of this Agreement and its implementation, DHS shall be deemed to provide, within the meaning of relevant EU data protection law, an adequate level of protection for PNR processing and use. In this respect, carriers which have provided PNR to DHS in compliance with this Agreement shall be deemed to have complied with applicable legal requirements in the EU related to the transfer of such data from the EU to the United States.

ARTICLE 20

Reciprocity

1. The Parties shall actively promote the cooperation of carriers within their respective jurisdictions with any PNR system operating or as may be adopted in the other's jurisdiction, consistent with this Agreement.

2. Given that the establishment of an EU PNR system could have a material effect on the Parties' obligations under this Agreement, if and when an EU PNR system is adopted, the Parties shall consult to determine whether this Agreement would need to be adjusted accordingly to ensure full reciprocity. Such consultations shall in particular examine whether any future EU PNR system would apply less stringent data protection standards than those provided for in this Agreement, and whether, therefore, this Agreement should be amended.

ARTICLE 21

Implementation and Non-Derogation

1. This Agreement shall not create or confer, under U.S. law, any right or benefit on any person or entity, private or public. Each Party shall ensure that the provisions of this Agreement are properly implemented.

2. Nothing in this Agreement shall derogate from existing obligations of the United States and EU Member States, including under the Agreement on Mutual Legal Assistance between the European Union and the United States of 25 June 2003 and the related bilateral mutual legal assistance instruments between the United States and EU Member States.

ARTICLE 22

Notification of Changes in Domestic Law

The Parties shall advise each other regarding the enactment of any legislation that materially affects the implementation of this Agreement.

ARTICLE 23

Review and Evaluation

1. The Parties shall jointly review the implementation of this Agreement one year after its entry into force and regularly thereafter as jointly agreed. Further, the Parties shall jointly evaluate this Agreement four years after its entry into force.

2. The Parties shall jointly determine in advance the modalities and terms of the joint review and shall communicate to each other the composition of their respective teams. For the purpose of the joint review, the European Union shall be represented by the European Commission, and the United States shall be represented by DHS. The teams may include appropriate experts on data protection and law enforcement. Subject to applicable laws, participants in the joint review shall be required to have appropriate security clearances and to respect the confidentiality of the discussions. For the purpose of the joint review, DHS shall ensure appropriate access to relevant documentation, systems, and personnel.

3. Following the joint review, the European Commission shall present a report to the European Parliament and the Council of the European Union. The United States shall be given an opportunity to provide written comments which shall be attached to the report.

ARTICLE 24

Resolution of Disputes and Suspension of Agreement

1. Any dispute arising from the implementation of this Agreement, and any matters related thereto, shall give rise to consultations between the Parties, with a view to reaching a mutually agreeable resolution, including providing an opportunity for either Party to cure within a reasonable time.

2. In the event that consultations do not result in a resolution of the dispute, either Party may suspend the application of this Agreement by written notification through diplomatic channels, with any such suspension to take effect 90 days from the date of such notification, unless the Parties otherwise agree to a different effective date.

3. Notwithstanding any suspension of this Agreement, all PNR obtained by DHS pursuant to this Agreement prior to its suspension shall continue to be processed and used in accordance with the safeguards of this Agreement.

ARTICLE 25

Termination

1. Either Party may terminate this Agreement at any time by written notification through diplomatic channels.

2. Termination shall take effect 120 days from the date of such notification, unless the Parties otherwise agree to a different effective date.

3. Prior to any termination of this Agreement, the Parties shall consult each other in a manner which allows sufficient time for reaching a mutually agreeable resolution.

4. Notwithstanding any termination of this Agreement, all PNR obtained by DHS pursuant to this Agreement prior to its termination shall continue to be processed and used in accordance with the safeguards of this Agreement.

ARTICLE 26

Duration

1. Subject to Article 25, this Agreement shall remain in force for a period of seven years from the date of its entry into force.

2. Upon the expiry of the period set forth in paragraph 1 of this Article, as well as any subsequent period of renewal under this paragraph, the Agreement shall be renewed for a subsequent period of seven years unless one of the Parties notifies the other in writing through diplomatic channels, at least twelve months in advance, of its intention not to renew the Agreement.

3. Notwithstanding the expiration of this Agreement, all PNR obtained by DHS under the terms of this Agreement shall continue to be processed and used in accordance with the safeguards of this Agreement. Similarly, all PNR obtained by DHS under the terms of the Agreement Between the United States of America and the European Union on the processing and transfer of Passenger Name Record (PNR) Data by air carriers to the United States Department of Homeland Security (DHS), signed at Brussels and Washington July 23 and 26, 2007, shall continue to be processed and used in accordance with the safeguards of that Agreement.

ARTICLE 27

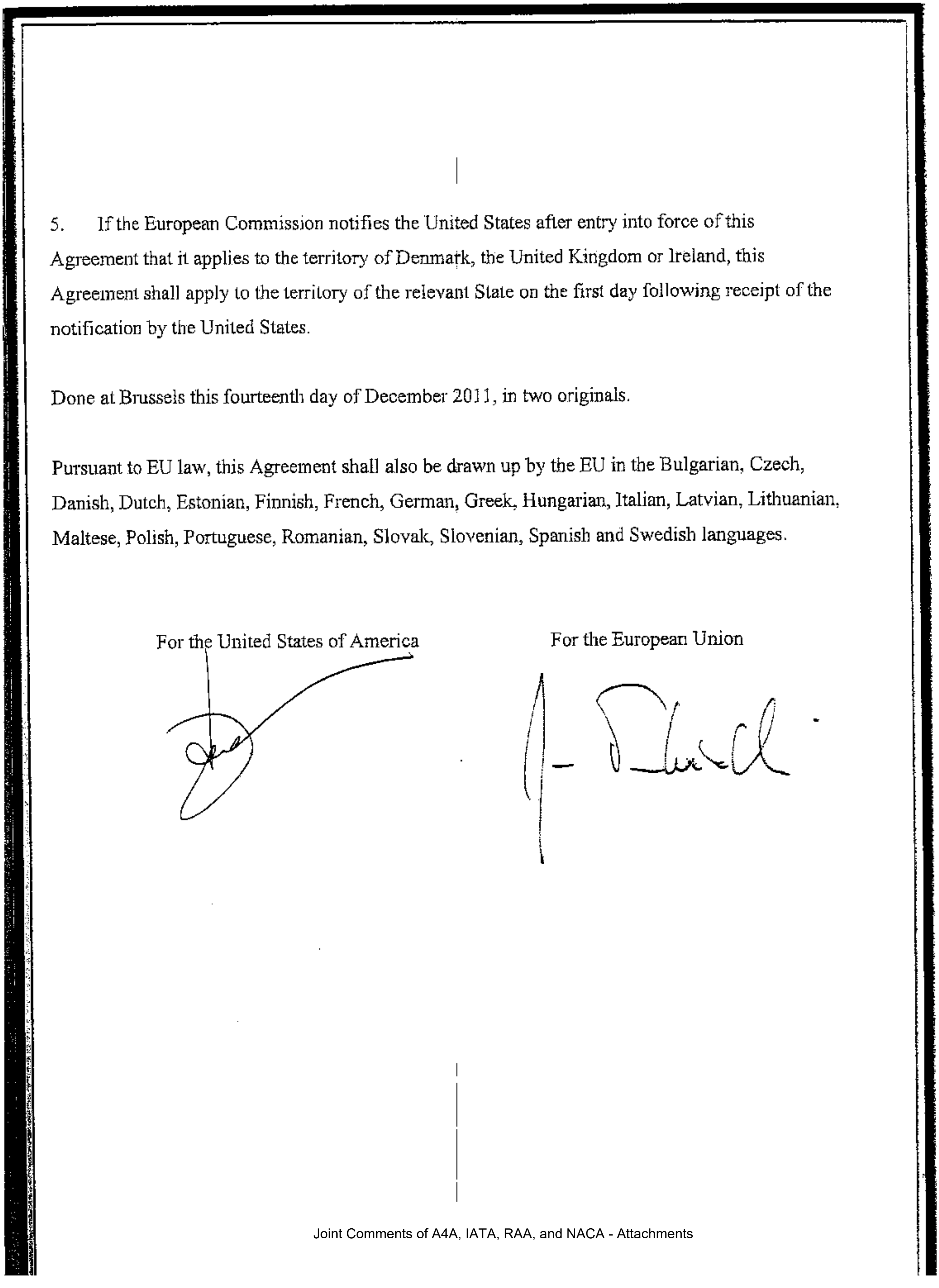
Final provisions

1. This Agreement shall enter into force on the first day of the month after the date on which the Parties have exchanged notifications indicating that they have completed their internal procedures for this purpose.

2. This Agreement, as of the date of its entry into force, shall supersede the July 23 and 26, 2007 Agreement.

3. This Agreement will only apply to the territory of Denmark, the United Kingdom or Ireland, if the European Commission notifies the United States in writing that Denmark, the United Kingdom or Ireland has chosen to be bound by this Agreement.

4. If the European Commission notifies the United States before the entry into force of this Agreement that it will apply to the territory of Denmark, the United Kingdom or Ireland, this Agreement shall apply to the territory of the relevant State on the same day as for the other EU Member States bound by this Agreement.



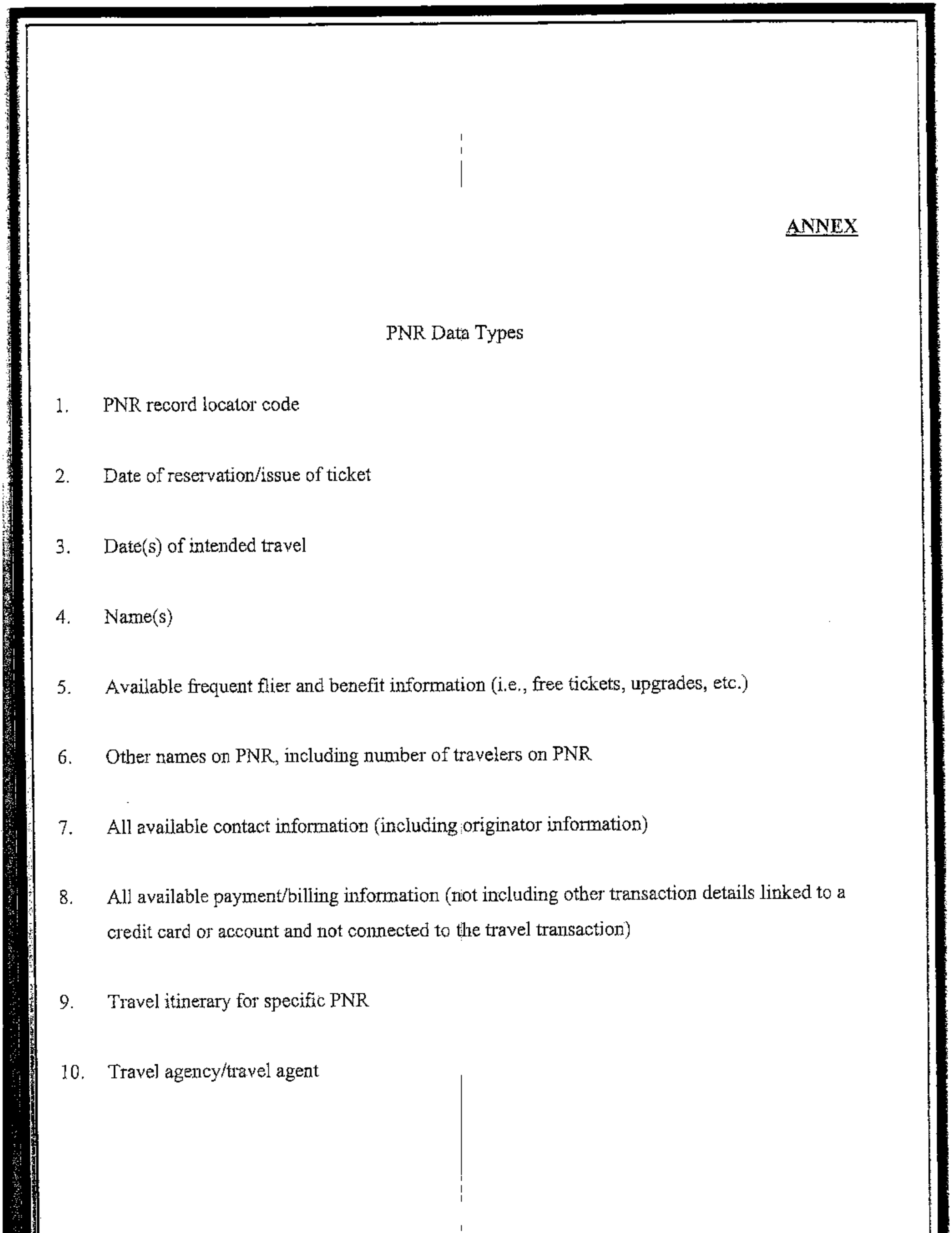
5. If the European Commission notifies the United States after entry into force of this Agreement that it applies to the territory of Denmark, the United Kingdom or Ireland, this Agreement shall apply to the territory of the relevant State on the first day following receipt of the notification by the United States.

Done at Brussels this fourteenth day of December 2011, in two originals.

Pursuant to EU law, this Agreement shall also be drawn up by the EU in the Bulgarian, Czech, Danish, Dutch, Estonian, Finnish, French, German, Greek, Hungarian, Italian, Latvian, Lithuanian, Maltese, Polish, Portuguese, Romanian, Slovak, Slovenian, Spanish and Swedish languages.

For the United States of America

For the European Union



ANNEX

PNR Data Types

1. PNR record locator code

2. Date of reservation/issue of ticket

3. Date(s) of intended travel

4. Name(s)

5. Available frequent flier and benefit information (i.e., free tickets, upgrades, etc.)

6. Other names on PNR, including number of travelers on PNR

7. All available contact information (including originator information)

8. All available payment/billing information (not including other transaction details linked to a credit card or account and not connected to the travel transaction)

9. Travel itinerary for specific PNR

10. Travel agency/travel agent

11. Code share information

12. Split/divided information

13. Travel status of passenger (including confirmations and check-in status)

14. Ticketing information, including ticket number, one way tickets and Automated Ticket Fare Quote

15. All baggage information

16. Seat information, including seat number

17. General remarks including OSI, SSI and SSR information

18. Any collected APIS information

19. All historical changes to the PNR listed under points 1 to 18

JOINT COMMENTS OF
AIRLINES FOR AMERICA,
THE INTERNATIONAL AIR TRANSPORT ASSOCIATION,
THE REGIONAL AIRLINE ASSOCIATION, AND
THE NATIONAL AIR CARRIER ASSOCIATION

Docket CDC-2020-0013

ATTACHMENT 21

ARTICLE 29 DATA PROTECTION WORKING PARTY

17/EN
WP259 rev.01

Article 29 Working Party
Guidelines on consent under Regulation 2016/679

Adopted on 28 November 2017

As last Revised and Adopted on 10 April 2018

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE

PROCESSING OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

having regard to Articles 29 and 30 thereof,

having regard to its Rules of Procedure,

HAS ADOPTED THE PRESENT GUIDELINES:

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 02/013.

Website: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936

Contents

1. Introduction

These Guidelines provide a thorough analysis of the notion of consent in Regulation 2016/679, the General Data Protection Regulation (hereafter: GDPR). The concept of consent as used in the Data Protection Directive (hereafter: Directive 95/46/EC) and in the e-Privacy Directive to date, has evolved. The GDPR provides further clarification and specification of the requirements for obtaining and demonstrating valid consent. These Guidelines focus on these changes, providing practical guidance to ensure compliance with the GDPR and building upon Opinion 15/2011 on consent. The obligation is on controllers to innovate to find new solutions that operate within the parameters of the law and better support the protection of personal data and the interests of data subjects.

Consent remains one of six lawful bases to process personal data, as listed in Article 6 of the GDPR.[1] When initiating activities that involve processing of personal data, a controller must always take time to consider what would be the appropriate lawful ground for the envisaged processing.

Generally, consent can only be an appropriate lawful basis if a data subject is offered control and is offered a genuine choice with regard to accepting or declining the terms offered or declining them without detriment. When asking for consent, a controller has the duty to assess whether it will meet all the requirements to obtain valid consent. If obtained in full compliance with the GDPR, consent is a tool that gives data subjects control over whether or not personal data concerning them will be processed. If not, the data subject's control becomes illusory and consent will be an invalid basis for processing, rendering the processing activity unlawful.[2]

The existing Article 29 Working Party (WP29) Opinions on consent[3] remain relevant, where consistent with the new legal framework, as the GDPR codifies existing WP29 guidance and general good practice and most of the key elements of consent remain the same under the GDPR. Therefore, in this document, WP29 expands upon and completes earlier Opinions on specific topics that include reference to consent under Directive 95/46/EC, rather than replacing them.

As stated in Opinion 15/2011 on the definition on consent, inviting people to accept a data processing operation should be subject to rigorous requirements, since it concerns the fundamental rights of data subjects and the controller wishes to engage in a processing operation that would be unlawful without the data subject's consent.[4] The crucial role of consent is underlined by Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. Furthermore, obtaining consent also does not negate or in any way diminish the controller's obligations to observe the principles of processing enshrined in the GDPR, especially Article 5 of the GDPR with regard to fairness, necessity and proportionality, as well as data quality. Even if the processing of personal data is

[1] Article 9 GDPR provides a list of possible exemptions to the ban on processing special categories of data. One of the exemptions listed is the situation where the data subject provides explicit consent to the use of this data.

[2] See also Opinion 15/2011 on the definition of consent (WP 187), pp. 6-8, and/or Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP 217), pp. 9, 10, 13 and 14.

[3] Most notably, Opinion 15/2011 on the definition of consent (WP 187).

[4] Opinion 15/2011, page on the definition of consent (WP 187), p. 8

based on consent of the data subject, this would not legitimise collection of data which is not necessary in relation to a specified purpose of processing and be fundamentally unfair.[5]

Meanwhile, WP29 is aware of the review of the ePrivacy Directive (2002/58/EC). The notion of consent in the draft ePrivacy Regulation remains linked to the notion of consent in the GDPR.[6] Organisations are likely to need consent under the ePrivacy instrument for most online marketing messages or marketing calls, and online tracking methods including by the use of cookies or apps or other software. WP29 has already provided recommendations and guidance to the European legislator on the Proposal for a Regulation on ePrivacy.[7]

With regard to the existing e-Privacy Directive, WP29 notes that references to the repealed Directive 95/46/EC shall be construed as references to the GDPR.[8] This also applies to references to consent in the current Directive 2002/58/EC, as the ePrivacy Regulation will not (yet) be in force from 25 May 2018. According to Article 95 GDPR, additional obligations in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks shall not be imposed insofar the e-Privacy Directive imposes specific obligations with the same objective. WP29 notes that the requirements for consent under the GDPR are not considered to be an 'additional obligation', but rather as preconditions for lawful processing. Therefore, the GDPR conditions for obtaining valid consent are applicable in situations falling within the scope of the e-Privacy Directive.

2. Consent in Article 4(11) of the GDPR

Article 4(11) of the GDPR defines consent as: "*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.*"

The basic concept of consent remains similar to that under the Directive 95/46/EC and consent is one of the lawful grounds on which personal data processing has to be based, pursuant to Article 6 of the GDPR.[9] Besides the amended definition in Article 4(11), the GDPR provides additional

[5] See also Opinion 15/2011 on the definition of consent (WP 187), and Article 5 GDPR.

[6] According to Article 9 of the proposed ePrivacy Regulation, the definition of and the conditions for consent provided for in Articles 4(11) and Article 7 of the GDPR apply.

[7] See Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (WP 240).

[8] See Article 94 GDPR.

[9] Consent was defined in Directive 95/46/EC as "*any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed*" which must be '*unambiguously given*' in order to make the processing of personal data legitimate (Article 7(a) of Directive 95/46/EC)). See WP29 Opinion 15/2011 on the definition of consent (WP 187) for examples on the appropriateness of consent as lawful basis. In this Opinion, WP29 has provided guidance to distinguish where consent is an appropriate lawful basis from those where relying on the legitimate interest ground (perhaps with an opportunity to opt out) is sufficient or a contractual relation would be recommended. See also WP29 Opinion 06/2014, paragraph III.1.2, p. 14 and further. Explicit consent is also one of the exemptions to the prohibition on the processing of special categories of data: See Article 9 GDPR.

guidance in Article 7 and in recitals 32, 33, 42, and 43 as to how the controller must act to comply with the main elements of the consent requirement.

Finally, the inclusion of specific provisions and recitals on the withdrawal of consent confirms that consent should be a reversible decision and that there remains a degree of control on the side of the data subject.

3. Elements of valid consent

Article 4(11) of the GDPR stipulates that consent of the data subject means any:

- freely given,
- specific,
- informed and
- unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

In the sections below, it is analysed to what extent the wording of Article 4(11) requires controllers to change their consent requests/forms, in order to ensure compliance with the GDPR.[10]

3.1. Free / freely given[11]

The element "free" implies real choice and control for data subjects. As a general rule, the GDPR prescribes that if the data subject has no real choice, feels compelled to consent or will endure negative consequences if they do not consent, then consent will not be valid.[12] If consent is bundled up as a non-negotiable part of terms and conditions it is presumed not to have been freely given. Accordingly, consent will not be considered to be free if the data subject is unable to refuse or withdraw his or her consent without detriment.[13] The notion of imbalance between the controller and the data subject is also taken into consideration by the GDPR.

When assessing whether consent is freely given, one should also take into account the specific situation of tying consent into contracts or the provision of a service as described in Article 7(4). Article 7(4) has been drafted in a non-exhaustive fashion by the words "inter alia", meaning that there may be a range of other situations which are caught by this provision. In general terms, any

[10] For guidance with regard to ongoing processing activities based on consent in Directive 95/46, see chapter 7 of this document and recital 171 of the GDPR.

[11] In several opinions, the Article 29 Working Party has explored the limits of consent in situations where it cannot be freely given. This was notably the case in its Opinion 15/2011 on the definition of consent (WP 187), Working Document on the processing of personal data relating to health in electronic health records (WP 131), Opinion 8/2001 on the processing of personal data in the employment context (WP48), and Second opinion 4/2009 on processing of data by the World Anti-Doping Agency (WADA) (International Standard for the Protection of Privacy and Personal Information, on related provisions of the WADA Code and on other privacy issues in the context of the fight against doping in sport by WADA and (national) anti-doping organizations (WP 162).

[12] See Opinion 15/2011 on the definition of consent (WP187), p. 12

[13] See Recitals 42, 43 GDPR and WP29 Opinion 15/2011 on the definition of consent, adopted on 13 July 2011, (WP 187), p. 12.

element of inappropriate pressure or influence upon the data subject (which may be manifested in many different ways) which prevents a data subject from exercising their free will, shall render the consent invalid.

> [Example 1]
> A mobile app for photo editing asks its users to have their GPS localisation activated for the use of its services. The app also tells its users it will use the collected data for behavioural advertising purposes. Neither geo-localisation or online behavioural advertising are necessary for the provision of the photo editing service and go beyond the delivery of the core service provided. Since users cannot use the app without consenting to these purposes, the consent cannot be considered as being freely given.

3.1.1. Imbalance of power

Recital 43[14] clearly indicates that it is unlikely that **public authorities** can rely on consent for processing as whenever the controller is a public authority, there is often a clear imbalance of power in the relationship between the controller and the data subject. It is also clear in most cases that the data subject will have no realistic alternatives to accepting the processing (terms) of this controller. WP29 considers that there are other lawful bases that are, in principle, more appropriate to the activity of public authorities.[15]

Without prejudice to these general considerations, the use of consent as a lawful basis for data processing by public authorities is not totally excluded under the legal framework of the GDPR. The following examples show that the use of consent can be appropriate under certain circumstances.

> [Example 2] A local municipality is planning road maintenance works. As the road works may disrupt traffic for a long time, the municipality offers its citizens the opportunity to subscribe to an email list to receive updates on the progress of the works and on expected delays. The municipality makes clear that there is no obligation to participate and asks for consent to use email addresses for this (exclusive) purpose. Citizens that do not consent will not miss out on any core service of the municipality or the exercise of any right, so they are able to give or refuse their consent to this use of data freely. All information on the road works will also be available on the municipality's website.

> [Example 3] An individual who owns land needs certain permits from both her local municipality and from the provincial government under which the municipality resides. Both public bodies require the same information for issuing their permit, but are not accessing each other's databases. Therefore, both ask for the same information and the land owner sends out her details to both public bodies. The municipality and the provincial authority ask for her consent to merge the files, to avoid duplicate procedures and correspondence. Both public bodies ensure that this is optional and that the permit requests will still be processed separately if she decides not to consent to the merger of her data. The land owner is able to give consent to the authorities for the purpose of merging the files freely.

[14] Recital 43 GDPR states: *"In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. (…)"*

[15] See Article 6 GDPR, notably paragraphs (1c) and (1e).

> [Example 4] A public school asks students for consent to use their photographs in a printed student magazine. Consent in these situations would be a genuine choice as long as students will not be denied education or services and could refuse the use of these photographs without any detriment.[16]

An imbalance of power also occurs in the **employment** context.[17] Given the dependency that results from the employer/employee relationship, it is unlikely that the data subject is able to deny his/her employer consent to data processing without experiencing the fear or real risk of detrimental effects as a result of a refusal. It is unlikely that an employee would be able to respond freely to a request for consent from his/her employer to, for example, activate monitoring systems such as camera-observation in a workplace, or to fill out assessment forms, without feeling any pressure to consent.[18] Therefore, WP29 deems it problematic for employers to process personal data of current or future employees on the basis of consent as it is unlikely to be freely given. For the majority of such data processing at work, the lawful basis cannot and should not be the consent of the employees (Article 6(1)(a)) due to the nature of the relationship between employer and employee.[19]

However this does not mean that employers can never rely on consent as a lawful basis for processing. There may be situations when it is possible for the employer to demonstrate that consent actually is freely given. Given the imbalance of power between an employer and its staff members, employees can only give free consent in exceptional circumstances, when it will have no adverse consequences at all whether or not they give consent.[20]

> [Example 5]
> A film crew is going to be filming in a certain part of an office. The employer asks all the employees who sit in that area for their consent to be filmed, as they may appear in the background of the video. Those who do not want to be filmed are not penalised in any way but instead are given equivalent desks elsewhere in the building for the duration of the filming.

Imbalances of power are not limited to public authorities and employers, they may also occur in other situations. As highlighted by WP29 in several Opinions, consent can only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences (e.g. substantial extra costs) if he/she does not consent. Consent will not be free in cases where there is any element of compulsion, pressure or inability to exercise free will.

3.1.2. Conditionality

[16] For the purposes of this example, a public school means a publically funded school or any educational facility that qualifies as a public authority or body by national law.

[17] See also Article 88 GDPR, where the need for protection of the specific interests of employees is emphasized and a possibility for derogations in Member State law is created. See also Recital 155.

[18] See Opinion 15/2011 on the definition of consent (WP 187), pp. 12-14 , Opinion 8/2001 on the processing of personal data in the employment context (WP 48), Chapter 10, Working document on the surveillance of electronic communications in the workplace (WP 55), paragraph 4.2 and Opinion 2/2017 on data processing at work (WP 249), paragraph 6.2.

[19] See Opinion 2/2017 on data processing at work, page 6-7

[20] See also Opinion 2/2017 on data processing at work (WP249), paragraph 6.2.

To assess whether consent is freely given, Article 7(4) GDPR plays an important role.[21]
Article 7(4) GDPR indicates that, inter alia, the situation of "bundling" consent with acceptance of terms or conditions, or "tying" the provision of a contract or a service to a request for consent to process personal data that are not necessary for the performance of that contract or service, is considered highly undesirable. If consent is given in this situation, it is presumed to be not freely given (recital 43). Article 7(4) seeks to ensure that the purpose of personal data processing is not disguised nor bundled with the provision of a contract of a service for which these personal data are not necessary. In doing so, the GDPR ensures that the processing of personal data for which consent is sought cannot become directly or indirectly the counter-performance of a contract. The two lawful bases for the lawful processing of personal data, i.e. consent and contract cannot be merged and blurred.

Compulsion to agree with the use of personal data additional to what is strictly necessary limits data subject's choices and stands in the way of free consent. As data protection law is aiming at the protection of fundamental rights, an individual's control over their personal data is essential and there is a strong presumption that consent to the processing of personal data that is unnecessary, cannot be seen as a mandatory consideration in exchange for the performance of a contract or the provision of a service.

Hence, whenever a request for consent is tied to the performance of a contract by the controller, a data subject that does not wish to make his/her personal data available for processing by the controller runs the risk to be denied services they have requested.

To assess whether such a situation of bundling or tying occurs, it is important to determine what the scope of the contract is and what data would be necessary for the performance of that contract.
According to Opinion 06/2014 of WP29, the term "necessary for the performance of a contract" needs to be interpreted strictly. The processing must be necessary to fulfil the contract with each individual data subject. This may include, for example, processing the address of the data subject so that goods purchased online can be delivered, or processing credit card details in order to facilitate payment. In the employment context, this ground may allow, for example, the processing of salary information and bank account details so that wages can be paid.[22] There needs to be a direct and objective link between the processing of the data and the purpose of the execution of the contract.

If a controller seeks to process personal data that are in fact necessary for the performance of a contract, then consent is not the appropriate lawful basis.[23]

[21] Article 7(4) GDPR: "*When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.*" See also Recital 43 GDPR, that states: "*[…] Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent, despite such consent not being necessary for such performance.*"
[22] For more information and examples, see Opinion 06/2014 on the notion of legitimate interest of the data controller under Article 7 of Directive 95/46/EC, adopted by WP29 on 9 April 2014, p. 16-17. (WP 217).
[23] The appropriate lawful basis could then be Article 6(1)(b) (contract).

Article 7(4) is only relevant where the requested data are **not** necessary for the performance of the contract, (including the provision of a service), and the performance of that contract is made conditional on the obtaining of these data on the basis of consent. Conversely, if processing **is** necessary to perform the contract (including to provide a service), then Article 7(4) does not apply.

> [Example 6]
> A bank asks customers for consent to allow third parties to use their payment details for direct marketing purposes. This processing activity is not necessary for the performance of the contract with the customer and the delivery of ordinary bank account services. If the customer's refusal to consent to this processing purpose would lead to the denial of banking services, closure of the bank account, or, depending on the case, an increase of the fee, consent cannot be freely given.

The choice of the legislator to highlight conditionality, amongst others, as a presumption of a lack of freedom to consent, demonstrates that the occurrence of conditionality must be carefully scrutinized. The term "utmost account" in Article 7(4) suggests that special caution is needed from the controller when a contract (which could include the provision of a service) has a request for consent to process personal data tied to it.

As the wording of Article 7(4) is not construed in an absolute manner, there might be very limited space for cases where this conditionality would not render the consent invalid. However, the word "presumed" in Recital 43 clearly indicates that such cases will be highly exceptional.

In any event, the burden of proof in Article 7(4) is on the controller.[24] This specific rule reflects the general principle of accountability which runs throughout the GDPR. However, when Article 7(4) applies, it will be more difficult for the controller to prove that consent was given freely by the data subject.[25]

The controller could argue that his organisation offers data subjects genuine choice if they were able to choose between a service that includes consenting to the use of personal data for additional purposes on the one hand, and an equivalent service offered by the same controller that does not involve consenting to data use for additional purposes on the other hand. As long as there is a possibility to have the contract performed or the contracted service delivered by this controller without consenting to the other or additional data use in question, this means there is no longer a conditional service. However, both services need to be genuinely equivalent.

The WP29 considers that consent cannot be considered as freely given if a controller argues that a choice exists between its service that includes consenting to the use of personal data for additional purposes on the one hand, and an equivalent service offered by a different controller on the other

[24] See also Article 7(1) GDPR, which states that the controller needs to demonstrate that the data subject's agreement was freely given.

[25] To some extent, the introduction of this paragraph is a codification of existing WP29 guidance. As described in Opinion 15/2011, when a data subject is in a situation of dependence on the data controller – due to the nature of the relationship or to special circumstances – there may be a strong presumption that freedom to consent is limited in such contexts (e.g. in an employment relationship or if the collection of data is performed by a public authority). With Article 7(4) in force, it will be more difficult for the controller to prove that consent was given freely by the data subject. See: Opinion 15/2011 on the definition of consent (WP 187), pp. 12-17.

hand. In such a case, the freedom of choice would be made dependant on what other market players do and whether an individual data subject would find the other controller’s services genuinely equivalent. It would furthermore imply an obligation for controllers to monitor market developments to ensure the continued validity of consent for their data processing activities, as a competitor may alter its service at a later stage. Hence, using this argument means this consent fails to comply with the GDPR.

3.1.3. Granularity

A service may involve multiple processing operations for more than one purpose. In such cases, the data subjects should be free to choose which purpose they accept, rather than having to consent to a bundle of processing purposes. In a given case, several consents may be warranted to start offering a service, pursuant to the GDPR.

Recital 43 clarifies that consent is presumed not to be freely given if the process/procedure for obtaining consent does not allow data subjects to give separate consent for personal data processing operations respectively (e.g. only for some processing operations and not for others) despite it being appropriate in the individual case. Recital 32 states “*Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them*”.

If the controller has conflated several purposes for processing and has not attempted to seek separate consent for each purpose, there is a lack of freedom. This granularity is closely related to the need of consent to be specific, as discussed in section 3.2 further below. When data processing is done in pursuit of several purposes, the solution to comply with the conditions for valid consent lies in granularity, i.e. the separation of these purposes and obtaining consent for each purpose.

> [Example 7]
> Within the same consent request a retailer asks its customers for consent to use their data to send them marketing by email and also to share their details with other companies within their group. This consent is not granular as there is no separate consents for these two separate purposes, therefore the consent will not be valid. In this case, a specific consent should be collected to send the contact details to commercial partners. Such specific consent will be deemed valid for each partner (see also section 3.3.1), whose identity has been provided to the data subject at the time of the collection of his or her consent, insofar as it is sent to them for the same purpose (in this example: a marketing purpose).

3.1.4. Detriment

The controller needs to demonstrate that it is possible to refuse or withdraw consent without detriment (recital 42). For example, the controller needs to prove that withdrawing consent does not lead to any costs for the data subject and thus no clear disadvantage for those withdrawing consent.

Other examples of detriment are deception, intimidation, coercion or significant negative consequences if a data subject does not consent. The controller should be able to prove that the data subject had a free or genuine choice about whether to consent and that it was possible to withdraw consent without detriment.

If a controller is able to show that a service includes the possibility to withdraw consent without any negative consequences e.g. without the performance of the service being downgraded to the detriment of the user, this may serve to show that the consent was given freely. The GDPR does not preclude all incentives but the onus would be on the controller to demonstrate that consent was still freely given in all the circumstances.

> [Example 8]
> When downloading a lifestyle mobile app, the app asks for consent to access the phone's accelerometer. This is not necessary for the app to work, but it is useful for the controller who wishes to learn more about the movements and activity levels of its users. When the user later revokes that consent, she finds out that the app now only works to a limited extent. This is an example of detriment as meant in Recital 42, which means that consent was never validly obtained (and thus, the controller needs to delete all personal data about users' movements collected this way).
>
> [Example 9]
> A data subject subscribes to a fashion retailer's newsletter with general discounts. The retailer asks the data subject for consent to collect more data on shopping preferences to tailor the offers to his or her preferences based on shopping history or a questionnaire that is voluntary to fill out. When the data subject later revokes consent, he or she will receive non-personalised fashion discounts again. This does not amount to detriment as only the permissible incentive was lost.
>
> [Example: 10]
> A fashion magazine offers readers access to buy new make-up products before the official launch.
> The products will shortly be made available for sale, but readers of this magazine are offered an exclusive preview of these products. In order to enjoy this benefit, people must give their postal address and agree to subscription on the mailing list of the magazine. The postal address is necessary for shipping and the mailing list is used for sending commercial offers for products such as cosmetics or t-shirts year round.
> The company explains that the data on the mailing list will only be used for sending merchandise and paper advertising by the magazine itself and is not to be shared with any other organisation.
> In case the reader does not want to disclose their address for this reason, there is no detriment, as the products will be available to them anyway.

3.2. Specific

Article 6(1)(a) confirms that the consent of the data subject must be given in relation to "one or more specific" purposes and that a data subject has a choice in relation to each of them.[26] The requirement that consent must be '*specific'* aims to ensure a degree of user control and transparency for the data subject. This requirement has not been changed by the GDPR and remains closely linked to the requirement of 'informed' consent. At the same time it must be interpreted in line with the requirement for 'granularity' to obtain 'free' consent.[27] In sum, to comply with the element of 'specific' the controller must apply:

(i) Purpose specification as a safeguard against function creep,

(ii) Granularity in consent requests, and

(iii) Clear separation of information related to obtaining consent for data processing activities from information about other matters.

[26] Further guidance on the determination of 'purposes' can be found in Opinion 3/2013 on purpose limitation (WP 203).

[27] Recital 43 GDPR states that separate consent for different processing operations will be needed wherever appropriate. Granular consent options should be provided to allow data subjects to consent separately to separate purposes.

Ad. (i): Pursuant to Article 5(1)(b) GDPR, obtaining valid consent is always preceded by the determination of a specific, explicit and legitimate purpose for the intended processing activity.[28] The need for specific consent in combination with the notion of purpose limitation in Article 5(1)(b) functions as a safeguard against the gradual widening or blurring of purposes for which data is processed, after a data subject has agreed to the initial collection of the data. This phenomenon, also known as function creep, is a risk for data subjects, as it may result in unanticipated use of personal data by the controller or by third parties and in loss of data subject control.

If the controller is relying on Article 6(1)(a), data subjects must always give consent for a specific processing purpose.[29] In line with the concept of *purpose limitation*, Article 5(1)(b) and recital 32, consent may cover different operations, as long as these operations serve the same purpose. It goes without saying that specific consent can only be obtained when data subjects are specifically informed about the intended purposes of data use concerning them.

Notwithstanding the provisions on compatibility of purposes, consent must be specific to the purpose. Data subjects will give their consent with the understanding that they are in control and their data will only be processed for those specified purposes. If a controller processes data based on consent and wishes to process the data for another purpose, too, that controller needs to seek additional consent for this other purpose unless there is another lawful basis which better reflects the situation.

> [Example 11] A cable TV network collects subscribers' personal data, based on their consent, to present them with personal suggestions for new movies they might be interested in based on their viewing habits. After a while, the TV network decides it would like to enable third parties to send (or display) targeted advertising on the basis of the subscriber's viewing habits. Given this new purpose, new consent is needed.

Ad. (ii): Consent mechanisms must not only be granular to meet the requirement of 'free', but also to meet the element of 'specific'. This means, a controller that seeks consent for various different purposes should provide a separate opt-in for each purpose, to allow users to give specific consent for specific purposes.

Ad. (iii): Lastly, controllers should provide specific information with each separate consent request about the data that are processed for each purpose, in order to make data subjects aware of the impact of the different choices they have. Thus, data subjects are enabled to give specific consent. This issue overlaps with the requirement that controllers must provide clear information, as discussed in paragraph 3.3. below.

3.3. Informed

The GDPR reinforces the requirement that consent must be informed. Based on Article 5 of the GDPR, the requirement for transparency is one of the fundamental principles, closely related to the

[28] See WP 29 Opinion 3/2013 on purpose limitation (WP 203), p. 16, : "*For these reasons, a purpose that is vague or general, such as for instance 'improving users' experience', 'marketing purposes', 'IT-security purposes' or 'future research' will - without more detail - usually not meet the criteria of being 'specific'.*"

[29] This is consistent with WP29 Opinion 15/2011 on the definition of consent (WP 187), for example on p. 17.

principles of fairness and lawfulness. Providing information to data subjects prior to obtaining their consent is essential in order to enable them to make informed decisions, understand what they are agreeing to, and for example exercise their right to withdraw their consent. If the controller does not provide accessible information, user control becomes illusory and consent will be an invalid basis for processing.

The consequence of not complying with the requirements for informed consent is that consent will be invalid and the controller may be in breach of Article 6 of the GDPR.

3.3.1. Minimum content requirements for consent to be 'informed'

For consent to be informed, it is necessary to inform the data subject of certain elements that are crucial to make a choice. Therefore, WP29 is of the opinion that at least the following information is required for obtaining valid consent:

(i) the controller's identity, [30]

(ii) the purpose of each of the processing operations for which consent is sought,[31]

(iii) what (type of) data will be collected and used, [32]

(iv) the existence of the right to withdraw consent,[33]

(v) information about the use of the data for automated decision-making in accordance with Article 22 (2)(c)[34] where relevant, and

(vi) on the possible risks of data transfers due to absence of an adequacy decision and of appropriate safeguards as described in Article 46.[35]

With regard to item (i) and (iii), WP29 notes that in a case where the consent sought is to be relied upon by multiple (joint) controllers or if the data is to be transferred to or processed by other controllers who wish to rely on the original consent, these organisations should all be named. Processors do not need to be named as part of the consent requirements, although to comply with Articles 13 and 14 of the GDPR, controllers will need to provide a full list of recipients or categories of recipients including processors. To conclude, WP29 notes that depending on the circumstances and context of a case, more information may be needed to allow the data subject to genuinely understand the processing operations at hand.

3.3.2. How to provide information

The GDPR does not prescribe the form or shape in which information must be provided in order to fulfil the requirement of informed consent. This means valid information may be presented in various ways, such as written or oral statements, or audio or video messages. However, the GDPR

[30] See also Recital 42 GDPR: " *[…]For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended.[…].*"

[31] Again, see Recital 42 GDPR

[32] See also WP29 Opinion 15/2011 on the definition of consent (WP 187) pp.19-20

[33] See Article 7(3) GDPR

[34] See also WP29 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251), paragraph IV.B, p. 20 onwards.

[35] Pursuant to Article 49 (1)(a), specific information is required about the absence of safeguards described in Article 46, when explicit consent is sought. See also WP29 Opinion 15/2011 on the definition of consent (WP 187)p. 19

puts several requirements for informed consent in place, predominantly in Article 7(2) and Recital 32. This leads to a higher standard for the clarity and accessibility of the information.

When seeking consent, controllers should ensure that they use clear and plain language in all cases. This means a message should be easily understandable for the average person and not only for lawyers. Controllers cannot use long privacy policies that are difficult to understand or statements full of legal jargon. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form. This requirement essentially means that information relevant for making informed decisions on whether or not to consent may not be hidden in general terms and conditions.[36]

A controller must ensure that consent is provided on the basis of information that allows the data subjects to easily identify who the controller is and to understand what they are agreeing to. The controller must clearly describe the purpose for data processing for which consent is requested.[37]

Other specific guidance on the accessibility has been provided in the WP29 guidelines on transparency. If consent is to be given by electronic means, the request must be clear and concise. Layered and granular information can be an appropriate way to deal with the two-fold obligation of being precise and complete on the one hand and understandable on the other hand.

A controller must assess what kind of audience it is that provides personal data to their organisation. For example, in case the targeted audience includes data subjects that are underage, the controller is expected to make sure information is understandable for minors.[38] After identifying their audience, controllers must determine what information they should provide and, subsequently how they will present the information to data subjects.

Article 7(2) addresses pre-formulated written declarations of consent which also concern other matters. When consent is requested as part of a (paper) contract, the request for consent should be clearly distinguishable from the other matters. If the paper contract includes many aspects that are unrelated to the question of consent to the use of personal data, the issue of consent should be dealt with in a way that clearly stands out, or in a separate document. Likewise, if consent is requested by electronic means, the consent request has to be separate and distinct, it cannot simply be a paragraph within terms and conditions, pursuant to Recital 32.[39] To accommodate for small screens or situations with restricted room for information, a layered way of presenting information can be considered, where appropriate, to avoid excessive disturbance of user experience or product design.

[36] The declaration of consent must be named as such. Drafting, such as “I know that…” does not meet the requirement of clear language.

[37] See Articles 4(11) and 7(2) GDPR.

[38] See also Recital 58 regarding information understandable for children.

[39] See also Recital 42 and Directive 93/13/EC, notably Article 5 (plain intelligible language and in case of doubt, the interpretation will be in favour of consumer) and Article 6 (invalidity of unfair terms, contract continues to exist without these terms only if still sensible, otherwise the whole contract is invalid).

A controller that relies on consent of the data subject must also deal with the separate information duties laid down in Articles 13 and 14 in order to be compliant with the GDPR. In practice, compliance with the information duties and compliance with the requirement of informed consent may lead to an integrated approach in many cases. However, this section is written in the understanding that valid "informed" consent can exist, even when not all elements of Articles 13 and/or 14 are mentioned in the process of obtaining consent (these points should of course be mentioned in other places, such as the privacy notice of a company). WP29 has issued separate guidelines on the requirement of transparency.

> [Example 12]
> Company X is a controller that received complaints that it is unclear to data subjects for what purposes of data use they are asked to consent to. The company sees the need to verify whether its information in the consent request is understandable for data subjects. X organises voluntary test panels of specific categories of its customers and presents new updates of its consent information to these test audiences before communicating it externally. The selection of the panel respects the principle of independence and is made on the basis of standards ensuring a representative, non-biased outcome. The panel receives a questionnaire and indicates what they understood of the information and how they would score it in terms of understandable and relevant information. The controller continues testing until the panels indicate that the information is understandable. X draws up a report of the test and keeps this available for future reference. This example shows a possible way for X to demonstrate that data subjects were receiving clear information before consenting to personal data processing by X.

> [Example 13]
> A company engages in data processing on the basis of consent. The company uses a layered privacy notice that includes a consent request. The company discloses all basic details of the controller and the data processing activities envisaged.[40] However, the company does not indicate how their data protection officer can be contacted in the first information layer of the notice. For the purposes of having a valid lawful basis as meant in Article 6, this controller obtained valid "informed" consent, even when the contact details of the data protection officer have not been communicated to the data subject (in the first information layer), pursuant to Article 13(1)(b) or 14(1)(b) GDPR.

3.4. Unambiguous indication of wishes

The GDPR is clear that consent requires a statement from the data subject or a clear affirmative act which means that it must always be given through an active motion or declaration. It must be obvious that the data subject has consented to the particular processing.

Article 2(h) of Directive 95/46/EC described consent as an "indication of wishes by which the data subject signifies his agreement to personal data relating to him being processed". Article 4(11) GDPR builds on this definition, by clarifying that valid consent requires an *unambiguous* indication by means of a *statement or by a clear affirmative action,* in line with previous guidance issued by the WP29.

[40] Note that when the identity of the controller or the purpose of the processing is not apparent from the first information layer of the layered privacy notice (and are located in further sub-layers), it will be difficult for the data controller to demonstrate that the data subject has given informed consent, unless the data controller can show that the data subject in question accessed that information prior to giving consent.

A “clear affirmative act” means that the data subject must have taken a deliberate action to consent to the particular processing.[41] Recital 32 sets out additional guidance on this. Consent can be collected through a written or (a recorded) oral statement, including by electronic means.

Perhaps the most literal way to fulfil the criterion of a “written statement” is to make sure a data subject writes in a letter or types an email to the controller explaining what exactly he/she agrees to. However, this is often not realistic. Written statements can come in many shapes and sizes that could be compliant with the GDPR.

Without prejudice to existing (national) contract law, consent can be obtained through a recorded oral statement, although due note must be taken of the information available to the data subject, prior to the indication of consent. The use of pre-ticked opt-in boxes is invalid under the GDPR. Silence or inactivity on the part of the data subject, as well as merely proceeding with a service cannot be regarded as an active indication of choice.

> [Example 14]
> When installing software, the application asks the data subject for consent to use non-anonymised crash reports to improve the software. A layered privacy notice providing the necessary information accompanies the request for consent. By actively ticking the optional box stating, “I consent”, the user is able to validly perform a ´clear affirmative act´ to consent to the processing.

A controller must also beware that consent cannot be obtained through the same motion as agreeing to a contract or accepting general terms and conditions of a service. Blanket acceptance of general terms and conditions cannot be seen as a clear affirmative action to consent to the use of personal data. The GDPR does not allow controllers to offer pre-ticked boxes or opt-out constructions that require an intervention from the data subject to prevent agreement (for example ‘opt-out boxes’).[42]

When consent is to be given following a request by electronic means, the request for consent should not be *unnecessarily* disruptive to the use of the service for which the consent is provided.[43] An active affirmative motion by which the data subject indicates consent can be necessary when a less infringing or disturbing modus would result in ambiguity. Thus, it may be necessary that a consent request interrupts the use experience to some extent to make that request effective.

[41] See Commission Staff Working Paper, Impact Assessment, Annex 2, p. 20 and also pp. 105-106: “*As also pointed out in the opinion adopted by WP29 on consent, it seems essential to clarify that valid consent requires the use of mechanisms that leave no doubt of the data subject’s intention to consent, while making clear that – in the context of the on-line environment – the use of default options which the data subject is required to modify in order to reject the processing ('consent based on silence') does not in itself constitute unambiguous consent. This would give individuals more control over their own data, whenever processing is based on his/her consent. As regards impact on data controllers, this would not have a major impact as it solely clarifies and better spells out the implications of the current Directive in relation to the conditions for a valid and meaningful consent from the data subject. In particular, to the extent that 'explicit' consent would clarify – by replacing "unambiguous" – the modalities and quality of consent and that it is not intended to extend the cases and situations where (explicit) consent should be used as a ground for processing, the impact of this measure on data controllers is not expected to be major.*”

[42] See Article 7(2). See also Working Document 02/2013 on obtaining consent for cookies (WP 208), pp. 3-6.

[43] See Recital 32 GDPR.

However, within the requirements of the GDPR, controllers have the liberty to develop a consent flow that suits their organisation. In this regard, physical motions can be qualified as a clear affirmative action in compliance with the GDPR.

Controllers should design consent mechanisms in ways that are clear to data subjects. Controllers must avoid ambiguity and must ensure that the action by which consent is given can be distinguished from other actions. Therefore, merely continuing the ordinary use of a website is not conduct from which one can infer an indication of wishes by the data subject to signify his or her agreement to a proposed processing operation.

> **[**Example 15]
> Swiping a bar on a screen, waiving in front of a smart camera, turning a smartphone around clockwise, or in a figure eight motion may be options to indicate agreement, as long as clear information is provided, and it is clear that the motion in question signifies agreement to a specific request (e.g. if you swipe this bar to the left, you agree to the use of information X for purpose Y. Repeat the motion to confirm). The controller must be able to demonstrate that consent was obtained this way and data subjects must be able to withdraw consent as easily as it was given.

> [Example 16]
> Scrolling down or swiping through a website will not satisfy the requirement of a clear and affirmative action. This is because the alert that continuing to scroll will constitute consent may be difficult to distinguish and/or may be missed when a data subject is quickly scrolling through large amounts of text and such an action is not sufficiently unambiguous.

In the digital context, many services need personal data to function, hence, data subjects receive multiple consent requests that need answers through clicks and swipes every day. This may result in a certain degree of click fatigue: when encountered too many times, the actual warning effect of consent mechanisms is diminishing.

This results in a situation where consent questions are no longer read. This is a particular risk to data subjects, as, typically, consent is asked for actions that are in principle unlawful without their consent. The GDPR places upon controllers the obligation to develop ways to tackle this issue.

An often-mentioned example to do this in the online context is to obtain consent of Internet users via their browser settings. Such settings should be developed in line with the conditions for valid consent in the GDPR, as for instance that the consent shall be granular for each of the envisaged purposes and that the information to be provided, should name the controllers.

In any event, consent must always be obtained before the controller starts processing personal data for which consent is needed. WP29 has consistently held in previous opinions that consent should be given prior to the processing activity.[44] Although the GDPR does not literally prescribe in Article 4(11) that consent must be given prior to the processing activity, this is clearly implied. The heading of Article 6(1) and the wording "has given" in Article 6(1)(a) support this interpretation. It follows logically from Article 6 and Recital 40 that a valid lawful basis must be present before

[44] WP29 has consistently held this position since Opinion 15/2011 on the definition of consent (WP 187), pp. 30-31.

starting a data processing. Therefore, consent should be given prior to the processing activity. In principle, it can be sufficient to ask for a data subject's consent once. However, controllers do need to obtain a new and specific consent if purposes for data processing change after consent was obtained or if an additional purpose is envisaged.

4. Obtaining explicit consent

Explicit consent is required in certain situations where serious data protection risk emerge, hence, where a high level of individual control over personal data is deemed appropriate. Under the GDPR, explicit consent plays a role in Article 9 on the processing of special categories of data, the provisions on data transfers to third countries or international organisations in the absence of adequate safeguards in Article 49[45], and in Article 22 on automated individual decision-making, including profiling.[46]

The GDPR prescribes that a "statement or clear affirmative action" is a prerequisite for 'regular' consent. As the 'regular' consent requirement in the GDPR is already raised to a higher standard compared to the consent requirement in Directive 95/46/EC, it needs to be clarified what extra efforts a controller should undertake in order to obtain the *explicit* consent of a data subject in line with the GDPR.

The term *explicit* refers to the way consent is expressed by the data subject. It means that the data subject must give an express statement of consent. An obvious way to make sure consent is explicit would be to expressly confirm consent in a written statement. Where appropriate, the controller could make sure the written statement is signed by the data subject, in order to remove all possible doubt and potential lack of evidence in the future.[47]

However, such a signed statement is not the only way to obtain explicit consent and, it cannot be said that the GDPR prescribes written and signed statements in all circumstances that require valid explicit consent. For example, in the digital or online context, a data subject may be able to issue the required statement by filling in an electronic form, by sending an email, by uploading a scanned document carrying the signature of the data subject, or by using an electronic signature. In theory, the use of oral statements can also be sufficiently express to obtain valid explicit consent, however, it may be difficult to prove for the controller that all conditions for valid explicit consent were met when the statement was recorded.

[45] According to Article 49 (1)(a) GDPR, explicit consent can lift the ban on data transfers to countries without adequate levels of data protection law. Also note Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995 (WP 114), p. 11, where WP29 has indicated that consent for data transfers that occur periodically or on an on-going basis is inappropriate.

[46] In Article 22, the GDPR introduces provisions to protect data subjects against decision-making based solely on automated processing, including profiling. Decisions made on this basis are allowed under certain legal conditions. Consent plays a key role in this protection mechanism, as Article 22(2)(c) GDPR makes clear that a controller may proceed with automated decision making, including profiling, that may significantly affect the individual, with the data subject's explicit consent. WP29 have produced separate guidelines on this issue: WP29 Guidelines on Automated decision-making and Profiling for the purposes of Regulation 2016/679, 3 October 2017 (WP 251).

[47] See also WP29 Opinion 15/2011, on the definition of consent (WP 187), p. 25.

An organisation may also obtain explicit consent through a telephone conversation, provided that the information about the choice is fair, intelligible and clear, and it asks for a specific confirmation from the data subject (e.g. pressing a button or providing oral confirmation).

> [Example 17] A data controller may also obtain explicit consent from a visitor to its website by offering an explicit consent screen that contains Yes and No check boxes, provided that the text clearly indicates the consent, for instance "I, hereby, consent to the processing of my data", and not for instance, "It is clear to me that my data will be processed". It goes without saying that the conditions for informed consent as well as the other conditions for obtaining valid consent should be met.

> [Example 18] A clinic for cosmetic surgery seeks explicit consent from a patient to transfer his medical record to an expert whose second opinion is asked on the condition of the patient. The medical record is a digital file. Given the specific nature of the information concerned, the clinic asks for an electronic signature of the data subject to obtain valid explicit consent and to be able to demonstrate that explicit consent was obtained.[48]

Two stage verification of consent can also be a way to make sure explicit consent is valid. For example, a data subject receives an email notifying them of the controller's intent to process a record containing medical data. The controller explains in the email that he asks for consent for the use of a specific set of information for a specific purpose. If the data subjects agrees to the use of this data, the controller asks him or her for an email reply containing the statement 'I agree'. After the reply is sent, the data subject receives a verification link that must be clicked, or an SMS message with a verification code, to confirm agreement.

Article 9(2) does not recognize "necessary for the performance of a contract" as an exception to the general prohibition to process special categories of data. Therefore controllers and Member States that deal with this situation should explore the specific exceptions in Article 9(2) subparagraphs (b) to (j). Should none of the exceptions (b) to (j) apply, obtaining explicit consent in accordance with the conditions for valid consent in the GDPR remains the only possible lawful exception to process such data.

> [Example 19]
> An airline company, Holiday Airways, offers an assisted travelling service for passengers that cannot travel unassisted, for example due to a disability. A customer books a flight from Amsterdam to Budapest and requests travel assistance to be able to board the plane. Holiday Airways requires her to provide information on her health condition to be able to arrange the appropriate services for her (hence, there are many possibilities e.g. wheelchair on the arrival gate, or an assistant travelling with her from A to B.) Holiday Airways asks for explicit consent to process the health data of this customer for the purpose of arranging the requested travel assistance. -The data processed on the basis of consent should be necessary for the requested service. Moreover, flights to Budapest remain available without travel assistance. Please note that since that data are necessary for the provision of the requested service, Article 7 (4) does not apply.

> [Example 20]
> A successful company is specialised in providing custom-made ski- and snowboard goggles, and other types of customised eyewear for outdoors sports. The idea is that people could wear these without their own glasses on. The company receives orders at a central point and delivers products from a single location all across the EU.

[48] This example is without prejudice to EU Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.

> In order to be able to provide its customised products to customers who are short-sighted, this controller requests consent for the use of information on customers' eye condition. Customers provide the necessary health data, such as their prescription data online when they place their order. Without this, it is not possible to provide the requested customized eyewear. The company also offers series of goggles with standardized correctional values. Customers that do not wish to share health data could opt for the standard versions. Therefore, an explicit consent under Article 9 is required and consent can be considered to be freely given.

5. Additional conditions for obtaining valid consent

The GDPR introduces requirements for controllers to make additional arrangements to ensure they obtain, and maintain and are able to demonstrate, valid consent. Article 7 of the GDPR sets out these additional conditions for valid consent, with specific provisions on keeping records of consent and the right to easily withdraw consent. Article 7 also applies to consent referred to in other articles of GDPR, e.g. Articles 8 and 9. Guidance on the additional requirement to demonstrate valid consent and on withdrawal of consent is provided below.

5.1.Demonstrate consent

In Article 7(1), the GDPR clearly outlines the explicit obligation of the controller to demonstrate a data subject's consent. The burden of proof will be on the controller, according to Article 7(1).

Recital 42 states: *"Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation."*

Controllers are free to develop methods to comply with this provision in a way that is fitting in their daily operations. At the same time, the duty to demonstrate that valid consent has been obtained by a controller, should not in itself lead to excessive amounts of additional data processing. This means that controllers should have enough data to show a link to the processing (to show consent was obtained) but they shouldn't be collecting any more information than necessary.

It is up to the controller to prove that valid consent was obtained from the data subject. The GDPR does not prescribe exactly how this must be done. However, the controller must be able to prove that a data subject in a given case has consented. As long as a data processing activity in question lasts, the obligation to demonstrate consent exists. After the processing activity ends, proof of consent should be kept no longer then strictly necessary for compliance with a legal obligation or for the establishment, exercise or defence of legal claims, in accordance with Article 17(3)(b) and (e).

For instance, the controller may keep a record of consent statements received, so he can show how consent was obtained, when consent was obtained and the information provided to the data subject at the time shall be demonstrable. The controller shall also be able to show that the data subject was informed and the controller´s workflow met all relevant criteria for a valid consent. The rationale behind this obligation in the GDPR is that controllers must be accountable with regard to obtaining valid consent from data subjects and the consent mechanisms they have put in place. For example, in an online context, a controller could retain information on the session in which consent was expressed, together with documentation of the consent workflow at the time of the session, and a copy of the information that was presented to the data subject at that time. It would not be sufficient to merely refer to a correct configuration of the respective website.

> [Example 21] A hospital sets up a scientific research programme, called project X, for which dental records of real patients are necessary. Participants are recruited via telephone calls to patients that voluntarily agreed to be on a list of candidates that may be approached for this purpose. The controller seeks explicit consent from the data subjects for the use of their dental record. Consent is obtained during a phone call by recording an oral statement of the data subject in which the data subject confirms that they agree to the use of their data for the purposes of project X.

There is no specific time limit in the GDPR for how long consent will last. How long consent lasts will depend on the context, the scope of the original consent and the expectations of the data subject. If the processing operations change or evolve considerably then the original consent is no longer valid. If this is the case, then new consent needs to be obtained.

WP29 recommends as a best practice that consent should be refreshed at appropriate intervals. Providing all the information again helps to ensure the data subject remains well informed about how their data is being used and how to exercise their rights.[49]

5.2. Withdrawal of consent

Withdrawal of consent is given a prominent place in the GDPR. The provisions and recitals on withdrawal of consent in the GDPR can be regarded as codification of the existing interpretation of this matter in WP29 Opinions.[50]

Article 7(3) of the GDPR prescribes that the controller must ensure that consent can be withdrawn by the data subject as easy as giving consent and at any given time. The GDPR does not say that giving and withdrawing consent must always be done through the same action.

However, when consent is obtained via electronic means through only one mouse-click, swipe, or keystroke, data subjects must, in practice, be able to withdraw that consent equally as easily. Where consent is obtained through use of a service-specific user interface (for example, via a website, an app, a log-on account, the interface of an IoT device or by e-mail), there is no doubt a data subject must be able to withdraw consent via the same electronic interface, as switching to another interface for the sole reason of withdrawing consent would require undue effort. Furthermore, the data subject should be able to withdraw his/her consent without detriment. This means, inter alia, that a controller must make withdrawal of consent possible free of charge or without lowering service levels.[51]

[49] See WP29 guidelines on transparency. [Citation to be finalized when available]

[50] WP29 has discussed this subject in their Opinion on consent (see Opinion 15/2011 on the definition of consent (WP 187), pp. 9, 13, 20, 27 and 32-33) and, inter alia, their Opinion on the use of location data. (see Opinion 5/2005 on the use of location data with a view to providing value-added services (WP 115), p. 7).

[51] See also opinion WP29 Opinion 4/2010 on the European code of conduct of FEDMA for the use of personal data in direct marketing (WP 174) and the Opinion on the use of location data with a view to providing value-added services (WP 115).

> [Example 22] A music festival sells tickets through an online ticket agent. With each online ticket sale, consent is requested in order to use contact details for marketing purposes. To indicate consent for this purpose, customers can select either No or Yes. The controller informs customers that they have the possibility to withdraw consent. To do this, they could contact a call centre on business days between 8am and 5pm, free of charge. The controller in this example does not comply with article 7(3) of the GDPR. Withdrawing consent in this case requires a telephone call during business hours, this is more burdensome than the one mouse-click needed for giving consent through the online ticket vendor, which is open 24/7.

The requirement of an easy withdrawal is described as a necessary aspect of valid consent in the GDPR. If the withdrawal right does not meet the GDPR requirements, then the consent mechanism of the controller does not comply with the GDPR. As mentioned in section 3.1 on the condition of *informed* consent, the controller must inform the data subject of the right to withdraw consent prior to actually giving consent, pursuant to Article 7(3) of the GDPR. Additionally, the controller must as part of the transparency obligation inform the data subjects on how to exercise their rights.[52]

As a general rule, if consent is withdrawn, all data processing operations that were based on consent and took place before the withdrawal of consent - and in accordance with the GDPR - remain lawful, however, the controller must stop the processing actions concerned. If there is no other lawful basis justifying the processing (e.g. further storage) of the data, they should be deleted by the controller.[53]

As mentioned earlier in these guidelines, it is very important that controllers assess the purposes for which data is actually processed and the lawful grounds on which it is based prior to collecting the data. Often companies need personal data for several purposes, and the processing is based on more than one lawful basis, e.g. customer data may be based on contract and consent. Hence, a withdrawal of consent does not mean a controller must erase data that are processed for a purpose that is based on the performance of the contract with the data subject. Controllers should therefore be clear from the outset about which purpose applies to each element of data and which lawful basis is being relied upon.

Controllers have an obligation to delete data that was processed on the basis of consent once that consent is withdrawn, assuming that there is no other purpose justifying the continued retention.[54] Besides this situation, covered in Article 17 (1)(b), an individual data subject may request erasure of other data concerning him that is processed on another lawful basis, e.g. on the basis of Article 6(1)(b).[55] Controllers are obliged to assess whether continued processing of the data in question is appropriate, even in the absence of an erasure request by the data subject.[56]

[52] Recital 39 GDPR, which refers to Articles 13 and 14 of that Regulation, states that *"natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing.*

[53] See Article 17(1)(b) and (3) GDPR.

[54] In that case, the other purpose justifying the processing must have its own separate legal basis. This does not mean the controller can swap from consent to another lawful basis, see section 6 below.

[55] See Article 17, including exceptions that may apply, and Recital 65 GDPR

[56] See also Article 5 (1)(e) GDPR

In cases where the data subject withdraws his/her consent and the controller wishes to continue to process the personal data on another lawful basis, they cannot silently migrate from consent (which is withdrawn) to this other lawful basis. Any change in the lawful basis for processing must be notified to a data subject in accordance with the information requirements in Articles 13 and 14 and under the general principle of transparency.

6. Interaction between consent and other lawful grounds in Article 6 GDPR

Article 6 sets the conditions for a lawful personal data processing and describes six lawful bases on which a controller can rely. The application of one of these six bases must be established prior to the processing activity and in relation to a specific purpose.[57]

It is important to note here that if a controller chooses to rely on consent for any part of the processing, they must be prepared to respect that choice and stop that part of the processing if an individual withdraws consent. Sending out the message that data will be processed on the basis of consent, while actually some other lawful basis is relied on, would be fundamentally unfair to individuals.

In other words, the controller cannot swap from consent to other lawful bases. For example, it is not allowed to retrospectively utilise the legitimate interest basis in order to justify processing, where problems have been encountered with the validity of consent. Because of the requirement to disclose the lawful basis which the controller is relying upon at the time of collection of personal data, controllers must have decided in advance of collection what the applicable lawful basis is.

7. Specific areas of concern in the GDPR

7.1.Children (Article 8)

Compared to the current directive, the GDPR creates an additional layer of protection where personal data of vulnerable natural persons, especially children, are processed. Article 8 introduces additional obligations to ensure an enhanced level of data protection of children in relation to information society services. The reasons for the enhanced protection are specified in Recital 38: “ *[...] they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data [...]”* Recital 38 also states that “*Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child.”* The words ‘in particular’ indicate that the specific protection is not confined to marketing or profiling but includes the wider ‘collection of personal data with regard to children’.

Article 8(1) states that where consent applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful

[57] Pursuant to Articles 13 (1)(c) and/or 14(1)(c), the controller must inform the data subject thereof.

only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.[58] Regarding the age limit of valid consent the GDPR provides flexibility, Member States can provide by law a lower age, but this age cannot be below 13 years.

As mentioned in section 3.1. on informed consent, the information shall be understandable to the audience addressed by the controller, paying particular attention to the position of children. In order to obtain "informed consent" from a child, the controller must explain in language that is clear and plain for children how it intends to process the data it collects.[59] If it is the parent that is supposed to consent, then a set of information may be required that allows adults to make an informed decision.

It is clear from the foregoing that Article 8 shall only apply when the following conditions are met:

- The processing is related to the offer of information society services directly to a child.[60, 61]
- The processing is based on consent.

7.1.1. Information society service

To determine the scope of the term 'information society service" in the GDPR, reference is made in Article 4(25) GDPR to Directive 2015/1535.

While assessing the scope of this definition, WP29 also refers to case law of the ECJ.[62] The ECJ held that *information society services* cover contracts and other services that are concluded or transmitted on-line. Where a service has two economically independent components, one being the online component, such as the offer and the acceptance of an offer in the context of the conclusion of a contract or the information relating to products or services, including marketing activities, this component is defined as an information society service, the other component being the physical delivery or distribution of goods is not covered by the notion of an information society service. The online delivery of a service would fall within the scope of the term *information society service* in Article 8 GDPR.

[58] Without prejudice to the possibility of Member State law to derogate from the age limit, see Article 8(1).

[59] Recital 58 GDPR re-affirms this obligation, in stating that, where appropriate, a controller should make sure the information provided is understandable for children.

[60] According to Article 4(25) GDPR an information society service means a service as defined in point (b) of Article 1(1) of Directive 2015/1535: *"(b) 'service' means any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. For the purposes of this definition: (i) 'at a distance' means that the service is provided without the parties being simultaneously present; (ii) 'by electronic means' means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means; (iii) 'at the individual request of a recipient of services' means that the service is provided through the transmission of data on individual request."* An indicative list of services not covered by this definition is set out in Annex I of the said Directive. See also Recital 18 of Directive 2000/31.

[61] According to the UN Convention on the Protection of the Child, Article 1, *"[…] a child means every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier,"* see United Nations, General Assembly Resolution 44/25 of 20 November 1989 (Convention on the Rights of the Child).

[62] See European Court of Justice, 2 December 2010 Case C-108/09, (*Ker-Optika)*, paragraphs 22 and 28. In relation to 'composite services', WP29 also refers to Case C-434/15 *(Asociacion Profesional Elite Taxi v Uber Systems Spain SL),* para 40, which states that an information society service forming an integral part of an overall service whose main component is not an information society service (in this case a transport service), must not be qualified as 'an information society service'.

7.1.2. Offered directly to a child

The inclusion of the wording 'offered directly to a child' indicates that Article 8 is intended to apply to some, not all information society services. In this respect, if an information society service provider makes it clear to potential users that it is only offering its service to persons aged 18 or over, and this is not undermined by other evidence (such as the content of the site or marketing plans) then the service will not be considered to be 'offered directly to a child' and Article 8 will not apply.

7.1.3. Age

The GDPR specifies that *"Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years."* The controller must be aware of those different national laws, by taking into account the public targeted by its services. In particular it should be noted that a controller providing a cross-border service cannot always rely on complying with only the law of the Member State in which it has its main establishment but may need to comply with the respective national laws of each Member State in which it offers the information society service(s). This depends on whether a Member State chooses to use the place of main establishment of the controller as a point of reference in its national law, or the residence of the data subject. First of all the Member States shall consider the best interests of the child during making their choice. The Working Group encourages the Member States to search for a harmonized solution in this matter.

When providing information society services to children on the basis of consent, controllers will be expected to make reasonable efforts to verify that the user is over the age of digital consent, and these measures should be proportionate to the nature and risks of the processing activities.

If the users state that they are over the age of digital consent then the controller can carry out appropriate checks to verify that this statement is true. Although the need to undertake reasonable efforts to verify age is not explicit in the GDPR it is implicitly required, for if a child gives consent while not old enough to provide valid consent on their own behalf, then this will render the processing of data unlawful.

If the user states that he/she is below the age of digital consent then the controller can accept this statement without further checks, but will need to go on to obtain parental authorisation and verify that the person providing that consent is a holder of parental responsibility.

Age verification should not lead to excessive data processing. The mechanism chosen to verify the age of a data subject should involve an assessment of the risk of the proposed processing. In some low-risk situations, it may be appropriate to require a new subscriber to a service to disclose their year of birth or to fill out a form stating they are (not) a minor.[63] If doubts arise the controller

[63] Although this may not be a watertight solution in all cases, it is an example to deal with this provision

should review their age verification mechanisms in a given case and consider whether alternative checks are required.[64]

7.1.4. Children’s consent and parental responsibility

Regarding the authorisation of a holder of parental responsibility, the GDPR does not specify practical ways to gather the parent’s consent or to establish that someone is entitled to perform this action.[65] Therefore, the WP29 recommends the adoption of a proportionate approach, in line with Article 8(2) GDPR and Article 5(1)(c) GDPR (data minimisation). A proportionate approach may be to focus on obtaining a limited amount of information, such as contact details of a parent or guardian.

What is reasonable, both in terms of verifying that a user is old enough to provide their own consent, and in terms of verifying that a person providing consent on behalf of a child is a holder of parental responsibility, may depend upon the risks inherent in the processing as well as the available technology. In low-risk cases, verification of parental responsibility via email may be sufficient. Conversely, in high-risk cases, it may be appropriate to ask for more proof, so that the controller is able to verify and retain the information pursuant to Article 7(1) GDPR.[66] Trusted third party verification services may offer solutions which minimise the amount of personal data the controller has to process itself.

> [Example 23] An online gaming platform wants to make sure underage customers only subscribe to its services with the consent of their parents or guardians. The controller follows these steps:
> Step 1: ask the user to state whether they are under or over the age of 16 (or alternative age of digital consent)
> If the user states that they are under the age of digital consent:
> Step 2: service informs the child that a parent or guardian needs to consent or authorise the processing before the service is provided to the child. The user is requested to disclose the email address of a parent or guardian.
> Step 3: service contacts the parent or guardian and obtains their consent via email for processing and take reasonable steps to confirm that the adult has parental responsibility.
> Step 4: in case of complaints, the platform takes additional steps to verify the age of the subscriber.
> If the platform has met the other consent requirements, the platform can comply with the additional criteria of Article 8 GDPR by following these steps.

The example shows that the controller can put itself in a position to show that reasonable efforts have been made to ensure that valid consent has been obtained, in relation to the services provided to a child. Article 8(2) particularly adds that “*The controller shall make reasonable efforts to verify that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.*”

[64] See WP29 Opinion 5/2009 on social networking services (WP 163).

[65] WP 29 notes that it not always the case that the holder of parental responsibility is the natural parent of the child and that parental responsibility can be held by multiple parties which may include legal as well as natural persons.

[66] For example, a parent or guardian could be asked to make a payment of €0,01 to the controller via a bank transaction, including a brief confirmation in the description line of the transaction that the bank account holder is a holder of parental responsibility over the user. Where appropriate, an alternative method of verification should be provided to prevent undue discriminatory treatment of persons that do not have a bank account.

It is up to the controller to determine what measures are appropriate in a specific case. As a general rule, controllers should avoid verification solutions which themselves involve excessive collection of personal data.

WP29 acknowledges that there may be cases where verification is challenging (for example where children providing their own consent have not yet established an 'identity footprint', or where parental responsibility is not easily checked. This can be taken into account when deciding what efforts are reasonable, but controllers will also be expected to keep their processes and the available technology under constant review.

With regard to the data subject's autonomy to consent to the processing of their personal data and have full control over the processing, consent by a holder of parental responsibility or authorized by a holder of parental responsibility for the processing of personal data of children can be confirmed, modified or withdrawn, once the data subject reaches the age of digital consent.

In practice, this means that if the child does not take any action, consent given by a holder of parental responsibility or authorized by a holder of parental responsibility for the processing of personal data given prior to the age of digital consent, will remain a valid ground for processing.

After reaching the age of digital consent, the child will have the possibility to withdraw the consent himself, in line with Article 7(3). In accordance with the principles of fairness and accountability, the controller must inform the child about this possibility.[67]

It is important to point out that in accordance with Recital 38, consent by a parent or guardian is not required in the context of preventive or counselling services offered directly to a child. For example the provision of child protection services offered online to a child by means of an online chat service do not require prior parental authorisation.

Finally, the GDPR states that the rules concerning parental authorization requirements vis-à-vis minors shall not interfere with "the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child". Therefore, the requirements for valid consent for the use of data about children are part of a legal framework that must be regarded as separate from national contract law. Therefore, this guidance paper does not deal with the question whether it is lawful for a minor to conclude online contracts. Both legal regimes may apply simultaneously, and, the scope of the GDPR does not include harmonization of national provisions of contract law.

7.2. Scientific research

The definition of scientific research purposes has substantial ramifications for the range of data processing activities a controller may undertake. The term *'scientific research'* is not defined in the GDPR. Recital 159 states "(…) *For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner.* (…)", however the WP29

[67] Also, data subjects should be aware of the right to be forgotten as laid down in Article 17, which is in particular relevant for consent given when the data subject was still a child, see recital 63.

considers the notion may not be stretched beyond its common meaning and understands that '*scientific research'* in this context means a research project set up in accordance with relevant sector-related methodological and ethical standards, in conformity with good practice.

When consent is the legal basis for conducting research in accordance with the GDPR, this consent for the use of personal data should be distinguished from other consent requirements that serve as an ethical standard or procedural obligation. An example of such a procedural obligation, where the processing is based not on consent but on another legal basis, is to be found in the Clinical Trials Regulation. In the context of data protection law, the latter form of consent could be considered as an additional safeguard.[68] At the same time, the GDPR does not restrict the application of Article 6 to consent alone, with regard to processing data for research purposes. As long as appropriate safeguards are in place, such as the requirements under Article 89(1), and the processing is fair, lawful, transparent and accords with data minimisation standards and individual rights, other lawful bases such as Article 6(1)(e) or (f) may be available.[69] This also applies to special categories of data pursuant to the derogation of Article 9(2)(j).[70]

Recital 33 seems to bring some flexibility to the degree of specification and granularity of consent in the context of scientific research. Recital 33 states: "*It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose*."

First, it should be noted that Recital 33 does not disapply the obligations with regard to the requirement of specific consent. This means that, in principle, scientific research projects can only include personal data on the basis of consent if they have a well-described purpose. For the cases where purposes for data processing within a scientific research project cannot be specified at the outset, Recital 33 allows as an exception that the purpose may be described at a more general level.

Considering the strict conditions stated by Article 9 GDPR regarding the processing of special categories of data, WP29 notes that when special categories of data are processed on the basis of explicit consent, applying the flexible approach of Recital 33 will be subject to a stricter interpretation and requires a high degree of scrutiny.

When regarded as a whole, the GDPR cannot be interpreted to allow for a controller to navigate around the key principle of specifying purposes for which consent of the data subject is asked.

[68] See also Recital 161 of the GDPR.

[69] Article 6(1)(c) may also be applicable for parts of the processing operations specifically required by law, such as gathering reliable and robust data following the protocol as approved by the Member State under the Clinical Trial Regulation.

[70] Specific testing of medicinal products may take place on the basis of an EU or national law pursuant to Article 9(2)(i).

When research purposes cannot be fully specified, a controller must seek other ways to ensure the essence of the consent requirements are served best, for example, to allow data subjects to consent for a research purpose in more general terms and for specific stages of a research project that are already known to take place at the outset. As the research advances, consent for subsequent steps in the project can be obtained before that next stage begins. Yet, such a consent should still be in line with the applicable ethical standards for scientific research.

Moreover, the controller may apply further safeguards in such cases. Article 89(1), for example, highlights the need for safeguards in data processing activities for scientific or historical or statistical purposes. These purposes "*shall be subject to appropriate safeguards, in accordance with this regulation, for the rights and freedoms of data subject*." Data minimization, anonymisation and data security are mentioned as possible safeguards.[71] Anonymisation is the preferred solution as soon as the purpose of the research can be achieved without the processing of personal data.

Transparency is an additional safeguard when the circumstances of the research do not allow for a specific consent. A lack of purpose specification may be offset by information on the development of the purpose being provided regularly by controllers as the research project progresses so that, over time, the consent will be as specific as possible. When doing so, the data subject has at least a basic understanding of the state of play, allowing him/her to assess whether or not to use, for example, the right to withdraw consent pursuant to Article 7(3).[72]

Also, having a comprehensive research plan available for data subjects to take note of, before they consent could help to compensate a lack of purpose specification.[73] This research plan should specify the research questions and working methods envisaged as clearly as possible. The research plan could also contribute to compliance with Article 7(1), as controllers need to show what information was available to data subjects at the time of consent in order to be able to demonstrate that consent is valid.

It is important to recall that where consent is being used as the lawful basis for processing there must be a possibility for a data subject to withdraw that consent. WP29 notes that withdrawal of consent could undermine types scientific research that require data that can be linked to individuals, however the GDPR is clear that consent can be withdrawn and controllers must act upon this – there

[71] See for example Recital 156. The processing of personal data for scientific purposes should also comply with other relevant legislation such as on clinical trials, see Recital 156, mentioning Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use. See also WP29 Opinion 15/2011 on the definition of consent (WP 187), p. 7: "*Moreover, obtaining consent does not negate the controller's obligations under Article 6 with regard to fairness, necessity and proportionality, as well as data quality. For instance, even if the processing of personal data is based on the consent of the user, this would not legitimise the collection of data which is excessive in relation to a particular purpose*." *[…] As a principle, consent should not be seen as an exemption from the other data protection principles, but as a safeguard. It is primarily a ground for lawfulness, and it does not waive the application of other principles."*

[72] Other transparency measures may also be relevant. When controllers engage in data processing for scientific purposes, while full information cannot be provided at the outset, they could designate a specific contact person for data subjects to address with questions.

[73] Such a possibility can be found in Article 14(1) of the current Personal Data Act of Finland (*Henkilötietolaki*, 523/1999)

is no exemption to this requirement for scientific research. If a controller receives a withdrawal request, it must in principle delete the personal data straight away if it wishes to continue to use the data for the purposes of the research.[74]

7.3.Data subject's rights

If a data processing activity is based on a data subject's consent, this will affect that individual's rights. Data subjects may have the right to data portability (Article 20) when processing is based on consent. At the same time, the right to object (Article 21) does not apply when processing is based on consent, although the right to withdraw consent at any time may provide a similar outcome.

Articles 16 to 20 of the GDPR indicate that (when data processing is based on consent), data subjects have the right to erasure when consent has been withdrawn and the rights to restriction, rectification and access.[75]

8. Consent obtained under Directive 95/46/EC

Controllers that currently process data on the basis of consent in compliance with national data protection law are not automatically required to completely refresh all existing consent relations with data subjects in preparation for the GDPR. Consent which has been obtained to date continues to be valid in so far as it is in line with the conditions laid down in the GDPR.

It is important for controllers to review current work processes and records in detail, before 25 May 2018, to be sure existing consents meet the GDPR standard (see Recital 171 of the GDPR[76]). In practice, the GDPR raises the bar with regard to implementing consent mechanisms and introduces several new requirements that require controllers to alter consent mechanisms, rather than rewriting privacy policies alone.[77]

For example, as the GDPR requires that a controller must be able to demonstrate that valid consent was obtained, all presumed consents of which no references are kept will automatically be below the consent standard of the GDPR and will need to be renewed. Likewise as the GDPR requires a "statement or a clear affirmative action", all presumed consents that were based on a more implied form of action by the data subject (e.g. a pre-ticked opt-in box) will also not be apt to the GDPR standard of consent.

[74] See also WP29 Opinion 05/2014 on "Anonymisation Techniques" (WP216).

[75] In cases where certain data processing activities are restricted in accordance with Article 18, GDPR, consent of the data subject may be needed to lift restrictions.

[76] Recital 171 GDPR states: "*Directive 95/46/EC should be repealed by this Regulation. Processing already under way on the date of application of this Regulation should be brought into conformity with this Regulation within the period of two years after which this Regulation enters into force. Where processing is based on consent pursuant to Directive 95/46/EC, it is not necessary for the data subject to give his or her consent again if the manner in which the consent has been given is in line with the conditions of this Regulation, so as to allow the controller to continue such processing after the date of application of this Regulation. Commission decisions adopted and authorisations by supervisory authorities based on Directive 95/46/EC remain in force until amended, replaced or repealed.*"

[77] As indicated in the introduction, the GDPR provides further clarification and specification of the requirements for obtaining and demonstrating valid consent. Many of the new requirements build upon Opinion 15/2011 on consent.

Furthermore, to be able to demonstrate that consent was obtained or to allow for more granular indications of the data subject's wishes, operations and IT systems may need revision. Also, mechanisms for data subjects to withdraw their consent easily must be available and information about how to withdraw consent must be provided. If existing procedures for obtaining and managing consent do not meet the GDPR's standards, controllers will need to obtain fresh GDPR-compliant consent.

On the other hand, as not all elements named in Articles 13 and 14 must always be present as a condition for informed consent, the extended information obligations under the GDPR do not necessarily oppose the continuity of consent which has been granted before the GDPR enters into force (see page 15 above). Under Directive 95/46/EC, there was no requirement to inform data subjects of the basis upon which the processing was being conducted.

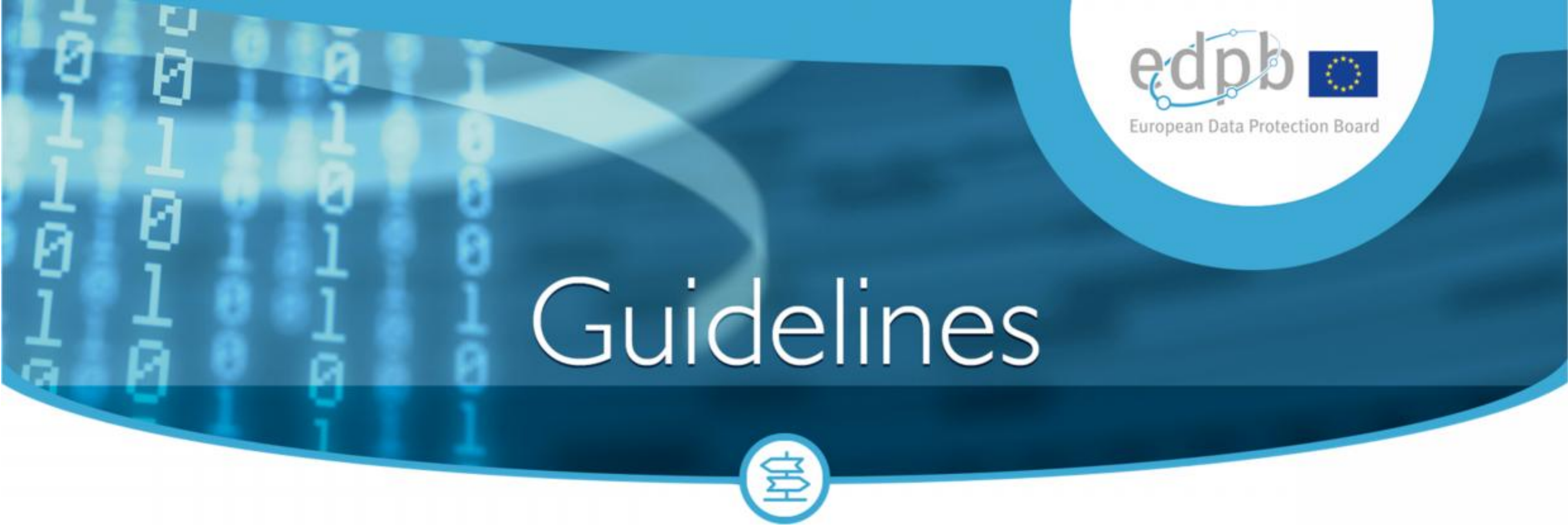
If a controller finds that the consent previously obtained under the old legislation will not meet the standard of GDPR consent, then controllers must undertake action to comply with these standards, for example by refreshing consent in a GDPR-compliant way. Under the GDPR, it is not possible to swap between one lawful basis and another. If a controller is unable to renew consent in a compliant way and is also unable –as a one off situation- to make the transition to GDPR compliance by basing data processing on a different lawful basis while ensuring that continued processing is fair and accounted for, the processing activities must be stopped. In any event the controller needs to observe the principles of lawful, fair and transparent processing.

-*-*-*-*-*-*-*-*-*-*-*-*-*-* END OF DOCUMENT *-*

JOINT COMMENTS OF
AIRLINES FOR AMERICA,
THE INTERNATIONAL AIR TRANSPORT ASSOCIATION,
THE REGIONAL AIRLINE ASSOCIATION, AND
THE NATIONAL AIR CARRIER ASSOCIATION

Docket CDC-2020-0013

ATTACHMENT 22



Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects

Version 2.0

8 October 2019

Version history

Version 2.0	8 October 2019	Adoption of the Guidelines after public consultation
Version 1.0	9 April 2019	Adoption of the Guidelines for publication consultation

The European Data Protection Board

Having regard to Article 70(1)e of Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC,

HAS ADOPTED THE FOLLOWING GUIDELINES

1 PART 1 – INTRODUCTION

1.1 Background

1. Pursuant to Article 8 of the Charter of Fundamental Rights of the European Union, personal data must be processed fairly for specified purposes and on the basis of a legitimate basis laid down by law. In this regard, Article 6(1) of the General Data Protection Regulation[1] (GDPR) specifies that processing shall be lawful only on the basis of one of six specified conditions set out in Article 6(1)(a) to (f). Identifying the appropriate legal basis that corresponds to the objective and essence of the processing is of essential importance. Controllers must, *inter alia,* take into account the impact on data subjects' rights when identifying the appropriate lawful basis in order to respect the principle of fairness.

2. Article 6(1)(b) GDPR provides a lawful basis for the processing of personal data to the extent that "processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract*"*.[2] This supports the freedom to conduct a business, which is guaranteed by Article 16 of the Charter, and reflects the fact that sometimes the contractual obligations towards the data subject cannot be performed without the data subject providing certain personal data. If the specific processing is part and parcel of delivery of the requested service, it is in the interests of both parties to process that data, as otherwise the service could not be provided and the contract could not be performed. However, the ability to rely on this or one of the other legal bases mentioned in Article 6(1) does not exempt the controller from compliance with the other requirements of the GDPR.

3. Articles 56 and 57 of the Treaty on the Functioning of the European Union define and regulate the freedom to provide services within the European Union. Specific EU legislative measures have been adopted in respect of 'information society services'.[3] These services are defined as "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services." This definition extends to services that are not paid for directly by the persons who receive them,[4] such as online services funded through advertising. 'Online services' as used in these guidelines refers to 'information society services'.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[2] See also recital 44.

[3] See for example Directive (EU) 2015/1535 of the European Parliament and of the Council, and Article 8 GDPR.

[4] See Recital 18 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

4. The development of EU law reflects the central importance of online services in modern society. The proliferation of always-on mobile internet and the widespread availability of connected devices have enabled the development of online services in fields such as social media, e-commerce, internet search, communication, and travel. While some of these services are funded by user payments, others are provided without monetary payment by the consumer, instead financed by the sale of online advertising services allowing for targeting of data subjects. Tracking of user behaviour for the purposes of such advertising is often carried out in ways the user is often not aware of,[5] and it may not be immediately obvious from the nature of the service provided, which makes it almost impossible in practice for the data subject to exercise an informed choice over the use of their data.

5. Against this background, the European Data Protection Board[6] (EDPB) considers it appropriate to provide guidance on the applicability of Article 6(1)(b) to processing of personal data in the context of online services, in order to ensure that this lawful basis is only relied upon where appropriate.

6. The Article 29 Working Party (WP29) has previously expressed views on the contractual necessity basis under Directive 95/46/EC in its opinion on the notion of legitimate interests of the data controller.[7] Generally, that guidance remains relevant to Article 6(1)(b) and the GDPR.

1.2 Scope of these guidelines

7. These guidelines are concerned with the applicability of Article 6(1)(b) to processing of personal data in the context of contracts for online services, irrespective of how the services are financed. The guidelines will outline the elements of lawful processing under Article 6(1)(b) GDPR and consider the concept of ‘necessity’ as it applies to ’necessary for the performance of a contract’.

8. Data protection rules govern important aspects of how online services interact with their users, however, other rules apply as well. Regulation of online services involves cross-functional responsibilities in the fields of, *inter alia,* consumer protection law, and competition law. Considerations regarding these fields of law are beyond the scope of these guidelines.

9. Although Article 6(1)(b) can only apply in a contractual context, these guidelines do not express a view on the validity of contracts for online services generally, as this is outside the competence of the EDPB. Nonetheless, contracts and contractual terms must comply with the requirements of contract laws and, as the case may be for consumer contracts, consumer protection laws in order for processing based on those terms to be considered fair and lawful.

10. Some general observations on data protection principles are included below, but not all data protection issues that may arise when processing under Article 6(1)(b) will be elaborated on. Controllers must always ensure that they comply with the data protection principles set out in Article 5 and all other requirements of the GDPR and, where applicable, the ePrivacy legislation.

2 PART 2 - ANALYSIS OF ARTICLE 6(1)(B)

2.1 General observations

[5] In this regard, controllers need to fulfil the transparency obligations set out in the GDPR.

[6] Established under Article 68 GDPR.

[7] Article 29 Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP217). See in particular pages 11, 16, 17, 18 and 55.

11. The lawful basis for processing on the basis of Article 6(1)(b) needs to be considered in the context of the GDPR as a whole, the objectives set out in Article 1, and alongside controllers' duty to process personal data in compliance with the data protection principles pursuant to Article 5. This includes processing personal data in a fair and transparent manner and in line with the purpose limitation and data minimisation obligations.

12. Article 5(1)(a) GDPR provides that personal data must be processed lawfully, fairly and transparently in relation to the data subject. The principle of fairness includes, inter alia, recognising the reasonable expectations[8] of the data subjects, considering possible adverse consequences processing may have on them, and having regard to the relationship and potential effects of imbalance between them and the controller.

13. As mentioned, as a matter of lawfulness, contracts for online services must be valid under the applicable contract law. An example of a relevant factor is whether the data subject is a child. In such a case (and aside from complying with the requirements of the GDPR, including the 'specific protections' which apply to children),[9] the controller must ensure that it complies with the relevant national laws on the capacity of children to enter into contracts. Furthermore, to ensure compliance with the fairness and lawfulness principles, the controller needs to satisfy other legal requirements. For example, for consumer contracts, Directive 93/13/EEC on unfair terms in consumer contracts (the "Unfair Contract Terms Directive") may be applicable.[10] Article 6(1)(b) is not limited to contracts governed by the law of an EEA member state.[11]

14. Article 5(1)(b) of the GDPR provides for the purpose limitation principle, which requires that personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

15. Article 5(1)(c) provides for data minimisation as a principle, i.e. processing as little data as possible in order to achieve the purpose. This assessment complements the necessity assessments pursuant to Article 6(1)(b) to (f).

16. Both purpose limitation and data minimisation principles are particularly relevant in contracts for online services, which typically are not negotiated on an individual basis. Technological advancements make it possible for controllers to easily collect and process more personal data than ever before. As a result, there is an acute risk that data controllers may seek to include general processing terms in contracts in order to maximise the possible collection and uses of data, without adequately specifying those purposes or considering data minimisation obligations. WP29 has previously stated:

> *The purpose of the collection must be clearly and specifically identified: it must be detailed enough to determine what kind of processing is and is not included within the specified purpose, and to allow that compliance with the law can be assessed and data protection safeguards*

[8] Some personal data are expected to be private or only processed in certain ways, and data processing should not be surprising to the data subject. In the GDPR, the concept of 'reasonable expectations' is specifically referenced in recitals 47 and 50 in relation to Article 6(1)(f) and (4).

[9] See Recital 38, which refers to children meriting specific protection with regard to their personal data as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data.

[10] A contractual term that has not been individually negotiated is unfair under the Unfair Contract Terms Directive "if, contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer". Like the transparency obligation in the GDPR, the Unfair Contract Terms Directive mandates the use of plain, intelligible language. Processing of personal data that is based on what is deemed to be an unfair term under the Unfair Contract Terms Directive, will generally not be consistent with the requirement under Article 5(1)(a) GDPR that processing is lawful and fair.

[11] The GDPR applies to certain controllers outside the EEA; see Article 3 GDPR.

> *applied. For these reasons, a purpose that is vague or general, such as for instance 'improving users' experience', 'marketing purposes', 'IT-security purposes' or 'future research' will - without more detail - usually not meet the criteria of being 'specific'.* [12]

2.2 Interaction of Article 6(1)(b) with other lawful bases for processing

17. Where processing is not considered 'necessary for the performance of a contract', i.e. when a requested service can be provided without the specific processing taking place, the EDPB recognises that another lawful basis may be applicable, provided the relevant conditions are met. In particular, in some circumstances it may be more appropriate to rely on freely given consent under Article 6(1)(a). In other instances, Article 6(1)(f) may provide a more appropriate lawful basis for processing. The legal basis must be identified at the outset of processing, and information given to data subjects in line with Articles 13 and 14 must specify the legal basis.

18. It is possible that another lawful basis than Article 6(1)(b) may better match the objective and context of the processing operation in question. The identification of the appropriate lawful basis is tied to principles of fairness and purpose limitation.[13]

19. The WP29 guidelines on consent also clarify that where "a controller seeks to process personal data that are in fact necessary for the performance of a contract, then consent is not the appropriate lawful basis". Conversely, the EDPB considers that where processing is not in fact necessary for the performance of a contract, such processing can take place only if it relies on another appropriate legal basis.[14]

20. In line with their transparency obligations, controllers should make sure to avoid any confusion as to what the applicable legal basis is. This is particularly relevant where the appropriate legal basis is Article 6(1)(b) and a contract regarding online services is entered into by data subjects. Depending on the circumstances, data subjects may erroneously get the impression that they are giving their consent in line with Article 6(1)(a) when signing a contract or accepting terms of service. At the same time, a controller might erroneously assume that the signature of a contract corresponds to a consent in the sense of article 6(1)(a). These are entirely different concepts. It is important to distinguish between accepting terms of service to conclude a contract and giving consent within the meaning of Article 6(1)(a), as these concepts have different requirements and legal consequences.

21. In relation to the processing of special categories of personal data, in the guidelines on consent, WP29 has also observed that:

> *Article 9(2) does not recognize 'necessary for the performance of a contract' as an exception to the general prohibition to process special categories of data. Therefore controllers and Member States that deal with this situation should explore the specific exceptions in Article 9(2) subparagraphs (b) to (j). Should none of the exceptions (b) to (j) apply, obtaining explicit*

[12] Article 29 Working Party Opinion 03/2013 on purpose limitation (WP203), page 15–16.

[13] When controllers set out to identify the appropriate legal basis in line with the fairness principle, this will be difficult to achieve if they have not first clearly identified the purposes of processing, or if processing personal data goes beyond what is necessary for the specified purposes.

[14] For more information on implications in relation to Article 9, see Article 29 Working Party Guidelines on consent under Regulation 2016/679 (WP259), endorsed by the EDPB, pages 19–20.

> *consent in accordance with the conditions for valid consent in the GDPR remains the only possible lawful exception to process such data.*[15]

2.3 Scope of Article 6(1)(b)

22. Article 6(1)(b) applies where either of two conditions are met: the processing in question must be objectively necessary for the performance of a contract with a data subject, or the processing must be objectively necessary in order to take pre-contractual steps at the request of a data subject.

2.4 Necessity

23. Necessity of processing is a prerequisite for both parts of Article 6(1)(b). At the outset, it is important to note that the concept of what is 'necessary for the performance of a contract' is not simply an assessment of what is permitted by or written into the terms of a contract. The concept of necessity has an independent meaning in European Union law, which must reflect the objectives of data protection law.[16] Therefore, it also involves consideration of the fundamental right to privacy and protection of personal data,[17] as well as the requirements of data protection principles including, notably, the fairness principle.

24. The starting point is to identify the purpose for the processing, and in the context of a contractual relationship, there may be a variety of purposes for processing. Those purposes must be clearly specified and communicated to the data subject, in line with the controller's purpose limitation and transparency obligations.

25. Assessing what is 'necessary' involves a combined, fact-based assessment of the processing "for the objective pursued and of whether it is less intrusive compared to other options for achieving the same goal".[18] If there are realistic, less intrusive alternatives, the processing is not 'necessary'.[19] Article 6(1)(b) will not cover processing which is useful but not objectively necessary for performing the contractual service or for taking relevant pre-contractual steps at the request of the data subject, even if it is necessary for the controller's other business purposes.

[15] Article 29 Working Party Guidelines on consent under Regulation 2016/679 (WP259), endorsed by the EDPB, page 19.

[16] The CJEU stated in *Huber* that "what is at issue is a concept [necessity] which has its own independent meaning in Community law and which must be interpreted in a manner which fully reflects the objective of that Directive, [Directive 95/46], as laid down in Article 1(1) thereof". CJEU, Case C-524/06, *Heinz Huber v Bundesrepublik Deutschland,* 18 December 2008, para. 52.

[17] See Articles 7 and 8 of the Charter of Fundamental Rights of the European Union

[18] See EDPS Toolkit: Assessing the Necessity of Measures that limit the fundamental right to the protection of personal data, page 5.

[19] In *Schecke*, the CJEU held that, when examining the necessity of processing personal data, the legislature needed to take into account alternative, less intrusive measures. CJEU, Joined Cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*, 9. November 2010. This was repeated by the CJEU in the *Rīgas* case where it held that "As regards the condition relating to the necessity of processing personal data, it should be borne in mind that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary". CJEU, Case C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA 'Rīgas satiksme'*, para. 30. A strict necessary test is required for any limitations on the exercise of the rights to privacy and to personal data protection with regard to the processing of personal data, see EDPS Toolkit: Assessing the Necessity of Measures that limit the fundamental right to the protection of personal data, page 7.

2.5 Necessary for performance of a contract with the data subject

26. A controller can rely on the first option of Article 6(1)(b) to process personal data when it can, in line with its accountability obligations under Article 5(2), establish both that the processing takes place in the context of a valid contract with the data subject and that processing is necessary in order that the *particular contract* with the data subject can be performed. Where controllers cannot demonstrate that (a) a contract exists, (b) the contract is valid pursuant to applicable national contract laws, and (c) that the processing is objectively necessary for the performance of the contract, the controller should consider another legal basis for processing.

27. Merely referencing or mentioning data processing in a contract is not enough to bring the processing in question within the scope of Article 6(1)(b). On the other hand, processing may be objectively necessary even if not specifically mentioned in the contract. In any case, the controller must meet its transparency obligations. Where a controller seeks to establish that the processing is based on the performance of a contract with the data subject, it is important to assess what is *objectively necessary* to perform the contract. 'Necessary for performance' clearly requires something more than a contractual clause. This is also clear in light of Article 7(4). Albeit this provision only regards validity of consent, it illustratively makes a distinction between processing activities necessary for the performance of a contract, and *clauses* making the service conditional on certain processing activities that are not in fact necessary for the performance of the contract.

28. In this regard, the EDPB endorses the guidance previously adopted by WP29 on the equivalent provision under the previous Directive that 'necessary for the performance of a contract with the data subject':

> *… must be interpreted strictly and does not cover situations where the processing is not genuinely necessary for the performance of a contract, but rather unilaterally imposed on the data subject by the controller. Also the fact that some processing is covered by a contract does not automatically mean that the processing is necessary for its performance. […] Even if these processing activities are specifically mentioned in the small print of the contract, this fact alone does not make them 'necessary' for the performance of the contract.*[20]

29. The EDPB also recalls the same WP29 guidance stating:

> *There is a clear connection here between the assessment of necessity and compliance with the purpose limitation principle. It is important to determine the exact rationale of the contract, i.e. its substance and fundamental objective, as it is against this that it will be tested whether the data processing is necessary for its performance.*[21]

30. When assessing whether Article 6(1)(b) is an appropriate legal basis for processing in the context of an online contractual service, regard should be given to the particular aim, purpose, or objective of the service. For applicability of Article 6(1)(b), it is required that the processing is *objectively necessary* for a purpose that is integral to the delivery of that contractual service to the data subject. Not excluded is processing of payment details for the purpose of charging for the service. The controller should be able to demonstrate how the main subject-matter of the *specific contract with the data subject* cannot, as a matter of fact, be performed if the specific processing of the *personal data in question* does not

[20] Article 29 Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP217), page 16–17.
[21] Ibid., page 17.

occur. The important issue here is the nexus between the personal data and processing operations concerned, and the performance or non-performance of the service provided under the contract.

31. Contracts for digital services may incorporate express terms that impose additional conditions about advertising, payments or cookies, amongst other things. A contract cannot artificially expand the categories of personal data or types of processing operation that the controller needs to carry out for the performance of the contract within the meaning of Article 6(1)(b).

32. The controller should be able to justify the necessity of its processing by reference to the fundamental and mutually understood contractual purpose. This depends not just on the controller's perspective, but also a reasonable data subject's perspective when entering into the contract, and whether the contract can still be considered to be 'performed' without the processing in question. Although the controller may consider that the processing is necessary for the contractual purpose, it is important that they examine carefully the perspective of an average data subject in order to ensure that there is a genuine mutual understanding on the contractual purpose.

33. In order to carry out the assessment of whether Article 6(1)(b) is applicable, the following questions can be of guidance:

- What is the nature of the service being provided to the data subject? What are its distinguishing characteristics?
- What is the exact rationale of the contract (i.e. its substance and fundamental object)?
- What are the essential elements of the contract?
- What are the mutual perspectives and expectations of the parties to the contract? How is the service promoted or advertised to the data subject? Would an ordinary user of the service reasonably expect that, considering the nature of the service, the envisaged processing will take place in order to perform the contract to which they are a party?

34. If the assessment of what is 'necessary for the performance of a contract', which must be conducted prior to the commencement of processing, shows that the intended processing goes beyond what is objectively necessary for the performance of a contract, this does not render such future processing unlawful per se. As already mentioned, Article 6 makes clear that other lawful bases are potentially available prior to the initiation of the processing.[22]

35. If, over the lifespan of a service, new technology is introduced that changes how personal data are processed, or the service otherwise evolves, the criteria above need to be assessed anew to determine if any new or altered processing operations can be based on Article 6(1)(b).

Example 1

A data subject buys items from an online retailer. The data subject wants to pay by credit card and for the products to be delivered to their home address. In order to fulfil the contract, the retailer must process the data subject's credit card information and billing address for payment purposes and the data subject's home address for delivery. Thus, Article 6(1)(b) is applicable as a legal basis for these processing activities.

[22] See Article 29 Working Party Guidelines on consent under Regulation 2016/679 (WP259), endorsed by the EDPB, page 31, in which it is stated that: "Under the GDPR, it is not possible to swap between one lawful basis and another."

However, if the customer has opted for shipment to a pick-up point, the processing of the data subject's home address is no longer necessary for the performance of the purchase contract. Any processing of the data subject's address in this context will require a different legal basis than Article 6(1)(b).

Example 2

The same online retailer wishes to build profiles of the user's tastes and lifestyle choices based on their visits to the website. Completion of the purchase contract is not dependent upon building such profiles. Even if profiling is specifically mentioned in the contract, this fact alone does not make it 'necessary' for the performance of the contract. If the on-line retailer wants to carry out such profiling, it needs to rely on a different legal basis.

36. Within the boundaries of contractual law, and if applicable, consumer law, controllers are free to design their business, services and contracts. In some cases, a controller may wish to bundle several separate services or elements of a service with different fundamental purposes, features or rationale into one contract. This may create a 'take it or leave it' situation for data subjects who may only be interested in one of the services.

37. As a matter of data protection law, controllers need to take into account that the processing activities foreseen must have an appropriate legal basis. Where the contract consists of several separate services or elements of a service that can in fact reasonably be performed independently of one another, the question arises to which extent Article 6(1)(b) can serve as a legal basis. The applicability of Article 6(1)(b) should be assessed in the context of each of those services *separately*, looking at what is objectively necessary to perform each of the individual services which the data subject has actively requested or signed up for. This assessment may reveal that certain processing activities are not necessary for the individual services requested by the data subject, but rather necessary for the controller's wider business model. In that case, Article 6(1)(b) will not be a legal basis for those activities. However, other legal bases may be available for that processing, such as Article 6(1)(a) or (f), provided that the relevant criteria are met. Therefore, the assessment of the applicability of Article 6(1)(b) does not affect the legality of the contract or the bundling of services as such.

38. As WP29 has previously observed, the legal basis only applies to what is necessary for the *performance* of a contract.[23] As such, it does not automatically apply to all further actions triggered by non-compliance or to all other incidents in the execution of a contract. However, certain actions can be reasonably foreseen and necessary within a normal contractual relationship, such as sending formal reminders about outstanding payments or correcting errors or delays in the performance of the contract. Article 6(1)(b) may cover processing of personal data which is necessary in relation to such actions.

[23] Article 29 Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP217) page 17–18.

Example 3

A company sells products online. A customer contacts the company because the colour of the product purchased is different from what was agreed upon. The processing of personal data of the customer for the purpose of rectifying this issue can be based on Article 6(1)(b).

39. Contractual warranty may be part of performing a contract, and thus storing certain data for a specified retention time after exchange of goods/services/payment has been finalised for the purpose of warranties may be necessary for the performance of a contract.

2.6 Termination of contract

40. A controller needs to identify the appropriate legal basis for the envisaged processing operations before the processing commences. Where Article 6(1)(b) is the basis for some or all processing activities, the controller should anticipate what happens if that contract is terminated.[24]

41. Where the processing of personal data is based on Article 6(1)(b) and the contract is terminated in full, then as a general rule, the processing of that data will no longer be necessary for the performance of that contract and thus the controller will need to stop processing. The data subject might have provided their personal data in the context of a contractual relationship trusting that the data would only be processed as a necessary part of that relationship. Hence, it is generally unfair to swap to a new legal basis when the original basis ceases to exist.

42. When a contract is terminated, this may entail some administration, such as returning goods or payment. The associated processing may be based on Article 6(1)(b).

43. Article 17(1)(a) provides that personal data shall be erased when they are no longer necessary in relation to the purposes for which they were collected. Nonetheless, this does not apply if processing is necessary for certain specific purposes, including compliance with a legal obligation pursuant to Article 17(3)(b), or the establishment, exercise or defence of legal claims, pursuant to Article 17(3)(e). In practice, if controllers see a general need to keep records for legal purposes, they need to identify a legal basis for this at the outset of processing, and they need to communicate clearly from the start for how long they plan to retain records for these legal purposes after the termination of a contract. If they do so, they do not need to delete the data upon the termination of the contract.

44. In any case, it may be that several processing operations with separate purposes and legal bases were identified at the outset of processing. As long as those other processing operations remain lawful and the controller communicated clearly about those operations at the commencement of processing in line with the transparency obligations of the GDPR, it will still be possible to process personal data about the data subject for those separate purposes after the contract has been terminated.

[24] If a contract is subsequently invalidated, it will impact the lawfulness (as understood in Article 5(1)(a)) of continued processing. However, it does not automatically imply that the choice of Article 6(1)(b) as the legal basis was incorrect.

Example 4

An online service provides a subscription service that can be cancelled at any time. When a contract for the service is concluded, the controller provides information to the data subject on the processing of personal data.

The controller explains, *inter alia*, that as long as the contract is in place, it will process data about the use of the service to issue invoices. The applicable legal basis is Article 6(1)(b) as the processing for invoicing purposes can be considered to be objectively necessary for the performance of the contract. However, when the contract is terminated and assuming there are no pending, relevant legal claims or legal requirements to retain the data, the usage history will be deleted.

Furthermore, the controller informs data subjects that it has a legal obligation in national law to retain certain personal data for accounting purposes for a specified number of years. The appropriate legal basis is Article 6(1)(c), and retention will take place even if the contract is terminated.

2.7 Necessary for taking steps prior to entering into a contract

45. The second option of Article 6(1)(b) applies where *processing is necessary in order to take steps at the request of the data subject prior to entering into a contract*. This provision reflects the fact that preliminary processing of personal data may be necessary before entering into a contract in order to facilitate the actual entering into that contract.

46. At the time of processing, it may not be clear whether a contract will actually be entered into. The second option of Article 6(1)(b) may nonetheless apply as long as the data subject makes the request in the context of *potentially* entering into a contract and the processing in question is necessary to take the steps requested. In line with this, where a data subject contacts the controller to enquire about the details of the controller's service offerings, the processing of the data subject's personal data for the purpose of responding to the enquiry can be based on Article 6(1)(b).

47. In any case, this provision would not cover unsolicited marketing or other processing which is carried out solely on the initiative of the data controller, or at the request of a third party.

Example 5

A data subject provides their postal code to see if a particular service provider operates in their area. This can be regarded as processing necessary to take steps at the request of the data subject prior to entering into a contract pursuant to Article 6(1)(b).

Example 6

In some cases, financial institutions have a duty to identify their customers pursuant to national laws. In line with this, before entering into a contract with data subjects, a bank requests to see their identity documents.

In this case, the identification is necessary for a legal obligation on behalf of the bank rather than to take steps at the data subject's request. Therefore, the appropriate legal basis is not Article 6(1)(b), but Article 6(1)(c).

3 PART 3 – APPLICABILITY OF ARTICLE 6(1)(B) IN SPECIFIC SITUATIONS

3.1 Processing for 'service improvement'[25]

48. Online services often collect detailed information on how users engage with their service. In most cases, collection of organisational metrics relating to a service or details of user engagement, cannot be regarded as necessary for the provision of the service as the service could be delivered in the absence of processing such personal data. Nevertheless, a service provider may be able to rely on alternative lawful bases for this processing, such as legitimate interest or consent.

49. The EDPB does not consider that Article 6(1)(b) would generally be an appropriate lawful basis for processing for the purposes of improving a service or developing new functions within an existing service. In most cases, a user enters into a contract to avail of an existing service. While the possibility of improvements and modifications to a service may routinely be included in contractual terms, such processing usually cannot be regarded as being objectively necessary for the performance of the contract with the user.

3.2 Processing for 'fraud prevention'

50. As WP29 has previously noted,[26] processing for fraud prevention purposes may involve monitoring and profiling customers. In the view of the EDPB, such processing is likely to go beyond what is objectively necessary for the performance of a contract with a data subject. However, the processing of personal data strictly necessary for the purposes of preventing fraud may constitute a legitimate interest of the data controller[27] and could thus be considered lawful, if the specific requirements of Article 6(1)(f)(legitimate interests) are met by the data controller. In addition Article 6(1)(c) (legal obligation) could also provide a lawful basis for such processing of data.

3.3 Processing for online behavioural advertising

51. Online behavioural advertising, and associated tracking and profiling of data subjects, is often used to finance online services. WP29 has previously stated its view on such processing, stating:

> *[contractual necessity] is not a suitable legal ground for building a profile of the user's tastes and lifestyle choices based on his clickstream on a website and the items purchased. This is because the data controller has not been contracted to carry out profiling, but rather to deliver particular goods and services, for example.*[28]

52. As a general rule, processing of personal data for behavioural advertising is not necessary for the performance of a contract for online services. Normally, it would be hard to argue that the contract

[25] Online services may also need to take into account Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services (OJ L 136, 22.05.2019, p. 1), which will apply as from 1 January 2022.

[26] Article 29 Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP217), page 17.

[27] See Recital 47, sixth sentence.

[28] Article 29 Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP217), page 17.

had not been performed because there were no behavioural ads. This is all the more supported by the fact that data subjects have the absolute right under Article 21 to object to processing of their data for direct marketing purposes.

53. Further to this, Article 6(1)(b) cannot provide a lawful basis for online behavioural advertising simply because such advertising indirectly funds the provision of the service. Although such processing may support the delivery of a service, this in itself is not sufficient to establish that it is necessary for the performance of the contract at issue. The controller would need to consider the factors outlined in paragraph 33.

54. Considering that data protection is a fundamental right guaranteed by Article 8 of the Charter of Fundamental Rights, and taking into account that one of the main purposes of the GDPR is to provide data subjects with control over information relating to them, personal data cannot be considered as a tradeable commodity. Even if the data subject can agree to the processing of personal data,[29] they cannot trade away their fundamental rights through this agreement.[30]

55. The EDPB also notes that, in line with ePrivacy requirements and the existing WP29 opinion on behavioural advertising,[31] and Working Document 02/2013 providing guidance on obtaining consent for cookies,[32] controllers must obtain data subjects' prior consent to place the cookies necessary to engage in behavioural advertising.

56. The EDPB also notes that tracking and profiling of users may be carried out for the purpose of identifying groups of individuals with similar characteristics, to enable targeting advertising to similar audiences. Such processing cannot be carried out on the basis of Article 6(1)(b), as it cannot be said to be objectively necessary for the performance of the contract with the user to track and compare users' characteristics and behaviour for purposes which relate to advertising to other individuals.[33]

3.4 Processing for personalisation of content[34]

57. The EDPB acknowledges that personalisation of content <u>may</u> (but does not always) constitute an intrinsic and expected element of certain online services, and therefore <u>may</u> be regarded as necessary for the performance of the contract with the service user in some cases. Whether such processing can be regarded as an intrinsic aspect of an online service, will depend on the nature of the service provided, the expectations of the average data subject in light not only of the terms of service but also the way the service is promoted to users, and whether the service can be provided without personalisation. Where personalisation of content is not objectively necessary for the purpose of the underlying contract, for example where personalised content delivery is intended to increase user

[29] See Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services.

[30] Besides the fact that the use of personal data is regulated by the GDPR, there are additional reasons why processing of personal data is conceptually different from monetary payments. For example, money is countable, meaning that prices can be compared in a competitive market, and monetary payments can normally only be made with the data subject's involvement. Furthermore, personal data can be exploited by several services at the same time. Once control over one's personal data has been lost, that control may not necessarily be regained.

[31] Article 29 Working Party Opinion 2/2010 on online behavioural advertising (WP171).

[32] Article 29 Working Party Working Document 02/2013 providing guidance on obtaining consent for cookies (WP208).

[33] See also Article 29 Working Party Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251rev.01), endorsed by the EDPB, page 13.

[34] Online services may also need to take into account Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services (OJ L 136, 22.05.2019, p. 1), which will apply as from 1 January 2022.

engagement with a service but is not an integral part of using the service, data controllers should consider an alternative lawful basis where applicable.

Example 7

An online hotel search engine monitors past bookings of users in order to create a profile of their typical expenditure. This profile is subsequently used to recommend particular hotels to the user when returning search results. In this case, profiling of user's past behaviour and financial data would not be objectively necessary for the performance of a contract, i.e. the provision of hospitality services based on particular search criteria provided by the user. Therefore, Article 6(1)(b) would not be applicable to this processing activity.

Example 8

An online marketplace allows potential buyers to browse for and purchase products. The marketplace wishes to display personalised product suggestions based on which listings the potential buyers have previously viewed on the platform in order to increase interactivity. This personalisation it is not objectively necessary to provide the marketplace service. Thus, such processing of personal data cannot rely on Article 6(1)(b) as a legal basis.

JOINT COMMENTS OF
AIRLINES FOR AMERICA,
THE INTERNATIONAL AIR TRANSPORT ASSOCIATION,
THE REGIONAL AIRLINE ASSOCIATION, AND
THE NATIONAL AIR CARRIER ASSOCIATION

Docket CDC-2020-0013

ATTACHMENT 23

ARTICLE 29 DATA PROTECTION WORKING PARTY

844/14/EN
WP 217

Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC

Adopted on 9 April 2014

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 02/013.

Website: http://ec.europa.eu/justice/data-protection/index_en.htm

Table of contents

Executive Summary

This Opinion analyses the criteria set down in Article 7 of Directive 95/46/EC for making data processing legitimate. Focusing on the legitimate interests of the controller, it provides guidance on how to apply Article 7(f) under the current legal framework and makes recommendations for future improvements.

Article 7(f) is the last of six grounds for the lawful processing of personal data. In effect it requires a balancing of the legitimate interests of the controller, or any third parties to whom the data are disclosed, against the interests or fundamental rights of the data subject. The outcome of this balancing test will determine whether Article 7(f) may be relied upon as a legal ground for processing.

The WP29 recognises the significance and usefulness of the Article 7(f) criterion, which in the right circumstances and subject to adequate safeguards may help prevent over-reliance on other legal grounds. Article 7(f) should not be treated as 'a last resort' for rare or unexpected situations where other grounds for legitimate processing are deemed not to apply. However, it should not be automatically chosen, or its use unduly extended on the basis of a perception that it is less constraining than the other grounds.

A proper Article 7(f) assessment is not a straightforward balancing test consisting merely of weighing two easily quantifiable and comparable 'weights' against each other. Rather, the test requires full consideration of a number of factors, so as to ensure that the interests and fundamental rights of data subjects are duly taken into account. At the same time it is scalable which can vary from simple to complex and need not be unduly burdensome. Factors to consider when carrying out the balancing test include:

- the nature and source of the legitimate interest and whether the data processing is necessary for the exercise of a fundamental right, is otherwise in the public interest, or benefits from recognition in the community concerned;

- the impact on the data subject and their reasonable expectations about what will happen to their data, as well as the nature of the data and how they are processed;

- additional safeguards which could limit undue impact on the data subject, such as data minimisation, privacy-enhancing technologies; increased transparency, general and unconditional right to opt-out, and data portability.

For the future, the WP29 recommends implementing a recital to the proposed Regulation on the key factors to consider when applying the balancing test. The WP29 also recommends that a recital be added requiring the controller, when appropriate, to document its assessment in the interests of greater accountability. Finally, the WP29 would also support a substantive provision for controllers to explain to data subjects why they believe their interests would not be overridden by the data subject's interests, fundamental rights and freedoms.

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

having regard to Articles 29 and 30 paragraphs 1(a) and 3 of that Directive,

having regard to its Rules of Procedure,

HAS ADOPTED THE PRESENT OPINION:

I. Introduction

This Opinion analyses the criteria set forth in Article 7 of Directive 95/46/EC[1] (the 'Directive') for making data processing legitimate. It focuses, in particular, on the legitimate interests of the controller, under Article 7(f).

The criteria listed in Article 7 are related to the broader principle of 'lawfulness' set forth in Article 6(1)(a), which requires that personal data must be processed 'fairly and lawfully'.

Article 7 requires that personal data shall only be processed if at least one of six legal grounds listed in that Article apply. In particular, personal data shall only be processed (a) based on the data subject's unambiguous consent[2]; or if - briefly put[3] - processing is necessary for:

(b) performance of a contract with the data subject;
(c) compliance with a legal obligation imposed on the controller;
(d) protection of the vital interests of the data subject;
(e) performance of a task carried out in the public interest; or
(f) legitimate interests pursued by the controller, subject to an additional balancing test against the data subject’s rights and interests.

This last ground allows processing 'necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests (f)or[4] fundamental rights and freedoms of the data subject which require protection under Article 1(1)'. In other words, Article 7(f) allows processing subject to a balancing test, which weighs the legitimate interests of the controller - or the third party or parties to whom the data are disclosed – against the interests or fundamental rights of the data subjects.[5]

[1] Directive 95/46/EC of the European Parliament and of the Council of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281,23.11.1995, p. 31).

[2] See Opinion 15/2011 of the Article 29 Data Protection Working Party on the definition of consent, adopted on 13.07.2011 (WP187).

[3] These provisions are discussed in greater detail at a later stage.

[4] As explained in Section III.3.2, the English version of the Directive appears to contain a typo: the text should read ‘interests or fundamental rights’ rather than ‘interests for fundamental rights’.

[5] The reference to Article 1(1) should not be interpreted to limit the scope of the interests and fundamental rights and freedoms of the data subject. Rather, the role of this reference is to emphasise the overall objective of data

Need for a more consistent and harmonized approach across Europe

Studies conducted by the Commission in the framework of the review of the Directive[6] as well as cooperation and exchange of views between national data protection authorities ('DPAs') have shown a lack of harmonised interpretation of Article 7(f) of the Directive, which has led to divergent applications in the Member States. In particular, although a true balancing test is required to be performed in several Member States, Article 7(f) is sometimes incorrectly seen as an 'open door' to legitimise any data processing which does not fit in one of the other legal grounds.

The lack of a consistent approach may result in lack of legal certainty and predictability, may weaken the position of data subjects and may also impose unnecessary regulatory burdens on businesses and other organisations operating across borders. Such inconsistencies have already led to litigation before the Court of Justice of the European Union ('ECJ')[7].

It is therefore particularly timely, as work towards a new general Data Protection Regulation continues, that the sixth ground for processing (referring to 'legitimate interests') and its relationship with the other grounds for processing, be more clearly understood. In particular, the fact that fundamental rights of data subjects are at stake, entails that the application of all six grounds should - duly and equally - take into account the respect of these rights. Article 7(f) should not become an easy way out from compliance with data protection law.

This is why the Article 29 Data Protection Working Party ('Working Party'), as part of its Work Programme for 2012-2013, has decided to take a careful look at this subject and - to execute this Work Programme[8] - committed to draft this Opinion.

Implementing the current legal framework and preparing for the future

The Work Programme itself clearly stated two objectives: 'ensuring the correct implementation of the current legal framework' and also 'preparing for the future'.

Accordingly, the first objective of this Opinion is to ensure a common understanding of the existing legal framework. This objective follows earlier Opinions on other key provisions of

protection laws and the Directive itself. Indeed, Article 1(1) does not only refer to the protection of privacy but also to the protection of all other 'rights and freedoms of natural persons', of which privacy is only one.

[6] On 25 January 2012, the European Commission adopted a package for reforming the European data protection framework. The package includes (i) a 'Communication' (COM(2012)9 final), (ii) a proposal for a general 'Data Protection Regulation' ('proposed Regulation') (COM(2012)11 final), and (iii) a proposal for a 'Directive' on data protection in the area of criminal law enforcement (COM(2012)10 final). The accompanying 'Impact Assessment', which contains 10 annexes, is set forth in a Commission Working Paper (SEC(2012)72 final). See, in particular, the study entitled 'Evaluation of the implementation of the Data Protection Directive', which forms Annex 2 to the Impact Assessment accompanying the European Commission's data protection reform package.

[7] See page 7, under the heading 'II.1 Brief History', *'Implementation of the Directive; the ASNEF and FECEMD judgment'.*

[8] See Work programme 2012-2013 of the Article 29 Data Protection Working Party adopted on 1 February 2012 (WP190).

the Directive[9]. Secondly, building on the analysis, the Opinion will also formulate policy recommendations to be considered during the review of the data protection legal framework.

Structure of the Opinion

After a brief overview of the history and role of legitimate interests and other grounds for processing in Chapter II, Chapter III will examine and interpret the relevant provisions of the Directive, taking into account common ground in their national implementation. This analysis is illustrated with practical examples based on national experience. The analysis supports the recommendations in Chapter IV both on the application of the current regulatory framework and in the context of the review of the Directive.

II. <u>General observations and policy issues</u>

II.1. Brief history

This overview focuses on how the concepts of lawfulness and legal grounds for processing, including legitimate interests, have developed. It explains in particular how the need for a legal basis was first used as a requirement in the context of derogations to privacy rights, and subsequently developed into a separate requirement in the data protection context.

European Convention on Human Rights ('ECHR')

Article 8 of the European Convention on Human Rights, adopted in 1950, incorporates the right to privacy - i.e. respect for everyone's private and family life, home and correspondence. It prohibits any interference with the right to privacy except if 'in accordance with the law' and 'necessary in a democratic society' in order to satisfy certain types of specifically listed, compelling public interests.

Article 8 ECHR focuses on the protection of private life, and requires justification for any interference with privacy. This approach is based on a general prohibition of interference with the right of privacy and allows exceptions only under strictly defined conditions. In cases where there is 'interference with privacy' a legal basis is required, as well as the specification of a legitimate purpose as a precondition to assess the necessity of the interference. This approach explains that the ECHR does not provide for a list of possible legal grounds but concentrates on the necessity of a legal basis, and on the conditions this legal basis should meet.

Convention 108

The Council of Europe's Convention 108[10], opened for signature in 1981, introduces the protection of personal data as a separate concept. The underlying idea at the time was not that processing of personal data should always be seen as *'interference* with privacy', but rather that to *protect* everyone's fundamental rights and freedoms, and notably their right to privacy,

[9] Such as Opinion 3/2013 on purpose limitation, adopted on 03.04.2013 (WP203), Opinion 15/2011 on the definition of consent (cited in footnote 2), Opinion 8/2010 on applicable law, adopted on 16.12.2010 (WP179) and Opinion 1/2010 on the concepts of 'controller' and 'processor', adopted on 16.02.2010 (WP169).

[10] Convention 108 for the Protection of Individuals with regard to automatic processing of personal data.

processing of personal data should always fulfil certain conditions. Article 5 thus establishes the fundamental principles of data protection law, including the requirement that 'personal data undergoing automatic processing shall be: (a) obtained and processed fairly and lawfully'. However, the Convention did not provide detailed grounds for processing.[11]

OECD Guidelines[12]

The OECD Guidelines, prepared in parallel with Convention 108 and adopted in 1980, share similar ideas of 'lawfulness', although the concept is expressed in a different way. The guidelines were updated in 2013, without substantive changes to the principle of lawfulness. Article 7 of the OECD Guidelines in particular provides that 'there should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.' Here the legal ground of consent is explicitly mentioned as an option, to be used ‘where appropriate’. This will require an appreciation of the interests and rights at stake, as well as assessing how intrusive the processing is. In this sense the OECD approach shows some similarities with the – much more developed – criteria provided in Directive 95/46/EC.

Directive 95/46/EC

When adopted in 1995, the Directive was built on early data protection instruments, including Convention 108 and the OECD Guidelines. Early experience with data protection in some Member States was also considered.

In addition to a broader requirement set forth in its Article 6(1)(a) that personal data must be processed 'fairly and lawfully', the Directive added a specific set of additional requirements, not yet present as such in either Convention 108 or the OECD Guidelines: the processing of personal data must be based on one of the six legal grounds specified in Article 7.

Implementation of the Directive; the ASNEF and FECEMD judgment[13]

The report of the Commission entitled 'Evaluation of the implementation of the Data Protection Directive'[14] underlines that the implementation of the provisions of the Directive in national law has sometimes been unsatisfactory. In the technical analysis of the transposition of the Directive in the Member States[15], the Commission gives further details on the implementation of Article 7. The analysis explains that while laws in most Member States set out the six legal grounds in relatively similar terms to the ones used in the Directive, the flexibility of these principles, in fact, has led to divergent applications.

It is particularly relevant given this context that in its judgment of 24 November 2011 in *ASNEF and FECEMD*, the ECJ held that Spain had not transposed correctly Article 7(f) of

[11] The draft text of the modernised Convention adopted by the T-PD plenary of November 2012 states that data processing can be carried out on the basis of consent of the data subject or on the basis 'of some legitimate basis laid down by law', similarly to the European Union Charter of Fundamental Rights mentioned below on page 8.

[12] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 11 July 2013.

[13] ECJ judgment of 24.11.2011 in cases C-468/10 and C-469/10 (*ASNEF and FECEMD*).

[14] See Annex 2 of the Impact Assessment to the Commission's data protection reform package, cited in footnote 6 above.

[15] Analysis and impact study on the implementation of Directive EC 95/46 in Member States. See http://ec.europa.eu/justice/policies/privacy/docs/lawreport/consultation/technical-annex_en.pdf.

the Directive, by requiring that - in the absence of the data subject's consent - any relevant data used should appear in public sources. The judgment also held that Article 7(f) has direct effect. The judgment limits the margin of discretion that Member States have in implementing Article 7(f). In particular, they must not overstep the fine line between clarification on the one hand, and setting additional requirements, which would amend the scope of Article 7(f) on the other hand.

The judgment, making it clear that Member States are not allowed to impose additional unilateral restrictions and requirements regarding the legal grounds for lawful data processing in their national laws, has significant consequences. National courts and other relevant bodies must interpret national provisions in light of this judgment and, if necessary, set aside any conflicting national rules and practices.

In light of the judgment, it is all the more important that a clear and common understanding be found by national data protection authorities ('DPA's) and/or European legislators on the applicability of Article 7(f). This should be done in a balanced way, without either unduly restricting or unduly broadening the scope of this provision.

The Charter of Fundamental Rights

Since the Lisbon Treaty entered into force on 1 December 2009, the European Union Charter of Fundamental Rights ('the Charter') enjoys 'the same legal value as the Treaties'.[16] The Charter enshrines the protection of personal data as a fundamental right under Article 8, which is distinct from the respect for private and family life under Article 7. Article 8 lays down the requirement for a legitimate basis for the processing. In particular, it provides that personal data must be processed 'on the basis of the consent of the person concerned or some other legitimate basis laid down by law'.[17] These provisions reinforce both the importance of the principle of lawfulness and the need for an adequate legal basis for the processing of personal data.

The proposed Data Protection Regulation

In the context of the data protection review process, the scope of the grounds for lawfulness under Article 7, and in particular, the scope of Article 7(f) is now subject to discussion.

Article 6 of the proposed Regulation lists the grounds for lawful processing of personal data. With some exceptions (as will be described further), the six available grounds remain largely unchanged from those currently provided in Article 7 of the Directive. The Commission has however proposed to provide further guidance in the form of delegated acts.

It is interesting to note that, in the context of the work in the relevant European Parliamentary Committee,[18] attempts were made to clarify the concept of legitimate interests in the proposed

[16] See Article 6(1) TEU.

[17] See Article 8(2) of the Charter.

[18] Draft Report of the Committee on Civil Liberties, Justice and Home Affairs (LIBE) on the Proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), dated 16.1.2013 ('Draft LIBE Committee Report').

Regulation itself. A list of cases was drafted in which the legitimate interests of the data controller as a rule would override the legitimate interests and fundamental rights and freedoms of the data subject, and a second list of cases in which this would be the other way around. These lists - laid down either in provisions or in recitals - provide relevant input to the assessment of the balance between the rights and interests of the controller and the data subject, and are taken into account in this Opinion.[19]

II.2. Role of concept

Legitimate interests of the controller: balancing test as a final option?

Article 7(f) is listed as the last option among six grounds allowing for the lawful processing of personal data. It calls for a balancing test: what is necessary for the legitimate interests of the controller (or third parties) must be balanced against the interests or fundamental rights and freedoms of the data subject. The outcome of the balancing test determines whether Article 7(f) may be relied upon as a legal ground for processing.

The open-ended nature of this provision raises many important questions regarding its exact scope and application, which will be analysed in turn in this Opinion. However, as will be explained below, it does not necessarily mean that this option should be seen as one that can only be used sparingly to fill in gaps for rare and unforeseen situations as ‘a last resort’, or as a last chance if no other grounds apply. Nor should it be seen as a preferred option and its use unduly extended because it would be considered as less constraining than the other grounds.

Instead, it may well be that Article 7(f) has its own natural field of relevance and that it can play a very useful role as a ground for lawful processing, provided that a number of key conditions are fulfilled.

Appropriate use of Article 7(f), in the right circumstances and subject to adequate safeguards, may also help prevent misuse of, and over-reliance on, other legal grounds.

The first five grounds of Article 7 rely on the data subject’s consent, contractual arrangement, legal obligation or other specifically identified rationale as ground for legitimacy. When processing is based on one of these five grounds, it is considered as *a priori* legitimate and therefore only subject to compliance with other applicable provisions of the law. There is in other words a presumption that the balance between the different rights and interests at stake – including those of the controller and the data subject - is satisfied - assuming, of course, that all other provisions of data protection law are complied with. Article 7(f) on the other hand requires a *specific* test, for cases that do not fit in the scenarios pre-defined under grounds (a) to (e). It ensures that, outside these scenarios, any processing has to meet the requirement of a balancing test, taking duly into account the interests and fundamental rights of the data subject.

This test may lead to the conclusion in certain cases that the balance weighs in favour of the interests and fundamental rights of the data subjects, and that consequently the processing

See, in particular, amendments 101 and 102. See also the amendments adopted by the Committee on 21.10.2013 in their final report ('Final LIBE Committee Report').

[19] See Section III.3.1, in particular, the bullet-points on pages 24-25 containing a non-exhaustive list of some of the most common contexts in which the issue of legitimate interest under Article 7(f) may arise.

activity cannot take place. On the other hand, an appropriate assessment of the balance under Article 7(f), often with an opportunity to opt-out of the processing, may in other cases be a valid alternative to inappropriate use of, for instance, the ground of 'consent' or 'necessity for the performance of a contract'. Considered in this way, Article 7(f) presents complementary safeguards - which require appropriate measures - compared to the other pre-determined grounds. It should thus not be considered as 'the weakest link' or an open door to legitimise all data processing activities which do not fall under any of the other legal grounds.

The Working Party reiterates that when interpreting the scope of Article 7(f), it aims at a balanced approach, which ensures the necessary flexibility for data controllers for situations where there is no undue impact on data subjects, while at the same time providing sufficient legal certainty and guarantees to data subjects that this open-ended provision will not be misused.

II.3. Related concepts

Relationship of Article 7(f) with other grounds for lawfulness

Article 7 starts with consent, and goes on to list the other grounds for lawfulness, including contracts and legal obligations, moving gradually to the legitimate interest test, which is listed as the last among the six available grounds. The order in which the legal grounds are listed under Article 7 has sometimes been interpreted as an indication of the respective importance of the different grounds. However, as already emphasised in the Working Party's Opinion on the notion of consent[20], the text of the Directive does not make a legal distinction between the six grounds and does not suggest that there is a hierarchy among them. There is not any indication that Article 7(f) should only be applied in exceptional cases and the text also does not otherwise suggest that the specific order of the six legal grounds would have any legally relevant effect. At the same time, the precise meaning of Article 7(f) and its relation with other grounds for lawfulness have long been rather unclear.

Against this background and considering the historical and cultural diversities and the open-ended language of the Directive, different approaches have developed: some Member States have tended to see Article 7(f) as a least preferred ground, which is meant to fill the gaps only in a few exceptional cases when none of the five other grounds could or would apply.[21] Other Member States, in contrast, see it only as one of six options, and one which is no more or no less important than the other options, and which may apply in a large number and large variety of situations, provided the necessary conditions are met.

Considering these diversities, and also in light of the ASNEF and FECEMD judgment, it is important to clarify the relationship of the 'legitimate interests' ground with the other grounds of lawfulness - e.g. in relation to consent, contracts, tasks of public interest - and also in relation to the right of the data subject to object. This may help better define the role and function of the legitimate interests ground and thus may contribute to legal certainty.

[20] See footnote 2 above.

[21] It should also be noted that the Draft LIBE Committee Report, in its Amendment 100 proposed to separate Article 7(f) from the rest of the legal grounds and also proposed additional requirements for the case when this legal ground is relied on, including more transparency and stronger accountability, as will be shown later.

It should also be noted that the legitimate interests ground, along with the other grounds apart from consent, requires a 'necessity' test. This strictly limits the context in which they each can apply. The European Court of Justice considered that ‘necessity’ is a concept which has its own independent meaning in Community law.[22] The European Court of Human Rights also provided helpful guidance.[23]

Moreover, having an appropriate legal ground does not relieve the data controller of its obligations under Article 6 with regard to fairness, lawfulness, necessity and proportionality, as well as data quality. For instance, even if the processing of personal data is based on the legitimate interests ground, or on the performance of a contract, this would not allow for the collection of data which is excessive in relation to the purpose specified.

Legitimate interests and other grounds of Article 7 are alternative grounds and thus, it is sufficient if only one of them applies. However, they come as cumulative not only with the requirements of Article 6, but also with all other data protection principles and requirements that may be applicable.

Other balancing tests

Article 7(f) is not the only balancing test foreseen in the Directive. For example, Article 9 calls for balancing the right to the protection of personal data and freedom of expression. This Article allows Member States to provide the necessary exemptions and derogations for the processing of personal data 'carried out solely for journalistic purposes or the purpose of artistic or literary expression' if these are 'necessary to reconcile the right to privacy with the rules governing freedom of expression'.

In addition, many other provisions of the Directive also require case-by-case analysis, balancing of interests and rights at stake, and a flexible multi-factor assessment. These include the provisions on necessity, proportionality, and purpose limitation, Article 13 exceptions, and scientific research, just to name a few.

Indeed, it appears that the Directive was designed to leave room for interpretation and balancing of interests. This was, of course, at least in part meant to leave further room for Member States for implementation into national law. However, in addition to this, the need for some flexibility also comes from the very nature of the right to the protection of personal data and the right to privacy. Indeed, these two rights, along with most (but not all) other fundamental rights, are considered relative, or qualified, human rights.[24] These types of rights

[22] Judgment of the European Court of Justice of 16 December 2008 in case C-524/06 (Heinz Huber v Bundesrepublik Deutschland), para 52: 'Consequently, having regard to the objective of ensuring an equivalent level of protection in all Member States, the concept of necessity laid down by Article 7(e) of Directive 95/46, the purpose of which is to delimit precisely one of the situations in which the processing of personal data is lawful, cannot have a meaning which varies between the Member States. It therefore follows that what is at issue is a concept which has its own independent meaning in Community law and which must be interpreted in a manner which fully reflects the objective of that directive, as laid down in Article 1(1) thereof.'

[23] Judgment of the European Court of Human Rights in case Silver & Others v United Kingdom of 25 March 1983, para 97 discussing the term 'necessary in a democratic society': 'the adjective "necessary" is not synonymous with "indispensable", neither has it the flexibility of such expressions as "admissible", "ordinary", "useful", "reasonable" or "desirable" ….'

[24] There are only a few human rights that cannot be balanced against the rights of others, or the interests of the wider community. These are known as absolute rights. These rights can never be limited or restricted, whatever

must always be interpreted in context. Subject to appropriate safeguards, they can be balanced against the rights of others. In some situations - and also subject to appropriate safeguards - they can also be restricted on public interest grounds.

II.4. Context and strategic consequences

Ensuring legitimacy but also flexibility: means for specification of Article 7(f)

The current text of Article 7(f) of the Directive is open-ended. This means that it can be relied upon in a wide range of situations, as long as its requirements, including the balancing test, are satisfied. However, such flexibility may also have negative implications. To prevent it from leading to inconsistent national application or lack of legal certainty, further guidance would play an important role.

The Commission foresees such guidance in the proposed Regulation in the form of delegated acts. Other options include providing clarifications and detailed provisions in the text of the proposed Regulation itself[25], and/or entrusting the European Data Protection Board ('EDPB') with the task of providing further guidance in this area.

Each of these options in turn, has benefits and drawbacks. If the assessment were to be made case by case without any further guidance, this would risk inconsistent application and lack of predictability, as it has been the case in the past.

On the other hand, providing, in the text of the proposed Regulation itself, for detailed and exhaustive lists of situations in which the legitimate interests of the controller as a rule prevail over the fundamental rights of the data subject or vice versa, could risk being misleading, unnecessarily prescriptive, or both.

These approaches could nevertheless inspire a balanced solution, providing for some more detail in the proposed Regulation itself, and further guidance in delegated acts or in EDPB guidance.[26]

The analysis in Chapter III aims to lay the groundwork for finding such an approach, neither too general so as to be meaningless, nor too specific so as to be overly rigid.

the circumstances – even in a state of war or emergency. One example is the right not to be tortured or treated in an inhuman or degrading way. It is never permissible to torture or treat someone in an inhuman or degrading way, regardless of the circumstances. Examples of non-absolute human rights include the right to respect for private and family life, the right to freedom of expression and the right to freedom of thought, conscience and religion.

[25] See Section II.1 Brief History, under *'The proposed Data Protection Regulation'* on pages 8-9.

[26] As to delegated acts and EDPB guidance, the Working Party's Opinion 08/2012 providing further input on the data protection reform discussions, adopted on 05.10.201 (WP199) expressed a strong preference for the latter (see p. 13-14).

III. Analysis of provisions

III.1. Overview of Article 7

Article 7 requires that personal data shall only be processed if at least one of the six legal grounds listed in that Article apply. Before analysing each of these grounds, this Section III.1 gives an overview of Article 7 and its relationship with Article 8 on special categories of data.

III.1.1. Consent or 'necessary for...'

A distinction can be made between the case when personal data are processed based on the data subject's unambiguous consent (Article 7(a)) and the remaining five cases (Article 7(b)-(f)). These five cases - briefly put – describe scenarios where processing may be necessary in a specific context, such as the performance of a contract with the data subject, compliance with a legal obligation imposed on the controller, etc.

In the first case, under Article 7(a), it is the data subjects themselves who authorise the processing of their personal data. It is up to them to decide whether to allow their data to be processed. At the same time, consent does not eliminate the need to respect the principles provided in Article 6[27]. In addition, consent still has to fulfil certain essential conditions to be legitimate, as explained in Opinion 15/2011 of the Working Party[28]. As the processing of the user's data is ultimately at his/her discretion, the emphasis is on the validity and the scope of the data subject's consent.

In other words, the first ground, Article 7(a), focuses on the self-determination of the data subject as a ground for legitimacy. All other grounds, in contrast, allow processing – subject to safeguards and measures – in situations where, irrespective of consent, it is appropriate and necessary to process the data within a certain context in pursuit of a specific legitimate interest.

Paragraphs (b), (c), (d) and (e) each specify a criterion making the processing legitimate:

(b) performance of a contract with the data subject;
(c) compliance with a legal obligation imposed on the controller;
(d) protection of the vital interests of the data subject;
(e) performance of a task carried out in the public interest.

Paragraph (f) is less specific and refers, more generally, to (any kind of) legitimate interest pursued by the controller (in any context). This general provision, however, is specifically made subject to an additional balancing test, which aims to protect the interests and rights of the data subjects, as will be shown below in Section III.2.

[27] Judgment of the Dutch Supreme Court of 9 September 2011 in case ECLI:NL:HR:2011:BQ8097, §3.3(e) as to the principle of proportionality. See also page 7 of the Working Party Opinion 15/2011 cited in footnote 2 above: '... obtaining consent does not negate the controller's obligations under Article 6 with regard to fairness, necessity and proportionality, as well as data quality. For instance, even if the processing of personal data is based on the consent of the user, this would not legitimise the collection of data which is excessive in relation to a particular purpose.'

[28] See pages 11-25 of Opinion 15/2011, cited in footnote 2 above.

The assessment of whether the criteria set out in Article 7 (a) - (f) have been fulfilled, is in all cases, initially made by the data controller, subject to applicable law and guidance on how the law should be applied. In the second instance, the legitimacy of the processing may be subject to further evaluation, and may possibly be challenged, by data subjects, other stakeholders, the data protection authorities, and ultimately decided on by the courts.

To complete this brief overview, it should be mentioned that, as will be discussed in Section III.3.6, at least in the cases referred to in paragraphs (e) and (f), the data subject can exercise the right to object as provided for in Article 14[29]. This will trigger a new evaluation of the interests at stake, or, in the case of direct marketing (Article 14(b)), will require the controller to stop the processing of personal data without any further evaluation.

III.1.2. Relationship with Article 8

Article 8 of the Directive regulates further the processing of certain special categories of personal data. It applies specifically to data 'revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life' (Article 8(1)), and to data 'relating to offences or criminal convictions' (Article 8(5)).

The processing of such data is in principle prohibited, subject to some exceptions. Article 8(2) provides for a number of exceptions from such prohibition, under paragraphs (a) through (e). Article 8(3) and (4) provides for further exceptions. Some of these provisions are similar - but not identical – to the provisions set forth in Article 7(a) through (f).

The specific conditions of Article 8, as well as the fact that some of the grounds listed in Article 7 resemble the conditions set forth in Article 8, raise the question of the relationship between the two provisions.

If Article 8 is designed as a *lex specialis*, it should be considered whether it excludes the applicability of Article 7 altogether. If so, it would mean that special categories of personal data can be processed without satisfying Article 7, provided one of the exceptions in Article 8 applies. It is, however, also possible that the relationship is more complex and Articles 7 and 8 should be applied cumulatively.[30]

Either way, it is clear that the policy objective is to provide additional protection for special categories of data. Therefore, the final outcome of the analysis should be equally clear: the application of Article 8, whether in itself or in a cumulative way with Article 7, aims at providing for a higher level of protection to special categories of data.

In practice, while in some cases Article 8 brings stricter requirements - such as 'explicit' consent in Article 8(2)(a), compared to 'unambiguous consent' in Article 7 - this is not true

[29] Further to Article 14(a), this right applies 'save where otherwise provided by national legislation'. For instance, in Sweden national law does not allow the possibility to object to a processing which is based on Article 7(e).

[30] Since Article 8 is set up as a *prohibition with exceptions*, these exceptions may be seen as requirements, which only limit the scope of the prohibition but do not, in and of themselves, provide a sufficient legal ground for the processing. In this reading, the applicability of Article 8 exceptions does not exclude the applicability of the requirements in Article 7, and the two, when appropriate, must be applied cumulatively.

for all provisions. Some exceptions foreseen by Article 8 do not appear equivalent or stricter than the grounds listed in Article 7. It would be inappropriate to conclude for instance that the fact that someone has made special categories of data manifestly public under Article 8(2)(e) would be - always and in and of itself - a sufficient condition to allow any type of data processing, without an assessment of the balance of interests and rights at stake as required in Article 7(f)[31].

In some situations, the fact that the data controller is a political party would also lift the prohibition on processing special categories of data under Article 8(2)(d). This, however, does not mean that any processing within the scope of that provision is necessarily lawful. This has to be assessed separately and the controller may have to demonstrate, for instance, that the data processing is necessary for the performance of a contract (Article 7(b)), or that its legitimate interest under Article 7(f) prevails. In this latter case, the balancing test under Article 7(f) needs to be conducted, after it has been assessed that the data controller complies with Article 8 requirements.

In a similar way, the mere fact that ‘the processing of data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services’, and those data are processed under an obligation of secrecy - all as mentioned in Article 8(3) - implies that such processing of sensitive data is *exempted from the prohibition* of Article 8(1). This is however not necessarily sufficient to also ensure lawfulness under Article 7, and will require a legal ground such as a contract with the patient under Article 7(b), a legal obligation under Article 7(c), performance of a task carried out in the public interest under Article 7(e) or an assessment under Article 7(f).

In conclusion, the Working Party considers that an analysis has to be made on a case-by-case basis whether Article 8 in itself provides for stricter and sufficient conditions[32], or whether a cumulative application of both Article 8 and 7 is required to ensure full protection of data subjects. In no case shall the result of the examination lead to a lower protection for special categories of data[33].

This also means that a controller processing special categories of data may never invoke *solely* a legal ground under Article 7 to legitimise a data processing activity. Where applicable, Article 7 will not *prevail* but always apply in a *cumulative* way with Article 8 to ensure that all relevant safeguards and measures are complied with. This will be all the more relevant in case Member States decide to add additional exemptions to those of Article 8, as foreseen in Article 8(4).

[31] Moreover, Article 8(2)(e) should not be interpreted *a contrario* as meaning that, when the data made public by the data subject are not sensitive, they can be processed without any additional condition. Publicly available data are still personal data subject to data protection requirements, including compliance with Article 7, irrespective whether or not they are sensitive data.

[32] See the analysis made in the WADA Opinion of the Working Party, point 3.3, which takes into consideration both Article 7 and Article 8 of the Directive: Second opinion 4/2009 on the World Anti-Doping Agency (WADA) International Standard for the Protection of Privacy and Personal Information, on related provisions of the WADA Code and on other privacy issues in the context of the fight against doping in sport by WADA and (national) anti-doping organizations, adopted on 06.04.2009 (WP162).

[33] It goes without saying that also in the case of application of Article 8 the respect for the other provisions of the Directive, including Article 6, must be ensured.

III.2. Article 7(a)-(e)

This Section III.2 provides a brief overview of each of the legal grounds in Article 7(a) through (e) of the Directive, before the Opinion focuses, in Section III.3, on Article 7(f). This analysis will also highlight some of the most common interfaces between these legal grounds, for instance involving 'contract', 'legal obligation' and 'legitimate interest', depending upon the particular context and the facts of the case.

III.2.1. Consent

Consent as a legal ground has been analysed in Opinion 15/2011 of the Working Party on the definition of consent. The main findings of the Opinion are that consent is one of several legal grounds to process personal data, rather than the main ground. It has an important role, but this does not exclude the possibility, depending on the context, that other legal grounds may be more appropriate either from the controller's or from the data subject's perspective. If it is correctly used, consent is a tool giving the data subject control over the processing of his data. If incorrectly used, the data subject's control becomes illusory and consent constitutes an inappropriate basis for processing.

Among its recommendations, the Working Party insisted on the need to clarify what 'unambiguous consent' means: "Clarification should aim at emphasizing that unambiguous consent requires the use of mechanisms that leave no doubt of the data subject's intention to consent. At the same time it should be made clear that the use of default options which the data subject is required to modify in order to reject the processing (consent based on silence) does not in itself constitute unambiguous consent. This is especially true in the on-line environment." [34] It also required data controllers to put in place mechanisms to demonstrate consent (within a general accountability obligation) and requested the legislator to add an explicit requirement regarding the quality and accessibility of the information forming the basis for consent.

III.2.2. Contract

Article 7(b) provides a legal ground in situations where 'processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract'. This covers two different scenarios.

i) First, the provision covers situations where processing is necessary for the performance of the contract to which the data subject is a party. This may include, for example, processing the address of the data subject so that goods purchased online can be delivered, or processing credit card details in order to effect payment. In the employment context this ground may allow, for example, processing salary information and bank account details so that salaries could be paid.

   The provision must be interpreted strictly and does not cover situations where the processing is not genuinely *necessary* for the performance of a contract, but rather unilaterally imposed on the data subject by the controller. Also the fact that some data

[34] See page 36 of the Working Party's Opinion 15/2011 on the definition of consent.

processing is covered by a contract does not automatically mean that the processing is necessary for its performance. For example, Article 7(b) is not a suitable legal ground for building a profile of the user's tastes and lifestyle choices based on his click-stream on a website and the items purchased. This is because the data controller has not been contracted to carry out profiling, but rather to deliver particular goods and services, for example. Even if these processing activities are specifically mentioned in the small print of the contract, this fact alone does not make them 'necessary' for the performance of the contract.

There is a clear connection here between the assessment of necessity and compliance with the purpose limitation principle. It is important to determine the exact *rationale* of the contract, i.e. its substance and fundamental objective, as it is against this that it will be tested whether the data processing is necessary for its performance.

In some borderline situations it may be arguable, or may require more specific fact-finding to determine whether processing is necessary for the performance of the contract. For example, the establishment of a company-wide internal employee contact database containing the name, business address, telephone number and email address of all employees, to enable employees reach their colleagues, may in certain situations be considered as necessary for the performance of a contract under Article 7(b) but it could also be lawful under Article 7(f) if the overriding interest of the controller is demonstrated and all appropriate measures are taken, including for instance adequate consultation of employees' representatives.

Other cases, for example, electronic monitoring of employee internet, email or telephone use, or video-surveillance of employees more clearly constitute processing that is likely to go beyond what is necessary for the performance of an employment contract, although here also this may depend on the nature of the employment. Fraud prevention - which may include, among others, monitoring and profiling customers - is another typical area, which is likely to be considered as going beyond what is necessary for the performance of a contract. Such processing could then still be legitimate under another ground of Article 7, for instance, consent where appropriate, a legal obligation or the legitimate interest of the controller (Article 7(a), (c) or (f)).[35] In the latter case, the processing should be subject to additional safeguards and measures to adequately protect the interests or rights and freedoms of data subjects.

Article 7(b) only applies to what is necessary for the *performance* of a contract. It does not apply to all further actions triggered by non-compliance or to all other incidents in the execution of a contract. As long as processing covers the normal execution of a contract, it could fall within Article 7(b). If there is an incident in the performance, which gives rise to a conflict, the processing of data may take a different course.

[35] Another example of multiple legal grounds can be found in the Working Party's Opinion 15/2011 on the definition of consent (cited in footnote 2). To buy a car, the data controller may be entitled to process personal data according to different purposes and on the basis of different grounds:
- Data necessary to buy the car: Article 7(b),
- To process the car's papers: Article 7(c),
- For client management services (e.g. to have the car serviced in different affiliate companies within the EU): Article 7(f),
- To transfer the data to third parties for their own marketing activities: Article 7(a).

Processing of basic information of the data subject, such as name, address and reference to outstanding contractual obligations, to send formal reminders should still be considered as falling within the processing of data necessary for the performance of a contract. With regard to more elaborated processing of data, which may or may not involve third parties, such as external debt collection, or taking a customer who has failed to pay for a service to court, it could be argued that such processing does not take place anymore under the ‘normal’ performance of the contract and would therefore not fall under Article 7(b). However, this would not make the processing illegitimate as such: the controller has a legitimate interest in seeking remedies to ensure that his contractual rights are respected. Other legal grounds, such as Article 7(f) could be relied upon, subject to adequate safeguards and measures, and meeting the balancing test.[36]

ii) Second, Article 7(b) also covers processing that takes place *prior* to entering into a contract. This covers pre-contractual relations, provided that steps are taken at the request of the data subject, rather than at the initiative of the controller or any third party. For example, if an individual requests a retailer to send her an offer for a product, processing for these purposes, such as keeping address details and information on what has been requested, for a limited period of time, will be appropriate under this legal ground. Similarly, if an individual requests a quote from an insurer for his car, the insurer may process the necessary data, for example, the make and age of the car, and other relevant and proportionate data, in order to prepare the quote.

However, detailed background checks, for example, processing the data of medical check-ups before an insurance company provides health insurance or life insurance to an applicant would not be considered as necessary steps made at the request of the data subject. Credit reference checks prior to the grant of a loan are also not made at the *request* of the data subject under Article 7(b), but rather, under Article 7(f), or under Article 7(c) in compliance with a legal obligation of banks to consult an official list of registered debtors.

Direct marketing at the initiative of the retailer/controller will also not be possible on this ground. In some cases, Article 7(f) could provide an appropriate legal ground instead of Article 7(b), subject to adequate safeguards and measures, and meeting the balancing test. In other cases including those involving extensive profiling, data-sharing, online direct marketing or behavioural advertisement, consent under Article 7(a) should be considered, as follows from the analysis below.[37]

[36] With regard to special categories of data, Article 8(1)(e) - 'necessary for the establishment, exercise or defence of legal claims' - may also need to be taken into account.

[37] See Section III.3.6 (b) under heading ' Illustration: the evolution in the approach to direct marketing' on pages 45-46.

III.2.3. Legal obligation

Article 7(c) provides a legal ground in situations where ‘processing is necessary for compliance with a legal obligation to which the controller is subject’. This may be the case, for example, where employers must report salary data of their employees to social security or tax authorities or where financial institutions are obliged to report certain suspicious transactions to the competent authorities under anti-money-laundering rules. It could also be an obligation to which a public authority is subject, as nothing limits the application of Article 7(c) to the private or public sector. This would apply for instance to the collection of data by a local authority for the handling of penalties for parking at unauthorised locations.

Article 7(c) presents similarities with Article 7(e), as a public interest task is often based on, or derived from, a legal provision. The scope of Article 7(c) is however strictly delimited.

For Article 7(c) to apply, the obligation must be imposed by law (and not for instance by a contractual arrangement). The law must fulfil all relevant conditions to make the obligation valid and binding, and must also comply with data protection law, including the requirement of necessity, proportionality[38] and purpose limitation.

It is also important to emphasise that Article 7(c) refers to the laws of the European Union or of a Member State. Obligations under the laws of third countries (such as, for example, the obligation to set up whistleblowing schemes under the Sarbanes–Oxley Act of 2002 in the United States) are not covered by this ground. To be valid, a legal obligation of a third country would need to be officially recognised and integrated in the legal order of the Member State concerned, for instance under the form of an international agreement[39]. On the other hand, the need to comply with a foreign obligation may represent a legitimate interest of the controller, but only subject to the balancing test of Article 7(f), and provided that adequate safeguards are put in place such as those approved by the competent data protection authority.

The controller must not have a choice whether or not to fulfil the obligation. Voluntary unilateral engagements and public-private partnerships processing data beyond what is required by law are thus not covered under Article 7(c). For example, if - without a clear and specific legal obligation to do so – an Internet service provider decides to monitor its users in an effort to combat illegal downloading, Article 7(c) will not be an appropriate legal ground for this purpose.

Further, the legal obligation itself must be sufficiently clear as to the processing of personal data it requires. Thus, Article 7(c) applies on the basis of legal provisions referring explicitly to the nature and object of the processing. The controller should not have an undue degree of discretion on how to comply with the legal obligation.

[38] See also the Working Party's Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector, adopted on 27.02.2014 (WP 211).

[39] See on this issue Section 4.2.2 of the Working Party's Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), adopted on 20.11.2006 (WP128) and Working Party's Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime, adopted on 01.02.2006 (WP 117).

The legislation may in some cases set only a general objective, while more specific obligations are imposed at a different level, for instance, either in secondary legislation or by a binding decision of a public authority in a concrete case. This may also lead to legal obligations under Article 7(c) provided that the nature and object of the processing is well defined and subject to an adequate legal basis.

However, this is different if a regulatory authority would only provide general policy guidelines and conditions under which it might consider using its enforcement powers (e.g. regulatory guidance to financial institutions on certain standards of due diligence). In such cases, the processing activities should be assessed under Article 7(f) and only be considered legitimate subject to the additional balancing test.[40]

As a general remark, it should be noted that some processing activities may appear to be close to falling under Article 7(c), or to Article 7(b), without fully meeting the criteria for these grounds to apply. This does not mean that such processing is always necessarily unlawful: it may sometimes be legitimate, but rather under Article 7(f), subject to the additional balancing test.

III.2.4. Vital interest

Article 7(d) provides for a legal ground in situations where ‘processing is necessary in order to protect the vital interests of the data subject’. This wording is different to the language used in Article 8(2)(c) which is more specific and refers to situations where ‘processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent’.

Both provisions nevertheless appear to suggest that this legal ground should have a limited application. First, the phrase ‘vital interest’ appears to limit the application of this ground to questions of life and death, or at the very least, threats that pose a risk of injury or other damage to the health of the data subject (or in case of Article 8(2)(c) also of another person).

Recital 31 confirms that the objective of this legal ground is to ‘protect an interest which is essential to the data subject’s life’. However, the Directive does not state precisely whether the threat must be immediate. This raises issues concerning the scope of the collection of data, for instance as a preventive measure or on a wide scale, such as the collection of airline passengers’ data where a risk of epidemiological disease or a security incident has been identified.

The Working Party considers that a restrictive interpretation must be given to this provision, consistent with the spirit of Article 8. Although Article 7(d) does not specifically limit the use of this ground to situations when consent cannot be used as a legal ground, for the reasons specified in Article 8(2)(c), it is reasonable to assume that in situations where there is a possibility and need to request a valid consent, consent should indeed be sought whenever practicable. This would also limit the application of this provision to a case by case analysis and cannot normally be used to legitimise any massive collection or processing of personal

[40] Guidance by a regulatory authority may still play a role in assessing the controller's legitimate interest (see Section III.3.4 under point (a) notably on page 36).

data. In case where this would be necessary, Article 7(c) or (e) would be more appropriate grounds for processing.

III.2.5. Public task

Article 7(e) provides a legal ground in situations where ‘processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed’.

It is important to note that just like Article 7(c), Article 7(e) refers to the public interest of the European Union or of a Member State. Similarly, 'official authority' refers to an authority granted by the European Union or a Member State. In other words, tasks carried out in the public interest of a third country or in the exercise of an official authority vested by virtue of foreign law do not fall within the scope of this provision.[41]

Article 7(e) covers two situations and is relevant both to the public and the private sector. First, it covers situations where the controller itself has an official authority or a public interest task (but not necessarily also a legal obligation to process data) and the processing is necessary for exercising that authority or performing that task. For example, a tax authority may collect and process an individual’s tax return in order to establish and verify the amount of tax to be paid. Or a professional association such as a bar association or a chamber of medical professionals vested with an official authority to do so may carry out disciplinary procedures against some of their members. Yet another example could be a local government body, such as a municipal authority, entrusted with the task of running a library service, a school, or a local swimming pool.

Second, Article 7(e) also covers situations where the controller does not have an official authority, but is requested by a third party having such authority to disclose data. For example, an officer of a public body competent for investigating crime may ask the controller for cooperation in an on-going investigation rather than ordering the controller to comply with a specific request to cooperate. Article 7(e) may furthermore cover situations where the controller proactively discloses data to a third party having such an official authority. This may be the case, for example, where a controller notices that a criminal offence has been committed, and provides this information to the competent law enforcement authorities at his own initiative.

Unlike in the case of Article 7(c), there is no requirement for the controller to act under a legal obligation. Using the example above, a controller accidentally noticing that theft or fraud has been committed, may not be under a legal obligation to report this to the police but may, in appropriate cases, nevertheless do so voluntarily on the basis of Article 7(e).

However, the processing must be 'necessary for the performance of a task carried out in the public interest'. Alternatively, either the controller or the third party to whom the controller discloses the data must be vested with an official authority and the data processing must be

[41] See Section 2.4 of the Working Party's working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, adopted on 25 November 2005 (WP114) for a similar interpretation of the notion of 'important public interest grounds' in Article 26(1)(d).

necessary to exercise the authority.[42] It is also important to emphasise that this official authority or public task will have been typically attributed in statutory laws or other legal regulations. If the processing implies an invasion of privacy or if this is otherwise required under national law to ensure the protection of the individuals concerned, the legal basis should be specific and precise enough in framing the kind of data processing that may be allowed.

These situations are becoming increasingly common, also outside the confines of the public sector, considering the trend to outsource governmental tasks to entities in the private sector. This can be the case, for instance, in the context of processing activities in the transport or health sector (e.g. epidemiological studies, research). This ground could also be invoked in a law enforcement context as already suggested in the examples above. However, the extent to which a private company may be allowed to cooperate with law enforcement authorities, for instance in the fight against fraud or illegal content on the Internet, requires analysis not only under Article 7, but also under Article 6, considering purpose limitation, lawfulness and fairness requirements[43].

Article 7(e) has potentially a very broad scope of application, which pleads for a strict interpretation and a clear identification, on a case by case basis, of the public interest at stake and the official authority justifying the processing. This broad scope also explains why, just like for Article 7(f), a right to object has been foreseen in Article 14 when processing is based on Article 7(e)[44]. Similar additional safeguards and measures may thus apply in both cases [45].

In that sense, Article 7(e) has similarities with Article 7(f), and in some contexts, especially for public authorities, Article 7(e) may replace Article 7(f).

When assessing the scope of these provisions to public sector bodies, especially in light of the proposed changes in the data protection legal framework, it is useful to note that the current text of Regulation 45/2001,[46] which contains the data protection rules applicable to European Union institutions and bodies, has no provision comparable to Article 7(f).

However, Recital 27 of this Regulation provides that ‘processing of personal data for the performance of tasks carried out *in the public interest* by the Community institutions and bodies includes the processing of personal data necessary for the management and functioning of those institutions and bodies.’ This provision thus allows data processing on a broadly interpreted ‘public task’ ground in a large variety of cases, which could have otherwise been covered by a provision similar to Article 7(f). Video-surveillance of premises for security

[42] In other words, in these cases the public relevance of the tasks, and the correspondent responsibility will continue to be present even if the exercise of the task has been moved to other entities, including private ones.

[43] See in that sense the Working Party's Opinion on SWIFT (cited in footnote 39 above), the Working Party's Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data, adopted on 13.06.2003 (WP78) and the Working Document on data protection issues related to intellectual property rights, adopted on 18.01.2005 (WP 104).

[44] As mentioned above, this possibility to object does not exist in some Member States (e.g. Sweden) for processing of data based on Article 7(e).

[45] As will be shown below, the Draft LIBE Committee Report suggested further safeguards – in particular, enhanced transparency – for the case when Article 7(f) applies.

[46] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. (OJ L 8, 12.1.2001, p. 1).

purposes, electronic monitoring of email traffic, or staff evaluations are just a few examples of what may come under this broadly interpreted provision of 'tasks carried out in the public interest'.

Looking ahead, it is also important to consider that the proposed Regulation, in Article 6(1)(f) specifically provides that the legitimate interest ground 'shall not apply to processing carried out by public authorities in the performance of their tasks'. If this provision is enacted and will be interpreted broadly, so as to altogether exclude public authorities from using legitimate interest as a legal ground, then the ‘public interest’ and ‘official authority’ grounds of Article 7(e) would need to be interpreted in a way as to allow public authorities some degree of flexibility, at least to ensure their proper management and functioning, just the way Regulation 45/2001 is interpreted now.

Alternatively, the referred last sentence of 6(1)(f) of the proposed Regulation could be interpreted in a way, so as not to altogether exclude public authorities from using legitimate interest as a legal ground. In this case, the terms 'processing carried out by public authorities in the performance of their tasks' in the proposed Article 6(1)(f) should be interpreted narrowly. This narrow interpretation would mean that processing for proper management and functioning of these public authorities would fall outside the scope of 'processing carried out by public authorities in the performance of their tasks'. As a result, processing for proper management and functioning of these public authorities could still be possible under the legitimate interest ground.

III.3. Article 7(f): legitimate interests

Article 7(f)[47] calls for a balancing test: the legitimate interests of the controller (or third parties) must be balanced against the interests or fundamental rights and freedoms of the data subject. The outcome of the balancing test largely determines whether Article 7(f) may be relied upon as a legal ground for processing.

It is worth mentioning already at this stage that this is not a straightforward balancing test which would simply consist of weighing two easily quantifiable and easily comparable 'weights' against each other. Rather, as will be described below in more detail, carrying out the balancing test may require a complex assessment taking into account a number of factors. To help structure and simplify the assessment, we have broken down the process into several steps to help ensure that the balancing test can be carried out effectively.

Section III.3.1 first examines one side of the balance: what constitutes 'legitimate interest pursued by the controller or by a third party to whom the data are disclosed'. In Section III.3.2, we examine the other side of the balance, what constitutes 'interests or fundamental rights and freedoms of the data subject which require protection under Article 1(1)'.

In Sections III.3.3 and III.3.4, guidance is provided on how to carry out the balancing test. Section III.3.3 gives a general introduction with the help of three different scenarios. Following this introduction, Section III.3.4 outlines the most important considerations that must be taken into account when carrying out the balancing test, including the safeguards and

[47] For a full text of Article 7(f) see page 4 above.

measures provided by the data controller.

In Sections III.3.5 and III.3.6, we will finally also look into some particular mechanisms, such as accountability, transparency and the right to object, that may help ensure - and further enhance – an appropriate balance of the various interests that may be at stake.

III.3.1. Legitimate interests of the controller (or third parties)

The concept of 'interest'

The concept of 'interest' is closely related to, but distinct from, the concept of 'purpose' mentioned in Article 6 of the Directive. In data protection discourse, 'purpose' is the specific reason why the data are processed: the aim or intention of the data processing. An interest, on the other hand, is the broader stake that a controller may have in the processing, or the benefit that the controller derives - or that society might derive - from the processing.

For instance, a company may have an *interest* in ensuring the health and safety of its staff working at its nuclear power-plant. Related to this, the company may have as a *purpose* the implementation of specific access control procedures which justifies the processing of certain specified personal data in order to help ensure the health and safety of staff.

An interest must be sufficiently clearly articulated to allow the balancing test to be carried out against the interests and fundamental rights of the data subject. Moreover, the interest at stake must also be 'pursued by the controller'. This requires a real and present interest, something that corresponds with current activities or benefits that are expected in the very near future. In other words, interests that are too vague or speculative will not be sufficient.

The nature of the interest may vary. Some interests may be compelling and beneficial to society at large, such as the interest of the press to publish information about government corruption or the interest in carrying out scientific research (subject to appropriate safeguards). Other interests may be less pressing for society as a whole, or at any rate, the impact of their pursuit on society may be more mixed or controversial. This may, for example, apply to the economic interest of a company to learn as much as possible about its potential customers so that it can better target advertisement about its products or services.

What makes an interest 'legitimate' or 'illegitimate'?

The objective of this question is to identify the threshold for what constitutes a legitimate interest. If the data controller's interest is illegitimate, the balancing test will not come into play as the initial threshold for the use of Article 7(f) will not have been reached.

In the view of the Working Party, the notion of legitimate interest could include a broad range of interests, whether trivial or very compelling, straightforward or more controversial. It will then be in a second step, when it comes to balancing these interests against the interests and fundamental rights of the data subjects, that a more restricted approach and more substantive analysis should be taken.

The following is a non-exhaustive list of some of the most common contexts in which the issue of legitimate interest in the meaning of Article 7(f) may arise. It is presented here without prejudice to whether the interests of the controller will ultimately prevail over the interests and rights of the data subjects when the balancing is carried out.

- exercise of the right to freedom of expression or information, including in the media and the arts
- conventional direct marketing and other forms of marketing or advertisement
- unsolicited non-commercial messages, including for political campaigns or charitable fundraising
- enforcement of legal claims including debt collection via out-of-court procedures
- prevention of fraud, misuse of services, or money laundering
- employee monitoring for safety or management purposes
- whistle-blowing schemes
- physical security, IT and network security
- processing for historical, scientific or statistical purposes
- processing for research purposes (including marketing research)

Accordingly, an interest can be considered as legitimate as long as the controller can pursue this interest in a way that is in accordance with data protection and other laws. In other words, a legitimate interest must be 'acceptable under the law'[48].

In order to be relevant under Article 7(f), a 'legitimate interest' must therefore:

- be lawful (i.e. in accordance with applicable EU and national law);
- be sufficiently clearly articulated to allow the balancing test to be carried out against the interests and fundamental rights of the data subject (i.e. sufficiently specific);
- represent a real and present interest (i.e. not be speculative).

The fact that the controller has such a legitimate interest in the processing of certain data does not mean that it can necessarily rely on Article 7(f) as a legal ground for the processing. The legitimacy of the data controller's interest is just a starting point, one of the elements that need to be analysed under Article 7(f). Whether Article 7(f) can be relied on will depend on the outcome of the balancing test that follows.

To illustrate: controllers may have a legitimate interest in getting to know their customers' preferences so as to enable them to better personalise their offers, and ultimately, offer products and services that better meet the needs and desires of the customers. In light of this, Article 7(f) may be an appropriate legal ground to be used for some types of marketing

[48] The observations about the nature of 'legitimacy' in Section III.1.3 of the Working Party's Opinion 3/2013 on purpose limitation (cited in footnote 9 above) also apply here *mutatis mutandis*. As in that Opinion on pages 19-20, 'the notion of 'law' is used here in the broadest sense. This includes other applicable laws such as employment, contract, or consumer protection law. Further, the notion of law 'includes all forms of written and common law, primary and secondary legislation, municipal decrees, judicial precedents, constitutional principles, fundamental rights, other legal principles, as well as jurisprudence, as such 'law' would be interpreted and taken into account by competent courts. Within the confines of law, other elements such as customs, codes of conduct, codes of ethics, contractual arrangements, and the general context and facts of the case, may also be considered when determining whether a particular purpose is legitimate. This will include the nature of the underlying relationship between the controller and the data subjects, whether it be commercial or otherwise.' Further, what can be considered as a legitimate interest 'can also change over time, depending on scientific and technological developments, and changes in society and cultural attitudes.'

activities, on-line and off-line, provided that appropriate safeguards are in place (including, among others, a workable mechanism to allow objecting to such a processing under Article 14(b), as will be shown in Section III.3.6 *The right to object and beyond*).

However, this does not mean that controllers would be able to rely on Article 7(f) to unduly monitor the on-line or off-line activities of their customers, combine vast amounts of data about them from different sources that were initially collected in other contexts and for different purposes, and create - and, for example, with the intermediary of data brokers, also trade in - complex profiles of the customers' personalities and preferences without their knowledge, a workable mechanism to object, let alone informed consent. Such a profiling activity is likely to present a significant intrusion into the privacy of the customer, and when this is so, the controller's interest would be overridden by the interests and rights of the data subject.[49]

As another example, in its opinion on SWIFT[50], although the Working Party acknowledged the legitimate interest of the company in complying with the subpoenas under US law, to avoid the risk of being sanctioned by US authorities, it concluded that Article 7(f) could not be relied on. The Working Party considered in particular that because of the far reaching effects on individuals of the processing of data in a ‘hidden, systematic, massive and long term manner’, ‘the interests (f)or fundamental rights and freedoms of the numerous data subjects override SWIFT’s interest not to be sanctioned by the US for eventual non-compliance with the subpoenas’.

As will be shown later, if the interest pursued by the controller is not compelling, the interests and rights of the data subject are more likely to override the legitimate - but less significant - interests of the controller. At the same time, this does not mean that less compelling interests of the controller cannot sometimes override the interests and rights of the data subjects: this typically happens when the impact of the processing on the data subjects is also less significant.

Legitimate interest in the public sector

The current text of the Directive does not specifically exclude controllers that are public authorities from processing data using Article 7(f) as a legal ground for processing[51].

However, the proposed Regulation[52] excludes this possibility for 'processing carried out by public authorities in the performance of their tasks'.

[49] The issue of tracking technologies and the role of consent under Article 5(3) of the e-Privacy Directive will be discussed separately. See Section III.3.6 (b) under heading 'Illustration: the evolution in the approach to direct marketing'.

[50] See Section 4.2.3 of the Opinion already cited in footnote 39 above. The legitimate interest of the controller in this case was also linked to the public interest of a third country, which could not be accommodated under Directive 95/46/EC.

[51] Originally the first Commission Proposal for the Directive covered separately data processing in the private sector and processing activities of the public sector. This formal distinction between the rules applying to the public sector and the private sector was dropped in the Amended Proposal. This may also have led to diversities in interpretation and implementation by the various Member States.

[52] See Article 6(1)(f) of the proposed Regulation.

The proposed legislative change highlights the importance of the general principle that public authorities, as a rule, should only process data in performance of their tasks if they have appropriate authorisation by law to do so. Adherence to this principle is particularly important - and clearly required by the case law of the European Court of Human Rights - in cases where the privacy of the data subjects is at stake and the activities of the public authority would interfere with such privacy.

Sufficiently *detailed and specific* authorisation by law is therefore required - also under the current Directive - in case the processing by public authorities interferes with the privacy of the data subjects. This may either take the form of a specific legal obligation to process data, which can satisfy Article 7(c), or a specific authorisation (but not necessarily an obligation) to process data, which can meet the requirements of Article 7(e) or (f).[53]

Legitimate interests of third parties

The current text of the Directive does not only refer to the 'legitimate interests pursued by the controller' but also allows Article 7(f) to be used when the legitimate interest is pursued by 'the third party or parties to whom the data are disclosed'[54]. The following examples illustrate some of the contexts where this provision may apply.

Publication of data for purposes of transparency and accountability. One important context where Article 7(f) may be relevant is the case of publication of data for purposes of transparency and accountability (for example, the salaries of top management in a company). In this case it can be considered that the public disclosure is done primarily not in the interest of the controller who publishes the data, but rather, in the interest of other stakeholders, such as employees or journalists, or the general public, to whom the data are disclosed.

From a data protection and privacy perspective, and to ensure legal certainty, in general, it is advisable that personal data be disclosed to the public on the basis of a law allowing and - when appropriate - clearly specifying the data to be published, the purposes of the publication and any necessary safeguards.[55] This also means that it may be preferable that Article 7(c), rather than Article 7(f) be used as a legal basis when personal data are disclosed for purposes of transparency and accountability[56].

[53] In this respect, see also Section III.2.5 above on public tasks (pages 21-23) as well as the discussions below under the heading *Legitimate interests of third parties* (on pages 27-28). See also reflections on the limits of 'private enforcement' of the law on page 35 under the heading 'public interests/the interests of the wider community'. In all these situations, it is particularly important to ensure that the limits of Article 7(f) and also 7(e) are fully respected.

[54] The proposed Regulation aims at limiting the use of this ground to 'legitimate interests pursued by a controller. It is not clear from the text alone whether the proposed language means a mere simplification of the text or whether its intention is to exclude situations where a controller might disclose data in the legitimate interests of others. This text is however not definitive. The interest of third parties was for instance reintroduced in the Final LIBE Committee Report on the occasion of the vote on compromised amendments by the LIBE Committee of the European Parliament on 21 October 2013. See amendment 100 on Article 6. Reintroduction of third parties into the Proposal is supported by the Working Party on grounds that its use may continue to be appropriate in some situations, including the ones described below.

[55] This best practice recommendation should not prejudice national legal rules on transparency and public access to documents.

[56] Indeed, in some Member States different rules have to be complied with in respect of processing carried out by public and private parties. For example, according to the Italian Data Protection Code the dissemination of personal data by a public body shall only be permitted if it is provided for by a law or regulation (Section 19.3).

However, in the absence of a specific legal obligation or permission to publish data, it would nevertheless be possible to disclose personal data to relevant stakeholders. In appropriate cases, it would also be possible to publish personal data for purposes of transparency and accountability.

In both cases - i.e. irrespective of whether personal data are disclosed on the basis of a law allowing so or not - disclosure directly depends on the result of the Article 7(f) balancing test and the implementation of appropriate safeguards and measures.[57]

In addition, further use for further transparency of already released personal data (for instance, re-publication of the data by the press, or further dissemination of the originally published dataset in a more innovative or user-friendly way by an NGO), may also be desirable. Whether such re-publication and re-use is possible, will also depend on the outcome of the balancing test, which should take into account, among others, the nature of the information and the effect of the re-publication or re-use on the individuals.[58]

Historical or other kinds of scientific research. Another important context where disclosure in the legitimate interests of third parties may be relevant is historical or other kinds of scientific research, particularly where access is required to certain databases. The Directive provides specific recognition of such activities, subject to appropriate safeguards and measures[59], but it should not be forgotten that the legitimate ground for these activities will often be a well-considered use of Article 7(f).[60]

General public interest or third party's interest. Finally, the legitimate interest of third parties may also be relevant in a different way. This is the case where a controller - sometimes encouraged by public authorities - is pursuing an interest that corresponds with a general public interest or a third party's interest. This may include situations where a controller goes beyond its specific legal obligations set in laws and regulations to assist law enforcement or private stakeholders in their efforts to combat illegal activities, such as money laundering,

[57] As explained in the Working Party's Opinion 06/2013 on open data (see page 9 of that Opinion, cited in footnote 88 below), 'any national practice or national legislation with regard to transparency must comply with Article 8 of the ECHR and Articles 7 and 8 of the EU Charter. This implies, as the European Court of Justice held in the *Österreichischer Rundfunk* and *Schecke* rulings, that it should be ascertained that the disclosure is necessary for and proportionate to the legitimate aim pursued by the law.' See ECJ 20 May 2003, Rundfunk, Joined Cases C-465/00, C-138/01 and C-139/01 and ECJ 9 November 2010, Volker und Markus Schecke, Joined Cases C-92/09 and C-93/09.

[58] Purpose limitation is also an important consideration here. On page 19 of the Working Party's Opinion 06/2013 on open data (cited in footnote 88 below), the WP29 recommends 'that any legislation calling for public access to data clearly specify the purposes for disclosing personal data. If this is not done, or only done in vague and broad terms, legal certainty and predictability will suffer. In particular, with regard to any request for re-use, it will be very difficult for the public sector body and potential re-users concerned to determine, what were the intended initial purposes of the publication, and subsequently, what further purposes would be compatible with these initial purposes. As it was already mentioned, even if personal data are published on the Internet, it is not to be assumed that they can be further processed for any possible purposes.'

[59] See e.g. Article 6(1)(b) and (e).

[60] As explained in Opinion 3/2013 of the Working Party on Purpose Limitation (cited in footnote 9 above), further use of data for secondary purposes should be subject to a double test. First, it should be ensured that the data will be used for compatible purposes. Second, it should be ensured that there will be an appropriate legal basis under Article 7 for the processing.

child grooming, or illegal file sharing online. In these situations, however, it is particularly important to ensure that the limits of Article 7(f) are fully respected.[61]

Processing must be necessary for the purpose(s) intended

Finally, the processing of personal data must also be 'necessary for the purpose of the legitimate interests' pursued either by the controller or - in the case of disclosure - by the third party. This condition complements the requirement of necessity under Article 6, and requires a connection between the processing and the interests pursued. This 'necessity' requirement applies in all situations mentioned in Article 7, paragraphs (b) to (f), but is particularly relevant in the case of paragraph (f) to ensure that processing of data based on legitimate interests will not lead to an unduly broad interpretation of the necessity to process data. As in other cases, this means that it should be considered whether other less invasive means are available to serve the same end.

III.3.2. Interests or rights of the data subject

Interests or rights (rather than interests for rights)

Article 7(f) of the Directive refers to 'the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1)'.

The Working Party noted, however, when comparing the different language versions of the Directive that the phrase 'interests for' has been translated as 'interests or' in other key languages which were used at the time when the text was negotiated.[62]

Further analysis suggests that the English text of the Directive is simply a result of a misspelling: 'or' was mistakenly typed as 'for'.[63] Thus, the correct text should read 'interests or fundamental rights and freedoms'.

'Interests' and 'rights' should be given a broad interpretation

The reference to 'interests or fundamental rights and freedoms' has a direct impact on the scope of application of the provision. It provides more protection for the data subject, namely it requires the data subjects' 'interests' to be also taken into account, not only his or her fundamental rights and freedoms. However, there is no reason to assume that the restriction in

[61] See in this respect, for instance, the Working document on data protection issues related to intellectual property rights, adopted on 18.01.2005 (WP104).

[62] For example, 'l'intérêt ou les droits et libertés fondamentaux de la personne concernée' in French, 'l'interesse o i diritti e le libertà fondamentali della persona interessata' in Italian; 'das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person' in German.

[63] The Working Party notes that the grammatically correct English version should have read 'interests in' rather than 'interests for', if this is what had been meant. In addition, the phrase 'interests for' or 'interest in' seems to be redundant, in the first place, because reference to 'fundamental rights and freedoms' should have normally sufficed, if this is what had been meant. The interpretation that there has been a misspelling is also confirmed by the fact that the Common Position (EC) No 1/95 adopted by the Council on 20 February 1995 also refers to 'interests or fundamental rights and freedoms'. Finally, the Working Party also notes that the Commission intended to correct this misspelling in the proposed Regulation: Article 6(1)(f) refers to 'the interests or fundamental rights and freedoms of the data subject which require protection of personal data' and not 'interests for' such rights.

Article 7(f) to fundamental rights 'which require protection under Article 1(1)' - and thus the explicit reference to the object of the Directive[64] - would not also apply to the term 'interests'. The clear message is nevertheless that all relevant interests of the data subject should be taken into account.

This interpretation of the text makes sense not only grammatically, but also when taking into account the broad interpretation of the notion of the 'legitimate interests' of the controller. If the controller - or the third party in the case of disclosure - can pursue any interests, provided they are not illegitimate, then the data subject should also be entitled to have all categories of interests to be taken into account and weighed against those of the controller, as long as they are relevant within the scope of the Directive.

At a time of increasing imbalance in 'informational power', when governments and business organisations alike amass hitherto unprecedented amounts of data about individuals, and are increasingly in the position to compile detailed profiles that will predict their behaviour (reinforcing informational imbalance and reducing their autonomy), it is ever more important to ensure that the interests of the individuals to preserve their privacy and autonomy be protected.

Finally, it is important to note that unlike the case of the controller's interests, the adjective 'legitimate' is not used here to precede the 'interests' of the data subjects. This implies a wider scope to the protection of individuals' interests and rights. Even individuals engaged in illegal activities should not be subject to disproportionate interference with their rights and interests[65]. For example, an individual who may have perpetrated theft in a supermarket could still see his interests prevailing against the publication of his picture and private address on the walls of the supermarket and/or on the Internet by the owner of the shop.

III.3.3. Introduction to applying the balancing test

It is useful to imagine both the legitimate interests of the controller and the impact on the interests and rights of the data subject on a spectrum. Legitimate interests can range from insignificant through somewhat important to compelling. Similarly, the impact on the interests and rights of the data subjects may be more or may be less significant and may range from trivial to very serious.

Legitimate interests of the controller, when minor and not very compelling may, in general, only override the interests and rights of data subjects in cases where the impact on these rights and interests are even more trivial. On the other hand, important and compelling legitimate interests may in some cases and subject to safeguards and measures justify even significant intrusion into privacy or other significant impact on the interests or rights of the data subjects[66].

[64] See Article 1(1): 'In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data'.

[65] Of course, one of the consequences of criminality might be the collection and possible publication of personal data about criminals and suspects. This, however, must be subject to strict conditions and safeguards.

[66] See as an illustration the reasoning of the Working Party in several opinions and working documents:
- Opinion 4/2006 on the Notice of proposed rule-making by the US Department of Health and Human Services on the control of communicable disease and the collection of passenger information of 20 November 2005

Here it is important to highlight the special role that safeguards may play[67] in reducing the undue impact on the data subjects, and thereby changing the balance of rights and interests to the extent that the data controller's legitimate interests will not be overridden. The use of safeguards alone is of course not sufficient to justify any kind of processing in all contexts. Further, the safeguards in question must be adequate and sufficient, and must unquestionably and significantly reduce the impacts on data subjects.

Introductory scenarios

Before moving on to provide guidance on how to carry out the balancing test, the following three introductory scenarios may give a first illustration of how balancing of interests and rights may look like in real life. All three examples build on a simple and innocent scenario that starts with a special offer for Italian take-away food. The examples gradually introduce new elements that show how the balance is tipped as the impact on the data subjects increases.

<u>Scenario 1: special offer by a pizza chain</u>

Claudia orders a pizza via a mobile app on her smartphone, but does not opt-out of marketing on the website. Her address and credit card details are stored for the delivery. A few days later Claudia receives discount coupons for similar products from the pizza chain in her letterbox at home.

<u>Brief analysis</u>: the pizza chain has a legitimate, but not particularly compelling, interest in attempting to sell more of its products to its customers. On the other hand, there does not appear to be any significant intrusion into Claudia's privacy, or any other undue impact on her interests and rights. The data and the context are relatively innocent (consumption of pizza). The pizza chain established some safeguards: only relatively limited information is used (contact details) and the coupons are sent by traditional mail. In addition, an easy-to-use opportunity is provided to opt-out of marketing on the website.

On balance, and considering also the safeguards and measures in place (including an easy-to-use opt-out tool), the interests and rights of the data subject do not appear to override the legitimate interests of the pizza chain to carry out this minimal amount of data processing.

(Control of Communicable Disease Proposed 42 CFR Parts 70 and 71), adopted on 14.06.2006 (WP 121), where serious specific public health threats are at stake.
- Opinion 1/2006 on whistleblowing schemes (cited above in footnote 39), where the seriousness of an alleged offence is one of the elements of the balancing test.
- Working Document on the surveillance of electronic communications in the workplace, adopted on 29.05.2002 (WP 55), which balances the employer's right to run his business efficiently against the human dignity of the worker, as well as secrecy of correspondence.

[67] Safeguards may include, among others, strict limitations on how much data are collected, immediate deletion of data after use, technical and organisational measures to ensure functional separation, appropriate use of anonymisation techniques, aggregation of data, and privacy-enhancing technologies but also increased transparency, accountability, and the possibility to opt-out of the processing. See further in Section III.3.4(d) and beyond.

Scenario 2: targeted advertisement for the same special offer

The context is the same, but this time not only Claudia's address and credit card details but also her recent order history (for the past three years) are stored by the pizza chain. In addition, the purchase history is combined with data from the supermarket where Claudia does her shopping online, which is operated by the same company as the one running the pizza chain. Claudia is provided by the pizza chain with special offers and targeted advertisement based on her order history for the two different services. She receives the adverts and special offers both online and off-line, by regular mail, email, and placement on the website of the company as well as on the website of a number of selected partners (when she accesses these sites on her computer or via her mobile telephone). Her browsing history (click-stream) is tracked as well. Her location data is also tracked via her mobile phone. An analytics software is run through the data and predicts her preferences and the times and locations when she will be most likely to make a larger purchase, willing to pay a higher price, susceptible to being influenced by a particular rate of discount, or when she craves most strongly for her favourite desserts or ready-meals.[68] Claudia is thoroughly annoyed by persistent ads popping up on her mobile phone when she is checking the bus schedule on her way home advertising the latest take-away offers she is trying to resist. She was unable to find user-friendly information or a simple way to switch off these advertisements although the company claims there is an industry-wide opt-out scheme in place. She was also surprised to see when she moved to a less affluent neighbourhood, that she no longer received her special offers. This resulted in an approximately 10% increase on her monthly food bill. A more tech-savvy friend showed her some speculations in an online blog that the supermarket was charging more for orders from 'bad neighbourhoods', on grounds of the statistically higher risks of credit card fraud in such cases. The company did not comment and claimed that their policy on discounts and the algorithm they are using to set prices are proprietary and cannot be disclosed.

Brief analysis: the data and the context remain of relatively innocent nature. However, the scale of data collection and the techniques used to influence Claudia (including various tracking techniques, predicting times and locations of food cravings and the fact that at these times Claudia is most vulnerable to succumb to temptation), are factors to be considered when assessing the impact of the processing. Lack of transparency about the logic of the company's data processing that may have led to *de facto* price discrimination based on the location where an order is placed, and the significant potential financial impact on the customers ultimately tip the balance even in the relatively innocent context of take-away foods and grocery shopping. Instead of merely offering the possibility to opt out of this type of profiling and targeted advertisement, an informed consent would be necessary, pursuant to Article 7(a) but also under Article 5(3) of the ePrivacy Directive. As a consequence, Article 7(f) should not be relied on as a legal ground for the processing.

[68] See, for example, http://www.stanfordlawreview.org/online/privacy-and-big-data/consumer-subject-review-boards: *'Recent research suggests that willpower is a finite resource that can be depleted or replenished over time.[10] Imagine that concerns about obesity lead a consumer to try to hold out against her favourite junk food. It turns out there are times and places when she cannot. Big data can help marketers understand exactly how and when to approach this consumer at her most vulnerable—especially in a world of constant screen time in which even our appliances are capable of a sales pitch.'*

Scenario 3: use of food orders to adapt health insurance premiums

Claudia's pizza consumption habits, including the time and nature of food orders, are sold by the chain to an insurance company, which uses them to adapt its health insurance premiums.

Brief analysis: the health insurance company may have a legitimate interest - to the extent applicable regulations allow this - in assessing the health risks of its customers and charge differentiated premiums according to the different risks. However, the way in which the data are collected and the scale of the data collection in itself are excessive. A reasonable person in the situation of Claudia would be unlikely to have expected that information about her pizza consumption would have been used to calculate her health insurance premiums.

In addition to the excessive nature of the profiling and possible inaccurate inferences (the pizza could be ordered for someone else), the inference of sensitive data (health data) from seemingly innocuous data (take-away-orders) contributes to tipping the balance in favour of the data subject's interests and rights. Finally, the processing also has a significant financial impact on her.

On balance, in this specific case the interests and rights of the data subject override the legitimate interests of the health insurance company. As a consequence, Article 7(f) should not be relied on as a legal ground for the processing. It is also questionable whether Article 7(a) could be used as a legal ground, considering the excessive scale of the data collection, and possibly, also due to further specific restrictions under national law.

The above scenarios and the possible introduction of variations with other elements underline the need for a limited number of key factors that can help focus the assessment, as well as the need for a pragmatic approach that allows the use of practical assumptions ('rules of thumb') based primarily on what a reasonable person would find acceptable under the circumstances ('reasonable expectations') and based on the consequences of the data processing activity for data subjects ('impact').

III.3.4. Key factors to be considered when applying the balancing test

Member States have developed a number of useful factors to be considered when carrying out the balancing test. These factors are discussed in this Section under the following four main headings: (a) assessing the controller's legitimate interest, (b) impact on the data subjects, (c) provisional balance and (d) additional safeguards applied by the controller to prevent any undue impact on the data subjects.[69]

To carry out the balancing test it is first important to consider the nature and source of the legitimate interests on the one hand and the impact on the data subjects on the other hand. This assessment should already take into account the measures that the controller plans to adopt to comply with the Directive (for example, to ensure purpose limitation and proportionality under Article 6, or to provide information to the data subjects under Articles 10 and 11).

[69] Due to their importance, some specific issues related to safeguards will be further discussed under separate headings in Sections III.3.5 and III.3.6.

After analysing and weighing the two sides against each other, a provisional 'balance' may be established. Where the outcome of the assessment still leaves doubts, the next step will be to assess whether additional safeguards, bringing more protection to the data subject, may tip the balance in a way that would legitimise the processing.

(a) Assessing the controller’s legitimate interest

Whereas the notion of legitimate interests is fairly broad, as explained in Section III.3.1 above, its nature plays a crucial role when it comes to the balancing of interests against the rights and interests of the data subjects. While it is impossible to make value judgments with regard to all possible legitimate interests, it is possible to provide some guidance. As mentioned above, such interest can range from trivial to compelling, and be straightforward or more controversial.

i) Exercise of a fundamental right

Among the fundamental rights and freedoms enshrined in the European Charter of Fundamental Rights (the 'Charter')[70] and the European Convention on Human Rights ('ECHR'), several may come into conflict with the right to privacy and the right to the protection of personal data, such as freedom of expression and information[71], freedom of the arts and sciences[72], right of access to documents[73], as well as for instance the right to liberty and security[74], the freedom of thought, conscience and religion[75], the freedom to conduct a business[76], the right to property[77], the right to an effective remedy and to a fair trial[78], or the presumption of innocence and right of defence[79].

For the controller's legitimate interest to prevail, the data processing must be 'necessary' and 'proportionate' in order to exercise the fundamental right concerned.

To illustrate, depending on the facts of the case it may well be necessary and proportionate for a newspaper to publish certain incriminating details about the spending habits of a high-level government official involved in an alleged corruption scandal. On the other hand, there should be no blanket permission for the media to publish any and all irrelevant details of the private life of public figures. These and similar cases typically raise complex issues of assessment, and to help guide the assessment, specific legislation, case law, jurisprudence,

[70] The provisions of the Charter are addressed to the institutions and bodies of the EU with due regard for the principle of subsidiarity and the national authorities only when they are implementing EU law.
[71] Article 11 of the Charter and Article 10 of the ECHR.
[72] Article 13 of the Charter and Articles 9 and 10 of the ECHR.
[73] Article 42 of the Charter. 'Any citizen of the Union, and any natural or legal person residing or having its registered office in a Member State, has a right of access to European Parliament, Council and Commission documents.' Similar rights of access exist in a number of Member States with regard to documents held by public bodies in those Member States.
[74] Article 6 of the Charter and Article 5 of the ECHR.
[75] Article 10 of the Charter and Article 9 of the ECHR.
[76] Article 16 of the Charter.
[77] Article 17 of the Charter and Article 1 of Protocol n°1 to the ECHR.
[78] Article 47 of the Charter and Article 6 of the ECHR.
[79] Article 48 of the Charter and Articles 6 and 13 of the ECHR.

guidelines, as well as codes of conduct and other formal or less formal standards may all play an important role.[80]

When appropriate, in this context also, additional safeguards may play an important role and help determine which way the - sometimes fragile - balance is to be struck.

ii) Public interests/the interests of the wider community

In some cases, the controller may wish to invoke the public interest or the interest of the wider community (whether or not this is provided for in national laws or regulations). For example, a charitable organisation may process personal data for purposes of medical research, or a non-profit organisation in order to raise awareness of government corruption.

It can also be the case that a private business interest of a company coincides with a public interest to some degree. This may happen, for example, with regard to combatting financial fraud or other fraudulent use of services.[81] A service provider may have a legitimate business interest in ensuring that its customers will not misuse the service (or will not be able to obtain services without payment), while at the same time, the customers of the company, taxpayers, and the public at large also have a legitimate interest in ensuring that fraudulent activities are discouraged and detected when they occur.

In general, the fact that a controller acts not only in its own legitimate (e.g. business) interest, but also in the interests of the wider community, can give more 'weight' to that interest. The more compelling the public interest or the interest of the wider community, and the more clearly acknowledged and expected it is in the community and by data subjects that the controller can take action and process data in pursuit of these interests, the more heavily this legitimate interest weighs in the balance.

On the other hand, 'private enforcement' of the law should not be used to legitimise intrusive practices that would, were they carried out by a government organisation, be prohibited pursuant to the case law of the European Court of Human Rights on grounds that the activities of the public authority would interfere with the privacy of data subjects without meeting the stringent test under Article 8(2) of the ECHR.

iii) Other legitimate interests

In some cases, as already discussed in Section III.2, the context in which a legitimate interest arises may come close to one of the contexts in which some of the other legal grounds, in particular, the legal grounds of Article 7(b) (contract), 7(c) (legal obligation), or 7(e) (public task) may apply. For example, a data processing activity may not be strictly necessary, but

[80] With regard to the criteria to be applied in cases involving freedom of expression, the case law of the European Court of Human Rights also provides useful guidance. See, for example, the judgment of the ECHR in the Case of von Hannover v Germany (No 2) on 7 February 2012, in particular, para 95-126. It must also be considered that Article 9 of the Directive (under the title *Processing of personal data and freedom of expression*) allows Member States to 'provide for exemptions or derogations from [certain provisions of the Directive] for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression' provided these are 'necessary to reconcile the right to privacy with the rules governing freedom of expression'.

[81] See, for example, 'Example 21: Smart metering data mined to detect fraudulent energy use' on page 67 in the Working Party's Opinion 3/2013 on purpose limitation (cited above in footnote 9).

can still be relevant to the performance of a contract - or, a law may only permit, but not require that certain data be processed. As we have seen, it may not always be easy to draw a clear dividing line between the different grounds, but this makes it all the more important to bring the Article 7(f) balancing test into the analysis.

Here also, as well as in all possible other cases not mentioned thus far, the more compelling the interest of the controller, and the more clearly acknowledged and expected it is in the wider community that the controller may take action and process data in pursuit of such an interest, the more heavily this legitimate interest weighs in the balance.[82] This brings us to the following, more general point.

iv) Legal and cultural/societal recognition of the legitimacy of the interests

In all the above contexts, it is certainly also relevant whether EU law or the law of a Member State specifically allows (even if it does not require) controllers to take steps in pursuit of the public or private interest concerned. The existence of any duly adopted, non-binding guidance issued by authoritative bodies, for example, by regulatory agencies, encouraging controllers to process data in pursuit of the interest concerned is also relevant.

Compliance with any non-binding guidance provided by data protection authorities or other relevant bodies with regard to the modalities of the data processing will also be likely to contribute towards a favourable assessment of the balance. Cultural and societal expectations, even when not reflected directly in legislative or regulatory instruments, may also play a role, and may help tip the balance either way.

The more explicitly recognised it is in the law, in other regulatory instruments - be they binding or not on the controller - or even in the culture of the given community overall without any specific legal basis, that the controllers may take action and process data in pursuit of a particular interest, the more heavily this legitimate interest weighs in the balance[83].

(b) <u>The impact on data subjects</u>

Looking at the other side of the balance, the impact of the processing on the interests or fundamental rights and freedoms of the data subject is a crucial criterion. The first subsection below discusses in general terms how to assess the impact on the data subject.

Several elements can be useful here and they are analysed in further subsections, including the nature of personal data, the way the information is being processed, the reasonable expectations of the data subjects and the status of the controller and data subject. We will also briefly discuss issues related to potential sources of risk that may lead to impact on the individuals concerned, the severity of any impacts on the individuals concerned and the likelihood of such impacts materialising.

[82] Of course, the assessment must also include reflection on the possible prejudice suffered by the controller, by third parties or the broader community if the data processing does not take place.

[83] This interest can however not be used to legitimise intrusive practices that would otherwise not meet the test of Article 8(2) of the ECHR.

i) Assessment of impact

In assessing the impact[84] of the processing, both positive and negative consequences should be taken into account. These may include potential future decisions or actions by third parties, and situations where the processing may lead to the exclusion of, or discrimination against, individuals, defamation, or more broadly, situations where there is a risk of damaging the reputation, negotiating power, or autonomy of the data subject.

In addition to adverse outcomes that can be specifically foreseen, broader emotional impacts also need to be taken into account, such as the irritation, fear and distress that may result from a data subject losing control over personal information, or realising that it has been or may be misused or compromised, – for example through exposure on the internet. The chilling effect on protected behaviour, such as freedom of research or free speech, that may result from continuous monitoring/tracking, must also be given due consideration.

The Working Party emphasises that it is crucial to understand that relevant 'impact' is a much broader concept than harm or damage to one or more specific data subjects. 'Impact' as used in this Opinion covers any possible (potential or actual) consequences of the data processing. For the sake of clarity, we also emphasise that the concept is unrelated to the notion of data breach and is much broader than impacts that may result from a data breach. Instead, the notion of impact, as used here, encompasses the various ways in which an individual may be affected - positively or negatively - by the processing of his or her personal data. [85]

It is also important to understand that more often than not a series of related and unrelated occurrences can lead cumulatively to the ultimate negative impact on the data subject and it may be difficult to identify which processing activity by which controller played a key role in the negative impact.

Considering that establishment of a case for compensation of a suffered harm or damage is often difficult for the data subjects in this context, even where the effect itself is very real, it is all the more important to focus on prevention and ensuring that data processing activities may only be carried out, provided they carry no risk or a very low risk of undue negative impact on the data subjects' interests or fundamental rights and freedoms.

When assessing impact, the terminology and methodology of traditional risk assessment may be helpful to some degree, and therefore some elements of this methodology will be briefly

[84] This assessment of impact must be understood in the context of Article 7(f). In other words, we do not refer to a ‘risk analysis’ or a 'data protection impact assessment' in the sense of the proposed Regulation (Articles 33 and 34) and the various LIBE amendments to it. The question what methodology should be followed in a 'risk analysis' or a 'data protection impact assessment' goes beyond the scope of this Opinion. On the other hand, it should be kept in mind that - one way or another - the analysis of impact under Article 7(f) can be an important part of any 'risk assessment' or 'data protection impact assessment' and can also help identify situations where the data protection authority should be consulted.

[85] The risk of financial damage, for example, if a data breach releases financial information that was meant to be in a secure environment, and this eventually leads to identity theft or other forms of fraud, or the risk of personal injury, pain, suffering and loss of amenity that might ultimately result from, for example, unauthorised alteration of medical records, and a subsequent mistreatment of a patient, must always be duly taken into account, although it is by no means limited to situations under the scope of Article 7(f). At the same time, such risks are not the only ones to be considered when assessing impact under Article 7(f).

highlighted below. However, a comprehensive methodology for assessment of impact - in the context of Article 7(f) or more broadly - would go beyond the scope of this Opinion.

In this context as elsewhere, it is important to identify the sources of potential impacts on the data subjects.

The likelihood that a risk can materialise is one of the elements to take into consideration. For example, access to the Internet, exchanges of data with sites outside the EU, interconnections with other systems and a high degree of system heterogeneity or variability can represent vulnerabilities that hackers could exploit. This risk source bears a relatively high likelihood for the risk of compromising data to materialise. Conversely, a homogeneous, stable system that has no interconnections and is disconnected from the Internet bears a far lower likelihood of compromising data.

Another element of the risk assessment is the severity of the consequences of a materialized risk. This severity can range from low levels (like the annoying need to enter again personal contact details lost by the data controller) to very high levels (like the loss of life when personal location patterns of protected individuals go into the hands of criminals or when power supply is remotely cut off through smart metering devices in critical weather or personal health conditions).

These two key elements - the likelihood that the risk materializes on the one hand, and the severity of the consequences on the other hand - each contribute to the overall assessment of the potential impact.

Finally, in applying the methodology, it should be recalled that assessing impact under Article 7(f) cannot lead to a mechanical and purely quantitative exercise. In traditional risk assessment scenarios, 'severity' can take into account the number of individuals potentially impacted. Nevertheless, it should be kept in mind that processing of personal data having an impact on a minority of data subjects - or even a single individual only - still requires a very careful analysis especially if such impact on each individual concerned is potentially significant.

ii) Nature of the data

It would first be important to evaluate whether the processing involves sensitive data, either because they belong to the special categories of data under Article 8 of the Directive, or for other reasons, as in the case of biometric data, genetic information, communication data, location data, and other kinds of personal information requiring special protection.[86]

To illustrate, in the view of the Working Party, as a general rule, the use of biometrics for general security requirements of property or individuals is regarded as a legitimate interest that would be overridden by the interests or fundamental rights and freedoms of the data subject. On the other hand, biometric data such as fingerprint and/or iris scan could be used

[86] Biometric data and genetic information are considered as special categories of data in the Proposal of the Commission for a Data Protection Regulation, read together with the amendments proposed by the LIBE Committee. See amendment 103 to Article 9 in the Final LIBE Committee Report. On the relationship between Articles 7 and 8 of Directive 95/46/EC, see Section II.1.2 above on pages 14-15.

for the security of a high-risk area such as a laboratory doing research on dangerous viruses, provided that the controller has demonstrated concrete evidence of a considerable risk[87].

In general, the more sensitive the information involved, the more consequences there may be for the data subject. This, however, does not mean that data that may in and of themselves seem innocuous, can be freely processed based on Article 7(f). Indeed, even such data, depending on the way they are processed, can have significant impact on individuals, as will be shown in Subsection (iii) below.

In this regard, whether the data has already been made publicly available by the data subject or by third parties may be relevant. Here, first of all, it is important to highlight that personal data, even if it has been made publicly available, continues to be considered as personal data, and its processing therefore continues to require appropriate safeguards.[88] There is no blanket permission to reuse and further process publicly available personal data under Article 7(f).

That said, the fact that personal data is publicly available may be considered as a factor in the assessment, especially if the publication was carried out with a reasonable expectation of further use of the data for certain purposes (e.g. for purposes of research or for purposes related to transparency and accountability).

iii) The way data are being processed

Assessing impact in a wider sense may involve considering whether the data are publicly disclosed or otherwise made accessible to a large number of persons, or whether large amounts of personal data are processed or combined with other data (e.g. in case of profiling, for commercial, law enforcement or other purposes). Seemingly innocuous data, when processed on a large scale and combined with other data may lead to inferences about more sensitive data, as shown above in Scenario 3 illustrating the relationship between pizza consumption patterns and health insurance premiums.

In addition to potentially leading to the processing of more sensitive data, such analysis may also lead to uncanny, unexpected, and sometimes also inaccurate predictions, for example, concerning the behaviour or personality of the individuals concerned. Depending on the nature and impact of these predictions, this may be highly intrusive to the individual's privacy.[89]

The Working Party also stressed in a previous Opinion the risks inherent in certain security solutions (including for firewalls, anti-virus or anti-spam), as they may lead to large scale

[87] See Opinion 3/2012 of the Article 29 Working Party on developments in biometric technologies (WP193). As another illustration, in its Opinion 4/2009 on the World Anti-Doping Agency (cited above in footnote 32), the Working Party emphasised that Article 7(f) would not be a valid ground to process medical data and data related to offences in the context of anti-doping investigations, in view of the 'gravity of privacy intrusions'. The processing of data should be foreseen by law and meet the requirements of Article 8(4) or (5) of the Directive.

[88] See the Working Party's Opinion 3/2013 on purpose limitation (cited in footnote 9 above) and the Working Party's Opinion 06/2013 on open data and public sector information ('PSI') reuse, adopted on 05.06.2013 (WP207).

[89] See Section III.2.5 and Annex 2 (Big data and open data) of the Opinion on Purpose Limitation (cited above in footnote 9).

deployment of deep packet inspection, which may have a significant influence on the assessment of the balance of rights[90].

In general, the more negative or uncertain the impact of the processing might be, the more unlikely it is that the processing will be considered, on balance, as legitimate. The availability of alternative methods to achieve the objectives pursued by the controller, with less negative impact for the data subject, would certainly have to be a relevant consideration in this context. When appropriate, privacy and data protection impact assessments can be used to determine whether this is a possibility.

iv) Reasonable expectations of the data subject

The reasonable expectations of the data subject with regard to the use and disclosure of the data are also very relevant in this respect. As also highlighted with regard to the analysis of the purpose limitation principle[91], it is 'important to consider whether the status of the data controller[92], the nature of the relationship or the service provided[93], or the applicable legal or contractual obligations (or other promises made at the time of collection) could give rise to reasonable expectations of stricter confidentiality and stricter limitations on further use. In general, the more specific and restrictive the context of collection, the more limitations there are likely to be on use. Here again, it is necessary to take account of the factual context rather than simply rely on text in small print.

v) Status of the data controller and data subject

The status of the data subject and the data controller is also relevant when assessing the impact of the processing. Depending on whether the data controller is an individual or a small organisation, a large multi-national company, or a public sector body, and on the specific circumstances, its position may be more or less dominant in respect of the data subject. A large multinational company may, for instance, have more resources and negotiating power than the individual data subject, and therefore, may be in a better position to impose on the data subject what it believes is in its 'legitimate interest'. This may be even more so if the company has a dominant position on the market. If left unchecked, this may happen to the detriment of the individual data subjects. Just as consumer protection and competition laws help ensure that this power will not be misused, data protection law could also play an important role in ensuring that the rights and interests of the data subjects will not be unduly prejudiced.

On the other hand, the status of the data subject is also relevant. While the balancing test should in principle be made against an average individual, specific situations should lead to a more case-by-case approach: for example, it would be relevant to consider whether the data subject is a child[94] or otherwise belongs to a more vulnerable segment of the population

[90] See Section 3.1 of the Working Party's Opinion 1/2009 on the proposals amending Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive) (WP159).

[91] See pages 24-25 of the Working Party's Opinion 3/2013 on purpose limitation (cited above in footnote 9).

[92] 'Such as, for example, an attorney or a physician.'

[93] 'Such as, for example, cloud computing services for personal document management, email services, diaries, e-readers equipped with note-taking features, and various life-logging applications that may contain very personal information.'

[94] See the Working Party's Opinion 2/2009 on the protection of children’s personal data, (General Guidelines and the special case of schools), adopted on 11.02.2009 (WP160). This opinion insists on the specific vulnerability of

requiring special protection, such as, for example, the mentally ill, asylum seekers, or the elderly. The question whether the data subject is an employee, a student, a patient, or whether there is otherwise an imbalance in the relationship between the position of the data subject and the controller must certainly be also relevant. It is important to assess the effect of actual processing on particular individuals.

Finally, it is important to emphasise that not all negative impact on the data subjects 'weighs' equally on the balance. The purpose of the Article 7(f) balancing exercise is not to prevent any negative impact on the data subject. Rather, its purpose is to prevent disproportionate impact. This is a crucial difference. For example, the publication of a well-researched and accurate newspaper article on alleged government corruption may damage the reputation of the government officials involved and may lead to significant consequences, including loss of reputation, loss of elections, or imprisonment, but it could still find a basis under Article 7(f).[95]

(c) Provisional balance

When balancing the interests and rights at stake as described above, the measures taken by the controller to comply with its general obligations under the Directive, including in terms of proportionality and transparency, will greatly contribute to ensuring that the data controller meets the requirements of Article 7(f). Full compliance should mean that the impact on individuals is reduced, that data subjects' interests or fundamental rights or freedoms are *less likely* to be interfered with and that therefore it is *more likely* that the data controller can rely on 7(f). This should encourage controllers to better comply with all horizontal provisions of the Directive[96].

This does not mean, however, that compliance with these horizontal requirements will as such always be sufficient to secure a legal basis based on Article 7(f). Indeed, if this were the case, Article 7(f) would be superfluous or become a loophole that would render meaningless the entire Article 7, which calls for an adequate specific legal basis for the processing.

For this reason, it is important to carry out a further assessment in the balancing exercise in cases where - based on the preliminary analysis - it is not clear which way the balance should be struck. The controller may consider whether it is possible to introduce additional measures, going beyond compliance with horizontal provisions of the Directive, to help reduce the undue impact of the processing on the data subjects.

Additional measures may include, for example, providing an easily workable and accessible mechanism to ensure an unconditional possibility for data subjects to opt-out of the processing. These additional measures may in some (but not all) cases help tip the balance and help ensure that the processing can be based on Article 7(f), while at the same time, also protecting the rights and interests of the data subjects.

the child, and in case the child is represented, on the need to take into account the child's best interest and not that of its representative.

[95] As explained above, any relevant derogations for processing for journalistic purposes under Article 9 of the Directive must also be taken into account.

[96] On the important role of 'horizontal compliance' see also page 54 of the Working Party's Opinion 3/2013 on purpose limitation, cited in footnote 9 above.

(d) Additional safeguards applied by the controller

As explained above, the way in which the controller would apply appropriate measures could, in some situations, help 'tip the balance' on the scale. Whether the result is acceptable will depend on the assessment as a whole. The more significant the impact on the data subject, the more attention should be given to relevant safeguards.

Examples of the relevant measures may include, among other things, strict limitation on how much data is collected, or immediate deletion of data after use. While some of these measures may already be compulsory under the Directive, they are often scalable and leave room for controllers to ensure better protection of data subjects. For instance, the controller may collect less data, or provide additional information compared to what is specifically listed in Articles 10 and 11 of the Directive.

In some other cases, the safeguards are not *explicitly* required under the Directive but may well be in the future under the proposed Regulation, or they are only required in specific situations, such as:

- technical and organisational measures to ensure that the data cannot be used to take decisions or other actions with respect to individuals ('functional separation' as is often the case in a research context)
- extensive use of anonymisation techniques
- aggregation of data
- privacy-enhancing technologies, privacy by design, privacy and data protection impact assessments
- increased transparency
- general and unconditional right to opt-out
- data portability & related measures to empower data subjects

The Working Party notes that with respect to some key issues, including functional separation and anonymisation techniques, some guidance has already been provided in the relevant parts of its Opinions on purpose limitation, on open data and on anonymisation techniques.[97]

As far as pseudonymisation and encryption are concerned, the Working Party would like to emphasise that if data are not directly identifiable, this does not as such affect the appreciation of the legitimacy of the processing: it should not be understood as turning an illegitimate processing into a legitimate one[98].

At the same time, pseudonymisation and encryption, just like any other technical and organisational measures introduced to protect personal information, will play a role with regard to the evaluation of the potential impact of the processing on the data subject, and thus, may in some cases play a role in tipping the balance in favour of the controller. The use of

[97] See Sections III.2.3, III.2.5 and Annex 2 f the Working Party's Opinion 3/2013 on purpose limitation, cited above in footnote 9, on further processing for historical, statistical and scientific purposes, and on big data and open data; see also relevant parts of the Working Party's Opinion 06/2013 on open data (cited in footnote 88 above) and Opinion 5/2014 on Anonymisation Techniques

[98] See on this point the amendments voted by the LIBE Committee in the Final LIBE Committee Report, and in particular amendment 15 on Recital 38 connecting pseudonymisation and the legitimate expectations of the data subject.

less risky forms of personal data processing (e.g. personal data that is encrypted while in storage or transit, or personal data that are less directly and less readily identifiable) should generally mean that the likelihood of data subjects' interests or fundamental rights and freedoms being interfered with is reduced.

In connection with these safeguards - and the overall assessment of the balance - the Working Party wishes to highlight three specific issues that often play a crucial role in the context of Article 7(f):

- the relationship between the balancing test, transparency, and the accountability principle;
- the right of the data subject to object to the processing, and beyond objection, the availability of an opt out without the need for any justification, and
- empowering data subjects: data portability and the availability of workable mechanisms for the data subject to access, modify, delete, transfer, or otherwise further process (or let third parties further process) their own data.

Due to their importance, these subjects will be discussed under separate headings.

III.3.5. Accountability and transparency

In the first place, before a processing operation on the basis of Article 7(f) is to take place, the controller has the responsibility to evaluate whether it has a legitimate interest; whether the processing is necessary for that legitimate interest and whether the interest is overridden by the interests and rights of the data subjects in the specific case.

In that sense, Article 7(f) is based on the accountability principle. The controller must perform a careful and effective test in advance, based on the specific facts of the case rather than in an abstract manner, taking also into account the reasonable expectations of data subjects. As a matter of good practice, where appropriate, carrying out this test should be documented in a sufficiently detailed and transparent way so that the complete and correct application of the test could be verified - when necessary - by relevant stakeholders including the data subjects and data protection authorities, and ultimately, by the courts.

The controller will first define the legitimate interest and make the balancing test, but this is not necessarily the final and definitive assessment: if, in reality, the interest pursued is not the one that was specified by the controller or if the controller only defined the interest in insufficient detail, the balance has to be re-assessed, based on the actual interest, to be determined either by a data protection authority or by a Court.[99] As is the case for other key aspects of data protection, such as the identification of the data controller or the specification of purpose[100], what matters is the reality behind any assertion made by the controller.

The notion of accountability is closely linked to the notion of transparency. In order to enable data subjects to exercise their rights, and to allow public scrutiny by stakeholders more broadly, the Working Party recommends that controllers explain to data subjects in a clear and user-friendly manner, the reasons for believing that their interests are not overridden by

[99] For example, following a complaint or an Article 14 objection.

[100] See Opinions cited in footnote 9.

the interests or fundamental rights and freedoms of the data subjects, and also explain to them the safeguards they have taken to protect personal data, including, where appropriate, the right to opt out of the processing.[101]

In this respect the Working Party emphasises that consumer protection law, in particular, laws protecting consumers against unfair commercial practices, is also highly relevant here.

If a controller hides important information regarding unexpected further use of the data in legalistic terms buried in the small print of a contract, this may infringe consumer protection rules concerning unfair contractual terms (including the prohibition against 'surprising terms'), and it will also not fulfil the requirements of Article 7(a) for a valid and informed consent, or the requirements of Article 7(f) in terms of reasonable expectations of the data subject and an overall acceptable balance of interests. It would of course also raise questions of compliance with Article 6 as to the need for a fair and lawful processing of personal data.

For instance, in a number of cases, users of ‘free’ online services, such as search, email, social media, file storage or other online or mobile applications, are not fully aware of the extent to which their activity is logged and analysed in order to generate value for the service provider and therefore they remain unconcerned of the risks involved.

In order to empower data subjects in these situations, a first necessary - but by no means in itself sufficient - precondition[102] is to make it clear that the services are not free, and that rather, the consumers pay using their personal data. The conditions and safeguards subject to which data may be used must also be clearly spelled out in each case to ensure the validity of Article 7(a) consent, or a favourable balance under Article 7(f).

III.3.6. The right to object and beyond

(a) The right to object under Article 14 of the Directive

Article 7(e) and (f) are particular in the sense that while they mainly rely on an objective assessment of the interests and rights involved, they also allow the self-determination of the data subject to come into play with a right to object[103]: at least in the case of these two grounds, Article 14(a) of the Directive provides that ('save where otherwise provided by national legislation') the data subject ‘can object at any time on compelling legitimate grounds

[101] As explained on page 46 of the Working Party's Opinion 3/2013 on purpose limitation (cited above in footnote 9), in case of profiling and automated decision-making, 'to ensure transparency, data subjects/consumers should be given access to their 'profiles', as well as to the logic of the decision-making (algorithm) that led to the development of the profile. In other words: organisations should disclose their decisional criteria. This is a crucial safeguard and all the more important in the world of big data'. Whether or not an organisation offers this transparency is a highly relevant factor to be considered also in the balancing exercise.

[102] For further possible safeguards with regard to the increasingly common situations in which consumers pay with their personal data, see Section III.3.6 in particular pages 47-48 on 'Data protection-friendly alternatives to 'free' on-line services' and on 'Data portability, 'midata' and related issues'.

[103] This right to object should not be confused with consent based on Article 7(a), where the data controller cannot process the data before he obtains such consent. In the context of Article 7(f), the controller can process the data, subject to conditions and safeguards, as long as the data subject has not objected. In this sense, the right to object can rather be considered as a specific form of opt-out. See more details in the Working Party's Opinion 15/2011 on the definition of consent (cited in footnote 2).

relating to his particular situation to the processing of data relating to him'. It adds that if the objection is justified the processing of their data must cease.

In principle, under current law, the data subject will thus have to demonstrate 'compelling legitimate interests' to stop the processing of his/her personal data (Article 14(a)), except in the context of direct marketing activities where the objection does not need to be justified (Article 14(b)).

This should not be seen as contradicting the balancing test of Article 7(f), which is made 'a priori': it rather complements the balance, in the sense that, where the processing is allowed further to a reasonable and objective assessment of the different rights and interests at stake, the data subject still has an *additional* possibility to object on grounds relating to his/her particular situation. This will then have to lead to a new assessment taking into account the particular arguments submitted by the data subject. This new assessment is in principle again subject to verification by a data protection authority or the courts.

(b) Beyond objection: the role of opt-out as an additional safeguard

The Working Party emphasises that, even if the Article 14(a) right to object is subject to justification by the data subject, nothing prevents the controller from offering an opt-out that would be broader, and that would not require any additional demonstration of legitimate interest (compelling or otherwise) from the data subject. Such an unconditional right would not need to be based on the specific situation of data subjects.

Indeed, and especially in borderline cases where the balance is difficult to strike, a well-designed and workable mechanism for opt-out, while not necessarily providing data subjects with all the elements that would satisfy a valid consent under Article 7(a), could play an important role in safeguarding the rights and interests of the data subjects.

For this a nuanced approach is required, which distinguishes between cases where an Article 7(a) opt-in consent is required, and cases where a workable opportunity to opt-out of the processing (combined with possible other additional measures) may contribute to protecting data subjects under Article 7(f).

The more widely applicable the mechanism for opt-out and the more easy it is to exercise it, the more it will contribute to tipping the balance in favour of the processing to find a legal ground in Article 7(f).

Illustration: the evolution in the approach to direct marketing

To illustrate how a distinction is made between cases where Article 7(a) consent is required and cases where an opt-out could be used as a safeguard under Article 7(f), it is helpful to use the example of direct marketing, for which traditionally there has been a specific opt-out provision included in Article 14(b) of the Directive. To address new technological developments, this provision has later been complemented by specific provisions in the ePrivacy Directive.[104]

[104] On Article 13 of the ePrivacy Directive, see also Section III.2.4 of the Working Party's Opinion 3/2013 on purpose limitation (cited above in footnote 9).

Under Article 13 of the ePrivacy Directive, for certain types of - more intrusive - direct marketing activities (such as e-mail marketing and automated calling machines) consent is the rule. As an exception, in existing client relationships where a controller advertises its own 'similar' products or services, it is sufficient to provide an (unconditional) opportunity to 'opt-out' without justification.

Technologies have evolved, which has called for similar, relatively simple solutions following a similar logic for new marketing practices.

First, the way in which marketing material is being delivered has evolved: instead of simple emails arriving to mailboxes, now targeted behavioural advertisements also pop up on smart phones and computer screens. In the near future, advertisement may also be embedded in smart objects linked within the internet of things.

Second, advertisements are becoming ever-more specifically targeted: rather than based on simple customer profiles, consumers' activities are increasingly tracked and stored online and offline and analysed with more sophisticated automated methods.[105]

As a result of these developments, the object of the balancing exercise has shifted: the issue is no longer about the right to free commercial speech, but primarily the economic interests of business organisations to get to know their customers by tracking and monitoring their activities online and offline, which should be balanced against the (fundamental) rights to privacy and the protection of personal data of these individuals and their interest not to be unduly monitored.

This shift in prevailing business models and the rise of the value of personal data as an asset to business organisations explains the recent requirement for consent in this context, pursuant to Article 5(3) and Article 13 of the ePrivacy Directive.

There are thus different specific rules, depending on the form of marketing, including:

- the unconditional right to object to direct marketing (designed for the traditional, postal mailing context, and for the marketing of similar products) under Article 14(b) of the Directive; Article 7(f) could be the legal ground in that case;
- the requirement for consent under Article 13 of the ePrivacy Directive for automated calling systems, fax, text messages and e-mail marketing (subject to exceptions)[106], and *de facto* application of Article 7(a) of the Data Protection Directive.
- the requirement for consent under Article 5(3) of the ePrivacy Directive (and Article 7(a) of the Data Protection Directive) for behavioural advertising based on tracking techniques such as cookies storing information in the terminal of the user[107].

While the legal grounds applicable are clear as far as Articles 5(3) and 13 of the ePrivacy Directive are concerned, not all forms of marketing are covered and it would be desirable to

[105] See Section III.2.5 and Annex 2 (on big data and open data) of the Working Party's Opinion 3/2013 on purpose limitation (cited above in footnote 9).

[106] See also Article 13(3) of the ePrivacy Directive, which leaves Member States the choice between opt-in and opt-out for direct marketing via other means.

[107] See for the application of this provision the Opinion 2/2010 of the Working Party on online behavioural advertising (WP171).

have guidance on which situations require Article 7(a) consent, and for which situations a balance under Article 7(f) is achieved, including an opportunity to opt-out.

In this respect, it is useful to recall the Working Party's Opinion on purpose limitation, where it is specifically stated that 'when an organisation specifically wants to analyse or predict the personal preferences, behaviour and attitudes of individual customers, which will subsequently inform 'measures or decisions' that are taken with regard to those customers .... free, specific, informed and unambiguous 'opt-in' consent would almost always be required, otherwise further use cannot be considered compatible. Importantly, such consent should be required, for example, for tracking and profiling for purposes of direct marketing, behavioural advertisement, data-brokering, location-based advertising or tracking-based digital market research.'[108]

Data protection-friendly alternatives to 'free' on-line services

In the context where customers signing up for 'free' online services actually ‘pay for’ these services by allowing the use of their personal data, it would also contribute towards a favourable assessment of the balance - or towards the finding that the consumer had a genuine freedom of choice, and therefore valid consent was provided under Article 7(a) - if the controller also offered an alternative version of its services, in which 'personal data' were not used for marketing purposes.

As long as such alternative services are not available, it is more difficult to argue that a valid (freely given) consent has been granted under Article 7(a) by the mere use of free services or that the balance under Article 7(f) should be struck in favour of the controller.

The above considerations underline the important role that additional safeguards, including a workable mechanism to opt-out of the processing may play in modifying the provisional balance. At the same time, they also suggest that in some cases, Article 7(f) cannot be relied on as a ground for processing and controllers must ensure a valid consent under Article 7(a) – or fulfil some other conditions of the Directive – for the processing to take place.

Data portability, 'midata' and related issues

Among the additional safeguards which might help tip the balance, special attention should be given to data portability and related measures, which may be increasingly relevant in an on-line environment. The Working Party recalls its Opinion on Purpose Limitation where it has emphasised that 'in many situations, safeguards such as allowing data subjects/customers to have direct access to their data in a portable, user-friendly and machine-readable format may help empower them, and redress the economic imbalance between large corporations on the one hand and data subjects/consumers on the other. It would also let individuals 'share the wealth' created by big data and incentivise developers to offer additional features and applications to their users.[109]

[108] See Annex II (on Big Data and Open Data) of the Opinion (cited in footnote 9 above), page 45.

[109] 'See initiatives such as 'midata' in the UK, which are based on the key principle that data should be released back to consumers. Midata is a voluntary programme, which over time should give consumers increasing access to their personal data in a portable, electronic format. The key idea is that consumers should also benefit from big data by having access to their own information to enable them to make better choices. See also 'Green button'

The availability of workable mechanisms for the data subjects to access, modify, delete, transfer, or otherwise further process (or let third parties further process) their own data will empower data subjects and let them benefit more from digital services. In addition, it can foster a more competitive market environment, by allowing customers more easily to switch providers (e.g. in the context of online banking or in case of energy suppliers in a smart grid environment). Finally, it can also contribute to the development of additional value-added services by third parties who may be able to access the customers' data at the request and based on the consent of the customers. In this perspective, data portability is therefore not only good for data protection, but also for competition and consumer protection.[110]

IV. Final observations

In this Opinion the Working Party analysed the criteria set forth in Article 7 of the Directive for making data processing legitimate. Beyond guidance on the practical interpretation and application of Article 7(f) under the current legal framework, it aims at formulating policy recommendations to assist policy makers as they consider changes to the current data protection legal framework. Before developing these recommendations, the main findings concerning the interpretation of Article 7 are summarised below.

IV.1. Conclusions

Overview of Article 7

Article 7 requires that personal data shall only be processed if at least one of six legal grounds listed in that Article apply.

The first ground, Article 7(a), focuses on the consent of the data subject as a ground for legitimacy. The rest of the grounds, in contrast, allow processing – subject to safeguards – in situations where, irrespective of consent, it is appropriate and necessary to process the data within a certain context in pursuit of a specific legitimate interest.

Paragraphs (b), (c), (d) and (e) each specify a particular context, within which the processing of personal data can be considered legitimate. The conditions which apply in each of these different contexts require careful attention, as they determine the scope of the various grounds for legitimacy. More specifically, the criteria 'necessary for the performance of a contract', 'necessary for compliance with a legal obligation', 'necessary in order to protect the vital interests of the data subject', and 'necessary for the performance of a task carried out in the public interest or in the exercise of official authority' contain different requirements, which have been discussed in Section III.2.

Paragraph (f) refers, more generally, to (any kind of) legitimate interest pursued by the controller (in any context). This general provision, however, is specifically made subject to an additional balancing test, which requires the legitimate interests of the controller - or the third

initiatives that allow consumers to access their own energy usage information.' For more information on initiatives in the UK and in France see http://www.midatalab.org.uk/ and http://mesinfos.fing.org/.

[110] On the right to data portability, see Article 18 of the Proposed Regulation.

party or parties to whom the data are disclosed – to be weighed against the interests or fundamental rights of the data subjects.

Role of Article 7(f)

Article 7(f) should not be seen as a legal ground that can only be used sparingly to fill in gaps for rare and unforeseen situation as ‘a last resort’ - or as a last chance if no other grounds may apply. Nor should it be seen as a preferred option and its use unduly extended because it would be considered as less constraining than the other grounds. Rather, it is as valid a means as any of the other grounds for legitimising the processing of personal data.

Appropriate use of Article 7(f), in the right circumstances and subject to adequate safeguards, may help prevent misuse of, and over-reliance on, other legal grounds. An appropriate assessment of the balance under Article 7(f), often with an opportunity to opt-out of the processing, may in some cases be a valid alternative to inappropriate use of, for instance, the ground of 'consent' or ‘necessary for the performance of a contract'. Considered in this way, Article 7(f) presents complementary safeguards compared to the other pre-determined grounds. It should thus not be considered as 'the weakest link' or an open door to legitimise all data processing activities which do not fall under any of the other legal grounds.

Legitimate interests of the controller / interests or fundamental rights of the data subject

The concept of 'interest' is the broader stake that a controller may have in the processing, or the benefit that it derives - or that society might derive - from the processing. It may be compelling, straightforward or more controversial. Situations referred to by Article 7(f) may thus range from the exercise of fundamental rights or the protection of important personal or social interests to other less obvious or even problematic contexts.

To be considered as 'legitimate' and be relevant under Article 7(f), the interest will need to be lawful, that is, in accordance with EU and national law. It must also be sufficiently clearly articulated and specific enough to allow the balancing test to be carried out against the interests and fundamental rights of the data subject. It must also represent a real and present interest - that is, it must not be speculative.

If the controller, or the third party to whom the data are to be disclosed, has such a legitimate interest, this does not necessarily mean that it can rely on Article 7(f) as a legal ground for the processing. Whether Article 7(f) can be relied on will depend on the outcome of the balancing test that follows. The processing must also be 'necessary for the purposes of the legitimate interests' pursued by the controller or - in the case of disclosure - by the third party. Less invasive means to serve the same purpose should therefore always be preferred.

The notion of the 'interests' of the data subjects is defined even more broadly as it does not require a ‘legitimacy’ element. If the data controller or third party can pursue any interests, provided they are not illegitimate, the data subject, in turn, is entitled to have all categories of interests to be taken into account and weighed against those of the controller or third party, as long as they are relevant within the scope of the Directive.

Applying the balancing test

When interpreting the scope of Article 7(f), the Working Party aims at a balanced approach, which ensures the necessary flexibility to data controllers for situations where there is no undue impact on data subjects, while at the same time providing sufficient legal certainty and guarantees to data subjects that this open-ended provision will not be misused.

To carry out this balancing test, it is first important to consider the nature and source of the legitimate interests, and whether the processing is necessary to pursue those interests, on the one hand, and the impact on the data subjects on the other hand. This initial assessment should take into account the measures, such as transparency or limited collection of data that the controller plans to adopt to comply with the Directive.

After analysing and weighing the two sides against each other, a provisional 'balance' may be established: a preliminary conclusion may be drawn as to whether the legitimate interests of the controller prevail over the rights and interests of the data subjects. There may however be cases where the outcome of the balancing test is unclear, and there is doubt on whether the legitimate interest of the controller (or third party) prevails and whether the processing can be based on Article 7(f).

For this reason, it is important to carry out a further assessment in the balancing exercise. In this phase, the controller may consider whether it is able to introduce additional measures, going beyond compliance with other horizontal provisions of the Directive, to help protect data subjects. Additional measures may include, for example, providing an easily workable and accessible mechanism to ensure an unconditional possibility for data subjects to opt-out of the processing.

Key factors to be considered when applying the balancing test

Based on the foregoing, useful factors to be considered when carrying out the balancing test include:

- <u>the nature and source of the legitimate interest</u>, including:

  - whether the data processing is necessary for the exercise of a fundamental right, or
  - is otherwise in the public interest or benefits from social, cultural or legal/regulatory recognition in the community concerned;

- <u>the impact on the data subjects</u>, including:

  - the nature of the data, such as whether the processing involves data that may be considered sensitive or has been obtained from publicly available sources;
  - the way data are being processed, including whether the data are publicly disclosed or otherwise made accessible to a large number of persons, or whether large amounts of personal data are processed or combined with other data (e.g. in case of profiling, for commercial, law enforcement or other purposes);
  - the reasonable expectations of the data subject, especially with regard to the use and disclosure of the data in the relevant context;

- the status of the data controller and data subject, including the balance of power between the data subject and the data controller, or whether the data subject is a child or otherwise belongs to a more vulnerable segment of the population.

- additional safeguards to prevent undue impact on the data subjects, including:

  - data minimisation (e.g. strict limitations on the collection of data, or immediate deletion of data after use);
  - technical and organisational measures to ensure that the data cannot be used to take decisions or other actions with respect to individuals ('functional separation');
  - extensive use of anonymisation techniques, aggregation of data, privacy-enhancing technologies, privacy by design, privacy and data protection impact assessments;
  - increased transparency, general and unconditional right to opt-out, data portability & related measures to empower data subjects.

Accountability, transparency, the right to object and beyond

In connection with these safeguards - and the overall assessment of the balance - three issues often play a crucial role in the context of Article 7(f) and therefore require special attention:

- the existence of some and possible need for additional measures to increase transparency and accountability;
- the right of the data subject to object to the processing, and beyond objection, the availability of opt-out without the need for any justification;
- empowering data subjects: data portability and the availability of workable mechanisms for the data subject to access, modify, delete, transfer, or otherwise further process (or let third parties further process) their own data.

IV. 2. Recommendations

The current text of Article 7(f) of the Directive is open-ended. This flexible wording leaves much room for interpretation and has sometimes - as experience has shown - led to lack of predictability and lack of legal certainty. However, if used in the right context, and with the application of the right criteria, as set out in this Opinion, Article 7(f) has an essential role to play as a legal ground for legitimate data processing.

The Working Party therefore supports the current approach in Article 6 of the proposed Regulation, which maintains the balance of interests as a separate legal ground. Further guidance would however be welcome to ensure an adequate application of the balancing test.

Scope and means for further specification

An essential requirement would be that the provision remains sufficiently flexible, and that it reflects both the perspectives of the data controller and the data subject, and the dynamic nature of the relevant contexts. For this reason, the Working Party is of the view that providing - in the text of the proposed Regulation or in delegated acts - for detailed and exhaustive lists of situations in which an interest would be qualified *de facto* as legitimate is not advisable, The Working Party would equally be against defining cases where the interest or right of one party should *as a principle* or *as a presumption* override the interest or right of the other party, merely because of the nature of such an interest or right, or because certain protective measures have been taken, for example, the data have merely been pseudonymised. This would risk being both misleading and unnecessarily prescriptive.

Rather than taking definitive judgments on the merits of different rights and interests, the Working Party insists on the *crucial role of the balancing test* in the assessment of Article 7(f). There is a need to keep the flexibility of the test, but the way it is carried out must be made more effective in practice and must allow for more effective compliance. This should translate into an *enhanced* obligation of *accountability* for data controllers, where the controller bears the responsibility to *demonstrate* that its interest is not overridden by the interests and rights of the data subject.

Guidance and accountability

To achieve this, the Working Party recommends that guidance be provided in the proposed Regulation, in the following way.

1) It would be helpful to identify and provide in a recital a non-exhaustive list of key factors to be considered when applying the balancing test, such as the nature and source of the legitimate interest, the impact on the data subjects, and the additional safeguards that may be applied by the controller to prevent any undue impact of the processing on the data subjects. These safeguards may include, among others,
   - functional separation of data, appropriate use of anonymisation techniques, encryption and other technical and organisational measures to limit the potential risks to the data subjects;
   - but also measures to ensure increased transparency and choice to data subjects, such as, where appropriate, the possibility for an unconditional opportunity to opt out of the processing, free of charge and in a manner that can be easily and effectively invoked.

2) The Working Party would also support further clarification in the proposed Regulation on how the controller could *demonstrate*[111] enhanced accountability.

   The change in the conditions for data subjects to exercise the right to object as foreseen in Article 19 of the proposed Regulation is already an important element of accountability. If the data subject objects to the processing of his/her data under Article 7(f), under the proposed Regulation it will be up to the data controller to demonstrate that his/her interest prevail. This reversal of the burden of proof is strongly supported by the Working Party as it contributes to an enhanced accountability obligation.

   If the data controller does not succeed in demonstrating to the data subject in a specific case that its interest prevails, this may also have broader consequences on the whole processing, not just with respect to the data subject who objected. As a result, the controller may put into question or decide to reorganise the processing, when appropriate for the benefit of not only the specific data subject but also for the benefit of all other data subjects who may be in a similar situation.[112]

[111] Such demonstration must remain reasonable and focus on outcome rather than administrative process.

[112] In addition to reversing the burden of proof, the Working Party also supports that the proposed Regulation would no longer require that an objection be made on '*compelling* legitimate grounds relating to [the] particular situation' [of the data subject]. Rather, pursuant to the proposed Regulation, reference to any (not necessarily

This requirement is necessary but not sufficient. To ensure protection from the start, and to avoid that the shifting of the burden of proof is circumvented[113], it is important that steps are taken *before* the processing starts, and not only in the course of ex-post ‘objection’ procedures.

It is therefore proposed that, in the first stage of any processing activity, the data controller shall take several steps. The two first steps could be listed in a recital of the proposed Regulation and the third one in a specific provision:

- Conduct an assessment[114], which should include the different stages of the analysis developed in this Opinion and summarised in Annex 1. The controller would have to identify explicitly the prevailing interest(s) at stake, and why they prevail over the interests of the data subjects. Such prior assessment should not be too burdensome, and remains *scalable*: it may be limited to essential criteria if the impact of the processing on the data subjects is *prima facie* insignificant, while on the other hand it should be performed more thoroughly if the balance was difficult to achieve and would require for instance adoption of several additional safeguards. Where appropriate - i.e. when a processing operation presents specific risks to the rights and freedoms of data subjects - a more comprehensive privacy and data protection impact assessment (according to Article 33 of the proposed Regulation) should be carried out, of which the assessment under Article 7(f) could become an important part.

- Document this assessment. Just as it is *scalable* in how much detail the assessment needs to be carried out, the extent of documentation should also be scalable. With that said, some basic documentation should be available in all but the most trivial cases, independently of the appreciation of the impact of the processing on the individual. It

'compelling') legitimate grounds relating to the particular situation of the data subject would be sufficient. Indeed, a further option, which was proposed in the Final LIBE Committee Report is to also do away with the requirement that the objection would have to relate to the particular situation of the data subject. The Working Party supports this approach in the sense that it recommends that data subjects would be able to take advantage of either or both opportunities, as appropriate, that is, either object based on their own particular situation, or with a more general scope, and in this latter case without being required to provide any specific justification. See in that sense amendment 114 to Article 19(1) of the proposed Regulation in the Final LIBE Committee Report.

[113] Data controllers, for example, may be tempted to avoid case-by-case demonstration that their interest prevails, by using standard justification forms, or may make the exercise of the right to object otherwise cumbersome.

[114] This assessment, as stated earlier in footnote 84, should not be confused with a comprehensive privacy and data protection impact assessment. At present, there is no comprehensive guidance on impact assessments at European level, although in some areas, namely for RFID and smart metering, a number of welcome efforts have been made to define a sector-specific methodology/framework (and/or template) that could apply across the European Union. See 'Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications' and 'Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems' prepared by Expert Group 2 of the Commission’s Smart Grid Task Force. The Working Party issued repeated opinions with regard to both these methodologies.
In addition, there have been some initiatives to define a generic data protection impact assessment methodology, from which 'field specific' efforts could benefit. See, for example, PIAF Project (A Privacy Impact Assessment Framework for data protection and privacy rights): http://www.piafproject.eu/.
Further, for guidance at national level, see, for example, CNIL methodology:
http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf
and the ICO's Privacy Impact Assessment Handbook at
http://ico.org.uk/pia_handbook_html_v2/files/PIAhandbookV2.pdf.

is on the basis of such documentation that the assessment of the controller may be further evaluated and possibly contested;

- Give transparency and visibility to this information to the data subjects and other stakeholders. Transparency should be ensured both towards data subjects and data protection authorities, and when appropriate, the public at large. As to data subjects, the Working Party refers to the Draft LIBE Committee Report[115], which stated that the controller should inform the data subject about the reasons for believing that its interests are not overridden by the data subject's interests or fundamental rights and freedoms. Such information should in the view of the Working Party be provided to data subjects together with the information the controller has to provide under Article 10 and 11 of the present Directive (Article 11 of the proposed Regulation). This will allow possible objection by the data subject in a second phase, and additional justification on a case-by-case basis by the controller of the prevailing interests. In addition, upon request, the documentation upon which the controller based their assessment should be made available to data protection authorities, in order to allow for possible verification and enforcement where relevant.

The Working Party would support that these three steps are explicitly included in the proposed Regulation in ways as set out above. This would recognise the specific role of legal grounds in the assessment of legitimacy, and would clarify the importance of the balancing test within the wider context of accountability measures and impact assessments in the proposed new legal framework.

The Working Party considers it also advisable to entrust the EDPB with providing further guidance where necessary on the basis of this framework. This approach would allow both sufficient clarity in the text and sufficient flexibility in its implementation.

[115] Draft Report on the Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))

Annex 1. Quick guide on how to carry out the Article 7(f) balancing test

Step 1: Assessing which legal ground may potentially apply under Article 7(a)-(f)

Data processing can be implemented only if one or more of the six grounds - (a) through (f) - of Article 7 applies (different grounds can be relied on at different stages of the same processing activity). If it *prima facie* appears that Article 7(f) might be appropriate as a legal ground, proceed to step 2.

Quick tips:

- Article 7(a) applies only if free, informed, specific and unambiguous consent is given; the fact that an individual has not objected to a processing under Article 14 should not be confused with Article 7(a) consent - however, an easy mechanism to object to a processing may be considered as an important safeguard under Article 7(f);
- Article 7(b) covers processing that is necessary for the implementation of the contract; just because the data processing is related to the contract, or foreseen somewhere in the terms and conditions of the contract does not necessarily mean that this ground applies; where appropriate, consider Article 7(f) as an alternative;
- Article 7(c) addresses only clear and specific legal obligations under the laws of the EU or a Member State; in case of non-binding guidelines (for instance by regulatory agencies), or a foreign legal obligation, consider Article 7(f) as an alternative.

Step 2: Qualifying an interest as 'legitimate' or ‘illegitimate’

To be considered as legitimate, an interest must cumulatively fulfil the following conditions:

- be lawful (i.e. in accordance with EU and national law);
- be sufficiently clearly articulated to allow the balancing test to be carried out against the interests and fundamental rights of the data subject (i.e. sufficiently concrete);
- represent a real and present interest (i.e. not be speculative).

Step 3: Determining whether the processing is necessary to achieve the interest pursued

To meet this requirement, consider whether there are other less invasive means to reach the identified purpose of the processing and serve the legitimate interest of the data controller.

Step 4: Establishing a provisional balance by assessing whether the data controller’s interest is overridden by the fundamental rights or interests of the data subjects

- Consider the nature of the interests of the controller (fundamental right, other type of interest, public interest);
- Evaluate the possible prejudice suffered by the controller, by third parties or the broader community if the data processing does not take place;
- Take into account the nature of the data (sensitive in a strict or broader sense?);
- Consider the status of the data subject (minor, employee, etc.) and of the controller (e.g. whether a business organisation is in a dominant market position);
- Take into account the way data are processed (large scale, data mining, profiling, disclosure to a large number of people or publication);
- Identify the fundamental rights and/or interests of the data subject that could be impacted;

- Consider data subjects' reasonable expectations;
- Evaluate impacts on the data subject and compare with the benefit expected from the processing by the data controller.

Quick tip: Consider the effect of actual processing on particular individuals – do not see this as an abstract or hypothetical exercise.

Step 5: Establishing a final balance by taking into account additional safeguards

Identify and implement appropriate additional safeguards resulting from the duty of care and diligence such as:
- data minimisation (e.g. strict limitations on the collection of data, or immediate deletion of data after use)
- technical and organisational measures to ensure that the data cannot be used to take decisions or other actions with respect to individuals ('functional separation')
- wide use of anonymisation techniques, aggregation of data, privacy-enhancing technologies, privacy by design, privacy and data protection impact assessments;
- increased transparency, general and unconditional right to object (opt-out), data portability & related measures to empower data subjects.

Quick tip: Using privacy enhancing technologies and approaches can tip the balance in favour of the data controller and protect individuals too.

Step 6: Demonstrate compliance and ensure transparency

- Draw a blueprint of steps 1 to 5 to justify the processing before its launch.
- Inform data subjects of the reasons for believing the balance tips in the controller's favour.
- Keep documentation available to data protection authorities.

Quick tip: This step is *scalable*: details of assessment and documentation should be adapted to the nature and context of the processing. These measures will be more extensive where a large amount of information about many people is being processed, in a way that could have a significant impact on them. A comprehensive privacy and data protection impact assessment (under Article 33 of the proposed Regulation) will only be necessary when a processing operation presents specific risks to the rights and freedoms of data subjects. In these cases, the assessment under Article 7(f) could become a key part of this broader impact assessment.

Step 7: What if the data subject exercises his/her right to object?

- Where only a qualified right to opt-out is available as a safeguard (this is explicitly required under Article 14(a) as a minimum safeguard): in case the data subject objects to the processing, it should be ensured that an appropriate and user-friendly mechanism is in place to re-assess the balance as for the individual concerned and stop processing his/her data if the re-assessment shows that his/her interests prevail.
- Where an unconditional right to opt-out is provided as an additional safeguard (either because this is explicitly required under Article 14(b) or because this is otherwise deemed a necessary or helpful additional safeguard): in case the data subject objects to the processing, it should be ensured that this choice is respected, without the need to take any further step or assessment.

Annex 2. Practical examples to illustrate the application of the Article 7(f) balancing test

This Annex provides examples with regard to some of the most common contexts in which the issue of legitimate interest in the meaning of Article 7(f) may arise. In most cases, we grouped together two or more related examples that are worth comparing under a single heading. Many of the examples are based on actual cases, or elements of actual cases handled by data protection authorities in the different Member States. However, we have sometimes changed the facts to some degree to help better illustrate how to carry out the balancing test.

The examples are included in order to illustrate the *thinking process* - the method to be used to carry out the multi-factor balancing test. In other words, the examples are *not* meant to provide a *conclusive* assessment of the cases described. Indeed, in many cases, by changing the facts of the case in some way (for example, if the controller were to adopt additional safeguards such as more complete anonymisation, better security measures, and more transparency and more genuine choice for the data subjects), the outcome of the balancing test could change.[116]

This should encourage controllers to better comply with all horizontal provisions of the Directive and offer additional protection where relevant based on privacy and data protection by design. The greater care controllers take to protect personal data overall, the more likely it is that they will satisfy the balancing test.

Exercise of the right to freedom of expression or information[117], including in the media and the arts

Example 1: NGO republishes expenses of Members of Parliament

A public authority publishes - under a legal obligation (Article 7(c)) - expenses of members of parliament; a transparency NGO, in turn, analyses and re-publishes data in an accurate, proportionate, but more informative annotated version, contributing to further transparency and accountability.

Assuming the NGO carries out the re-publication and annotation in an accurate and proportionate manner, adopts appropriate safeguards, and more broadly, respects the rights of the individuals concerned, it should be able to rely on Article 7(f) as a legal ground for the processing. Factors such as the nature of the legitimate interest (a fundamental right to freedom of expression or information), the interest of the public in transparency and accountability, and the fact that the data have already been published and concern (relatively

[116] Applying correctly Article 7(f) may raise complex issues of assessment, and to help guide the assessment, specific legislation, case law, jurisprudence, guidelines, as well as codes of conduct and other formal or less formal standards may all play an important role.

[117] On freedom of expression or information, see page 34 of the Opinion. Any relevant derogations under national law for processing for journalistic purposes under Article 9 of the Directive must also be taken into account when assessing these examples.

less sensitive) personal data related to the activities of the individuals relevant to the exercise of their public functions[118], all weigh in favour of the legitimacy of the processing. The fact that the initial publication has been required by law, and that individuals should thus expect their data would be published, also contribute to the favourable assessment. On the other side of the balance, the impact on the individual may be significant, for example, because of public scrutiny, the personal integrity of some individuals may be questioned, and this may lead, for instance, to loss of elections, or in some cases to a criminal investigation for fraudulent activities. The factors above, taken together, however, show that on the balance, the controller's interests (and the interests of the public to whom the data are disclosed) override the interests of the data subjects.

Example 2: Local councillor appoints his daughter as special assistant

A journalist publishes a factually accurate, well-researched article in a local online newspaper about a local councillor revealing that he has only attended one of the last eleven council meetings and he is unlikely to be re-elected because of a recent scandal involving the appointment of his seventeen-year-old daughter as a special assistant.

A similar analysis as in *Example 1* also applies here. On the facts, it is in the legitimate interests of the newspaper in question to publish the information. Even though personal data has been revealed about the councillor, the fundamental right to freedom of expression and to publish the story in the newspaper is not overridden by the right to privacy of the councillor. This is because the privacy rights of public figures are relatively limited in respect of their public activities and because of the special importance of freedom of expression – especially where publication of a story is in the public interest.

Example 3: Top search results continue to show minor criminal offence

The on-line archive of a newspaper contains an old article concerning an individual, once a local celebrity, captain of a small town amateur football team. The individual is identified with his full name, and the story relates to his involvement in a relatively minor criminal proceeding (drunk and disorderly behaviour). The criminal records of the individual are now clean and no longer show the past offence for which he served his sentence several years ago. What is most disturbing for the individual is that by searching his name with common search engines online, the link to this old piece of news is among the first results concerning him. Notwithstanding his request, the newspaper refuses to adopt technical measures, which would restrict the broader availability of the piece of news related to the data subject. For example, the paper refuses to adopt technical and organisational measures that would aim - to the extent technology allows - limiting access to the information from external search engines using the individual's name as a search category.

This is another case to illustrate the possible conflict between freedom of expression and privacy. It also shows that in some cases additional safeguards - such as ensuring that, at least in case of a justified objection under Article 14(a) of the Directive, the relevant part of the

[118] It cannot be excluded that some expenses may reveal more sensitive data, such as health data. If this is the case, these should be edited out of the dataset before it is published in the first place. It is good practice to take a 'proactive approach' and give individuals an opportunity to review their data before their publication and to clearly inform them about the possibilities and modalities of publication.

newspaper archives will no longer be accessible by external search engines or the format used to display the information will not allow search by name - may play a key role in striking an appropriate balance between the two fundamental rights concerned. This is without prejudice to any other measures that might be taken by search engines or other third parties.[119]

Conventional direct marketing and other forms of marketing or advertisement

Example 4: Computer store advertises similar products to clients

A computer store obtains from its customers their contact details in the context of the sale of a product, and uses these contact details for marketing by regular mail of its own similar products. The shop also sells products on-line and sends out promotional emails when a new product line comes into stock. Customers are clearly informed about their opportunity to object, free of charge and in an easy manner when their contact details are collected, and each time a message is sent, in case the customer did not object initially.

The transparency of the processing, the fact that the customer can reasonably expect to receive offers for similar products as a client of the shop, and the fact that he/she has the right to object helps strengthen the legitimacy of the processing and safeguard individuals' rights. On the other side of the balance, there appears to be no disproportionate impact on the individual's right to privacy (in this example we assumed that there are no complex profiles created by the computer shop of its consumers, for example, using detailed analysis of click-stream data).

Example 5: On-line pharmacy performs extensive profiling

An online pharmacy carries out marketing based on the medicines and other products customers have purchased, including products obtained by prescription. It analyses this information – combined with demographic information about customers – for example, their age and gender – to build up a 'health and wellbeing' profile of individual customers. Click-stream data is also used, which is collected not only about the products the customers purchased but also about other products and information they were browsing on the website. The customer profiles include information or predictions suggesting that a particular customer is pregnant, suffering from a particular chronic illness, or would be interested in purchasing dietary supplements, suntan lotion or other skin-care products at certain times of the year. The online pharmacy's analysts use this information to offer non-prescription medicines, health supplements and other products to particular individuals by email. In this case the pharmacy cannot rely on its legitimate interests when creating and using its customer profiles for marketing. There are several problems posed by the profiling described. The information is particularly sensitive and can reveal a great deal about matters that many individuals would expect to remain private.[120] The extent and manner of profiling (use of click-stream data, predictive algorithms) also suggest a high level of intrusiveness. Consent based on Article 7(a) and Article 8(2)(a) (where sensitive data are involved) could, however, be considered as an alternative where appropriate.

[119] See also Case C-131/12 Google Spain v Agencia Española de Proteccion de Datos, currently before the Court of Justice of the European Union.

[120] Beyond any restrictions posed by data protection laws, advertisement of prescription products is also strictly regulated in the EU, and there are also some restrictions regarding advertisement on non-prescription drugs. Further, the requirements of Article 8 on special categories of data (such as health data) must also be considered.

Unsolicited non-commercial messages, including for political campaigns or charitable fundraising

Example 6: Candidate in local election makes targeted use of electoral register

A candidate in local election uses the electoral register[121] to send an introduction letter promoting her campaign for the upcoming elections to each potential voter in her election district. The candidate uses the data obtained from the electoral register only to send the letter and does not retain the data once the campaign has ended.

Such use of the local register is in the reasonable expectations of individuals, when it takes place in the pre-election period: the interest of the controller is clear and legitimate. The limited and focused use of the information also contributes to tip the balance in favour of the legitimate interest of the controller. Such use of electoral registers may also be regulated by law at national level, in a public interest perspective, providing for specific rules, limitations and safeguards with regard to the use of the electoral register. If this is the case, compliance with these specific rules is also required to ensure the legitimacy of the processing.

Example 7: Non-profit-seeking body collects information for targeting purposes

A philosophical organisation dedicated to human and social development decides to organise fundraising activities based on the profile of its members. To this end, it collects data on social networking sites by means of ad-hoc software targeting individuals who 'liked' the organisation's page, 'liked' or 'shared' the messages the organisation posted on its page, regularly viewed certain items or re-tweeted the organisation's messages. It then sends messages and newsletters to its members according to their profiles. For example, elderly dog owners who 'liked' articles on animal shelters receive different fundraising appeals from families with small children; people from different ethnic groups also receive different messages.

The fact that special categories of data are processed (philosophical beliefs) requires compliance with Article 8, a condition which seems to be met as the processing takes place in the course of the legitimate activities of the organisation. However, this is not a sufficient condition in this case: the way data are being used exceeds the reasonable expectations of individuals. The amount of data collected, the lack of transparency about the collection and the reuse of data initially published for one purpose for a different purpose contribute to the conclusion that Article 7 (f), cannot be relied on in this case. The processing should therefore not be allowed except if another ground can be used, for instance the consent of individuals under Article 7(a).

[121] It is assumed that in the Member State where the example applies an electoral register is established by law.

Enforcement of legal claims, including debt collection via out-of-court procedures

Example 8: Dispute on quality of renovation work

A customer disputes the quality of kitchen renovation work and refuses to pay the full price. The building company transfers the relevant and proportionate data to his lawyer in order that he could remind the customer of payment and negotiate a settlement with the customer if he continues to refuse to pay.

In this case, the preliminary steps taken by the building company using basic information of the data subject (e.g. name, address, contract reference) to send a reminder to the data subject (directly or via its lawyer as in this case) may still fall within the processing necessary for the performance of the contract (Article 7(b)). Further steps taken,[122] including the involvement of a debt collection agency, should however be assessed under Article 7(f) considering, among others, their intrusiveness and impact on the data subject as will be shown in the following example.

Example 9: Customer disappears with car purchased on credit

A customer fails to pay for the instalments that are due on an expensive sports car purchased on credit, and then 'disappears'. The car dealer contracts a third-party 'collection agent'. The collection agent carries out an intrusive 'law-enforcement style' investigation, using, among others, practices such as covert video-surveillance and wire-tapping.

Although the interests of the car dealer and the collection agent are legitimate, the balance does not tip in their favour because of the intrusive methods used to collect information, some of which are explicitly prohibited by law (wire-tapping). The conclusion would be different if, for instance, the car dealer or the collection agent only carried out limited checks to confirm the contact details of the data subject in order to start a court procedure.

Prevention of fraud, misuse of services, or money laundering

Example 10: Verification of clients' data before opening of a bank account

A financial institution follows reasonable and proportionate procedures - as per non-binding guidelines of competent government financial supervisory authority - to verify the identity of any person seeking to open an account. It maintains records of the information used to verify the person's identity.

The interest of the controller is legitimate, the processing of data involves only limited and necessary information (standard practice in the industry, to be reasonably expected by data subjects, and recommended by competent authorities). Appropriate safeguards are in place to limit any disproportionate and undue impact on the data subjects. The controller can therefore rely on Article 7(f). Alternatively, and to the extent that the actions taken are specifically required by applicable law, Article 7(c) could apply.

[122] There is currently, among the different Member States, a degree of variance as to which measures may be considered necessary for the performance of a contract.

Example 11: Exchange of information to fight money laundering

A financial institution - after obtaining advice of the competent data protection authority – implements procedures based on specific and limited criteria to exchange data regarding suspected abuse of anti-money laundering rules with other companies within the same group, with strict limitation on access, security, and prohibition of any further use for other purposes.

For reasons similar to those explained above, and depending on the facts of the case, the processing of data could be based on Article 7(f). Alternatively, and to the extent that the actions taken are specifically required by applicable law, Article 7(c) could apply.

Example 12: Black list of aggressive drug-addicts

A group of hospitals create a joint black list of 'aggressive' individuals in search of drugs, with the aim of prohibiting them access to all medical premises of the participating hospitals.

Even if the interest of the controllers in maintaining safe and secure premises is legitimate, it has to be balanced against the fundamental right of privacy and other compelling concerns such as the need not to exclude the individuals concerned from access to health treatment. The fact that sensitive data are processed (e.g. health data related to drug addiction) also supports the conclusion that in this case the processing is unlikely to be acceptable under Article 7(f).[123] The processing might be acceptable if it were to be for instance regulated in a law providing for specific safeguards (checks and controls, transparency, prevention of automated decisions) ensuring that it would not result in discrimination or violation of fundamental rights of individuals[124]. In this latter case, depending on whether this specific law requires or only permits the processing, either Article 7(c) or Article 7(f) may be relied on as a legal ground.

Employee monitoring for safety or management purposes

Example 13: Working hours of lawyers used both for billing and bonus purposes

The number of billable hours worked by lawyers at a law firm is processed both for billing purposes and for determination of annual bonuses. The system is transparently explained to employees who have an explicit right to express disagreement with the conclusions in terms of both billing and bonus payment, to be then discussed with their management.

The processing appears necessary for the legitimate interests of the controller, and there does not appear to be a less intrusive way to achieve the purpose. The impact on employees is also limited due to the safeguards and processes put in place. Article 7(f) could therefore be an appropriate legal ground in this case. There may also be an argument to support that processing for one or both purposes is also necessary for the performance of the contract.

[123] The requirements of Article 8 on special categories of data (such as health data) must also be considered.

[124] See the Working document on Black Lists (WP 65) adopted on 3 October 2002.

Example 14: Electronic monitoring of internet use[125]

The employer monitors internet use during working hours by employees to check they are not making excessive personal use of the company's IT. The data collected include temporary files and cookies generated on the employees' computers, showing websites visited and downloads performed during working hours. The data is processed without prior consultation of data subjects and the trade union representatives/work council in the company. There is also insufficient information provided to the individuals concerned about these practices.

The amount and nature of the data collected represents a significant intrusion into the private life of the employees. In addition to proportionality issues, transparency about the practices, closely linked to the reasonable expectations of the data subjects, is also an important factor to be considered. Even if the employer has a legitimate interest in limiting the time spent by the employees visiting websites not directly relevant to their work, the methods used do not meet the balancing test of Article 7(f). The employer should use less intrusive methods (e.g. limiting accessibility of certain sites), which are, as best practice, discussed and agreed with employees' representatives, and communicated to the employees in a transparent way.

Whistle-blowing schemes

Example 15: Whistleblowing scheme to comply with foreign legal obligations

An EU branch of a US group establishes a limited whistle-blowing scheme to report serious infringements in the field of accounts and finance. The entities of the group are subjected to a code of good governance that calls for strengthening procedures for internal control and risk management. Because of its international activities, the EU branch is required to supply reliable financial data to other members of the group in the US. The scheme is designed to be compliant with both US law and the guidelines provided by the national data protection authorities in the EU.

Among the safeguards, employees are given clear guidance as to the circumstances in which the scheme should be used, through training sessions and other means. Staff are warned not to abuse the scheme – for example by making false or unfounded allegations against other members of staff. It is also explained to them that if they prefer they can use the scheme anonymously or if they wish they can identify themselves. In the latter case, employees are informed of the circumstances in which information identifying them will be fed back to their employer or passed-on to other agencies.

If the scheme were required to be established under EU law or under the law of an EU Member State, the processing could be based on Article 7(c). However, foreign legal obligations do not qualify as a legal obligation for purposes of Article 7(c), and therefore, such an obligation could not legitimise the processing under Article 7(c). However, the processing could be based on Article 7(f), for example, if there is a legitimate interest in guaranteeing the stability of financial markets, or the fight against corruption, and provided

[125] A few Member States consider that some limited electronic monitoring may be 'necessary for the performance of a contract', and therefore, may be based on the legal ground of Article 7(b) rather than 7(f).

that the scheme includes sufficient safeguards, in accordance with guidance from the relevant regulatory authorities in the EU.

Example 16: 'In-house' whistle-blowing scheme without consistent procedures

A financial services company decides to set up a whistle-blowing scheme because it suspects widespread theft and corruption amongst its staff and is keen to encourage employees to inform on each other. In order to save money, the company decides to operate the scheme in-house, staffed by members of its Human Resources department. In order to encourage employees to use the scheme it offers a cash 'no questions asked' reward to employees whose whistle-blowing activities lead to the detection of improper conduct and the recovery of monies.

The company does have a legitimate interest in detecting and preventing theft and corruption. However, its whistle-blowing scheme is so badly designed and lacking in safeguards that its interests are overridden by both the interests and right to privacy of its employees – particular those who may be the victim of false reports filed purely for financial gain. The fact that the scheme is operated in-house rather than independently is another problem here, as is the lack of training and guidance on the use of the scheme.

Physical security, IT and network security

Example 17: Biometric controls in a research laboratory

A scientific research laboratory working with lethal viruses uses a biometric entrance system due to the high risk to public health in case these viruses were to escape the premises. Appropriate safeguards are applied, including the fact that biometric data are stored on personal employee cards and not in a centralised system.

Even if data are sensitive in the broad sense, the reason for their processing is in the public interest. This and the fact that risks of misuse are reduced by appropriate use of safeguards make Article 7(f) an appropriate basis for the processing.

Example 18: Hidden cameras to identify smoking visitors and employees

A company makes use of hidden cameras to identify employees and visitors who smoke in unauthorised areas of the building.

While the controller has a legitimate interest to ensure compliance with non-smoking rules, the means used to reach this end are - generally speaking - disproportionate and unnecessarily intrusive. There are less intrusive and more transparent methods (such as smoke detectors and visible signs) available. The processing thus fails to comply with Article 6, which requires data to be 'not excessive' in relation to the purposes for which they are collected or further processed. At the same time, it will probably fail to meet the balancing test of Article 7.

Scientific research

Example 19: Research on effects of divorce and parental unemployment on children's education attainment

Under a research programme adopted by the government, and authorised by a competent ethics committee, research is performed into the relationship between divorce, parental unemployment and children's educational attainment. While not classified as 'special categories of data', the research is nevertheless focusing on issues that for many families, would be considered very intimate personal information. The research will allow special educational assistance to be targeted at children who may otherwise fall into absenteeism, poor educational attainment, adult unemployment and criminality. The law of the Member State concerned explicitly allows processing of personal data (other than special categories of data) for research purposes, provided the research is necessary for important public interests, and carried out subject to adequate safeguards, which are then further detailed in implementing legislation. This legal framework includes specific requirements but also an accountability framework that allows for assessment on a case-by-case basis of the permissibility of the research (if carried out without the consent of the individuals concerned) and the specific measures to be applied to protect the data subjects.

The researcher runs a secure research facility and, under secure conditions, the relevant information is provided to it by the population registry, courts, unemployment agencies, and schools. The research centre then 'hashes' individuals' identities so that divorce, unemployment and education records can be linked, but without revealing individuals' 'civic' identities – e.g. their names and addresses. All the original data is then irretrievably deleted. Further measures are also taken to ensure functional separation (i.e. that data will only be used for research purposes) and reduce any further risk of re-identification.

Staff members working at the research centre receive rigorous security training and are personally - possibly even criminally - liable for any security breach they are responsible for. Technical and organisational measures are taken, for example, to ensure that staff using USB sticks could not remove personal data from the facility.

It is in the legitimate interests of the research centre to carry out the research, in which there is a strong public interest. It is also in the legitimate interests of the employment, educational and other bodies involved in the scheme, because it will help them to plan and deliver services to those that most need them. The privacy aspects of the scheme have been well designed and the safeguards that are in place mean that the legitimate interests of the organisations involved in carrying out the research are not overridden by either the interests or privacy rights of the parents or children whose records formed the basis of the research.

Example 20: Research study on obesity

A university wants to carry out research into levels of childhood obesity in several cities and rural communities. Despite generally having difficulties gaining access to the relevant data from schools and other institutions, it does manage to persuade a few dozens of school teachers to monitor for a period of time children in their classes who appear obese and to ask them questions about their diet, levels of physical activity, computer-game use and so forth. These school teachers also record the names and addresses of the children interviewed so that an online music voucher can be sent to them as a reward for taking part in the research. The researchers then compile a database of children, correlating levels of obesity with physical activity and other factors. The paper copies of the completed interview questionnaires – still in a form that identifies particular children – are kept in the university archives for an indefinite period of time and without adequate security measures. Photocopies of all questionnaires are shared on request with any MD or PhD student of the same and of partner universities across the world who show interest in further use of the research data.

Although it is in the legitimate interests of the university to carry out research, there are several aspects of the research design that mean these interests are overridden by the interests and rights to privacy of the children. Besides the research methodology, which is lacking in scientific rigour, the problem emanates in particular from the lack of privacy enhancing approaches in the research design and the broad access to the personal data collected. At no point are children's records coded or anonymised and no other measures are taken to ensure either security of the data or functional separation. Valid Article 7(a) and Article 8(2)(a) consent is not obtained, either, and it is not clear that it has been explained to either the children or their parents what their personal data will be used for or with whom it will be shared.

Foreign legal obligation

Example 21: Compliance with third country tax law requirements

EU banks collect and transfer some of their clients' data for purposes of their clients' compliance with third country taxation obligations. The collection and transfer is specified in and takes place under conditions and safeguards agreed between the EU and the foreign country in an international agreement.

While a foreign obligation in itself cannot be considered a legitimate basis for processing under Article 7(c), it may well be if such obligation is upheld in an international agreement. In this latter case, the processing could be considered necessary for complying with a legal obligation incorporated into the internal legal framework by the international agreement. However, if there is no such agreement in place, the collection and transfer will have to be assessed under Article 7(f) requirements, and may only be considered permissible provided that adequate safeguards are put in place such as those approved by the competent data protection authority (see also *Example 15* above).

Example 22: Transfer of data on dissidents

Upon request, an EU company transfers data of foreign residents to an oppressive regime in a third country that wishes to access data of dissidents (e.g. their email traffic data, email content, browsing history, or private messages in social networks).

In this case, unlike in the previous example, there is no international agreement that would allow for applying Article 7(c) as a legal ground. Besides, several elements argue against Article 7(f) as an appropriate ground for processing. Although the controller may have an economic interest in ensuring that it complies with foreign government requests (otherwise it might suffer less favourable treatment by the third country government compared to other companies), the legitimacy and proportionality of the transfer is highly questionable under the EU fundamental rights framework. Its potentially huge impact on the individuals concerned (e.g. discrimination, imprisonment, death penalty) also greatly argue in favour of the interests and rights of the individuals concerned.

Reuse of publicly available data

Example 23: Rating of politicians[126]

A transparency NGO uses publicly available data on politicians (promises made at the time of their election and actual voting records) to rate them based on how well they kept their promises.

Even if the impact on politicians concerned may be significant, the fact that processing is based on public information and in relation to their public responsibilities makes, with a clear purpose of enhancing transparency and accountability, the balance tips in the interest of the controller[127].

Children and other vulnerable persons

Example 24: Information website for teenagers

An NGO website offering advice to teenagers regarding issues such as drug abuse, unwanted pregnancy and alcohol abuse collects data via its own server about visitors to the site. It then immediately anonymises these data and turns them into general statistics about which parts of the website are most popular among visitors coming from different geographical regions of the country.

Article 7(f) could be used as a legal ground even if data concerning vulnerable individuals are concerned, because the processing is in the public interest and strict safeguards are put in place (the data are immediately rendered anonymous and only used for the creation of statistics), which helps tipping the balance in favour of the controller.

Privacy by design solutions as additional safeguards

Example 25: Access to mobile phone numbers of users and non-users of an app: 'compare and forget'

Personal data of individuals are processed to check whether they had already granted unambiguous consent in the past (i.e., 'compare and forget' as a safeguard).

An application developer is required to have the data subjects' unambiguous consent for processing their personal data: for example, the app developer wishes to access and collect the entire electronic address book of users of the app, including the mobile phone numbers of contacts that are not using the app. To be able to do this, it may first have to assess whether

[126] See and compare also with Example 7 above.

[127] As in *Examples 1 and 2,* we assumed that the publication is accurate and proportionate - lack of safeguards and other factors may change the balance of interests depending on the facts of the case.

the holders of the mobile phone numbers in the address books of users of the app have granted their unambiguous consent (under Article 7(a)) for their data to be processed.

For this limited initial processing (i.e., short-term read access to the full address book of a user of the app), the app developer may rely on Article 7(f) as a legal ground, subject to safeguards. These safeguards should include technical and organisational measures to ensure that the company only uses this access to help the user identify which of his contact persons are already users, and which therefore had already granted unambiguous consent in the past to the company to collect and process phone numbers for this purpose. The mobile phone numbers of non-users may only be collected and used for the strictly limited objective of verifying whether they have granted their unambiguous consent for their data to be processed, and they should be immediately deleted thereafter.

Combination of personal information across web services

Example 26: Combination of personal information across web services

An internet company providing various services including search engine, video sharing, social networking, develops a privacy policy which contains a clause that enables it 'to combine all personal information' collected on each of its users in relation to the different services they use, without defining any data retention period. According to the company, this is done in order to 'guarantee the best possible quality of service'.

The company makes some tools available to different categories of users so that they can exercise their rights (e.g. deactivate targeted advertisement, oppose to the setting of a specific type of cookies).

However, the tools available do not allow users to effectively control the processing of their data: users cannot control the specific combinations of their data across services and users cannot object to the combination of data about them. Overall, there is an imbalance between the company's legitimate interest and the protection of users' fundamental rights and Article 7(f) should not be relied on as a legal ground for processing. Article 7(a) would be a more appropriate ground to be used, provided that the conditions for a valid consent are met.

JOINT COMMENTS OF
AIRLINES FOR AMERICA,
THE INTERNATIONAL AIR TRANSPORT ASSOCIATION,
THE REGIONAL AIRLINE ASSOCIATION, AND
THE NATIONAL AIR CARRIER ASSOCIATION

Docket CDC-2020-0013

ATTACHMENT 24

Report of the WHO-China Joint Mission on Coronavirus Disease 2019 (COVID-19)

16-24 February 2020

Table of Contents

I. The Mission

Goal and Objectives

The overall goal of the Joint Mission was to rapidly inform national (China) and international planning on next steps in the response to the ongoing outbreak of the novel coronavirus disease (COVID-19[1]) and on next steps in readiness and preparedness for geographic areas not yet affected.

The major objectives of the Joint Mission were as follows:

- To enhance understanding of the evolving COVID-19 outbreak in China and the nature and impact of ongoing containment measures;
- To share knowledge on COVID-19 response and preparedness measures being implemented in countries affected by or at risk of importations of COVID-19;
- To generate recommendations for adjusting COVID-19 containment and response measures in China and internationally; and
- To establish priorities for a collaborative programme of work, research and development to address critical gaps in knowledge and response and readiness tools and activities.

Members & Method of Work

The Joint Mission consisted of 25 national and international experts from China, Germany, Japan, Korea, Nigeria, Russia, Singapore, the United States of America and the World Health Organization (WHO). The Joint Mission was headed by Dr Bruce Aylward of WHO and Dr Wannian Liang of the People's Republic of China. The full list of members and their affiliations is available in Annex A. The Joint Mission was implemented over a 9-day period from 16-24 February 2020. The schedule of work is available in Annex B.

The Joint Mission began with a detailed workshop with representatives of all of the principal ministries that are leading and/or contributing to the response in China through the National Prevention and Control Task Force. A series of in-depth meetings were then conducted with national level institutions responsible for the management, implementation and evaluation of the response, particularly the National Health Commission and the China Centers for Disease Control and Prevention (China CDC). To gain first-hand knowledge on the field level implementation and impact of the national and local response strategy, under a range of epidemiologic and provincial contexts, visits were conducted to Beijing Municipality and the provinces of Sichuan (Chengdu), Guangdong (Guangzhou, Shenzhen) and Hubei (Wuhan). The field visits included community centers and health clinics, country/district hospitals, COVID-19 designated hospitals, transportations hubs (air, rail, road), a wet market, pharmaceutical and personal protective equipment (PPE) stocks warehouses, research institutions, provincial health commissions, and local Centers for

[1] In the Chinese version of this report, COVID-19 is referred to throughout as novel coronavirus pneumonia or NCP, the term by which COVID-19 is most widely known in the People's Republic of China.

Disease Control (provincial and prefecture). During these visits, the team had detailed discussion and consultations with Provincial Governors, municipal Mayors, their emergency operations teams, senior scientists, frontline clinical, public health and community workers, and community neighbourhood administrators. The Joint Mission concluded with working sessions to consolidate findings, generate conclusions and propose suggested actions.

To achieve its goal, the Joint Mission gave particular focus to addressing key questions related to the natural history and severity of COVID-19, the transmission dynamics of the COVID-19 virus in different settings, and the impact of ongoing response measures in areas of high (community level), moderate (clusters) and low (sporadic cases or no cases) transmission.

The findings in this report are based on the Joint Mission's review of national and local governmental reports, discussions on control and prevention measures with national and local experts and response teams, and observations made and insights gained during site visits. The figures have been produced using information and data collected during site visits and with the agreement of the relevant groups. References are available for any information in this report that has already been published in journals.

The final report of the Joint Mission was submitted on 28 February 2020.

II. Major findings

The major findings are described in six sections: the virus, the outbreak, transmission dynamics, disease progression and severity, the China response and knowledge gaps. More detailed descriptions of technical findings are provided in Annex C.

The virus

On 30 December 2019, three bronchoalveolar lavage samples were collected from a patient with pneumonia of unknown etiology – a surveillance definition established following the SARS outbreak of 2002-2003 – in Wuhan Jinyintan Hospital. Real-time PCR (RT-PCR) assays on these samples were positive for pan-Betacoronavirus. Using Illumina and nanopore sequencing, the whole genome sequences of the virus were acquired. Bioinformatic analyses indicated that the virus had features typical of the coronavirus family and belonged to the Betacoronavirus 2B lineage. Alignment of the full-length genome sequence of the COVID-19 virus and other available genomes of Betacoronavirus showed the closest relationship was with the bat SARS-like coronavirus strain BatCov RaTG13, identity 96%.

Virus isolation was conducted with various cell lines, such as human airway epithelial cells, Vero E6, and Huh-7. Cytopathic effects (CPE) were observed 96 hours after inoculation. Typical crown-like particles were observed under transmission electron microscope (TEM) with negative staining. The cellular infectivity of the isolated viruses could be completely neutralized by the sera collected from convalescent patients. Transgenic human ACE2 mice and Rhesus monkey intranasally challenged by this virus isolate induced multifocal pneumonia with interstitial hyperplasia. The COVID-19 virus was subsequently detected and isolated in the lung and intestinal tissues of the challenged animals.

Whole genome sequencing analysis of 104 strains of the COVID-19 virus isolated from patients in different localities with symptom onset between the end of December 2019 and mid-February 2020 showed 99.9% homology, without significant mutation (Figure 1).

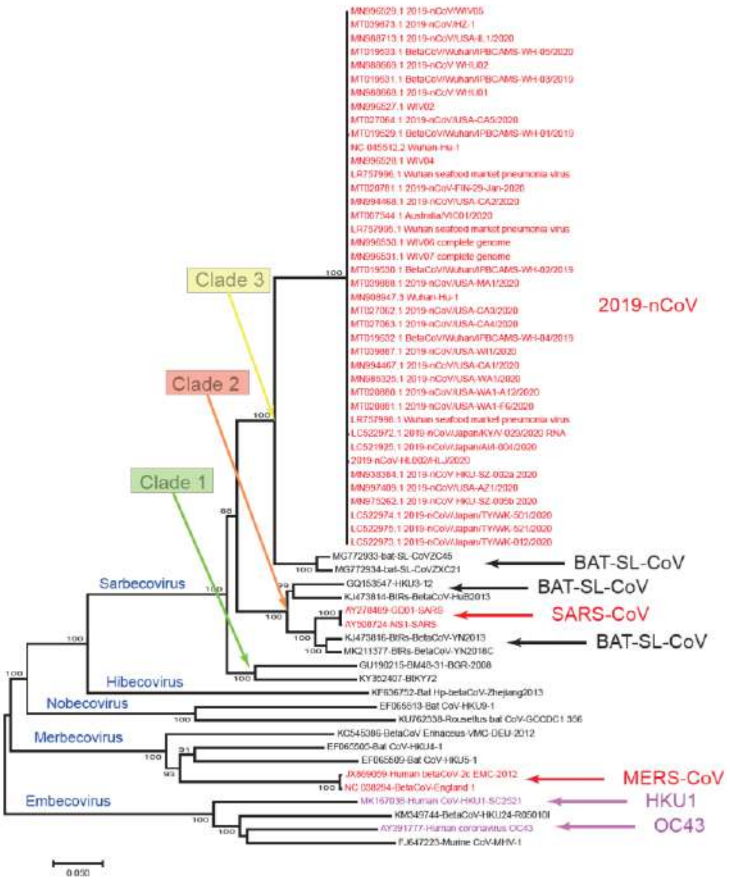

MN996529.1 2019-nCoV/WIV05
MT039873.1 2019-nCoV/HZ-1
MN988713.1 2019-nCoV/USA-IL1/2020
MT019533.1 BetaCoV/Wuhan/IPBCAMS-WH-05/2020
MN988669.1 2019-nCoV WHU02
MT019531.1 BetaCoV/Wuhan/IPBCAMS-WH-03/2019
MN988668.1 2019-nCoV WHU01
MN996527.1 WIV02
MT027064.1 2019-nCoV/USA-CA5/2020
MT019529.1 BetaCoV/Wuhan/IPBCAMS-WH-01/2019
NC 045512.2 Wuhan-Hu-1
MN996528.1 WIV04
LR757996.1 Wuhan seafood market pneumonia virus
MT020781.1 2019-nCoV-FIN-29-Jan-2020
MN994468.1 2019-nCoV/USA-CA2/2020
MT007544.1 Australia/VIC01/2020
LR757995.1 Wuhan seafood market pneumonia virus
MN996530.1 WIV06 complete genome
MN996531.1 WIV07 complete genome
MT019530.1 BetaCoV/Wuhan/IPBCAMS-WH-02/2019
MT039888.1 2019-nCoV/USA-MA1/2020
MN908947.3 Wuhan-Hu-1
MT027062.1 2019-nCoV/USA-CA3/2020
MT027063.1 2019-nCoV/USA-CA4/2020
MT019532.1 BetaCoV/Wuhan/IPBCAMS-WH-04/2019
MT039887.1 2019-nCoV/USA-WI1/2020
MN994467.1 2019-nCoV/USA-CA1/2020
MN985325.1 2019-nCoV/USA-WA1/2020
MT020880.1 2019-nCoV/USA-WA1-A12/2020
MT020881.1 2019-nCoV/USA-WA1-F6/2020
LR757998.1 Wuhan seafood market pneumonia virus
LC522972.1 2019-nCoV/Japan/KY/V-029/2020 RNA
LC521925.1 2019-nCoV/Japan/AI/I-004/2020
2019-nCoV-HL002/HLJ/2020
MN938384.1 2019-nCoV HKU-SZ-002a 2020
MN997409.1 2019-nCoV/USA-AZ1/2020
MN975262.1 2019-nCoV HKU-SZ-005b 2020
LC522974.1 2019-nCoV/Japan/TY/WK-501/2020
LC522975.1 2019-nCoV/Japan/TY/WK-521/2020
LC522973.1 2019-nCoV/Japan/TY/WK-012/2020
2019-nCoV
Clade 3
Clade 2
Clade 1
100
100
100
88
99
100
100
100
100
100
100
100
100
91
93
100
100
100
MG772933-bat-SL-CoVZC45
MG772934-bat-SL-CoVZXC21
BAT-SL-CoV
GQ153547-HKU3-12
KJ473814-BtRs-BetaCoV-HuB2013
BAT-SL-CoV
AY278489-GD01-SARS
AY508724-NS1-SARS
SARS-CoV
KJ473816-BtRs-BetaCoV-YN2013
MK211377-BtRs-BetaCoV-YN2018C
BAT-SL-CoV
GU190215-BM48-31-BGR-2008
KY352407-BtKY72
Sarbecovirus
Hibecovirus
KF636752-Bat Hp-betaCoV-Zhejiang2013
Nobecovirus
EF065513-Bat CoV-HKU9-1
KU762338-Rousettus bat CoV-GCCDC1 356
Merbecovirus
KC545386-BetaCoV Erinaceus VMC-DEU-2012
EF065505-Bat CoV-HKU4-1
EF065509-Bat CoV-HKU5-1
JX869059-Human betaCoV 2c EMC-2012
NC 038294-BetaCoV-England 1
MERS-CoV
Embecovirus
MK167038-Human CoV-HKU1-SC2521
HKU1
KM349744-BetaCoV-HKU24-R05010I
AY391777-Human coronavirus OC43
OC43
FJ647223-Murine CoV-MHV-1
0.050

Figure 1. Phylogenetic analysis of the COVID-19 virus and its closely related reference genomes

Note: COVID-19 virus is referred to as 2019-nCoV in the figure, the interim virus name WHO announced early in the outbreak.

Post-mortem samples from a 50-year old male patient from Wuhan were taken from the lung, liver, and heart. Histological examination showed bilateral diffuse alveolar damage with cellular fibromyxoid exudates. The lung showed evident desquamation of pneumocytes and hyaline membrane formation, indicating acute respiratory distress syndrome (ARDS). Lung tissue also displayed cellular and fibromyxoid exudation, desquamation of pneumocytes and pulmonary oedema. Interstitial mononuclear inflammatory infiltrates, dominated by lymphocytes, were seen in both lungs. Multinucleated syncytial cells with atypical enlarged pneumocytes characterized by large nuclei, amphophilic granular cytoplasm, and prominent nucleoli were identified in the intra-alveolar spaces, showing viral cytopathic-like changes. No obvious intranuclear or intracytoplasmic viral inclusions were identified.

The outbreak

As of 20 February 2020, a cumulative total of 75,465 COVID-19 cases were reported in China. Reported cases are based on the National Reporting System (NRS) between the

National and Provincial Health Commissions. The NRS issues daily reports of newly recorded confirmed cases, deaths, suspected cases, and contacts. A daily report is provided by each province at 0300hr in which they report cases from the previous day.

The epidemic curves presented in Figures 2 and 3 are generated using China's National Infectious Disease Information System (IDIS), which requires each COVID-19 case to be reported electronically by the responsible doctor as soon as a case has been diagnosed. It includes cases that are reported as asymptomatic and data are updated in real time. Individual case reporting forms are downloaded after 2400hr daily. Epidemiologic curves for Wuhan, Hubei (outside of Wuhan), China (outside Hubei) and China by symptom onset are provided in Figure 2.

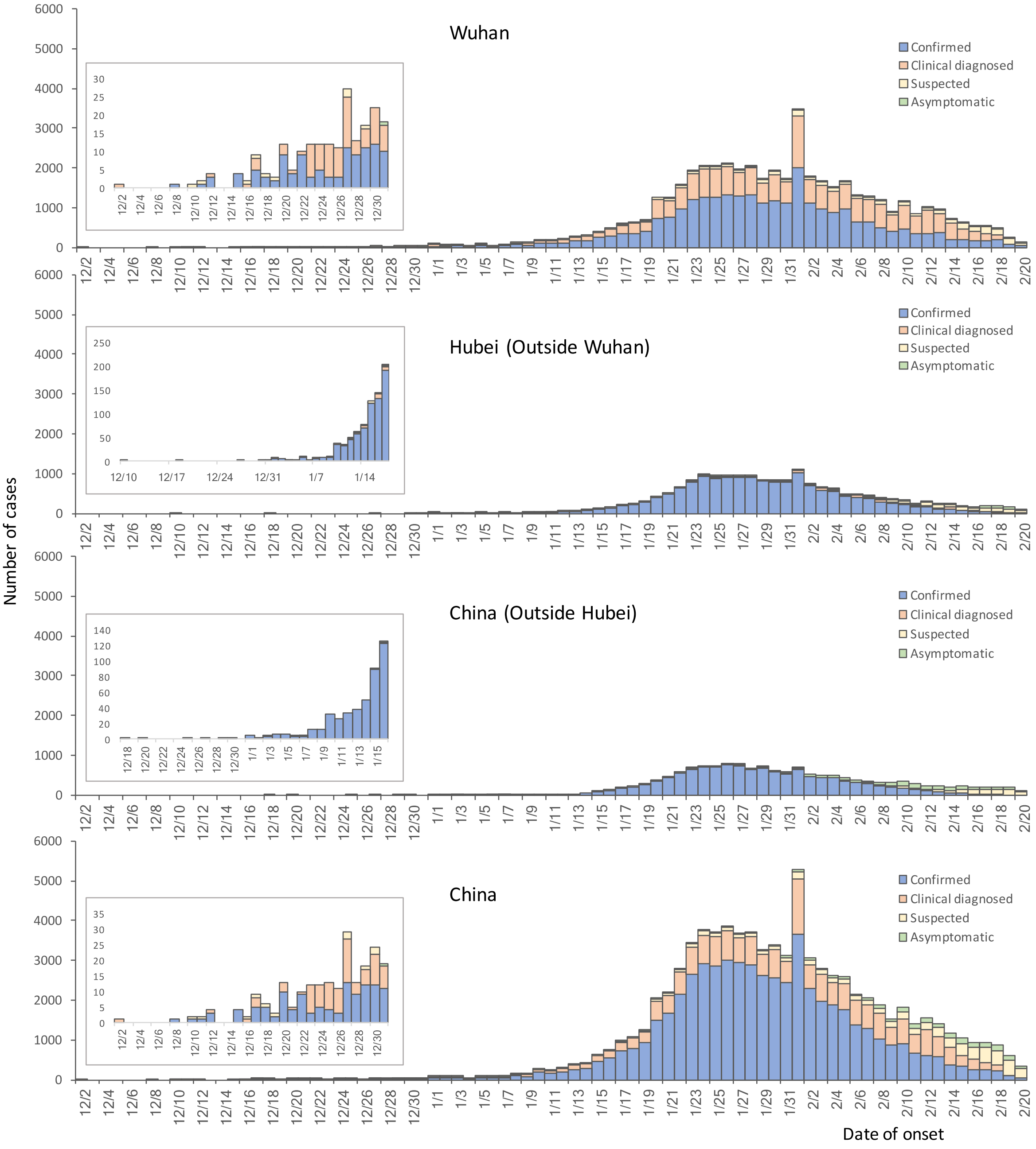


Figure 2 Epidemiologic curve of COVID-19 laboratory confirmed cases, by date of onset of illness, reported in China, as of 20 February 2020

Figure 3 presents epidemic curves of laboratory-confirmed cases, by symptom onset and separately by date of report, at 5, 12, and 20 February 2020. Figures 2 and 3 illustrate that the epidemic rapidly grew from 10-22 January, reported cases peaked and plateaued between 23 January and 27 January, and have been steadily declining since then, apart from the spike that was reported on 1 February (note: at a major hospital in Wuhan, fever clinic patients fell from a peak of 500/day in late January to average 50/day since mid-February).

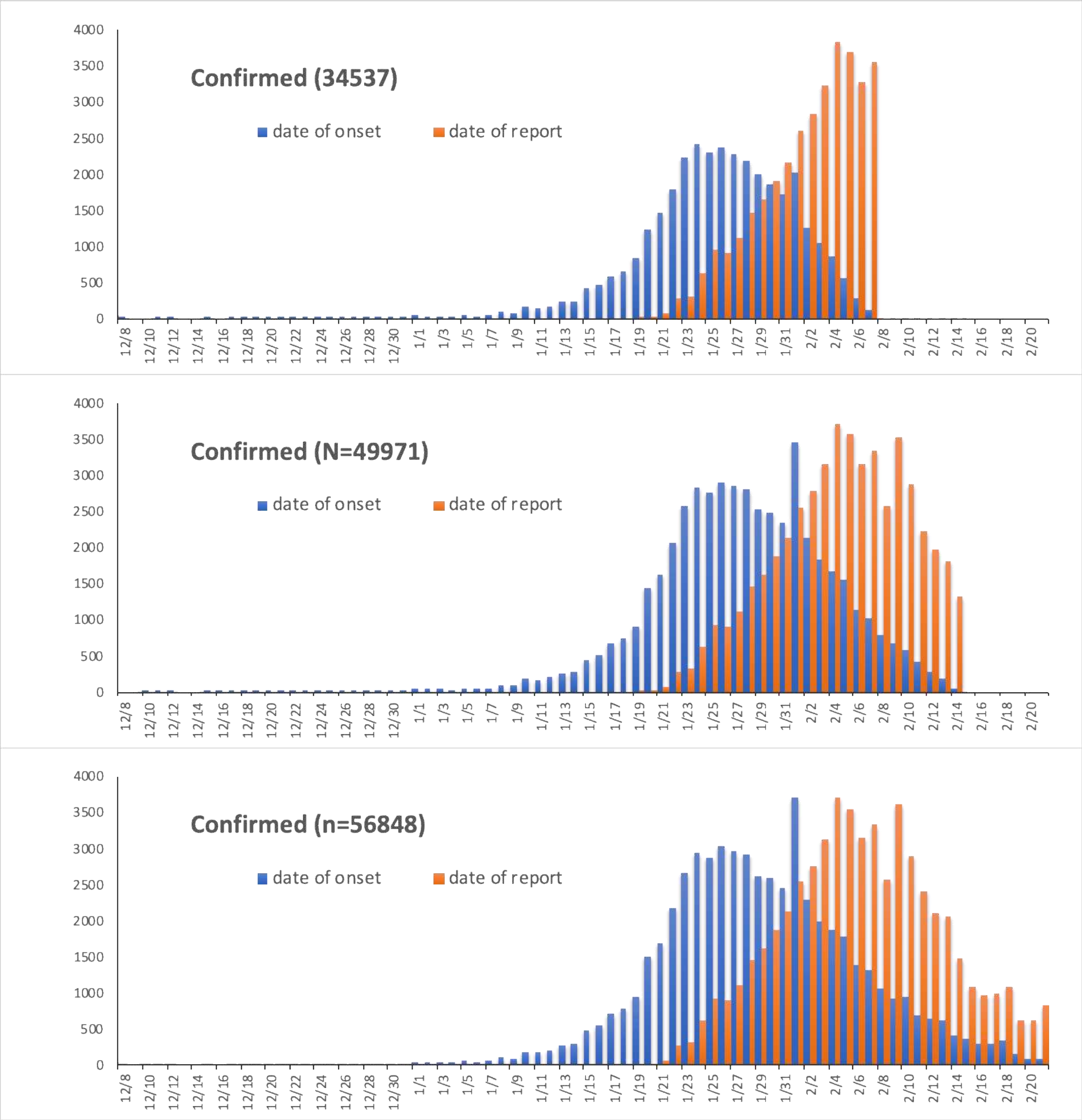


Figure 3. Epidemic curves by symptom onset and date of report as of 5 February (top panel), 12 February (middle panel) and 20 February 2020 (lower panel) for laboratory confirmed COVID-19 cases for all of China

Based on these epidemic curves, the published literature, and our on-site visits in Wuhan (Hubei), Guangdong (Shenzhen and Guangzhou), Sichuan (Chengdu), and Beijing, the Joint Mission team has made the following epidemiological observations:

Demographic characteristics

Among 55,924 laboratory confirmed cases reported as of 20 February 2020, the median age is 51 years (range 2 days-100 years old; IQR 39-63 years old) with the majority of cases (77.8%) aged between 30–69 years. Among reported cases, 51.1% are male, 77.0% are from Hubei and 21.6% are farmers or laborers by occupation.

Zoonotic origins

COVID-19 is a zoonotic virus. From phylogenetics analyses undertaken with available full genome sequences, bats appear to be the reservoir of COVID-19 virus, but the intermediate host(s) has not yet been identified. However, three important areas of work are already underway in China to inform our understanding of the zoonotic origin of this outbreak. These include early investigations of cases with symptom onset in Wuhan throughout December 2019, environmental sampling from the Huanan Wholesale Seafood Market and other area markets, and the collection of detailed records on the source and type of wildlife species sold at the Huanan market and the destination of those animals after the market was closed.

Routes of transmission

COVID-19 is transmitted via droplets and fomites during close unprotected contact between an infector and infectee. Airborne spread has not been reported for COVID-19 and it is not believed to be a major driver of transmission based on available evidence; however, it can be envisaged if certain aerosol-generating procedures are conducted in health care facilities. Fecal shedding has been demonstrated from some patients, and viable virus has been identified in a limited number of case reports. However, the fecal-oral route does not appear to be a driver of COVID-19 transmission; its role and significance for COVID-19 remains to be determined. Viral shedding is discussed in the Technical Findings (Annex C).

Household transmission

In China, human-to-human transmission of the COVID-19 virus is largely occurring in families. The Joint Mission received detailed information from the investigation of clusters and some household transmission studies, which are ongoing in a number of Provinces. Among 344 clusters involving 1308 cases (out of a total 1836 cases reported) in Guangdong Province and Sichuan Province, most clusters (78%-85%) have occurred in families. Household transmission studies are currently underway, but preliminary studies ongoing in Guangdong estimate the secondary attack rate in households ranges from 3-10%.

Contact Tracing

China has a policy of meticulous case and contact identification for COVID-19. For example, in Wuhan more than 1800 teams of epidemiologists, with a minimum of 5 people/team, are tracing tens of thousands of contacts a day. Contact follow up is painstaking, with a high percentage of identified close contacts completing medical observation. Between 1% and 5% of contacts were subsequently laboratory confirmed cases of COVID-19, depending on location. For example:

- As of 17 February, in Shenzhen City, among 2842 identified close contacts, 2842 (100%) were traced and 2240 (72%) have completed medical observation. Among the close contacts, 88 (2.8%) were found to be infected with COVID-19.

- As of 17 February, in Sichuan Province, among 25493 identified close contacts, 25347 (99%) were traced and 23178 (91%) have completed medical observation. Among the close contacts, 0.9% were found to be infected with COVID-19.
- As of 20 February, in Guangdong Province, among 9939 identified close contacts, 9939 (100%) were traced and 7765 (78%) have completed medical observation. Among the close contacts, 479 (4.8%) were found to be infected with COVID-19.

Testing at fever clinics and from routine ILI/SARI surveillance

The Joint Mission systematically enquired about testing for COVID-19 from routine respiratory disease surveillance systems to explore if COVID-19 is circulating more broadly and undetected in the community in China. These systems could include RT-PCR testing of COVID-19 virus in influenza-like-illness (ILI) and severe acute respiratory infection (SARI) surveillance systems, as well as testing of results among all visitors to fever clinics.

In Wuhan, COVID-19 testing of ILI samples (20 per week) in November and December 2019 and in the first two weeks of January 2020 found no positive results in the 2019 samples, 1 adult positive in the first week of January, and 3 adults positive in the second week of January; all children tested were negative for COVID-19 although a number were positive for influenza. In Guangdong, from 1-14 January, only 1 of more than 15000 ILI/SARI samples tested positive for the COVID-19 virus. In one hospital in Beijing, there were no COVID-19 positive samples among 1910 collected from 28 January 2019 to 13 February 2020. In a hospital in Shenzhen, 0/40 ILI samples were positive for COVID-19.

Within the fever clinics in Guangdong, the percentage of samples that tested positive for the COVID-19 virus has decreased over time from a peak of 0.47% positive on 30 January to 0.02% on 16 February. Overall in Guangdong, 0.14% of approximately 320,000 fever clinic screenings were positive for COVID-19.

Susceptibility

As COVID-19 is a newly identified pathogen, there is no known pre-existing immunity in humans. Based on the epidemiologic characteristics observed so far in China, everyone is assumed to be susceptible, although there may be risk factors increasing susceptibility to infection. This requires further study, as well as to know whether there is neutralising immunity after infection.

The transmission dynamics

Inferring from Figures 2 and 3, and based on our observations at the national and provincial/municipal levels during the Joint Mission, we summarize and interpret the transmission dynamics of COVID-19 thus far. It is important to note that transmission dynamics of any outbreak are inherently contextual. For COVID-19, we observe four major types of transmission dynamics during the epidemic growth phase and in the post-control period, and highlight what is known about transmission in children, as follows:

Transmission in Wuhan

Early cases identified in Wuhan are believed to be have acquired infection from a zoonotic source as many reported visiting or working in the Huanan Wholesale Seafood Market. As of 25 February, an animal source has not yet been identified.

At some point early in the outbreak, some cases generated human-to-human transmission chains that seeded the subsequent community outbreak prior to the implementation of the comprehensive control measures that were rolled out in Wuhan. The dynamics likely approximated mass action and radiated from Wuhan to other parts of Hubei province and China, which explains a relatively high R_0 of 2-2.5.

The *cordon sanitaire* around Wuhan and neighboring municipalities imposed since 23 January 2020 has effectively prevented further exportation of infected individuals to the rest of the country.

Transmission in Hubei, other than Wuhan

In the prefectures immediately adjoining Wuhan (Xiaogan, Huanggang, Jingzhou and Ezhou), transmission is less intense. For other prefectures, due to fewer transport links and human mobility flows with Wuhan, the dynamics are more closely aligned with those observed in the other areas of the country. Within Hubei, the implementation of control measures (including social distancing) has reduced the community force of infection, resulting in the progressively lower incident reported case counts.

Transmission in China outside of Hubei

Given Wuhan's transport hub status and population movement during the Chinese New Year (chunyun), infected individuals quickly spread throughout the country, and were particularly concentrated in cities with the highest volume of traffic with Wuhan. Some of these imported seeds generated limited human-to-human transmission chains at their destination.

Given the Wuhan/Hubei experience, a comprehensive set of interventions, including aggressive case and contact identification, isolation and management and extreme social distancing, have been implemented to interrupt the chains of transmission nationwide. To date, most of the recorded cases were imported from or had direct links to Wuhan/Hubei. Community transmission has been very limited. Most locally generated cases have been clustered, the majority of which have occurred in households, as summarized above.

Of note, the highly clustered nature of local transmission may explain a relatively high R_0 (2-2.5) in the absence of interventions and low confirmed case counts with intense quarantine and social distancing measures.

Special settings

We note that instances of transmission have occurred within health care settings prisons and other closed settings. At the present time, it is not clear what role these settings and groups play in transmission. However, they do not appear to be major drivers of the overall epidemic dynamics. Specifically, we note:

(a) **Transmission in health care settings and among health care workers (HCW)** – The Joint Mission discussed nosocomial infection in all locations visited during the Mission. As of 20 February 2020, there were 2,055 COVID-19 laboratory-confirmed cases reported among HCW from 476 hospitals across China. The majority of HCW cases (88%) were reported from Hubei.

Remarkably, more than 40,000 HCW have been deployed from other areas of China to support the response in Wuhan. Notwithstanding discrete and limited instances of nosocomial outbreaks (e.g. a nosocomial outbreak involving 15 HCW in Wuhan), transmission within health care settings and amongst health care workers does not appear to be a major transmission feature of COVID-19 in China. The Joint Mission learned that, among the HCW infections, most were identified early in the outbreak in Wuhan when supplies and experience with the new disease was lower. Additionally, investigations among HCW suggest that many may have been infected within the household rather than in a health care setting. Outside of Hubei, health care worker infections have been less frequent (i.e. 246 of the total 2055 HCW cases). When exposure was investigated in these limited cases, the exposure for most was reported to have been traced back to a confirmed case in a household.

The Joint Team noted that attention to the prevention of infection in health care workers is of paramount importance in China. Surveillance among health care workers identified factors early in the outbreak that placed HCW at higher risk of infection, and this information has been used to modify policies to improve protection of HCW.

(b) **Transmission in closed settings** – There have been reports of COVID-19 transmission in prisons (Hubei, Shandong, and Zhejiang, China), hospitals (as above) and in a long-term living facility. The close proximity and contact among people in these settings and the potential for environmental contamination are important factors, which could amplify transmission. Transmission in these settings warrants further study.

Children

Data on individuals aged 18 years old and under suggest that there is a relatively low attack rate in this age group (2.4% of all reported cases). Within Wuhan, among testing of ILI samples, no children were positive in November and December of 2019 and in the first two weeks of January 2020. From available data, and in the absence of results from serologic studies, it is not possible to determine the extent of infection among children, what role children play in transmission, whether children are less susceptible or if they present differently clinically (i.e. generally milder presentations). The Joint Mission learned that infected children have largely been identified through contact tracing in households of adults. Of note, people interviewed by the Joint Mission Team could not recall episodes in which transmission occurred from a child to an adult.

The signs, symptoms, disease progression and severity

Symptoms of COVID-19 are non-specific and the disease presentation can range from no symptoms (asymptomatic) to severe pneumonia and death. As of 20 February 2020 and based on 55924 laboratory confirmed cases, typical **signs and symptoms** include: fever (87.9%), dry cough (67.7%), fatigue (38.1%), sputum production (33.4%), shortness of breath (18.6%), sore throat (13.9%), headache (13.6%), myalgia or arthralgia (14.8%), chills (11.4%), nausea or vomiting (5.0%), nasal congestion (4.8%), diarrhea (3.7%), and hemoptysis (0.9%), and conjunctival congestion (0.8%).

People with COVID-19 generally develop signs and symptoms, including mild respiratory symptoms and fever, on an average of 5-6 days after infection (mean incubation period 5-6 days, range 1-14 days).

Most people infected with COVID-19 virus have mild disease and recover. Approximately 80% of laboratory confirmed patients have had **mild to moderate disease**, which includes non-pneumonia and pneumonia cases, 13.8% have **severe disease** (dyspnea, respiratory frequency ≥30/minute, blood oxygen saturation ≤93%, PaO2/FiO2 ratio <300, and/or lung infiltrates >50% of the lung field within 24-48 hours) and 6.1% are **critical** (respiratory failure, septic shock, and/or multiple organ dysfunction/failure). **Asymptomatic infection** has been reported, but the majority of the relatively rare cases who are asymptomatic on the date of identification/report went on to develop disease. The proportion of truly asymptomatic infections is unclear but appears to be relatively rare and does not appear to be a major driver of transmission.

Individuals at **highest risk** for severe disease and death include people aged over 60 years and those with underlying conditions such as hypertension, diabetes, cardiovascular disease, chronic respiratory disease and cancer. Disease in **children** appears to be relatively rare and mild with approximately 2.4% of the total reported cases reported amongst individuals aged under 19 years. A very small proportion of those aged under 19 years have developed severe (2.5%) or critical disease (0.2%).

As of 20 February, 2114 of the 55,924 laboratory confirmed cases have died (**crude fatality ratio** [CFR[2]] 3.8%) (note: at least some of whom were identified using a case definition that included pulmonary disease). The overall CFR varies by location and intensity of transmission (i.e. 5.8% in Wuhan vs. 0.7% in other areas in China). In China, the overall CFR was higher in the early stages of the outbreak (17.3% for cases with symptom onset from 1-10 January) and has reduced over time to 0.7% for patients with symptom onset after 1 February (Figure 4). The Joint Mission noted that the standard of care has evolved over the course of the outbreak.

Mortality increases with age, with the highest mortality among people over 80 years of age (CFR 21.9%). The CFR is higher among males compared to females (4.7% vs. 2.8%). By occupation, patients who reported being retirees had the highest CFR at 8.9%. While patients who reported no comorbid conditions had a CFR of 1.4%, patients with comorbid conditions had much higher rates: 13.2% for those with cardiovascular disease, 9.2% for diabetes, 8.4% for hypertension, 8.0% for chronic respiratory disease, and 7.6% for cancer.

[2] The Joint Mission acknowledges the known challenges and biases of reporting crude CFR early in an epidemic.

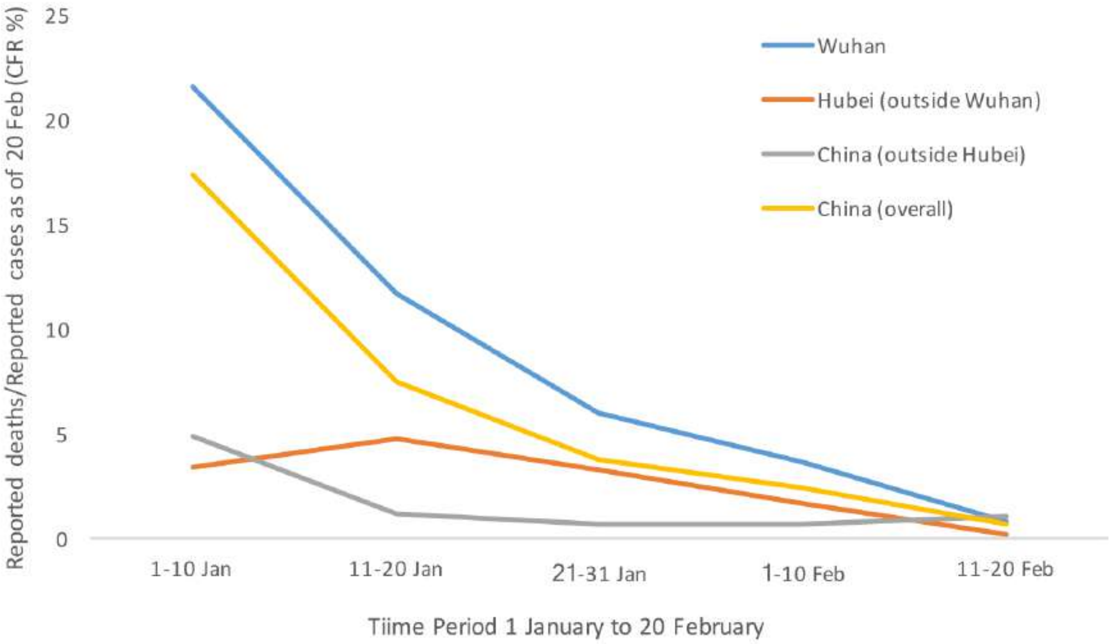


Figure 4 Case fatality ratio (reported deaths among total cases) for COVID-19 in China over time and by location, as of 20 February 2020

Data on the **progression of disease** is available from a limited number of reported hospitalized cases (Figure 5). Based on available information, the median time from symptom onset to laboratory confirmation nationally decreased from 12 days (range 8-18 days) in early January to 3 days (1-7) by early February 2020, and in Wuhan from 15 days (10-21) to 5 days (3-9), respectively. This has allowed for earlier case and contact identification, isolation and treatment.

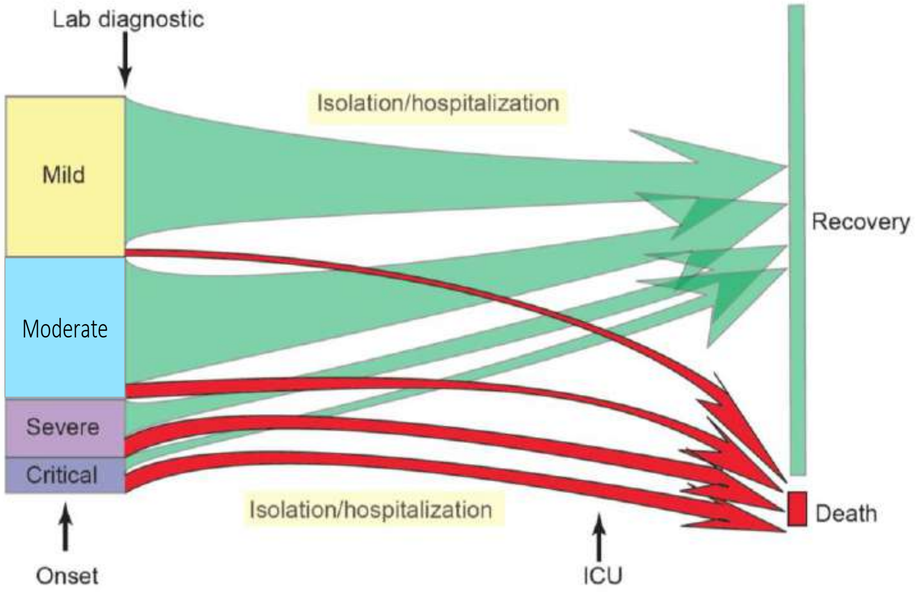


Figure 5. Pattern of disease progression for COVID-19 in China

Note: the relative size of the boxes for disease severity and outcome reflect the proportion of cases reported as of 20 February 2020. The size of the arrows indicates the proportion of cases who recovered or died. Disease definitions are described above. Moderate cases have a mild form of pneumonia.

Using available preliminary data, the median time from onset to clinical recovery for mild cases is approximately 2 weeks and is 3-6 weeks for patients with severe or critical disease. Preliminary data suggests that the time period from onset to the development of severe disease, including hypoxia, is 1 week. Among patients who have died, the time from symptom onset to outcome ranges from 2-8 weeks.

An increasing number of patients have **recovered**; as of 20 February, 18264 (24%) reported cases have recovered. Encouragingly, a report on 20 February from the Guangdong CDC suggests that of 125 severe cases identified in Guangdong, 33 (26.4%) have recovered and been released from hospital, and 58 (46.4%) had improved and were reclassified as having mild/moderate disease (i.e. + milder pneumonia). Among severe cases reported to date, 13.4% have died. Early identification of cases and contacts allows for earlier treatment.

The China response

Upon the detection of a cluster of pneumonia cases of unknown etiology in Wuhan, the CPC Central Committee and the State Council launched the national emergency response. A **Central Leadership Group for Epidemic Response** and the **Joint Prevention and Control Mechanism** of the State Council were established. General Secretary Xi Jinping personally directed and deployed the prevention and control work and requested that the prevention and control of the COVID-19 outbreak be the top priority of government at all levels. Prime Minister Li Keqiang headed the Central Leading Group for Epidemic Response and went to Wuhan to inspect and coordinate the prevention and control work of relevant departments and provinces (autonomous regions and municipalities) across the country. Vice Premier Sun Chunlan, who has been working on the frontlines in Wuhan, has led and coordinated the frontline prevention and control of the outbreak.

The prevention and control measures have been implemented rapidly, from the early stages in Wuhan and other key areas of Hubei, to the current overall national epidemic. It has been undertaken in **three main phases**, with two important events defining those phases. First, COVID-19 was included in the statutory report of Class B infectious diseases and border health quarantine infectious diseases on 20 January 2020, which marked the transition from the initial partial control approach to the comprehensive adoption of various control measures in accordance with the law. The second event was the State Council's issuing, on 8 February 2020, of The Notice on Orderly Resuming Production and Resuming Production in Enterprises, which indicated that China's national epidemic control work had entered a stage of overall epidemic prevention and control together with the restoration of normal social and economic operations.

The first stage

During the early stage of the outbreak, the main strategy focused on preventing the exportation of cases from Wuhan and other priority areas of Hubei Province, and preventing the importation of cases by other provinces; the overall aim was to control the source of infection, block transmission and prevent further spread. The response mechanism was initiated with multi-sectoral involvement in joint prevention and control measures. Wet markets were closed, and efforts were made to identify the zoonotic source. Information on the epidemic was notified to WHO on 3 January, and whole genome sequences of the COVID-19 virus were shared with WHO on 10 January. Protocols for COVID-19 diagnosis and treatment, surveillance, epidemiological investigation, management of close contacts, and laboratory testing were formulated, and relevant surveillance activities and epidemiological investigations conducted. Diagnostic testing kits were developed, and wildlife and live poultry markets were placed under strict supervision and control measures.

The second stage

During the second stage of the outbreak, the main strategy was to reduce the intensity of the epidemic and to slow down the increase in cases. In Wuhan and other priority areas of Hubei Province, the focus was on actively treating patients, reducing deaths, and preventing exportations. In other provinces, the focus was on preventing importations, curbing the spread of the disease and implementing joint prevention and control measures. Nationally, wildlife markets were closed and wildlife captive-breeding facilities were cordoned off. On 20 January, COVID-19 was included in the notifiable report of Class B infectious diseases and border health quarantine infectious diseases, with temperature checks, health care declarations, and quarantine against COVID-19 instituted at transportation depots in accordance with the law. On 23 January, Wuhan implemented strict traffic restrictions. The protocols for diagnosis, treatment and epidemic prevention and control were improved; case isolation and treatment were strengthened.

Measures were taken to ensure that all cases were treated, and close contacts were isolated and put under medical observation. Other measures implemented included the extension of the Spring Festival holiday, traffic controls, and the control of transportation capacity to reduce the movement of people; mass gathering activities were also cancelled. Information about the epidemic and prevention and control measures was regularly released. Public risk communications and health education were strengthened; allocation of medical supplies was coordinated, new hospitals were built, reserve beds were used and relevant premises were repurposed to ensure that all cases could be treated; efforts were made to maintain a stable supply of commodities and their prices to ensure the smooth operation of society.

The third stage

The third stage of the outbreak focused on reducing clusters of cases, thoroughly controlling the epidemic, and striking a balance between epidemic prevention and control, sustainable economic and social development, the unified command, standardized guidance, and scientific evidence-based policy implementation. For Wuhan and other priority areas of Hubei Province, the focus was on patient treatment and the interruption of transmission, with an emphasis on concrete steps to fully implement relevant measures for the testing, admitting and treating of all patients. A risk-based prevention and control approach was adopted with differentiated prevention and control measures for different regions of the country and provinces. Relevant measures were strengthened in the areas of epidemiological investigation, case management and epidemic prevention in high-risk public places.

New technologies were applied such as the use of big data and artificial intelligence (AI) to strengthen contact tracing and the management of priority populations. Relevant health insurance policies were promulgated on "health insurance payment, off-site settlement, and financial compensation". All provinces provided support to Wuhan and priority areas in Hubei Province in an effort to quickly curb the spread of the disease and provide timely clinical treatment. Pre-school preparation was improved, and work resumed in phases and batches. Health and welfare services were provided to returning workers in a targeted and 'one-stop' manner. Normal social operations are being restored in a stepwise fashion; knowledge about disease prevention is being popularized to improve public health literacy and skills; and a comprehensive program of emergency scientific research is being carried out to develop diagnostics, therapeutics and vaccines, delineate the spectrum of the disease, and identify the source of the virus.

Knowledge gaps

Since the start of the COVID-19 outbreak, there have been extensive attempts to better understand the virus and the disease in China. It is remarkable how much knowledge about a new virus has been gained in such a short time. However, as with all new diseases, and only 7 weeks after this outbreak began, key knowledge gaps remain. Annex D summarizes the key unknowns in a number of areas including the source of infection, pathogenesis and virulence of the virus, transmissibility, risk factors for infection and disease progression, surveillance, diagnostics, clinical management of severe and critically ill patients, and the effectiveness of prevention and control measures. The timely filling of these knowledge gaps is imperative to enhance control strategies.

III. Assessment

The Joint Mission drew four major conclusions from its work in China and four major conclusions from its knowledge of the broader global response to COVID-19. Recommendations are offered in five major areas to inform the ongoing response globally and in China.

The China Response & Next Steps

1. **In the face of a previously unknown virus, China has rolled out perhaps the most ambitious, agile and aggressive disease containment effort in history. The strategy that underpinned this containment effort was initially a national approach that promoted universal temperature monitoring, masking, and hand washing. However, as the outbreak evolved, and knowledge was gained, a science and risk-based approach was taken to tailor implementation. Specific containment measures were adjusted to the provincial, county and even community context, the capacity of the setting, and the nature of novel coronavirus transmission there.**

   While the fundamental principles of this strategy have been consistent since its launch, there has been constant refinement of specific aspects to incorporate new knowledge on the novel coronavirus, the COVID-19 disease, and COVID-19 containment, as rapidly as that knowledge has emerged. The remarkable speed with which Chinese scientists and public health experts isolated the causative virus, established diagnostic tools, and determined key transmission parameters, such as the route of spread and incubation period, provided the vital evidence base for China's strategy, gaining invaluable time for the response.

As striking, has been the uncompromising rigor of strategy application that proved to be a hallmark in every setting and context where it was examined. There has also been a relentless focus on improving key performance indicators, for example constantly enhancing the speed of case detection, isolation and early treatment. The implementation of these containment measures has been supported and enabled by the innovative and aggressive use of cutting edge technologies, from shifting to online medical platforms for routine care and schooling, to the use of 5G platforms to support rural response operations.

2. **Achieving China's exceptional coverage with and adherence to these containment measures has only been possible due to the deep commitment of the Chinese people to collective action in the face of this common threat. At a community level this is reflected in the remarkable solidarity of provinces and cities in support of the most vulnerable populations and communities. Despite ongoing outbreaks in their own areas, Governors and Mayors have continued to send thousands of health care workers and tons of vital PPE supplies into Hubei province and Wuhan city.**

   At the individual level, the Chinese people have reacted to this outbreak with courage and conviction. They have accepted and adhered to the starkest of containment measures – whether the suspension of public gatherings, the month-long 'stay at home' advisories or prohibitions on travel. Throughout an intensive 9-days of site visits across China, in frank discussions from the level of local community mobilizers and frontline health care providers to top scientists, Governors and Mayors, the Joint Mission was struck by the sincerity and dedication that each brings to this COVID-19 response.

3. **China's bold approach to contain the rapid spread of this new respiratory pathogen has changed the course of a rapidly escalating and deadly epidemic. A particularly compelling statistic is that on the first day of the advance team's work there were 2478 newly confirmed cases of COVID-19 reported in China. Two weeks later, on the final day of this Mission, China reported 409 newly confirmed cases. This decline in COVID-19 cases across China is real.**

   Several sources of data support this conclusion, including the steep decline in fever clinic visits, the opening up of treatment beds as cured patients are discharged, and the challenges to recruiting new patients for clinical trials. Based on a comparison of crude attack rates across provinces, the Joint Mission estimates that this truly all-of-Government and all-of-society approach that has been taken in China has averted or at least delayed hundreds of thousands of COVID-19 cases in the country. By extension, the reduction that has been achieved in the force of COVID-19 infection in China has also played a significant role in protecting the global community and creating a stronger first line of defense against international spread. Containing this outbreak, however, has come at great cost and sacrifice by China and its people, in both human and material terms.

   While the scale and impact of China's COVID-19 operation has been remarkable, it has also highlighted areas for improvement in public health emergency response capacity.

These include overcoming any obstacles to act immediately on early alerts, to massively scale-up capacity for isolation and care, to optimize the protection of frontline health care workers in all settings, to enhance collaborative action on priority gaps in knowledge and tools, and to more clearly communicate key data and developments internationally.

4. **China is already, and rightfully, working to bolster its economy, reopen its schools and return to a more normal semblance of its society, even as it works to contain the remaining chains of COVID-19 transmission. Appropriately, a science-based, risk-informed and phased approach is being taken, with a clear recognition and readiness of the need to immediately react to any new COVID-19 cases or clusters as key elements of the containment strategy are lifted.**

   Despite the declining case numbers, across China every province, city and community visited is urgently escalating their investments in acute care beds and public health capacity. It is crucial that this continues. Fifty thousand infected COVID-19 patient are still under treatment, across the country. However, the Joint Mission has come to understand the substantial knowledge, experience and capacities that China has rapidly built during this crisis. Consequently, it endorses China's working assumption that in most provinces and municipalities it should soon be possible to manage a resurgence in COVID-19 cases, using even more tailored and sustainable approaches that are anchored in very rapid case detection, instant activation of key containment activities, direct oversight by top leadership, and broad community engagement.

   As China works to resume a more normal level of societal and economic activity, it is essential that the world recognizes and reacts positively to the rapidly changing, and decreasing, risk of COVID-19 in the country. China's rapid return to full connectivity with the world, and to full productivity and economic output, is vital to China and to the world. The world urgently needs access to China's experience in responding to COVID-19, as well as the material goods it brings to the global response. It is even more urgent now, with escalating COVID-19 outbreaks outside of China, to constantly reassess any restrictions on travel and/or trade to China that go beyond the recommendations of the IHR Emergency Committee on COVID-19.

The Global Response & Next Steps

1. **The COVID-19 virus is a new pathogen that is highly contagious, can spread quickly, and must be considered capable of causing enormous health, economic and societal impacts in any setting. It is not SARS and it is not influenza. Building scenarios and strategies only on the basis of well-known pathogens risks failing to exploit all possible measures to slow transmission of the COVID-19 virus, reduce disease and save lives.**

   COVID-19 is not SARS and it is not influenza. It is a new virus with its own characteristics. For example, COVID-19 transmission in children appears to be limited compared with influenza, while the clinical picture differs from SARS. Such differences, while based on limited data, may be playing a role in the apparent efficacy of rigorously applied non-pharmaceutical, public health measures to interrupt chains of human-to-human transmission in a range of settings in China. The COVID-19 virus is unique among human coronaviruses in its combination of high transmissibility, substantial fatal outcomes in some high-risk groups, and ability to cause huge societal and economic disruption. For planning purposes, it must be assumed that the global population is susceptible to this virus. As the animal origin of the COVID-19 virus is unknown at present, the risk of reintroduction into previously infected areas must be constantly considered.

The novel nature, and our continuously evolving understanding, of this coronavirus demands a tremendous agility in our capacity to rapidly adapt and change our readiness and response planning as has been done continually in China. This is an extraordinary feat for a country of 1.4 billion people.

2. **China's uncompromising and rigorous use of non-pharmaceutical measures to contain transmission of the COVID-19 virus in multiple settings provides vital lessons for the global response. This rather unique and unprecedented public health response in China reversed the escalating cases in both Hubei, where there has been widespread community transmission, and in the importation provinces, where family clusters appear to have driven the outbreak.**

   Although the timing of the outbreak in China has been relatively similar across the country, transmission chains were established in a wide diversity of settings, from mega-cities in the north and south of the country, to remote communities. However, the rapid adaptation and tailoring of China's strategy demonstrated that containment can be adapted and successfully operationalized in a wide range of settings.

   China's experience strongly supports the efficacy and effectiveness of anchoring COVID-19 readiness and rapid response plans in a thorough assessment of local risks and of utilizing a differentiated risk-based containment strategy to manage the outbreak in areas with no cases vs. sporadic cases vs. clusters of cases vs. community-level transmission. Such a strategy is essential for ensuring a sustainable approach while minimizing the socio-economic impact.

3. **Much of the global community is not yet ready, in mindset and materially, to implement the measures that have been employed to contain COVID-19 in China. These are the only measures that are currently proven to interrupt or minimize transmission chains in humans. Fundamental to these measures is extremely proactive surveillance to immediately detect cases, very rapid diagnosis and immediate case isolation, rigorous tracking and quarantine of close contacts, and an exceptionally high degree of population understanding and acceptance of these measures.**

   Achieving the high quality of implementation needed to be successful with such measures requires an unusual and unprecedented speed of decision-making by top leaders, operational thoroughness by public health systems, and engagement of society.

Given the damage that can be caused by uncontrolled, community-level transmission of this virus, such an approach is warranted to save lives and to gain the weeks and months needed for the testing of therapeutics and vaccine development. Furthermore, as the majority of new cases outside of China are currently occurring in high and middle-income countries, a rigorous commitment to slowing transmission in such settings with non-pharmaceutical measures is vital to achieving a second line of defense to protect low income countries that have weaker health systems and coping capacities.

The time that can be gained through the full application of these measures – even if just days or weeks – can be invaluable in ultimately reducing COVID-19 illness and deaths. This is apparent in the huge increase in knowledge, approaches and even tools that has taken place in just the 7 weeks since this virus was discovered through the rapid scientific work that has been done in China.

4. **The time gained by rigorously applying COVID-19 containment measures must be used more effectively to urgently enhance global readiness and rapidly develop the specific tools that are needed to ultimately stop this virus.**

COVID-19 is spreading with astonishing speed; COVID-19 outbreaks in any setting have very serious consequences; and there is now strong evidence that non-pharmaceutical interventions can reduce and even interrupt transmission. Concerningly, global and national preparedness planning is often ambivalent about such interventions. However, to reduce COVID-19 illness and death, near-term readiness planning must embrace the large-scale implementation of high-quality, non-pharmaceutical public health measures. These measures must fully incorporate immediate case detection and isolation, rigorous close contact tracing and monitoring/quarantine, and direct population/community engagement.

A huge array of COVID-19 studies, scientific research projects and product R&D efforts are ongoing in China and globally. This is essential and to be encouraged and supported. However, such a large number of projects and products needs to be prioritized. Without prioritizing, this risks compromising the concentration of attention and resources and collaboration required to cut timelines by precious weeks and months. While progress has been made, the urgency of the COVID-19 situation supports an even more ruthless prioritization of research in the areas of diagnostics, therapeutics and vaccines.

Similarly, there is a long list of proposed studies on the origins of COVID-19, the natural history of the disease, and the virus's transmission dynamics. However, the urgency of responding to cases and saving lives makes it difficult for policy makers to consider and act on such comprehensive lists. This can be addressed by balancing studies with the immediate public health and clinical needs of the response. Studies can be prioritized in terms of the largest knowledge gaps that can be most rapidly addressed to have greatest immediate impact on response operations and patient management. This suggests prioritizing studies to identify risk factors for transmission in households, institutions and the community; convenience sampling for this virus in the population using existing surveillance systems; age-stratified sero-epidemiologic surveys; the analysis of clinical case series; and cluster investigations.

IV. Major Recommendations

For China

1. Maintain an appropriate level of emergency management protocols, depending on the assessed risk in each area and recognizing the real risk of new cases and clusters of COVID-19 as economic activity resumes, movement restrictions are lifted, and schools reopen;

2. Carefully monitor the phased lifting of the current restrictions on movement and public gatherings, beginning with the return of workers and migrant labor, followed by the eventual reopening of schools and lifting other measures;

3. Further strengthen the readiness of emergency management mechanisms, public health institutions (e.g. CDCs), medical facilities, and community engagement mechanisms to ensure sustained capacity to immediately launch containment activities in response to any resurgence in cases;

4. Prioritize research that rapidly informs response and risk management decisions, particularly household and health care facility studies, age-stratified sero-epidemiologic surveys and rigorous investigation of the animal-human interface; establish a centralized research program to fast-track the most promising rapid diagnostics and serologic assays, the testing of potential antivirals and vaccine candidates, and Chinese engagement in selected multi-country trials; and

5. As the country with the greatest knowledge on COVID-19, further enhance the systematic and real-time sharing of epidemiologic data, clinical results and experience to inform the global response.

For countries with imported cases and/or outbreaks of COVID-19

1. Immediately activate the highest level of national Response Management protocols to ensure the all-of-government and all-of-society approach needed to contain COVID-19 with non-pharmaceutical public health measures;

2. Prioritize active, exhaustive case finding and immediate testing and isolation, painstaking contact tracing and rigorous quarantine of close contacts;

3. Fully educate the general public on the seriousness of COVID-19 and their role in preventing its spread;

4. Immediately expand surveillance to detect COVID-19 transmission chains, by testing all patients with atypical pneumonias, conducting screening in some patients with upper respiratory illnesses and/or recent COVID-19 exposure, and adding testing for the COVID-19 virus to existing surveillance systems (e.g. systems for influenza-like-illness and SARI); and

5. Conduct multi-sector scenario planning and simulations for the deployment of even more stringent measures to interrupt transmission chains as needed (e.g. the suspension of large-scale gatherings and the closure of schools and workplaces).

For uninfected countries

1. Prepare to immediately activate the highest level of emergency response mechanisms to trigger the all-of-government and all-of society approach that is essential for early containment of a COVID-19 outbreak;

2. Rapidly test national preparedness plans in light of new knowledge on the effectiveness of non-pharmaceutical measures against COVID-19; incorporate rapid detection, largescale case isolation and respiratory support capacities, and rigorous contact tracing and management in national COVID-19 readiness and response plans and capacities;

3. Immediately enhance surveillance for COVID-19 as rapid detection is crucial to containing spread; consider testing all patients with atypical pneumonia for the COVID-19 virus, and adding testing for the virus to existing influenza surveillance systems;

4. Begin now to enforce rigorous application of infection prevention and control measures in all healthcare facilities, especially in emergency departments and outpatient clinics, as this is where COVID-19 will enter the health system; and

5. Rapidly assess the general population's understanding of COVID-19, adjust national health promotion materials and activities accordingly, and engage clinical champions to communicate with the media.

For the public

1. Recognize that COVID-19 is a new and concerning disease, but that outbreaks can managed with the right response and that the vast majority of infected people will recover;

2. Begin now to adopt and rigorously practice the most important preventive measures for COVID-19 by frequent hand washing and always covering your mouth and nose when sneezing or coughing;

3. Continually update yourself on COVID-19 and its signs and symptoms (i.e. fever and dry cough), because the strategies and response activities will constantly improve as new information on this disease is accumulating every day; and

4. Be prepared to actively support a response to COVID-19 in a variety of ways, including the adoption of more stringent 'social distancing' practices and helping the high-risk elderly population.

For the international community

1. Recognize that true solidarity and collaboration is essential between nations to tackle the common threat that COVID-19 represents and operationalize this principle;

2. Rapidly share information as required under the International Health Regulations (IHR) including detailed information about imported cases to facilitate contact tracing and inform containment measures that span countries;

3. Recognize the rapidly changing risk profile of COVID-19 affected countries and continually monitor outbreak trends and control capacities to reassess any 'additional health measures' that significantly interfere with international travel and trade.

____

Annexes

A. WHO-China Joint Mission Members

Bruce AYLWARD	Team Lead WHO-China Joint Mission on COVID-19, Senior Advisor to the Director-General, World Health Organization, Geneva, Switzerland
Wannian LIANG	Team Lead WHO-China Joint Mission on COVID-19, Head of Expert Panel, National Health Commission
Xiaoping DONG	Director and Researcher, Center for Global Public Health, Chinese Center for Disease Control and Prevention
Tim ECKMANNS	Head of Unit, Healthcare-associated Infections, Surveillance of Antibiotic Resistance and Consumption, Robert Koch Institute, Berlin, Germany
Dale FISHER	Professor of Medicine, Yong Loo Lin School of Medicine, National University of Singapore, Singapore, Singapore
Chikwe IHEKWEAZU	Director General, Nigeria Centre for Disease Control, Nigeria Centre for Disease Control, Abuja, Nigeria
Clifford LANE	Clinical Director, National Institute of Allergy and Infectious Diseases, US National Institutes of Health, Bethesda, United States
Jong-Koo LEE	Professor of Family Medicine, Seoul National University College of Medicine, Seoul, Republic of Korea
Gabriel LEUNG	Dean of Medicine, Helen and Francis Zimmern Professor in Population Health, The University of Hong Kong, Hong Kong SAR, China
Jiangtao LIN	Director and Professor, Department of Pulmonary and Critical Care Medicine, China-Japan Friendship Hospital, National Clinical Research Center for Respiratory Diseases, Beijing
Haiying LIU	Deputy Director and Researcher, Institute of Pathogen Biology, Chinese Academy of Medical Sciences, Beijing China
Natalia PSHENICHNAYA	Head of International Department and Consultant, Center of Infectious Diseases, National Medical Research Center of Phthisiopulmonology and Infectious Diseases, Moscow, Russia
Aleksandr SEMENOV	Deputy Director, Saint Petersburg Pasteur Institute, Saint Petersburg, Russia
Hitoshi TAKAHASHI	Senior Research Scientist, Influenza Virus Research Center, National Institute of Infectious Diseases, Tokyo, Japan
Maria VAN KERKHOVE	Head of Unit, Emerging Diseases & Zoonoses, Global Infectious Hazard Preparedness, World Health Organization, Geneva, Switzerland
Bin WANG	Deputy Team Leader, Deputy Director General, Disease Prevention and Control Bureau, National Health Commission
Guangfa WANG	Director, Department of Respiratory and Critical Care Medicine, Peking University First Hospital
Fan WU	Vice Dean, Shanghai Medical College, Fudan University
Zhongze WU	Director, Compliance and Enforcement Division, Department of Wildlife Conservation, National Forestry and Grassland Administration
Zunyou WU	Chief Epidemiologist, Chinese Center for Disease Control and Prevention
Jun XING	Head of Unit, Country Capacity for International Health Regulations, Health Security Preparedness, World Health Organization, Geneva, Switzerland
Kwok-Yung YUEN	Chair Professor and Co-Director of State Key Laboratory of Emerging Infectious Diseases, Department of Microbiology, The University of Hong Kong
Weigong ZHOU	Medical Officer, Influenza Division, National Center for Immunization and Respiratory Diseases, US Centers for Disease Control and Prevention, Atlanta, United States
Yong ZHANG	Assistant Director and Researcher, National Institute for Viral Disease Control and prevention, Chinese Center for Disease Control and Prevention.
Lei ZHOU	Chief and Researcher, Branch for Emerging Infectious Disease, Public Health Emergency Center, Chinese Center for Disease Control and Prevention

B. Summary Agenda of the Mission

Dates	Location	Activities
10-15 February 2020 (Advance Team)	Beijing	Advance Team and WHO Country team meetings with national counterparts and institutions
16 February 2020	Beijing	Meeting with the full international team for briefing at the WHO Country office
	Beijing	Workshop at the National Health Commission (NHC) with relevant departments of the Joint Prevention and Control Mechanism of the State Council
17 February 2020	Beijing	Site visit to Beijing Ditan Hospital
	Beijing	Site visit to Anhuali community and health service station, Anzhen street, Chaoyang District, Beijing
	Beijing	Workshop with Chinese Center for Disease Control and Prevention
18 February 2020 (Guangdong Team)	Shenzhen, Guangdong	Shenzhen customs at the airport
	Shenzhen, Guangdong	Shenzhen No.3 People's Hospital
	Shenzhen, Guangdong	Shenzhen Center for Disease Control and Prevention
	Shenzhen, Guangdong	Meeting at Tencent
19 February 2020 (Guangdong Team)	Shenzhen, Guangdong	Qiaoxiang community
	Shenzhen to Guangzhou	Visit to Futian High-speed Train Station, and travel to Guangzhou by train
	Guangzhou	Guangzhou Panyu Sanatorium
	Guangzhou	Guangdong Laboratory of Regenerative Medicine and Health
	Guangzhou	Guangzhou Tiyudongzhihui wet market
	Guangzhou	First Workshop with The People's government of Guangdong Province
20 February 2020 (Guangdong Team)	Guangzhou	Guangdong Provincial Center for Disease Control and Prevention
	Guangzhou	Renmin road campus of Guangzhou Women and Children Medical Center
	Guangzhou	The second Workshop with The People's government of Guangdong Province
18 February 2020 (Sichuan Team)	Beijing to Chengdu	
	Sichuan	Site visit to Chengdu Shuangliu International Airport
		Meeting with the Governor of Sichuan Provincial People's Government
		Site visit to Yong'an Township Central hospital with fever clinic
		Site visit to home community of Yong'an township
19 February 2020 (Sichuan Team)		Symposium with provincial and municipal authorities
		Sichuan Center for Disease Control and Prevention
		Site visit to West China Hospital- Designated COVID-19 hospital
20 February 2020 (Sichuan Team)		Site visit to Chengdu Women and Children's hospital
		Site visit to Pharmaceutical Logistics center
		Site visit to East Chengdu railway station

		Site visit to Chengdu Public Health Clinical Centre- Designated COVID 19 hospital
Sichuan and Guangdong teams reconvene in Guangzhou		
21-24 February 2020		Analyze major findings; Meetings of the WHO-China Joint mission to finalize the report
Feb 22 (Wuhan Team)	Guangzhou to Wuhan	Select team members only
23 February (Wuhan Team)		Site visit to Guanggu Campus of Wuhan Tongji Hospital
		Site visit to Mobile Cabin Hospital in Wuhan Sports Center
		Workshop with relevant departments of the Joint Prevention and Control Mechanism of Hubei Province
		Feedback Meeting with Minister Ma, NHC at the Wuhan Conference Center
24 February 2020	Guangzhou to Beijing	Finalize report, WHO-Joint Press conference in Beijing

C. Detailed Technical Findings

Response management, case and contact management, risk communication and community engagement

The response structures in China were rapidly put in place according to existing emergency plans and aligned from the top to the bottom. This was replicated at the four levels of government (national provincial, prefecture and county/district).

Organizational structure and response mechanism

Response activation at the national level: COVID-19 prevention and control mechanisms were initiated immediately after the outbreak was declared and nine working groups were set up to coordinate the response: a) Coordination b) Epidemic prevention and control c) Medical treatment d) Research e) Public communication f) Foreign affairs g) Medical material support h) Life maintenance supplies and i) Social stability. Each working group has a ministerial level leader. Emergency response laws and regulations for the emergency response to public health emergencies, prevention and control of infectious diseases have been developed or updated to guide the response.

Response activation in provinces: Each province set up a similar structure to manage the outbreak. The response is organized at the levels of national, provincial, prefecture, county/district and the community. By 29 January, all provinces across China had launched the highest level of response for major public health emergencies.

Response Strategy

A clear strategy was developed, and goals were well articulated and communicated across the entire response architecture. This strategy was rapidly adapted and adjusted to the outbreak, both in terms of the epidemiological situation over time and in different parts of the country.

The epidemiological situation has been used to define location into four areas:

- In areas without cases, the strategy in these areas is to "strictly prevent introduction". This includes quarantine arrangements in transportation hubs, monitoring for temperature changes, strengthening of triage arrangements, use of fever clinics, and ensuring normal economic and social operations.
- In areas with sporadic cases, the strategy is focused on "reducing importation, stopping transmission and providing appropriate treatment".
- In areas with community clusters, the strategy is focussed on "stopping transmission, preventing exportation, and strengthening treatment".
- In areas with community transmission, the strictest prevention and control strategies are being implemented, the entry and exit of people from these areas has been stopped and public health and medical treatment measures are comprehensively strengthened.

Main control measures implemented in China

The main control measures implemented in China are as follows and are illustrated in Figures 6A-6D, representing the national level response and examples of the response at the Provincial and municipal levels:

Monitoring and reporting: COVID-19 was included in the statutory reporting of infectious diseases on 20 January and plans were formulated to strengthen diagnosis, monitoring, and reporting.

Strengthening ports of entry and quarantine: The Customs Department launched the emergency plan for public health emergencies at ports across the country and restarted the health declaration card system for entry and exit into cities as well as strict monitoring of the temperature of entry and exit passengers.

Treatment: For severe or critical patients, the principle of "Four Concentrations" was implemented: i.e. concentrating patients, medical experts, resources and treatment into special centres. All cities and districts transformed relevant hospitals, increased the number of designated hospitals, dispatched medical staff, and set up expert groups for consultation, so as to minimise mortality of severe patients. Medical resources from all over China have been mobilized to support the medical treatment of patients in Wuhan.

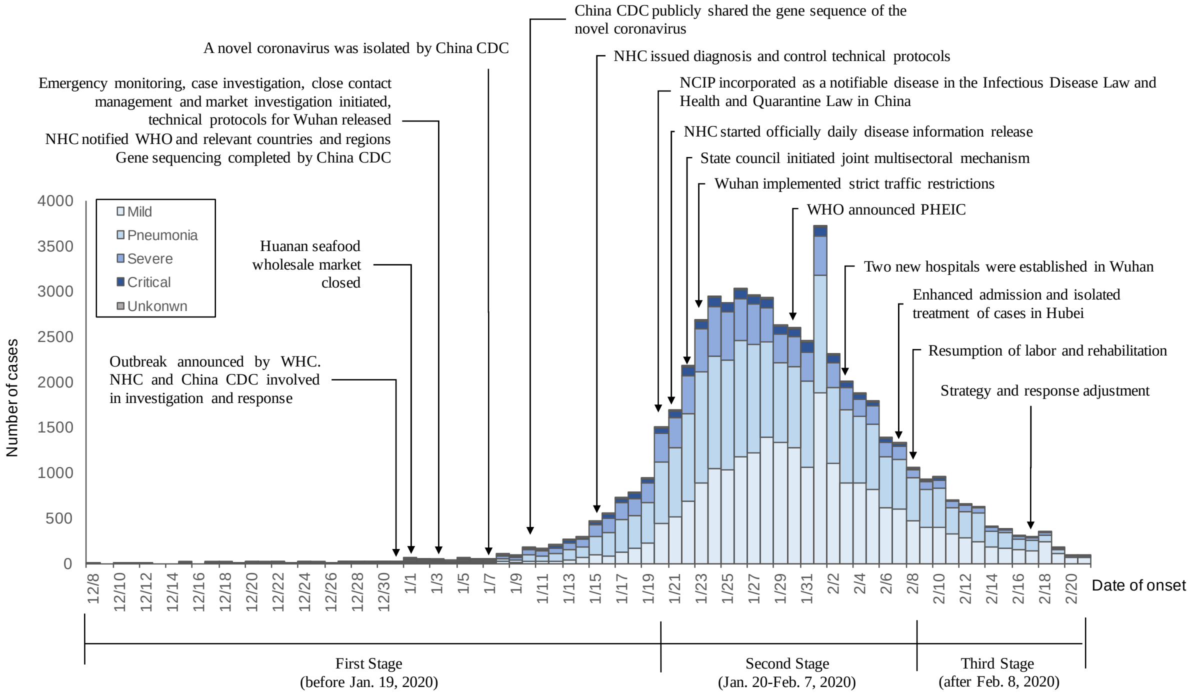
Epidemiological investigation and close contact management: Strong epidemiological investigations are being carried out for cases, clusters, and contacts to identify the source of infection and implement targeted control measures, such as contact tracing.

Social distancing: At the national level, the State Council extended the Spring Festival holiday in 2020, all parts of the country actively cancelled or suspended activities like sport events, cinema, theatre, and schools and colleges in all parts of the country postponed re-opening after the holiday. Enterprises and institutions have staggered their return to work. Transportation Departments setup thousands of health and quarantine stations in national service areas, and in entrances and exits for passengers at stations. Hubei Province adopted the most stringent traffic control measures, such as suspension of urban public transport, including subway, ferry and long-distance passenger transport. Every citizen has to wear a mask in public. Home support mechanisms were established. As a consequence of all of these measures, public life is very reduced.

Funding and material support: Payment of health insurance was taken over by the state, as well as the work to improve accessibility and affordability of medical materials, provide personal protection materials, and ensure basic living materials for affected people.

Emergency material support: The government restored production and expanded production capacity, organized key enterprises that have already started to exceed current production capacity, supported local enterprises to expand imports, and used cross-border e-commerce platforms and enterprises to help import medical materials and improve the ability to guarantee supplies.

A



China CDC publicly shared the gene sequence of the novel coronavirus

A novel coronavirus was isolated by China CDC

NHC issued diagnosis and control technical protocols

Emergency monitoring, case investigation, close contact management and market investigation initiated, technical protocols for Wuhan released
NHC notified WHO and relevant countries and regions
Gene sequencing completed by China CDC

NCIP incorporated as a notifiable disease in the Infectious Disease Law and Health and Quarantine Law in China

NHC started officially daily disease information release

State council initiated joint multisectoral mechanism

Wuhan implemented strict traffic restrictions

WHO announced PHEIC

Huanan seafood wholesale market closed

Two new hospitals were established in Wuhan

Enhanced admission and isolated treatment of cases in Hubei

Resumption of labor and rehabilitation

Outbreak announced by WHC. NHC and China CDC involved in investigation and response

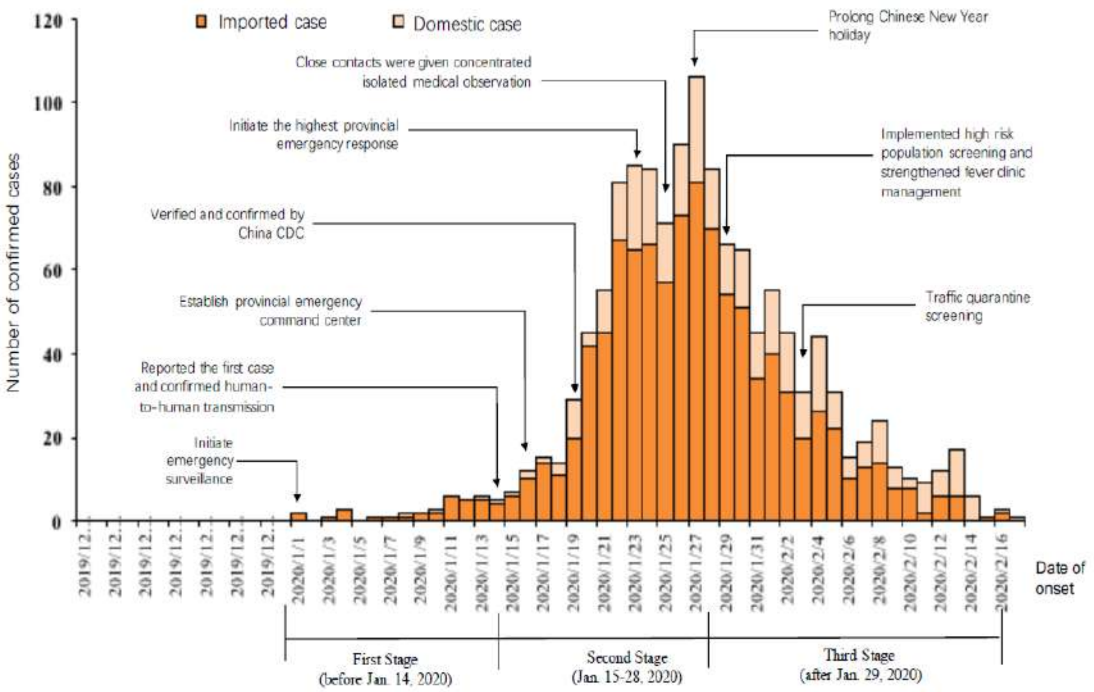
Strategy and response adjustment

First Stage
(before Jan. 19, 2020)

Second Stage
(Jan. 20-Feb. 7, 2020)

Third Stage
(after Feb. 8, 2020)

B



Prolong Chinese New Year holiday

Close contacts were given concentrated isolated medical observation

Initiate the highest provincial emergency response

Implemented high risk population screening and strengthened fever clinic management

Verified and confirmed by China CDC

Establish provincial emergency command center

Traffic quarantine screening

Reported the first case and confirmed human-to-human transmission

Initiate emergency surveillance

First Stage
(before Jan. 14, 2020)

Second Stage
(Jan 15-28, 2020)

Third Stage
(after Jan. 29, 2020)

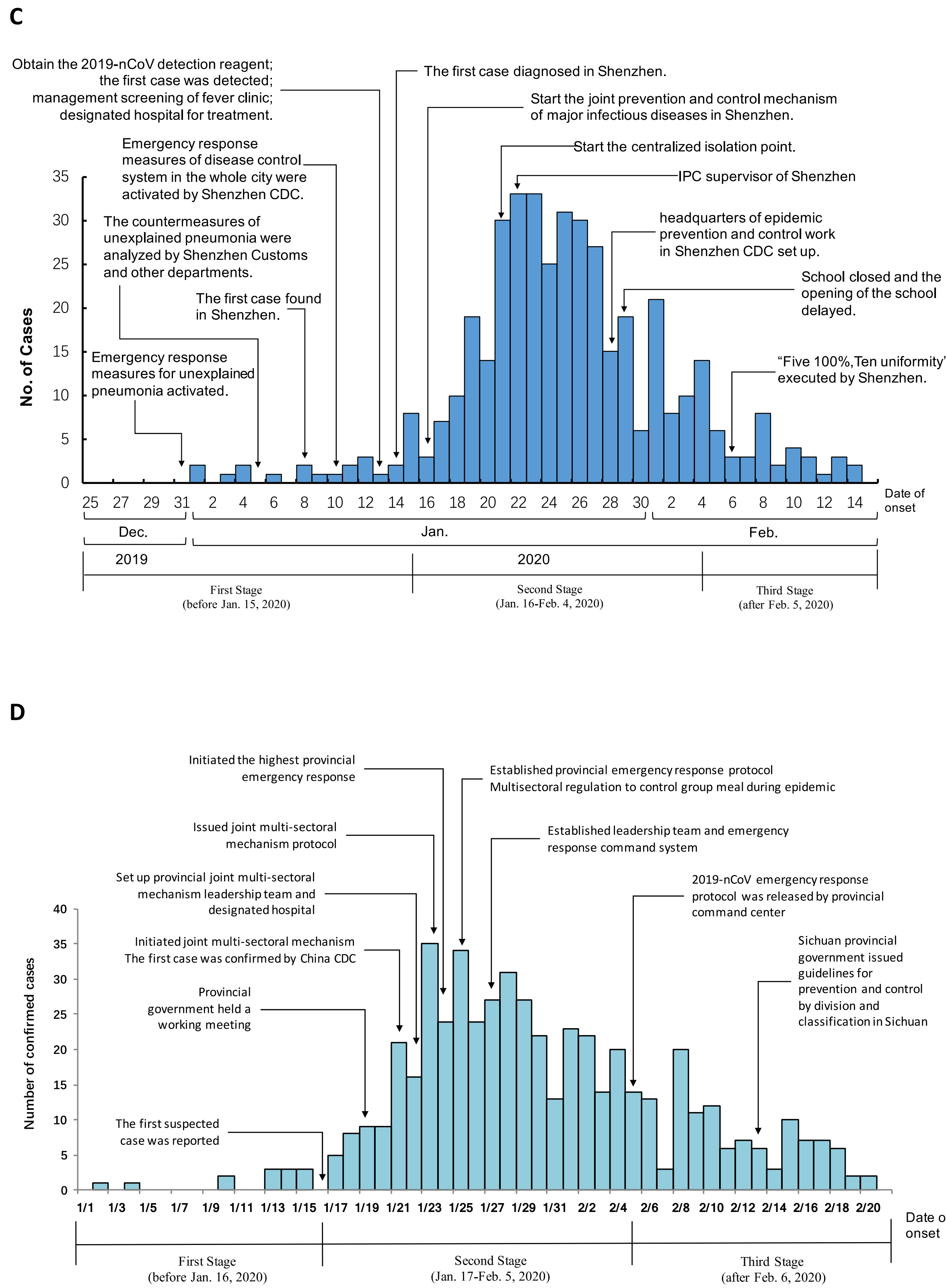


Figure 6. COVID-19 epidemic curves and major intervention measures in China as implemented at a) the national level b) in Guangdong province, c) in Shenzhen municipality and d) in Sichuan province

Risk communications (information release, public and media communications)

International and interregional cooperation and information sharing: From 3 January 2020, information on COVID-19 cases has been reported to WHO daily. Full genome sequences of the new virus were shared with WHO and the international community immediately after the pathogen was identified on 7 January. On 10 January, an expert group involving Hong Kong, Macao and Taiwanese technical experts and a World Health Organization team was invited to visit Wuhan. A set of nucleic acid primers and probes for PCR detection for COVID-19 was released on 21 January.

Daily updates: The National Health Commission announces the epidemic situation every day and holds daily press conferences to respond to emerging issues. The government also frequently invites experts to share scientific knowledge on COVID-19 and to address public concerns.

Psychological care: This is provided to patients and the public. Governments at all levels, NGOs and all sectors of society developed guidelines for emergency psychological crisis intervention and guidelines for public psychological self-support and counselling. A hotline for mental health services has been established for the public.

IT platform: China has capitalized on the use of technology, big data and AI for COVID-19 preparedness, readiness and response. Authoritative and reliable information, medical guidance, access to online services, provision of educational tools and remote work tools have been developed in and used across China. These services have increased accessibility to health services, reduced misinformation and minimized the impact of fake news.

Social mobilization and community engagement

Civil society organizations (community centers and public health centers) have been mobilized to support prevention and response activities. The community has largely accepted the prevention and control measures and is fully participating in the management of self-isolation and enhancement of public compliance. Community volunteers are organized to support self-isolation and help isolated residents at home to solve practical life difficulties. Measures were taken to limit the movement of the population through home-based support. Up to now, outside of Hubei, 30 provinces have registered and managed more than 5 million people coming from Wuhan.

Clinical case management and infection prevention and control

The main **signs and symptoms** of COVID-19 include fever, dry cough, fatigue, sputum production, shortness of breath, myalgia or arthralgia, sore throat, and headache. Nausea or vomiting has been reported in a small percentage of patients (5%). On 14 February, China CDC described the clinical features, outcomes, laboratory and radiologic findings of 44 672 laboratory-confirmed cases. Only 965 (2.2%) were under 20 years of age and there is just one recorded death (0.1%) in this age group. Most patients (77.8%) were aged 30 to 69 years. Patients aged over 80 years had a CFR of 14.8%. The CFR was highest in those with comorbidities including cardiovascular, diabetes, chronic respiratory disease, hypertension and cancer.

As opposed to Influenza A(H1N1)pdm09, **pregnant women** do not appear to be at higher risk of severe disease. In an investigation of 147 pregnant women (64 confirmed, 82 suspected and 1 asymptomatic), 8% had severe disease and 1% were critical.

Severe cases are defined as tachypnoea (≧30 breaths/ min) or oxygen saturation ≤93% at rest, or PaO2/FIO2 <300 mmHg. **Critical cases** are defined as respiratory failure requiring mechanical ventilation, shock or other organ failure that requires intensive care. About a quarter of severe and critical cases require mechanical ventilation while the remaining 75% require only oxygen supplementation.

China has a principle of **early identification**, early isolation, early diagnosis and early treatment. Early identification of suspect cases is critical to containment efforts and occurs via a process of temperature screening and questioning at entrances to many institutions, communities, travel venues (airports, train stations) and hospitals. Many hospitals have fever clinics that were established and maintained since the SARS outbreak. In China, laboratory tests were originally requested according to the case definitions, which included an epidemiological link to Hubei or other confirmed cases. However, more recently, a more **liberal clinical testing regimen** allows clinicians to test with a low index of suspicion.

Suspect cases are isolated in normal pressure single rooms, wear a surgical mask (for source control). Staff in China wear a cap, eye protection, n95 masks, gown and gloves (single use only). In Wuhan it is necessary for most suspects to be cohorted in a normal pressure isolation ward. Staff wear PPE continuously, changing it only when they leave the ward.

PCR test results are returned the same day. If positive, patients are transported to designated hospitals (including negative pressure ambulances in some cities). All patients, including the mild and asymptomatic, with a positive test are admitted. The designated hospitals are known and are strategically placed with at least one per district/county. Positive cases are cohorted by gender. Negative tested patients are managed based on clinical needs. All patients are evaluated with a respiratory multiplex to look for other diagnoses. This can add to the reassurance that a negative COVID-19 test reflects a lack of infection with COVID-19.

In Wuhan, there are 45 **designated hospitals**, 6 of which are designated for critical patients, and 39 for severe patients and/or any patients >65 years old. There are an additional 10 temporary hospitals reconstructed from gymnasium and exhibition centers, which are for mild patients. Other surge measures undertaken in Wuhan include two new temporary hospitals with 2600 beds, plus many makeshift hospitals to increase bed capacity. Bed capacity within Wuhan has increased to >50,000.

Patients are treated according to the **National Clinical guidelines** (edition 6) released by the China National Health Commission (NHC). There are no specific antiviral or immune modulating agents proven (or recommended) to improve outcomes. All patients are monitored by regular pulse oximetry. The guidelines include supportive care by clinical category (mild, moderate, severe and critical), as well as the role of investigational treatments such as chloroquine, phosphate, lopinavir/ritonavir, alpha interferon, ribavirin, arbidol. The application of intubation/invasive ventilation and ECMO in critically ill patients can improve survival. The Joint Mission Team was told of ECMO use in four patients at one hospital with one death and three who appeared to be improving. Clearly, though ECMO is very resource consumptive, any health system would need to carefully weigh the benefits. There is widespread use of Traditional Chinese Medicines (TCM), for which the affects must be fully evaluated.

Patients with COVID-19 are not permitted **visitors**. Staff use coveralls, masks, eye cover, and gloves, removing PPE only when they leave the ward.

Patients are discharged after clinical recovery (afebrile >3 days, resolution of symptoms and radiologic improvement) and 2 negative PCR tests taken 24 hours apart. Upon discharge, they are asked to minimise family and social contact and to wear a mask. There are expectations of clinical trial results within a matter of weeks, which will see further opportunities for treatment.

There are guidelines for **elderly care** specifically targeting prevention in individuals and introduction of COVID-19 to nursing homes.

Training programmes by video conference nationally are scaled up to inform staff of best practice and to ensure PPE usage. **Clinical champions** are created to disperse knowledge and provide local expertise.

Maintenance of usual healthcare activities is maintained by hospital zoning (e.g. clean/contaminated sections of the healthcare facility).

Laboratory, diagnostics and virology

The virus found to cause COVID-19 was initially isolated from a clinical sample on 7 January. It is notable that within weeks following the identification of the virus, a series of reliable and sensitive **diagnostic tools** were developed and deployed. On 16 January, the first RT-PCR assays for COVID-19 were distributed to Hubei. Real-time PCR kits were distributed to all the provinces on 19 January and were provided to Hong Kong SAR and Macao SAR on 21 January. Information regarding viral sequences and PCR primers and probes was shared with WHO and the international community by China CDC on 12 January 2020. To facilitate product development and research on the new virus, COVID-19 virus sequences were uploaded to the GISAID Database by China.

By 23 February, there were 10 kits for detection of COVID-19 approved in China by the NMPA, including 6 RT-PCR kits, 1 isothermal amplification kit, 1 virus sequencing product and 2 colloidal gold antibody detection kits. Several other tests are entered in the emergency approval procedure. Currently, there are at least 6 local producers of PCR test kits approved by NMPA. Overall, producers have the capacity to produce and distribute as many as 1,650,000 tests/week.

Specimens from both the upper respiratory tract (URT; nasopharyngeal and oropharyngeal) and lower respiratory tract (LRT; expectorated sputum, endotracheal aspirate, or bronchoalveolar lavage) are collected for COVID-19 testing by PCR.

COVID-19 virus has been detected in respiratory, fecal and blood specimens. According to preliminary data from Guangzhou CDC as of 20 February, virus can initially be detected in upper respiratory samples 1-2 days prior to symptom onset and persist for 7-12 days in moderate cases and up to 2 weeks in severe cases. Viral RNA has been detected in feces in up to 30% of patients from day 5 following onset of symptoms and has been noted for up to 4-5 weeks in moderate cases. However, it is not clear whether this correlates with the presence of infectious virus. While live virus has been cultured from stool in some cases, the role of fecal-oral transmission is not yet well understood. COVID-19 has been isolated from the clinical specimens using human airway epithelial cells, Vero E6 and Huh-7 cell lines.

Serological diagnostics are rapidly being developed but are not yet widely used. Joint Mission members met with local research teams at the China CDC, Guangzhou Regenerative Medicine and Health Guangdong Laboratory. The teams reported on the development of tests for IgM, IgG and IgM+IgG using rapid test platforms utilizing chemiluminiscence. ELISA assays are also under development.

Research & Development

The government of China has initiated a series of major emergency research programs on virus genomics, antivirals, traditional Chinese medicines, clinical trials, vaccines, diagnostics and animal models. Research includes fundamental basic research and human subjects research. For the purpose of this report, human studies are limited to those involving IRB approval and informed consent. Other forms of human subjects investigations are included in the sections on epidemiology in this report. Well-focused, robust research conducted in the setting of an outbreak has the potential of saving many lives by identifying the most effective ways to prevent, diagnose and treat disease.

Since the COVID-19 virus has a genome identity of 96% to a bat SARS-like coronavirus and 86%-92% to a pangolin SARS-like coronavirus, an animal source for COVID-19 is highly likely. This was corroborated by the high number of RT-PCR positive environmental samples taken from the Huanan Seafood Market in Wuhan.

At least 8 **nucleic acid-based methods** for direct detection of COVID-19 and two colloidal gold antibody detection kits have been approved in China by the NMPA. Several other tests are close to approval. It will be important to compare the sensitivities and specificities of these and future serologic tests. Development of rapid and accurate **point-of-care tests** which perform well in field settings are especially useful if the test can be incorporated into presently commercially available multiplex respiratory virus panels. This would markedly improve early detection and isolation of infected patients and, by extension, identification of contacts. **Rapid IgM and IgG antibody testing** are also important ways to facilitate early diagnosis. Standard serologic testing can be used for retrospective diagnoses in the context of serosurveys that help better understand the full spectrum of COVID-19 infection.

A variety of **repurposed drugs and investigational drugs** have been identified. Screening NMPA approved drug libraries and other chemical libraries have identified novel agents. Hundreds of clinical trials involving remdesivir, chloroquine, favipiravir, chloroquine, convalescent plasma, TCM and other interventions are planned or underway. Rapid completion of the most important of these studies is critical to identifying truly effective therapies. However, evaluation of investigational agents requires adequately powered, randomized, controlled trials with realistic eligibility criteria and appropriate stratification of patients. It is important for there to be a degree of coordination between those conducting studies within and beyond China.

The development of a safe and effective **vaccine** for this highly communicable respiratory virus is an important epidemic control measure. Recombinant protein, mRNA, DNA, inactivated whole virus and recombinant adenovirus vaccines are being developed and some are now entering animal studies. Vaccine safety is of prime concern in the area of coronavirus infection in view of the past experience of disease enhancement by inactivated whole virus measles vaccine and similar reports in animal experiments with SARS coronavirus vaccines. It will be important that these vaccine candidates rapidly move into appropriate clinical trials.

The ideal **animal model** for studying routes of virus transmission, pathogenesis, antiviral therapy, vaccine and immune responses has yet to be found. The ACE2 transgenic mouse model and Macaca Rhesus model are already used in research laboratories. Systematically addressing which models can accurately mimic human infection is required.

There is a global rush for masks, hand hygiene products and other personal protective equipment. The relative importance of **non-pharmaceutical control measures** including masks, hand hygiene, and social distancing require further research to quantify their impact.

There are distinct patterns of intra-familial transmission of COVID-19. It is unclear whether or not there are host factors, including genetic factors, that influence susceptibility or disease course. COVID-19 has a varied clinical course and a precise description of that course is not available. In addition, the long-term consequences of COVID-19 are unknown. An observational cohort study of patients with COVID-19 enrolled from the time of diagnosis (with appropriate controls) could provide in-depth information about clinical, virologic and immunologic characteristics of COVID-19. Table 1 summarizes priority research areas with immediate to longer term goals.

Table 1 Priority research areas with immediate, intermediate and longer-term goals

Immediate Goals	Intermediate Goals	Long-term goals
Diagnostics: RNA assays, antibody & antigen assays, point of care detection	Diagnostics: Multiplex diagnostic platforms	Diagnostics: Prognostic markers
Therapeutics: Remdesivir, favipiravir, chloroquine, plasma, TCM	Therapeutics: intravenous immunoglobulin (IVIg)	Therapeutics: Innovative approaches (CRISPR-CAS; RNAi; Cell-based; positive hits from library screening)
Vaccines: Development of animal models	Vaccines: mRNA candidates and candidate viral vectors	Vaccines: inactivated candidates and subunit candidates

D. Knowledge Gaps

Knowledge gaps and key questions to be answered to guide control strategies include:

Source of infection

- Animal origin and natural reservoir of the virus
- Human-animal interface of the original event
- Early cases whose exposure could not be identified

The pathogenesis and virulence evolution of the virus

Transmission dynamics

- Modes of Transmission:
  - Role of aerosol transmission in non-health care settings
  - Role of fecal-oral transmission
- Viral shedding in various periods of the clinical course in different biological samples (i.e. upper and lower respiratory tract, saliva, faeces, urine)
  - Before symptom onset and among asymptomatic cases
  - During the symptomatic period
  - After the symptomatic period / during clinical recovery

Risk factors for infection

- Behavioral and socio-economic risk factors for infection in
  - Households / institutions
  - the Community
- Risk factors for asymptomatic infection
- Risk factors for nosocomial infection
  - among health care workers
  - among patients

Surveillance and monitoring

- Monitoring community transmission through existing
  - ILI surveillance
  - SARI surveillance
- The outbreak trend and intervention dynamics
  - Basic reproduction numbers in various stages of the epidemic
  - The epidemic's relation to seasonality

Laboratory and diagnostics

- Sensitivity and specificity of different nucleic acid (PCR, NAATs and rapid tests), antibody and antigen tests
- Post-infection antibody titers and the duration of protection
- Sero-prevalence among
    - Health care workers
    - General population
    - Children

Clinical management of severe and critically ill patients

- Value of ECMO in the management of critically ill patients
- Best practice using mechanical ventilation in the management of critically ill patients
- Re-evaluation of the role of steroids in the management of severe and critically ill patients
- Identification of factors associated with successful clinical management and outcome
- Determination of the effectiveness of Traditional Chinese Medicines (TCM)
- Determination the effectiveness of additional investigational treatment options (e.g. intravenous immunoglobulin/IVIg, convalescent plasma)

Prevention and control measures

- Key epidemic indicators that inform evidence-based control strategy decision making and adjustments
- Effectiveness of infection prevention and control (IPC) measures in various health care settings
- Effectiveness of entry and exit screening
- Effectiveness of the public health control measures and their socio-economic impact
    - Restriction of movement
    - Social distancing
    - School and workplace closures
    - Wearing mask in general public
    - Mandatory quarantine
    - Voluntary quarantine with active surveillance

E. Operational & Technical Recommendations

Operational/programmatic recommendations

- Reassess risk and capacities based on different stages of the outbreak; approve different measures during the different phases of the response; assess different stages of the response; reach a balance between response and social development
- Initiate a timely scientific evidence based, efficient and flexible joint multi-sectoral mechanism, which is driven by strong government leadership

Technical recommendations

Epidemiology and transmission

- Continue enhanced surveillance across the country through existing respiratory disease systems, including ILI, SARI or pneumonia surveillance systems
- Prioritize early investigations, including household transmission studies, age-stratified sero-epidemiologic surveys including children, case-control studies, cluster investigations, and serologic studies in health care workers

Severity

- Continue to share information on patient management, disease progression and factors leading to severe disease and favorable outcomes
- Review and analyze the possible factors associated with the disease severity, which may include:
    - natural history studies to better understand disease progression in mild, severe and fatal patients
    - medical chart reviews about disease severity among vulnerable groups, (e.g. those with underlying conditions, older age groups, pregnant women and children) to develop appropriate standards of care
    - evaluation of factors leading to favorable outcomes (e.g. early identification and care)

Clinical care and infection prevention and control

- Suspect patients who have not yet been tested should be isolated in single normal pressure rooms; cohorting of positive cases is acceptable
- Physicians and all health care workers need to maintain a high level of clinical alert for COVID-19
- For affected countries, standardize training for clinical care and IPC and scale with the development of local (e.g. district level) experts
- Ensure concurrent testing for other viral pathogens to support a negative COVID-19 test
- Ensure maintenance of usual and essential services during the outbreak

- Ensure processes are in place for infection prevention among the most vulnerable, including the elderly

- Ensure readiness to provide clinical care and to meet IPC needs, including:
    a. anticipated respiratory support requirements (e.g. pulse oximeters, oxygen, and invasive support where appropriate)
    b. national guidelines for clinical care and IPC, revised for COVID-19
    c. nationally standardised trainings for disease understanding and PPE use for HCWs
    d. community engagement
    e. PPE and Medication stockpiles
    f. early identification protocols; triage, temperature screening, holding bays (triage, including pulse oximetry)
    g. treatment protocols including designated facilities, patient transportation
    h. enhanced uptake of influenza and pneumococcal vaccine according to national guidelines
    i. laboratory testing
    j. rapid response teams

Laboratory and virology

- Continue to perform whole genome analysis of COVID-19 viruses isolated from different times and places, to evaluate virus evolution
- Conduct pathogenesis studies using biopsy/post-mortem specimens of COVID-19 patients or infected animal models
- Evaluate available nucleic acid PCR diagnostics
- Rapidly develop and evaluate rapid/point-of-care diagnostics and serologic assays
- Conduct further study to interpret the result of positive COVID-19 RNA detection in feces in patients recovering from COVID-19
- Enhance international cooperation, especially in terms of biosafety and information sharing for increased understanding of the COVID-19 virus and traceability of the virus
- Consider monitoring proinflammatory cytokines via multiplex assays to predict the development of "cytokine storm"

Research and development

- Additional effort should be made to find the animal source, including the natural reservoir and any intermediate amplification host, to prevent any new epidemic foci or resurgence of similar epidemics

- Efforts should be made to consistently evaluate existing and future diagnostic tests for detection of COVID-19 using a harmonized set of standards for laboratory tests and a biorepository that can be used for evaluating these tests
- Consider the establishment of a centralized research program in China to oversee that portfolio and ensure the most promising research (vaccines, treatments, pathogenesis) are adequately supported and studied first; program staff dedicated to the clinical research would work at the clinical research site(s) to decrease the research workload of the clinicians at the site
- Consider including one or more sites within China in the ongoing and future multi-center, international trials; Chinese investigators should be actively engaged in international trials
- Continue to develop additional animal models, making every effort to ensure these mimic human infection and virus transmission as closely as possible
- Conduct studies to determine which of the commonly used forms of PPE are most effective in controlling the spread of COVID-19

____

JOINT COMMENTS OF
AIRLINES FOR AMERICA,
THE INTERNATIONAL AIR TRANSPORT ASSOCIATION,
THE REGIONAL AIRLINE ASSOCIATION, AND
THE NATIONAL AIR CARRIER ASSOCIATION

Docket CDC-2020-0013

ATTACHMENT 25

ARTICLE 29 Data Protection Working Party

1014/06/EN
WP 121

Opinion 4/2006
on the Notice of proposed rule making
by the US Department of Health and Human Services
on the control of communicable disease and
the collection of passenger information of 20 November 2005
(Control of Communicable Disease Proposed 42 CFR Parts 70 and 71)

Adopted on 14 June 2006

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Civil Justice, Rights and Citizenship) of the European Commission, Directorate General Justice, Freedom and Security, B-1049 Brussels, Belgium, Office No LX-46 01/43.

Website: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

EXECUTIVE SUMMARY

This opinion by the Article 29 Working Party is a reflection on the new US legislative proposal concerning the collection of passenger information by air carriers and shipping lines for the control of communicable diseases (Control of Communicable Disease Proposed 42 CFR Parts 70 and 71).

The US draft proposal if enacted would impose some general obligations on European air carriers and and shipping lines and would in particular require them to put into practice the following:

1.) to collect and store in the EU for 60 days a number of data regarding all passengers flying to the US that are currently not included neither in the companies' passenger name record system (PNR) nor in their departure control system (DCS) such as emergency contact numbers, email addresses, travelling companions and information on the return flight in order to being able to trace them later on;

2.) to send these passenger details electronically within a 12 hour period of a request directly to the Director of the US Center for Disease Control and Prevention (CDC).

The Article 29 Working Party finds that the fight against communicable diseases is a valuable goal shared by all nations and has, therefore, to be supported in the best possible way. It is in the interest of mankind to curb the spread of diseases and to use modern techniques in the fight against scourges affecting great parts of the world.

The Article 29 Working Party is on the other hand of the opinion that the fundamental right to personal data protection has to be respected when measures are taken to fight communicable diseases and that any measures have to be proportionate. The right to personal data protection and the fight against communicable diseases are no contradictions but may work well alongside if a balanced approach is chosen.

This opinion on the new US legislative proposal examines carefully the foreseen regulations and analyses them not only in the light of the EU-Directive on Data Protection 95/46/EC, but also in the light of the WHO International Health Regulations (2005) which is non-binding in its nature but intends to support nations in their fight against communicable diseases.

The Article 29 Working Party comes to the conclusion that the US proposal if enacted in its current version would conflict with pertinent privacy provisions of the EU-Data Protection Directive 95/46/EC and the WHO International Health Regulations (2005).

* * *

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1], and in particular Articles 29 and 30 paragraph 1 (b) thereof,

Having regard to the Rules of Procedure of the Working Party[2], and in particular Article 12 and 14 thereof,

HAS ADOPTED THE FOLLOWING OPINION:

1. ISSUE UNDER DISCUSSION

The Department of Health and Human Services (HHS) of the United States of America has published a Notice of proposed rule making in the US Federal Register (Vol. 70, No 229, 30 November 2005; Control of Communicable Disease Proposed 42 CFR Parts 70 and 71; hereinafter: "US proposal"). The notice is concerned with the prevention of the introduction and the spread of communicable diseases into the US.

The US proposal intends to amend the Public Health Service Act (42 U.S.C. 264-271), parts 70 and 71. The latter part concerns foreign arrivals. The intent of the proposed updates of parts 70 and 71 is to clarify and strengthen existing procedures with a view to enabling the US Centers for Disease Control and Prevention (CDC) to respond more effectively to current and potential communicable disease threats. Section 71.10 on passenger information contains provisions aimed at identifying suspects who may have been exposed to a communicable disease allowing them to provide those suspects with direct medical care while preventing further person-to-person spread of the disease.

Section 71.10 (a) requires any carrier operating flights or shipping lines operating ships on an international voyage bound for a US port to solicit from each passenger and crewmember the following information:

(1) Full name (first, last, middle, initial, suffix);
(2) Emergency contact information;
(3) E-mail address;
(4) Current home address (street, apartment, city, state/province, postal code);
(5) Passport number or travel document number, including the issuing country or organization;
(6) Name of travelling companions or group;
(7) Flight information or port of call;
(8) Returning flight (date, airline number, and flight number) or returning ports of call; and
(9) At least one of the following current phone numbers in order of preference: mobile, home, pager, or work (Section 71.10 (e)).

[1] OJ L 281, 23.11.1995, p. 31, hereinafter: 'Directive'; available at: http://ec.europa.eu/justice_home/fsj/privacy.

[2] Adopted by the Working Party at its third meeting held on 11.9.1996.

In addition, further unspecified details, where necessary to prevent the introduction, transmission, or spread of communicable diseases may be required by the Director of the CDC (who has the authority for implementing part 71) if they are in the airline's or shipping line's possession (Section 71.10 (f)).

This information collected by the companies has to be retained by the company for a period of 60 days from the end of the voyage (Section 17.10 (b)). Airlines and shipping lines shall ensure that passengers are informed on the purposes for which the information is collected at the time the passengers arrange their travel (Section 71.10 (i). The information collected under Section 71.10 may only be used for the purposes for which it is collected (Section 71.10 (h). Within 12 hours of a request by the Director to the airline's or shipping line's agent, the airline or shipping line, pursuant to a written plan approved under Section 71.11, shall transmit in an electronic format the requested data fields specified above to the Director of CDC (Section 71.10 (d)).

In case of non-compliance, US authorities may impose sanctions on the companies concerned.

2. COMPATIBILITY OF THE PROPOSAL WITH DIRECTIVE 95/46/EC

2.1. Application of the Directive

The Directive applies as the requested information involves the processing of personal data wholly or partly by automatic means.

The exemptions of Article 3 (2) of the Directive do not apply as the US proposal is about the protection of public health, but not about processing data in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union or to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law.

2.2. Data collection in the EU

The proposed general obligation placed on EU based transport carriers to collect personal data from their passengers and from third parties and store this information for 60 days, breaches the provisions of the Data Protection Directive 95/46/EC, as such processing must be considered as being not required and in particular excessive (Article 6 (1) (c) and, therefore, goes against the principles of data reduction and data economy:

- The US proposal does not seem to take full account of the amount of personal data already available to other US authorities as part of existing immigration and entry controls, such as landing cards, passenger name records (PNR) or Advanced Passenger Information System (APIS) data (e.g. providing full names of passengers and other passport information) which may be exchanged under certain conditions. Nor does it take account of other internationally recognised methods regarding the direct collection of information from passengers such as public health passenger locator cards.

- The US proposal would oblige air carriers to collect specific data on air passengers without any reference to a defined and specific health threat, i.e. without being necessary for a specific purpose and without the legal foreseeability of a triggering event. This would not be in line with Article 6 of the Directive and with the definitions in Article 1 of the International Health

Regulations (2005)[3], e.g. of a "public health emergency of international concern"[4].

- The US proposal does not foresee the possibility of Article 7 (a) of the Directive – the *unambiguous consent* of the passenger (coupled with the information requirements of the Directive[5]). According to Article 2 (h) of the Directive, 'consent' means any freely given specific and informed indication of his wishes by which the data subject – in this case the passenger – signifies his agreement to personal data relating to him being processed.
- Article 7 (c) of the Directive does not apply to the US proposal as processing is not necessary for compliance with a *legal obligation* imposed by Community or Member State law to which the data controller (transport carrier) is subject, as this is a legal obligation imposed by the USA. An obligation imposed by a foreign legal statute or regulation, other than one created by an international instrument, may not qualify as a legal obligation by virtue of which data processing in the EU would be made legitimate. Any other interpretation would make it easy for foreign rules to circumvent the EU rules laid down in Directive 95/46/EC. A legal basis other than an international treaty or agreement could also be the commitment by a state to follow on a voluntary basis the guidelines of an international body such as the WHO, e.g. the International Health Regulations (2005).
- Article 7 (d) of the Directive does not apply to the US proposal as processing is not necessary in order to protect the *vital interests* of the data subject in the absence of a relevant public health alert where a particular individual is already suspect of a communicable disease in the meaning of Article 1 and Article 30 of the International Health Regulations (2005)[6] or is at risk of contracting a communicable disease.
- Article 7 (e) of the Directive does in the first place not apply to the US proposal as processing is not necessary for the performance of a task carried out in the *public interest of a EU Member State*, but only in the interest of the US, unless necessary in accordance with an international instrument obligation. Such a public interest, however, could be a public health emergency of international concern which would also concern competent EU authorities. Only in such a case, in connection with Article 6 and Article 7 of the International

[3] World Health Organisation (WHO), revised International Health Regulations (2005), adopted on May 23, 2005 (hereinafter: "International Health Regulations (2005)" or IHR; available at: http://www.who.int/csr/ihr/en/).

[4] *IHR Article 1 Definitions: "'public health emergency of international concern' means an extraordinary event which is determined, as provided in these Regulations: (i) to constitute a public health risk to other States through the international spread of disease and (ii) to potentially require a coordinated international response".*

[5] The Directive lays down that information must be provided at least on the identity of the controller, on the purpose of the processing and, under certain circumstances, on other points (see Article 10 *et seq.*).

[6] *IHR Article 1 Definitions: "'suspect' means those persons, baggage, cargo, containers, conveyances, goods or postal parcels considered by a State Party as having been exposed, or possibly exposed, to a public health risk and that could be a possible source of spread of disease"; IHR Article 30 Travellers under public health observation: "Subject to Article 43 or as authorized in applicable international agreements, a suspect traveller who on arrival is placed under public health observation may continue an international voyage, if the traveller does not pose an imminent public health risk and the State Party informs the competent authority of the point of entry at destination, if known, of the traveller's expected arrival. On arrival, the traveller shall report to that authority.*"

Health Regulations (2005)[7] a data transfer, such as via competent health authorities[8], would be in line with Article 7 (e) of the Directive.

- Article 7 (f) might apply to the US proposal if processing were necessary for the purposes of a legitimate interest pursued by the controller i.e. the air carriers or by the third party to whom the data are disclosed. Such a reason would however only be acceptable on condition that such legitimate interests are not "*overridden by the interests for fundamental rights and freedoms of the data subject*". Article 7 (f) requires a balance to be struck between the legitimate interest served by the processing of personal data and the fundamental rights of data subjects. This balance of interest test under Article 7 (f) should take into account issues of proportionality, subsidiarity, the seriousness of the specific public health threat that needs to be prevented and the consequences for the data subjects. In the context of the balance of interest test, adequate safeguards will also have to be put in place. In particular, Article 14 of Directive 95/46/EC provides that, when data processing is based on Article 7 (f), individuals have the right to object at any time on compelling legitimate grounds to the processing of the data relating to them.

2.2.2 Nature of data and period of conservation

- The US proposal would impose a general obligation to store personal data for 60 days irrespective of the differences between different communicable diseases with regard to incubation periods and communicability. Since this obligation has no specific disease in mind it is from a medical point of view not clear whether the storage period in its proposed form is adequate for the different types of diseases. In some cases it may be too long in other cases too brief depending on the incubation periods.

- According to the proposed amended Section 71.10 (f), additional *unspecified* passenger information could be requested by the Center for Disease Control and Prevention (CDC) which would not be in line with Article 23[9] of the

[7] *IHR Article 6 Notification: "1. Each State Party shall assess events occurring within its territory by using the decision instrument in Annex 2. Each State Party shall notify WHO, by the most efficient means of communication available, by way of the National IHR Focal Point, and within 24 hours of assessment of public health information, of all events which may constitute a public health emergency of international concern within its territory in accordance with the decision instrument, as well as any health measure implemented in response to those events. If the notification received by WHO involves the competency of the International Atomic Energy Agency (IAEA), WHO shall immediately notify the IAEA.*
2. Following a notification, a State Party shall continue to communicate to WHO timely, accurate and sufficiently detailed public health information available to it on the notified event, where possible including case definitions, laboratory results, source and type of the risk, number of cases and deaths, conditions affecting the spread of the disease and the health measures employed; and report, when necessary, the difficulties faced and support needed in responding to the potential public health emergency of international concern"."
IHR Article 7 Information-sharing during unexpected or unusual public health events:" If a State Party has evidence of an unexpected or unusual public health event within its territory, irrespective of origin or source, which may constitute a public health emergency of international concern, it shall provide to WHO all relevant public health information. In such a case, the provisions of Article 6 shall apply in full."

[8] *IHR Article 1 Definitions: "'competent authority' means an authority responsible for the implementation and application of health measures under theses regulations."*

[9] *IHR Article 23 Health measures on arrival and departure: "1. Subject to applicable international agreements and relevant articles of these Regulations, a State Party may require for public health purposes, on arrival or departure: (a) with regard to travellers: (i) information concerning the traveller's destination so that the traveller may be contacted; (ii) information concerning the traveller's itinerary to ascertain if there was any travel in or near an affected area or other possible contacts with*

International Health Regulations (2005) which foresees a clearly *specified* catalogue of information that can be requested by the competent health authorities.

2.3. Data transfer from the EU to the USA

The obligation on EU transport carriers to transfer the personal data to the US upon request by the Director of the Center for Disease Control and Prevention breaches the provisions of the Data Protection Directive 95/46/EC, as such transfer has no legal basis under Article 26.

- The US does not benefit from a finding that there is an adequate level for the protection of personal data as required by Article 25 (6) of the Directive.

- Considering the different purposes of the collection of passenger data, none of the existing EU-US legal schemes[10] can apply: neither the PNR-Agreement which has been annulled by the European Court of Justice on May 30, 2005[11] nor the Safe Harbour scheme.

- By way of derogation from Article 25 of the Directive, the transfer of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that the data subject has given his consent – i.e. freely given specific and informed consent, as required by Article 2 (h) of the Directive – unambiguously to the proposed transfer. The US proposal does not foresee this possibility.

- Article 26 (d) of the Directive does not apply as the transfer is not necessary or legally required on important public interest grounds of a EU Member State, but only in the US interest, unless the transfer is based on international health agreements providing for harmonised health measures at an international or European level, e.g. within the meaning of Article 2[12] and Article 35[13] of the International Health Regulation (2005), under specific conditions.

infection or contamination prior to arrival, as well as review of the traveller's health documents if they are required under these Regulations; and/or (iii) a non-invasive medical examination which is the least intrusive examination that would achieve the public health objective; (b) inspection of baggage, cargo, containers, conveyances, goods, postal parcels and human remains.

2. On the basis of evidence of a public health risk obtained through the measures provided in paragraph 1 of this Article, or through other means, States Parties may apply additional health measures, in accordance with these Regulations, in particular, with regard to a suspect or affected traveller, on a case-by-case basis, the least intrusive and invasive medical examination that would achieve the public health objective of preventing the international spread of disease."

[10] Cf. http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm.

[11] European Court of Justice, 30 May 2006; Joint cases C-317/04 (European Parliament/Council) and C-318/04 (European Parliament/Commission).

[12] *IHR Article 2 Purpose and scope: "The purpose and scope of these Regulations are to prevent, protect against, control and provide a public health response to the international spread of disease in ways that are commensurate with and restricted to public health risks, and which avoid unnecessary interference with international traffic and trade."*

[13] *IHR Article 35 General rule: "No health documents, other than those provided for under these Regulations or in recommendations issued by WHO, shall be required in international traffic, provided however that this Article shall not apply to travellers seeking temporary or permanent residence, nor shall it apply to document requirements concerning the public health status of goods or cargo in international trade pursuant to applicable international agreements. The competent authority may request travellers to complete contact information forms and questionnaires on the health of travellers, provided that they meet the requirements set out in Article 23.*"

3. OTHER ISSUES

- Information of passengers: This US proposal requires some data elements which are currently usually not collected and/or retained by the transport carriers which means that they will have to organize this collection and retention only for the purpose of satisfying US requirements. Furthermore it has to be mentioned that it is not quite clear whether the rights of the passengers are fully respected once the proposal is enacted. Although air carriers and shipping lines would be obliged to inform the persons concerned about the collection and storage of their data (Section 71.10 (d)) doubts remain on how this information is given and whether the passenger is correctly informed about his fundamental rights to access and redress in the meaning of Article 10, 11 and 12 of the Directive regardless of the fact whether the data are only stored in the companies data bases or transferred upon request to the CDC.

- The WHO International Health Regulations (2005) also lay down specific requirements for the treatment of personal data: Article 45 requires health information which refers to an identified or identifiable person to be kept confidential and processed anonymously. Only where it would be essential for the purposes of assessing and managing a public health risk, as defined in the International Health Regulations (2005), State Parties and the WHO may process personal data. However they must ensure that the personal data are: (a) processed fairly and lawfully, and not further processed in a way incompatible with that purpose; (b) adequate, relevant and not excessive in relation to that purpose; (c) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete are erased or rectified; and (d) not kept longer than necessary.

4. CONCLUSIONS

The desire of States to put in place their own measures to control the spread of communicable diseases is a valuable goal shared by all nations and any measures in the fight against diseases must be fully supported. Most issues at stake mentioned in this opinion are beyond the competence of airline companies and have to be addressed by the EU Member States and as necessary by the European Commission.

For international travel purposes, the Working Party prefers global solutions over unilaterally imposed demands and measures. It has expressed this point of view in previous opinions with regard to requests by different countries to provide PNR data in order to fight terrorism and other serious crimes of a transnational nature.

1. The Working Party is of the opinion that the fight against communicable diseases goes alongside the protection and promotion of fundamental rights, such as the fundamental right to the protection of personal data. Furthermore the Working Party is of the opinion that economic aspects should be taken into account as well and that the costs related to the collection and processing of personal data should be proportionate.

2. The rules on the protection of personal data do not prevent health authorities to process necessary personal information in order to prevent the introduction, transmission or spread of communicable diseases.

3. In the case of a recognized and actual health threat, the EU data protection Directive 95/46/EC itself provides for several grounds for legitimately processing personal data, even sensitive data on health, e.g. with the freely given and informed consent of the person concerned, or when processing is necessary to protect the vital interests of the individual or to protect the rights and freedom of others (see Article 7 (a) and (d), Article 13 (g) of the Directive).

4. To prevent the spread of communicable diseases, the possibility of tracing passengers in specific cases may be necessary for public health reasons under certain circumstances. In the past, in case of a public health threat like Severe Acute Respiratory Syndrome (SARS), this has been done by asking passengers on concerned flights to fill in so-called "locator cards" thus directly providing for the necessary information.

5. However, the current US draft proposal regarding collection by airlines of passenger information to prevent the introduction of communicable diseases into the US would lead to the disproportionate and routine disclosure of information by airlines who are subject to the requirements of Directive 95/46/EC.

6. Regarding passenger rights it remains unclear whether the US proposal fully respects the provisions of Article 10, 11 and 12 of the Directive i.e. right to adequate information, the right to access and redress.

7. The Working Party is therefore of the opinion that the US proposals if adopted in its current version would be in conflict with the Data Protection Directive 95/46/EC.

8. In addition, the Working Party is of the opinion that the US proposal if adopted in its current version would also be in conflict with regulations and guidelines published by the WHO, in particular the International Health Regulations (2005).

9. The Working Party calls, therefore, upon States to work within the current framework of international agreements to ensure a consistent approach which incorporates essential data protection safeguards.

Done at Brussels, on 14 June 2006

For the Working Party
The Chairman
Peter SCHAAR

JOINT COMMENTS OF
AIRLINES FOR AMERICA,
THE INTERNATIONAL AIR TRANSPORT ASSOCIATION,
THE REGIONAL AIRLINE ASSOCIATION, AND
THE NATIONAL AIR CARRIER ASSOCIATION

Docket CDC-2020-0013

ATTACHMENT 26

AT-SD 219/2
17/2/2020

AIR TRANSPORT COMMITTEE (ATC)

219TH SESSION — SECOND MEETING

(Council Chamber, Friday, 7 February 2020 at 1000 hours)

SUMMARY OF DECISIONS[1]

Third Meeting of the Aviation Data and Analysis Panel (ADAP/3) (Subject No. 15.6) — AT-WP/2180

1. The Committee considered the convening of the Third Meeting of the Aviation Data and Analysis Panel (ADAP/3) presented in AT-WP/2180.

2. Some Committee Members questioned proposals in Agenda Item 4: ICAO Air Transport Reporting Forms (Appendix C) regarding the discontinuation of Form M – Fuel Consumption and Traffic and the introduction of a new reporting form to collect cybersecurity incidents. The Committee agreed to defer this discussion to the 220th Session when the final report of the ADAP/3 is presented to the ATC.

3. Pursuant to its discussions, the Committee approved the:

a) proposed Terms of Reference presented in paragraph 2 to the working paper;

b) convening of ADAP/3 to be held from 15 to 17 April 2020 at ICAO Headquarters in Montréal in all official languages of the Organization, subject to the working languages of the members attending the meeting; and

c) the provisional agenda as presented in Appendix C to the working paper.

Report of the Eleventh Meeting of the Facilitation Panel (FALP/11) (Subject No. 15.4) —AT-WP/2179

4. The Committee considered the report of the Eleventh Meeting of the Facilitation Panel (FALP/11) on the basis of AT-WP/2179 which included proposed amendments to Annex 9 – *Facilitation* on subjects including Passenger Name Record (PNR) data, the Public Key Directory (PKD) and unruly and disruptive passengers.

5. While there was broad support to the proposed amendments to Annex 9, questions were raised regarding the costs to States for the implementation of PNR; the reliability of private entities handling the PNR data; possible disputes between States and industry; audit procedures; list of PNR requirements; as well as concerns expressed by the International Air Transport Association (IATA). A Committee Member also requested that the wording and punctuation of paragraph 9.29 in the Spanish version be aligned with the English version. It was also understood that the implementation of the proposed amendments would need to be followed closely by the Council, should any issue appear that would require adjustments in the future.

[1] The Summary of Decisions includes items for which no Council report is presented.

6. Following discussions, the Committee:

a) endorsed the proposal~~s~~ for amendments to Annex 9 – *Facilitation* recommended by FALP/11 to be circulated for comments of Member States and relevant international organizations;

b) approved the Secretariat's suggestion in paragraph 2.6 b) that a State Letter be issued to explain the process by which customs representatives may participate in the work of the Contact Committee; and

c) agreed to revisit the FALP's proposal in paragraph 2.6 e) that Doc 10117, *Manual on the Legal Aspects of Unruly and Disruptive Passengers* be inserted in the existing Note to paragraph 6.44 following consultations with the Legal Affairs and External Relations Bureau.

Work Programme of Air Transport Committee for the 220th Session (Subject No. 13) — AT-WP/2181

7. The Committee considered and approved the work programme of the ATC as presented in AT-WP/2181.

Any other business

− *Effects of the Coronavirus on civil aviation*

8. The Committee expressed appreciation to the Secretariat for providing a detailed presentation on the *Effects of the Coronavirus on civil aviation*. The presentation covered: ICAO regulatory framework (including relevant Annexes and reference documents), relevant Assembly Resolutions in force, economic impact, as well as coordination with other United Nations entities (in particular the World Health Organization and the United Nations World Tourism Organization). The Committee also expressed appreciation to the information provided by the Airports Council International and the International Air Transport Association.

9. Following the presentation and discussions, the Committee invited the Secretariat to:

a) offer a short-term and long-term action plan with recommendations for urgent consideration by the ATC, including by written procedure if required;

b) issue a State letter in order to urge States to: implement relevant provisions of Annex 9; become members of Collaborative Arrangement for the prevention and Management of Public Health Events in Civil Aviation (CAPSCA) in order to assist with the prevention of the spread of disease; and implement effective collaboration and coordination strategies with all stakeholders; and

c) add a follow-up item on Coronavirus to the work programme of the ATC for the 220th Session.

—END—

JOINT COMMENTS OF
AIRLINES FOR AMERICA,
THE INTERNATIONAL AIR TRANSPORT ASSOCIATION,
THE REGIONAL AIRLINE ASSOCIATION, AND
THE NATIONAL AIR CARRIER ASSOCIATION

Docket CDC-2020-0013

ATTACHMENT 27

International
Civil Aviation
Organization

Organisation
de l'aviation civile
internationale

Organización
de Aviación Civil
Internacional

Международная
организация
гражданской
авиации

منظمة الطيران
المدني الدولي

国际民用
航空组织

Tel.: +1 514-954-8219 ext. 6156

Ref.: EC 6/3 – 20/14

25 February 2020

Subject: Proposed amendment to Annex 9

Action required: provide comments to
ICAO Secretariat by 31 March 2020

Sir/Madam,

I have the honour to inform you that the Air Transport Committee, at the second meeting of the 219th Session on 7 February 2020, considered proposals for Amendment 28 to Annex 9 to the Convention on International Civil Aviation — *Facilitation*. These proposals arise from the review of Annex 9 conducted by the Facilitation (FAL) Panel during its eleventh meeting, held in Montréal from 13 to 16 January 2020, on inter alia, issues related to, Passenger Name Record (PNR) data, the Public Key Directory (PKD) and unruly and disruptive passenger. The documentation of the Panel's meeting is available at https://www.icao.int/Meetings/FALP/Pages/FALP11-2020.aspx. In this regard, it was agreed that the views of States and relevant international organizations would be solicited. Attachment A presents the proposed Amendment 28.

The subsequent work of the Air Transport Committee would be greatly facilitated by specific statements regarding the acceptability of the proposals. Please note that comments received by the Committee are normally classified as "agreement with or without comments", "disagreement with or without comments", or "no indication of position", as indicated on the response form in Attachment B. If the expressions "no objections" or "no comments" are used, they will be taken to mean "agreement without comment" and "no indication of position", respectively.

I wish to request that comments on the proposed amendment be dispatched to reach me no later than 31 March 2020. Comments received after that date may not be considered by the Committee. Should you anticipate a delay in your reply, please advise in advance of the due date.

Accept, Sir/Madam, the assurances of my highest consideration.

Fang Liu
Secretary General

Enclosures:
A — Proposed Amendment 28 to Annex 9 – *Facilitation*
B — Response form

ATTACHMENT A to State Letter EC 6/3 – 20/14

PROPOSED AMENDMENT 28 TO ANNEX 9 — *FACILITATION*

NOTES ON THE PRESENTATION OF THE PROPOSED AMENDMENT

The text of the Amendment is arranged to show deleted text with a line through it and new text highlighted with grey shading. The following illustrates the various amending methods:

~~text to be deleted is shown with a line through it~~ followed by the new text which is highlighted with grey shading	new text to replace existing text
new text to be inserted is highlighted with grey shading	new text to be inserted
~~text to be deleted is shown with a line through it~~	existing text to be deleted

TEXT OF THE PROPOSED AMENDMENT 28 TO THE

INTERNATIONAL STANDARDS AND RECOMMENDED PRACTICES

FACILITATION

ANNEX 9 TO THE CONVENTION ON INTERNATIONAL CIVIL AVIATION

Amend Annex 9 as follows:

CHAPTER 3. ENTRY AND DEPARTURE OF PERSONS AND THEIR BAGGAGE

. . . .

C. Security of travel documents

3.9.1 *Recommended Practice — Contracting States issuing or intending to issue eMRTDs should join the ICAO Public Key Directory (PKD)* ~~*and upload their information to the PKD*~~.

3.9.2. Contracting States that participate in the ICAO PKD shall upload the public key data necessary for authentication of all electronic passports that they issue to the PKD.

Note.—The provision of the Contracting State's Country-Signing Public Key Certificate Authority Certificates (C_{CSCA}) at the time of first use is considered the minimum level of data provision sufficient to fulfil this standard. Upload of certificate revocation lists (CRLs) is highly recommended.

. . . .

CHAPTER 6. INTERNATIONAL AIRPORTS — FACILITIES AND SERVICES FOR TRAFFIC

. . . .

E. Unruly passengers

6.44 Each Contracting State shall take measures to ensure that relevant personnel are provided training to identify and manage unruly passenger situations.

Note.— Guidance material on the legal aspects of unruly/disruptive passengers can be found in Circular 288 — Guidance Material on the Legal Aspects of Unruly/Disruptive Passengers and *Doc 10117,* Manual on the Legal Aspects of Unruly and Disruptive Passengers.

. . . .

CHAPTER 9. PASSENGER DATA EXCHANGE SYSTEMS

A. General

9.X Contracting States shall not require aircraft operators to provide non-standard data elements as part of API, iAPI and /or PNR provisions.

9.XX Contracting States shall, when considering requiring elements that deviate from the standard, submit a request to the WCO/IATA/ICAO Contact Committee in conjunction with the WCO's Data Maintenance Request (DMR) process via a review and endorsement process for inclusion of the data element in the guidelines.

. . . .

B. Advance Passenger Information (API)

~~9.10 When seeking to implement a national API programme, Contracting States that are unable to comply fully with the provisions contained in 9.8 with respect to data element requirements shall ensure that only those data elements that have been defined for incorporation into the UN/EDIFACT PAXLST message are included in the national programme's requirement or follow the WCO's Data Maintenance Request (DMR) process for any deviation from the standard.~~

. . . . . .

D. Passenger Name Record (PNR) Data

9.23 Each Contracting State ~~requiring Passenger Name Record (PNR) data~~ shall:

(a) develop a capability to collect, use, process and protect Passenger Name Record (PNR) data for flights to and from its territory supported by appropriate legal and administrative framework (such as, inter alia, legislation, regulation or decree), and be consistent with all Standards contained in Section D, Chapter 9, Annex 9;

(b) align its PNR data requirements and its handling of such data with the guidelines contained in ICAO Doc 9944, *Guidelines on Passenger Name Record (PNR) Data*, and in PNRGOV message implementation guidance materials published and updated by the WCO and endorsed by ICAO and IATA~~.~~ ; and

~~9.23.1 Contracting States requiring the transfer of PNR data shall~~

(c) adopt and implement the ~~EDIFACT-based~~ PNRGOV message ~~as the primary method~~ for airline-to-government PNR data transferal to ensure global interoperability.

Note 1.— UN Security Council, in Resolution 2396 (2017) at paragraph 12, decided that Member States shall develop the capability to collect, process and analyse, in furtherance of ICAO standards and recommended practices, passenger name record (PNR) data, and to ensure PNR data is used by and shared with all their competent national authorities, with full respect for human rights and fundamental freedoms, for the purpose of preventing, detecting, and investigating terrorist offenses and related travel.

Note ~~1~~ 2.— The PNRGOV message is a standard electronic message format endorsed jointly by WCO/ICAO/IATA. Depending on the specific aircraft operator's Reservation and Departure Control Systems, specific data elements which have been collected and stored by the aircraft operator for their own operational and commercial purposes and can be efficiently transmitted via this standardized message structure.

~~*Note 2. This provision is not intended to replace or supersede any messages exchanged between aircraft operators and customs administrations to support local airport operations.*~~

~~*Note 3. In addition to the mandatory EDIFACT based PNRGOV message, Contracting States may also, optionally, consider implementation of the XML PNRGOV message format as a supplemental method of PNR data transfer, thereby allowing those aircraft operators with XML capability a choice of format for the transmission of PNR data.*~~

9.24 ~~**Recommended Practice.—**~~ Contracting States shall, with full respect for human rights and fundamental freedoms: ~~*requiring PNR data should consider the data privacy impact of PNR data collection and electronic transfer, within their own national systems and also in other States. Where necessary, Contracting States requiring PNR data and those States restricting such data exchange should engage in early cooperation to align legal requirements.*~~

(a) clearly identify in their legal and administrative framework the PNR data to be used in their operations;

(b) clearly set the purposes for which PNR data may be used by the authorities which should be no wider than what is necessary in view of the aims to be achieved, including in particular law enforcement and border security purposes to fight terrorism and serious crime; and

(c) limit the disclosure of PNR data to other authorities in the same State or in other Contracting States that exercise functions related to the purpose for which PNR data are processed, including in particular law enforcement and border security purposes, and ensure comparable protections as those afforded by the disclosing authority.

9.25 Contracting States shall:

(a) prevent unauthorised access, disclosure and use of PNR data and their legal and administrative framework shall provide penalties for misuse, unauthorised access, and unauthorised disclosure;

(b) ensure the safeguards applied to their collection, use, processing and protection of PNR data apply to all individuals without unlawful differentiation;

(c) take measures to ensure individuals are informed about the collection, use, processing and protection of PNR data and related privacy standards employed;

(d) take measures to ensure that aircraft operators inform their customers about the transfer of PNR data;

(e) provide for administrative and judicial redress mechanisms to enable individuals to seek a remedy for the unlawful processing of their PNR data by public authorities; and

(f) provide for appropriate mechanisms, established by their legal and administrative framework, for individuals to obtain access to their PNR data and to request, if necessary, corrections, deletions or notations.

9.26 **Recommended Practice.** — *Subject to necessary and proportionate restrictions, Contracting States should notify individuals of the processing of their PNR data and inform them about the rights and means of redress afforded to them as defined in their legal and administrative framework.*

9.27 Contracting States shall:

(a) base the automated processing of PNR data on objective, precise and reliable criteria that effectively indicate the existence of a risk, without leading to unlawful differentiation; and

(b) not make decisions that produce significant adverse actions affecting the legal interests of individuals based solely on the automated processing of PNR data.

9.28 Contracting States shall designate one (or more) competent domestic authority(ies) as defined in their legal and administrative framework with the power to conduct independent oversight of the protection of PNR data and determine whether PNR data are being collected, used, processed and protected with full respect for human rights and fundamental freedoms.

9.29 Contracting States shall:

(a) not require aircraft operators to collect PNR data that is not required as part of their normal business operating procedures nor to filter the data prior to transmission; and

(b) not use PNR data revealing an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or data concerning their health, sexual life or sexual orientation other than in exceptional and immediate circumstances to protect the vital interests of the data subject or of another natural person. In circumstances where such information is transferred, Contracting States shall delete such data as soon as practicable.

9.30 Contracting States shall:

(a) retain PNR data for a set period as defined in their legal and administrative framework which shall be that period necessary and proportionate for the purposes for which the PNR data is used;

(b) depersonalise retained PNR data, which enable direct identification of the data subject, after set periods, which do not exceed what is necessary as defined in their national laws and policies, except when used in connection with an identifiable ongoing case, threat or risk related to the purposes identified in 9.24 (b);

(c) only re-personalise or unmask PNR data when used in connection with an identifiable case, threat or risk for the purposes identified in 9.24 (b); and

(d) delete or anonymise PNR data at the end of the retention period except when used in connection with an identifiable ongoing case, threat or risk purposes identified in 9.24 (b).

Note 1. – Depersonalization of PNR data is the masking of information which enables direct identification of an individual, without hindering law enforcement use of PNR data, whereas PNR data anonymization is the permanent removal of identity information of a person from the PNR record.

Note 2. —This standard is not intended to restrict criminal justice proceedings in Contracting States, such as investigation, prosecution and criminal trials, related to the purposes identified in 9.24 (b).

9.31 **Recommended Practice.—** *Contracting States should retain PNR data for a maximum period of five years after the transfer of PNR data, except when required in the course of an investigation, prosecution, or court proceeding.*

9.32 **Recommended Practice.—** *Contracting States should depersonalise PNR data within six months of and no later than two years after the transfer of PNR data.*

9.33 Contracting States shall:

(a) as a rule acquire PNR data using the 'push' method, in order to protect the personal data that is contained in the operators' systems and that operators remain in control of their systems;

(b) seek, to the greatest extent possible, to limit the operational and administrative burdens on aircraft operators, while enhancing passenger facilitation;

(c) not impose fines and penalties on aircraft operators for any unavoidable errors caused by a systems failure which may have resulted in the transmission of no, or corrupted, PNR data; and

(d) minimise the number of times the same PNR data is transmitted for a specific flight.

Note.— In exceptional circumstances and when a PNR 'push' transfer method is not feasible, such as when an aircraft makes an emergency landing, alternative means of PNR data acquisition can be used by a Contracting State in order to maintain operational continuity.

9.34 Contracting States shall:

(a) not inhibit or prevent the transfer of PNR data by an aircraft operator or other relevant party, nor sanction, impose penalties or create unreasonable obstacles on aircraft operators or other relevant parties that transfer PNR data to another Contracting State provided that Contracting State's PNR data system is compliant with the Standards contained in Section D, Chapter 9 of Annex 9; and

(b) equally, retain the ability to introduce or maintain higher levels of protection of PNR data, in accordance with their legal and administrative framework and to enter into additional arrangements with other Contracting States in particular to: promote collective security; achieve higher levels of protection of PNR data, including on data retention; or establish more detailed provisions relating to the transfer of PNR data, provided those measures do not otherwise conflict with the Standards contained in Section D, Chapter 9 of Annex 9.

Note 1. - The term "other relevant parties" refers to entities that are transferring PNR data to Contracting States, such as tour operators and travel agencies.

9.35 Contracting States shall demonstrate, to any requesting Contracting State, their compliance with the Standards contained in Section D Chapter 9 of Annex 9. A demonstration of compliance with the PNR Standards, upon request, shall take place as soon as possible. Contracting States shall work through this process in good faith and in a timely manner.

Note 1. - Demonstration of compliance can occur, among other things, based on bilateral consultations and/or the information in the ICAO online compliance checklist for Annex 9 – Facilitation contained in the Electronic Filing of Differences (EFOD) system.

9.35 bis **Recommended Practice.—** *Contracting States should allow other Contracting States compliant with the PNR Standards to receive PNR data, at least provisionally, while engaging in consultations, as necessary.*

9.36 Where Contracting States have determined they must inhibit, prevent or otherwise obstruct the transfer of PNR data or might penalize an aircraft operator, they shall do so with transparency and with the intent of resolving the situation which caused that determination.

9.37 **Recommended Practice.—** *Contracting States establishing a PNR program, or making significant changes to an existing program, pursuant to these SARPs, should proactively notify other Contracting States maintaining air travel between them prior to receiving data, including whether they are complying with these SARPs, to encourage or facilitate rapid consultation where appropriate.*

9.38 **Recommended Practice.—** *While attempting to resolve PNR data transfer disputes, Contracting States should not penalize aircraft operators.*

— — — — — — — —

ATTACHMENT B to State Letter EC 6/3 – 20/14

RESPONSE FORM
TO BE COMPLETED AND RETURNED TO ICAO
TOGETHER WITH ANY COMMENTS YOU MAY HAVE
ON THE PROPOSED AMENDMENTS

To: The Secretary General
International Civil Aviation Organization
999 Robert-Bourassa Boulevard
Montréal, Quebec
Canada, H3C 5H7

State: ______________________________

Please make a checkmark (√) against one option for the following amendment. If you choose the option "agreement with comments" or "disagreement with comments", **please provide your comments on separate sheets.**

	Agreement without comments	*Agreement with comments**	*Disagreement without comments*	*Disagreement with comments*	*No position*
Amendment to Annex 9 (Attachment A refers)					

* "Agreement with comments" indicates that your State or organization agrees with the intent and overall thrust of the amendment proposal; the comments themselves may include, as necessary, your reservations concerning certain parts of the proposal and/or offer an alternative proposal in this regard.

Signature: ____________________ Date ____________________

— END —

JOINT COMMENTS OF
AIRLINES FOR AMERICA,
THE INTERNATIONAL AIR TRANSPORT ASSOCIATION,
THE REGIONAL AIRLINE ASSOCIATION, AND
THE NATIONAL AIR CARRIER ASSOCIATION

Docket CDC-2020-0013

ATTACHMENT 28

PASSENGER AND AIRPORT DATA INTERCHANGE STANDARDS

EDIFACT IMPLEMENTATION GUIDE

PNR DATA PUSHED TO STATES OR OTHER AUTHORITIES

PNRGOV MESSAGE

Version 13.1

(subject to approval and publication by the WCO API Contact Committee)

NOTICE

DISCLAIMER. The information contained in this publication is subject to constant review in the light of changing government requirements and regulations. No subscriber or other reader should act on the basis of any such information without referring to applicable laws and regulations and/or without taking appropriate professional advice. Although every effort has been made to ensure accuracy, the International Air Transport Association shall not be held responsible for loss or damage caused by errors, omissions, misprints or misinterpretation of the contents hereof. Furthermore, the International Air Transport Association expressly disclaims all and any liability to any person, whether a purchaser of this publication or not, in respect of anything done or omitted, and the consequences of anything done or omitted, by any such person in reliance on the contents of this publication.

Managing Director,
IATA Distribution and Financial Services
International Air Transport Association
800 Place Victoria
P.O. Box 113
Montreal, Quebec
Canada, H4Z 1M1

Passenger and Airport Data Interchange Standards EDIFACT Implementation Guide – PNRGOV
PADIS EDIFACT Implementation Guide – PNRGOV (version 13.1)

Montreal — Geneva

Revision History

Version	Date	Author	Section	Change History
10.1	19May 2010	M Irons		Initial Publication – Numbering to be kept in line with the PADIS EDIFACT MESSAGE STANDARD release schedule
10.1	29Dec 2010	P Heilig		Made editiorial changes to segment layouts and example.
11.1	09Jan 2011- 27Jul 2011	A Colbath M. Odgers M.Zitkova		- Editorial changes based on comments from governments and technical staff - Editorial changes based on comments from governments - Additional editorial changes based on comments from governments - Agreed changes from the 04-05May11 PNRGOV Working Group. - Removed business case examples and add them to Appendix - Editorial changes - Corrected an error in example 5 of section 5.25.
12.1	27 Jun 2012	M-C Colin/ A. Colbath		Agreed changes from 11-12Nov, 14-15Feb12 and 9-10 May12 PNRGOV Working Groups
12.1	17 Jul 2012	M.Zitkova		Formatting changes required for the publication
12.1	30 Jul 2012	M. Zitkova		Editorial changes
12.1	3 Aug 2012	M. Zitkova		Modification of example 3 in 5.28.1 and example 5 in 5.28.2.
13.1	17 Mar 2013	M-C Colin		Agreed changes from 14-16 Sep PNRGOV Working Groups
13.1	28 Mar 2013	M. Zitkova		Updates to reflect the version and approval status
13.1	May 2013	M. Zitkova		Updates made as a result of PNRGOV 07
13.1	Jul 2013	M-C Colin		Agreed changes/updates from PNRGOV 07
13.1	July 2013	M Zitkova		Formatting and editorial changes required for the publication

1. INTRODUCTION

The purpose of this document is to describe the recommended usage of the Passenger and Airport Data Interchange Standards PNRGOV EDIFACT Message Standards. These messages are intended to facilitate the exchange of data relevant to government requirements on PNR data and Airlines reservation systems.

This document was developed, and will be maintained, by the IATA/ATA PNRGOV Sub-Group in coordination with the Passenger and Airport Data Interchange Standards Reservations Sub-Group.
This will be a living document and will be updated as necessary. If there are any changes to the message structure, the change process defined in the PNRGOV Principles Document should be followed.

1.1. PNRGOV MESSAGE VERSION RELEASE

Version control will be handled in the following manner:

- Message structure change requires a new version of the message and new version of the Implementation Guide.
- Minor changes can be kept in the Errata document attached to a specific release of the Implementation Guide and eventually incorporated into the next new release and new version of the same.
- Any text pending formal approval by the WCO API Contact Committee and/or the PADIS Board will be shaded in grey.

1.1.1 PROGRESSION LISTING

This table lists all current PNRGOV EDIFACT messages and shows in which PNRGOV Implementation Guide document release a message was modified from its previous publication. A bold version release shows the first publication of that message. A minus "-" sign indicates the message was not modified in that particular version release of the Message Standards.

TAG	Version Release Progression															
PNRGOV	**10.1**	-	**11.1**	-	**12.1**	**13.1**										
ACKRES	**10.1**	-	**11.1**	-	**12.1**	-										
GOVREQ	**-**	-	**-**	-	**12.1**	-										

1.1.2 ERRATA

An ERRATA sheet will be maintained for each release and will be stored on the IATA website along with the corresponding Implementation Guide.

- Each entry in the Errata sheet will include a sequence number, date included in ERRATA, Implementation Guide paragraph reference, current text and/or problems description for charts, required change in text and/or change description for charts, reason for change, and who submitted the ERRATA item. .
- Once an entry is made in Errata sheet, the PNRGOV group will receive a notification.
- The Errata sheet is intended only for minor corrections. Issues which require debate by the group must be submitted, together with a proposed solution, as formal agenda items to a PNRGOV Working Group meeting.
- Once changes are approved by the PNRGOV group, the group will notify WCO of changes made to the PNRGOV implementation guide.

1.2. DOCUMENT STRUCTURE

This document contains the following eight sections:

Introduction
Contains an overview and guidelines for use of the document.

Message Relationships
Describes the relationships between query messages and the expected response message for the different business functions listed. The function of a message can be modified, in some cases, by the use of data element 1225 in a MSG segment. This will be indicated as such in the message relationship section.

Message Structure
Shows in diagrammatic format each approved PADIS PNRGOV message. The diagrams show the construction of the message and the data segments used. The hierarchy of the segments is indicated by means of data levels.

Service Segments
Refer to the Architecture for IATA Interactive EDIFACT, and the ISO 9735 for United Nations Service Segments standards. For use in the PADIS Reservations environment, the service segments including the UNH have been described in greater detail in Section 4.

Data Segments
Lists in alphabetical order all data segments that are part of the messages contained in this document. For each segment there will be a list of the composites and data elements used to construct the segment and an indication of how these elements are commonly used. To cater for different business requirements, there may be multiple definitions of the same data segment.

Examples
For every business function listed there will be at least one example of the data to be transmitted. No response is anticipated except for an acknowledgement that the message has been received.

States' Legal Requirements
Each States legal requirements will be listed separately including a mapping to the PNRGOV Message structure where the information is held. This information will be mapped out to segment and element level. The same information may be found in different places, depending on the structure and contents and how this is stored in different reservation systems.

The IATA PNRGOV Principles Document contains a recap of the governments requirements. Additionally, IATA maintains a copy of the legislation on their API-PNR World Tracker extranet site. Use the following link to access this information:

Link for already registered users:
https://extranet2.iata.org/sites/facilitation/Lists/API%20World%20Tracker/By%20Country.aspx

Link to register for access to the FAL extranet site containing the API-PNR World Tracker:
http://www2.iata.org/registration/getemailpage.aspx?siteurl=facilitation

Appendices
As necessary, appendices will be added to the Implementation Guide.

Appendix A – contains details concerning the UN CONTROL message (Syntax and Service Report).
Appendix B – contains detailed business examples from a number of airlines.
Appendix C – contains PADIS EDIFACT Message Processing - Background for PNRGOV Users

1.3. HOW TO USE THIS DOCUMENT

The PNRGOV, ACKRES and GOVREQ messages are currently the only EDIFACT Message documented in this Implementation guide.

The guide contains complete description of the Message Structure, segments and elements with notes and examples.

1.4. GUIDELINES AND RULES

For all implementation guide additions and updates to Section 5 (Segments), the following rules apply to the format and contents, including definitions of special notations:

1. Data segments appear for each business function in Section 5.0.

2. If the information is the same for multiple business functions, the data segment will not be repeated.

3. If an 'N/A' appears in the 'Mandatory/Conditional' column, it indicates that the composite element or data element is conditional in the PADIS Message Standards, but for this function no applicable use has been identified. In such cases, all columns of the chart are completed, except “Common Usage”, “Code Set” and “Comments”. “Common Usage” and “Code Set” columns are marked “--” and the “Comments” column is left blank. If a composite is conditional and all component data elements are N/A, the composite is shown as N/A. If the composite is N/A, then all the component data elements will be shown as N/A.

4. If a composite or data element is defined as conditional in the IATA approved message but must be mandatory to complete a business function, the composite or data element will be indicated with a M for mandatory along with an asterisk (*). The M* will indicate the status differs from the PADIS Message Standard.

5. All elements marked as “C” (conditional) or as “M” or “M*” (mandatory) will have all columns of the charts completed as appropriate. When an element has multiple occurrences and is marked as M or M*, the first occurrence is considered mandatory and subsequent occurrences are considered conditional.

6. Where a State’s requirements differ for “Conditional” fields from the standard implementation guide, a separate supplemental document will be provided by the State(s) detailing which “Conditional” fields are “Mandatory” for that State. Provisions in paragraphs 1.5.1 and 1.5.2 of the “Principles, Functional and Business Requirements PNRGOV” shall be respected. These differing requirements will not change the structure of the message.

7. Where a State’s requirements differ from the standard implementation guide, a separate supplemental document will be provided by the State(s). This will not change the structure of the message.

8. If an element is a coded value, “Yes” is indicated in the “Code Set” column. If it is not a coded value, the column is marked “--”.

9. In general, dates and times are expressed in local time except where specifically noted; such as, the UNB where the time will be expressed in Greenwich Mean Time (GMT) or Universal Time Coordinated (UTC). Where GMT is specified in the examples, UTC equally applies. However, due to different systems criteria, the subject of date/times in various fields from various sources (e.g., centralized reservations and DCS for local vs. centralized system) should be addressed in the bilateral discussions between governments/airlines/system providers. .

10. The ”Field Type” refers to the field length as defined within the message and should match the value indicated in the most current PADIS Message Standards document.

11. “Common Usage” refers to the length and characteristics typically used to define that data element. This information is used to show how a data element should be used for this segment within the travel industry. Because existing data elements were used to create certain elements, the ”Field Type” characteristics exceed the actual requirements of the data element. “Common Usage” exists to better define the characteristics of the data element. This column should be consistent with similar elements.

12. The “Comments” column will use consistent wording for the same elements across the segments if they are used in the same way.

13. Each segment is followed by “Notes” (if applicable) and by segment examples. However, “Notes” are only included if they are necessary to explain the usage.

14. Each segment and message will have enough examples to show the standard usage as defined by the PADIS group.

15. For numeric fields, see reference Part 1 ISO 9735 Syntax Rules, Section 10.

16. The full stop (period .) or the comma (,) is allowed to represent the decimal mark. Either is acceptable within the interchange but both cannot be used in the same interchange.

17. The length of a numeric data element value shall not include the minus sign (-), the decimal mark (.), or the exponent mark (E or e).

18. When a decimal mark is used, there shall be at least one digit after the decimal mark.

19. When a segment appears at more than one level, it is reflected only once, with composites and data elements conditional as applicable.

20. The first segment in a group is mandatory and is the segment that triggers the group. Some trigger segments may be exchanged without data. In such cases these are noted with a pound (#) sign in the message diagram segment list in Section 3.2

21. For the purpose of the PNRGOV documentation all Airlines are referred to as Carriers and all governments are referred to as States.

1.5. CODE SETS

Codes used in codesets are used to define the values for the relevant business item. All codesets utilized in the PNRGOV message are defined in the **PASSENGER AND AIRPORT DATA INTERCHANGE STANDARDS - Codeset Directory.**

If additional codes are required, requests should be submitted to the PADIS Reservation Sub-group for approval prior to them being submitted in the PADIS Board vote for inclusion in the standards.

1.6. REFERENCES

The following documents may be used as additional references to the PNRGOV Iimplementation Guide:

- IATA PNRGOV Principles Document
- IATA PASSENGER AND AIRPORT DATA INTERCHANGE STANDARDS - MESSAGE STANDARDS DOCUMENT
- IATA PADIS EDIFACT and XML Codeset
- IATA Reservations Interline Message Procedures – Passenger (AIRIMP)
- IATA Passenger Services Conference Resolutions Manual (PSCRM)
- IATA Airline Coding Directory
- ISO 9735 – Version 4
- IATA SYSTEMS AND COMMUNICATIONS REFERENCE, VOLUME 6 – INTERACTIVE EDIFACT ARCHITECTURE

Definitions of common terms used within the airline industry can be found on the IATA website by accessing the IATA website as follows:

1. Go to the home page **www.iata.org**
2. Do a search on the word "glossary"
3. Download the spreadsheet entitled "**passenger-glossary-of-terms.xls"**

2 MESSAGE RELATIONSHIP

This Section describes the possible query and response relationship of the messages developed for PNRGOV function. The following convention is used to represent the possible relationships between messages; a solid line (______) indicates the primary relationship; and a broken line (-------) indicates an optional relationship.

The message diagram depicts the message relationship by showing the query origin in the top box and the response origin in the bottom box.

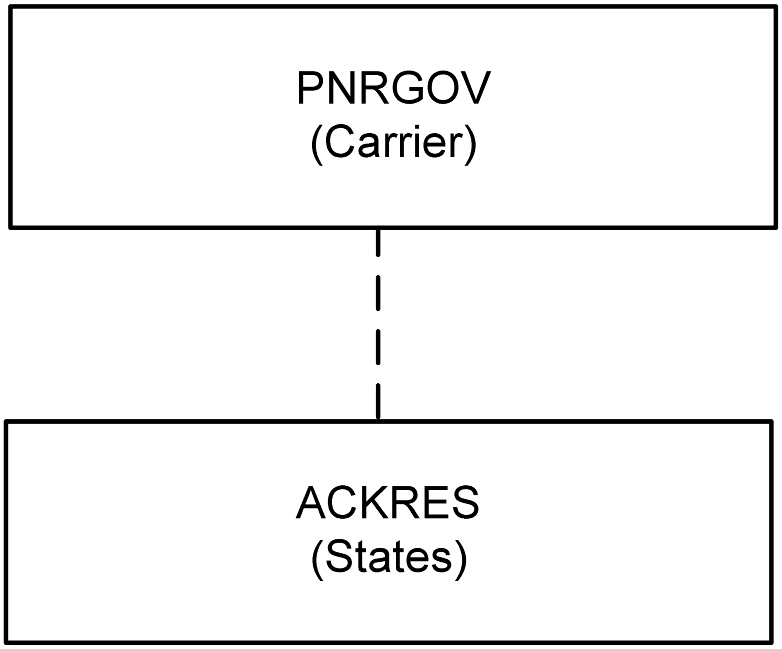
A CONTRL message (See Appendix A) is used:

(a) to respond to any message, indicating that a non-application error was encountered (usage not illustrated in message relationship diagrams)

(b) to acknowledge receipt of specific messages for which no paired response exists (as illustrated in the message relationship diagrams)

2.1 PNRGOV

The following messages are used by airlines, airline service suppliers and States to exchange PNR related data information.



.

Note: Data element 1225 of composite C302 in segment MSG defines the business function of the message.

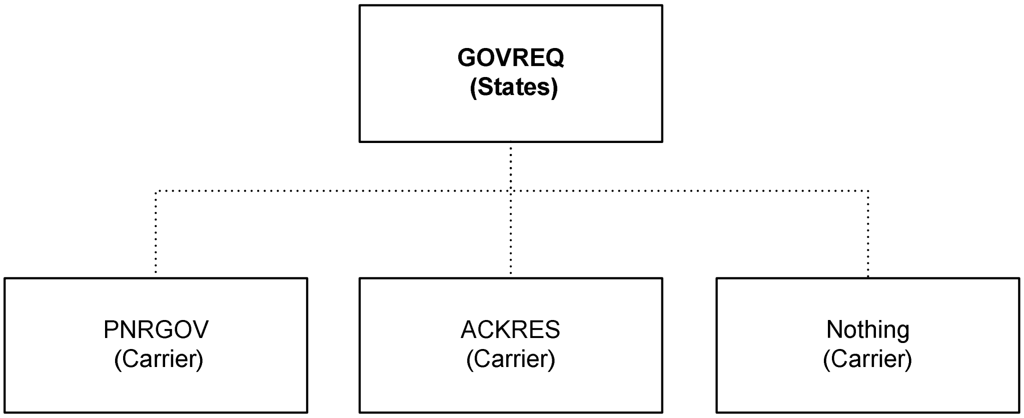
Message Functions:

PNRGOV	(Element 1225 = 22)	Push PNR data to States
PNRGOV	(Element 1225 = 141)	Update (used for update push)
ACKRES	(Element 1225 = 23)	Acknowledgement from States receipt of push PNR data

The ACKRES message is only sent where there is a Bilateral Agreement between Carrier and State to do so.

2.2 GOVREQ

The following messages are used by States to make an Adhoc request for a PNRGOV. The request may be for a specific airline/flight number/date or for a specific record locator. Implementation of this message requires a bilateral agreement between the government and the carrier. This message is to be used only in exceptional situations.



Notes: Date element 1225 of composite C302 in segment MSG defines the business function of the message.

Message Functions:

GOVREQ	(Element 1225 = 43)	Flight report
GOVREQ	(Element 1225 = 77)	Record locator request

The Bilateral Agreement defines the conditions under which the messages are exchanged. One of three results may occur:

- The carrier may respond with the PNRGOV message.
- The carrier may respond with the ACKRES message indicating one of two conditions: 1. The message is acknowledged and PNRs will be sent, or 2. errors are detected in the request, the ACKRES contains error codes to describe the error.
- The carrier may not respond and process according to carrier defined procedures.

3 MESSAGE STRUCTURE

This document describes the message structure for the IATA approved PADIS PNRGOVand other related EDIFACT messages to support the PNRGOVprocess.

In reference to the message diagrams, segments at Level 0 are not repeated and apply to the entire message. The first segment in a group is mandatory and is called the trigger segment. Segments at levels below the trigger segment apply to the group and not the entire message.

The order of segments within a group are read top to bottom, left to right.

If a group/segment is not shown in the diagram, this indicates it is not needed for the message function. Group numbers will remain for the full message diagram as defined in the message directory.

3.1 Message Segment Descriptions (PNRGOV)

The following information is intended to provide a high level understanding as to what data is contained in the individual segment at the various Groups and Levels in the PNRGOV message. More details are provided in the individual segment sections.

UNA -Service String Advice
UNB - Interchange Header Segment
UNG - Functional Group Header
UNH - message header information
MSG - specifies the function of the message
ORG - specifies the sender of the message
TVL - the flight (departure date/time, origin, destination, operating airline code, flight number, and operation suffix) for which passenger data is being sent.
EQN - the total number of PNRs being sent for the flight push

GR.1 - repeats for each passenger record sent
SRC - contains no data
RCI - the record locator(s) for this passenger record
SSR - special service data that applies to all passengers/ flights
DAT - date of most recent ticket issuance and last PNR transaction date/time
IFT - other service information (OSI) for all passengers/flights
ORG - origination of the booking
ADD - contact information
EBD - excess baggage information for all passengers

GR.2 - repeats for each surname in the passenger record
TIF - a passenger surname; indication of type - only use for group; a given name, PTC code, possible traveler reference to SSRs, FF's and other info, and a traveling with infant indicator. Repeats for each passenger name.
FTI - frequent traveler numbers for the passenger in the TIF
IFT - other service information (OSI) for this passenger
REF - unique passenger reference id
EBD - excess baggage information for this passenger(s)
FAR - fare info - PTC code, age, discounted fare type, percent of discount or country code, in-house fare type/corporate contract number, and fare basis code
SSR - special service data that applies to the passenger for all flights
ADD - emergency contact information and/or UMNR delivery and collection addresses

GR.3 - repeats for each ticket associated to this passenger
TKT - ticket number, total number of booklets issued, in connection doc info
MON - ticket amount
PTK - pricing information for this ticket
TXD - tax amounts for this ticket
DAT - Date of ticket issuance for each ticket

GR.4 - form of payment information
FOP - type of form of payment, credit card info, and other form of payment information associated with a ticket.
IFT - sponsor information
ADD - credit card billing information

GR.5 - repeats for each flight segment in the passenger record's itinerary
TVL - date/time of departure, arrival time, origin and destination, marketing & operating airline code(s), flight number, reservation booking designator, operational suffix.
TRA - operating carrier code, flight number and RBD.
RPI - flight booking status and number of passengers for this flight
APD - type of aircraft
SSR - special service requests that apply to this flight

RCI - passenger record locator specific to this flight
IFT - other service information (OSI) for this flight

GR.6 - Check in information for each flight in the itinerary
DAT - check-in time
ORG - the agent info that checked-in the passenger

GR.7 - boarding, seat number and checked bag info
TRI - sequence/boarding number for this check-in
TIF - the checked-in name
SSD - actual seat number (row and column)
TBD - checked bag information

GR.8 - split passenger record locator
EQN - the number of passengers split to/from a passenger record
RCI - the split record locators

GR.9 - non-air segments
MSG - specifies the type of non-air segment such as car, hotel, rail
TVL - non-air segment information

GR.10 - repeats for each occurrence of a history credit
ABI - originator of change and agent id
DAT - history time stamp

GR.11 - one line in a history credit
SAC - history action code
TIF - history passenger name changes
SSR - history special service requirement changes
IFT - history other service information changes
TBD – History Baggage Details

GR.12 - history flight information
TVL - flight dates, departure/arrival airport/city codes, airline, flight number, etc.
RPI - flight booking status and number of passengers

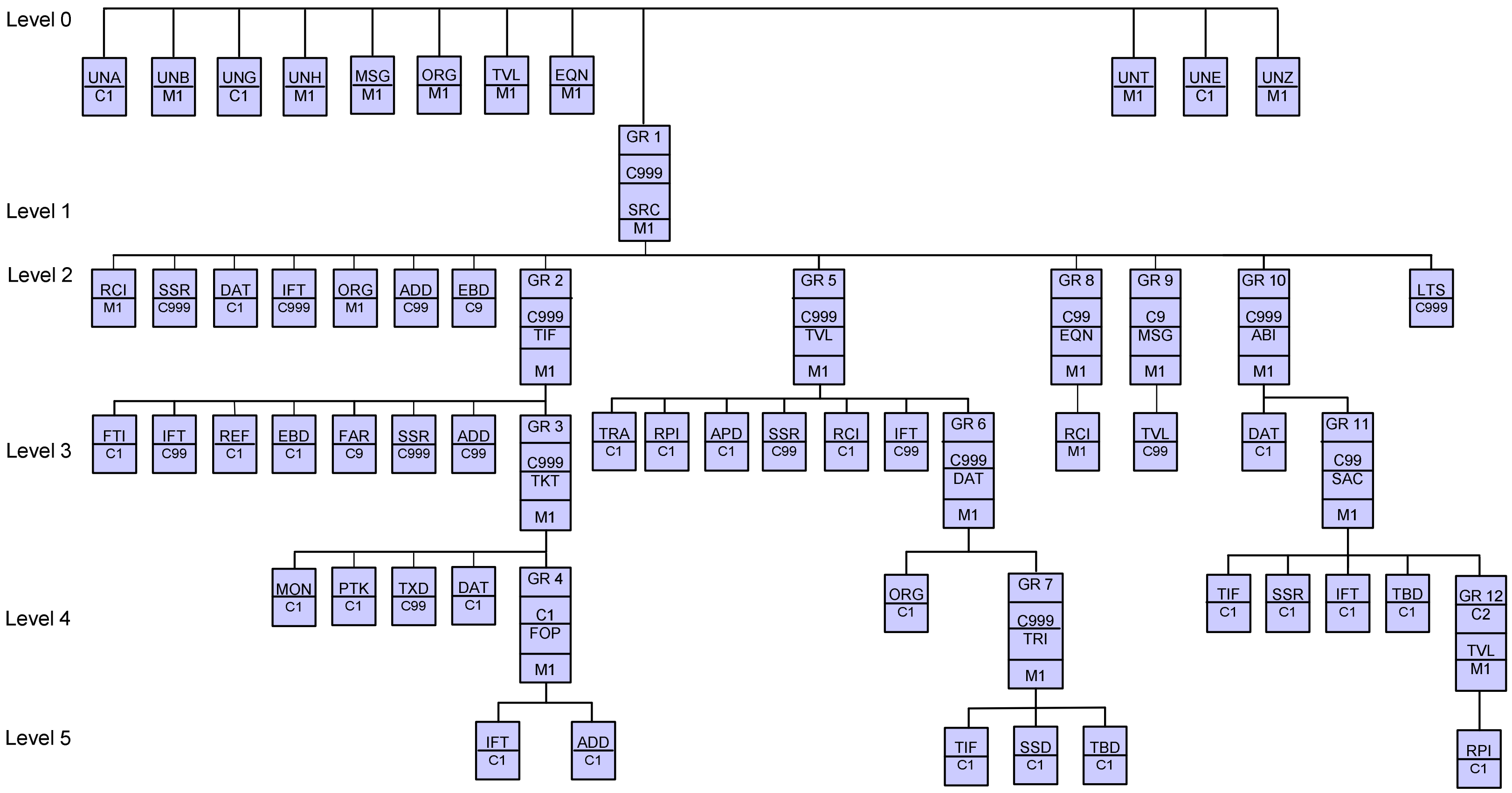
LTS - unformatted history information
UNT - Message Trailer Information
UNE- Functional Group Trailer
UNZ- Interchange Trailer

It should be noted that the message structure for ACKRES and GOVREQ are simple and therefore do not require a segment description as defined above for PNRGOV.

3.2 Push of PNR DATA to State - (PNRGOV)

Function: This message enables airlines to send data relevant to State requirements for passenger data in airline reservation systems.

PNRGov Message Structure



Segments:

ABI	Additional business source information
ADD	Address Information
APD	Additional product details
DAT	Date and time information
EBD	Excess Baggage Details
EQN	Number of units
FAR	Fare information
FOP	Form of Payment
FTI	Frequent Traveler Information
IFT	Interactive free text
LTS	Long Text String
MON	Monetary information
MSG	Message action details
ORG#	Originator of request details
PTK	Pricing/ticketing details
RCI	Reservation control information
REF	Reference information
RPI	Related product information
SAC	Source And Action Information
SRC#	Segment repetition control
SSD	Seat Selection Details
SSR	Special Requirements Details
TBD	Traveler Baggage Details
TIF	Traveler information
TKT	Ticket number detail
TRA	Transport identifier
TRI#	Traveller Reference Information
TVL	Travel product information
TXD	Tax details
UNA	Service String Advice
UNB	Interchange Header Segment
UNE	Functional Group Trailer
UNG	Functional Group Header
UNH	Message Header
UNT	Message Trailer
UNZ	Interchange Trailer

# Trigger segment

Some segments may occur multiple times in the structure. Some of these are due to name relation and/or segment relation.

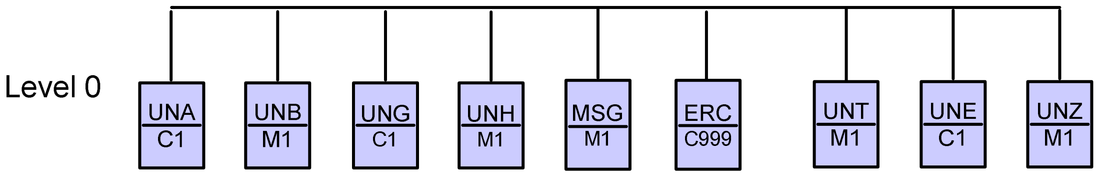
Where the usage differs depending on grp or level, an explanation is provided under each segment and also mapped back into each country's requirements in the Appendices.

3.3 ACKRES – Acknowledgement Response

Function: The ACKRES is used as a response under two possible conditions:

- If a State is responding to receipt of a PNRGOV from a carrier – As bilaterally agreed, to provide a response to the carriers as to whether the PNRGOV message was received.
- If a carrier is responding to receipt of a GOVREQ from a State – As bilaterally agreed, to provide a response to the State as to whether the GOVREQ message was received.

ACKRES – Acknowledgement Response



Segments:

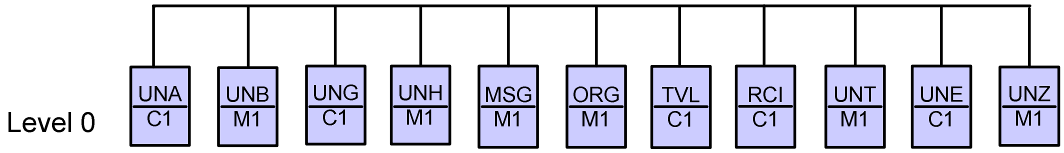
ERC	Errors identified in the message (coded) if sent to Carrier
MSG	To identify the message function being acknowledged and the result of the processing (successful, partially processed, etc.)
UNA	Service String Advice
UNB	Interchange Header Segment
UNE	Functional Group Trailer
UNG	Functional Group Header
UNH	Message Header Information
UNT	Message Trailer Information
UNZ	Interchange Trailer

Note: It is anticipated that through the provision of an acknowledgment message, Carriers will be able to automatically resend the messages if not delivered or incorrect data. This would be a system generated resend rather than one as a result of manual intervention.

3.4 PNRGOV ADHOC Request (GOVREQ)

Function: This message enables a State to make an adhoc request for PNRs of a specified airline/flight/date or record locator. The use of this message is controlled by a bilateral agreement between the State and the carrier.

GOVREQ – Government Request



Segments:

MSG	Message action details
ORG	Originator of request details
RCI	Reservation control information
TVL	Travel product information
UNA	Service String Advice
UNB	Interchange Header Segment
UNE	Functional Group Trailer
UNG	Functional Group Header
UNH	Message Header
UNT	Message Trailer
UNZ	Interchange Trailer

Notes:

1. The MSG should specify whether the request is for an airline/flight number/date or for a record locator.
2. If the request is for an airline/flight number/date, the TVL should be included in the request and the RCI should be omitted from the request.
3. If the request is for a record locator, the RCI should be included in the request and the TVL should be omitted from the request.

4 UNITED NATIONS SERVICE SEGMENTS

The United Nations Service Segments should be referenced in ISO 9735 and the Architecture for IATA Interactive EDIFACT. The IATA Architecture Strategy Group, along with its working groups, has made some changes to the service segments to satisfy the requirements of interactive EDIFACT. The UNB and UNZ should be implemented as they are described in the ISO 9735.

As per ISO 9735, the service segments are sequenced in a message in the following order:

UNA	Service String Advice
UNB	Interchange Header Segment
UNG	Functional Group Header
UNH	Message Header
	(BODY of MESSAGE)
UNT	Message Trailer
UNE	Functional Group Trailer
UNZ	Interchange Trailer

For ease in locating the service segment specification in this section, the service segments are defined in alphabetical order

4.1 UNA: SERVICE STRING ADVICE

Function: The Service String Advice (UNA) is Conditional and provides the capability to specify the service characters (delimitation syntax) used within the interchange. The UNA service string advice ***must*** be used if the service characters differ from the defaults. The UNA is optional if the default characters are used.

When used, the service string advice appears immediately before the interchange header segment. The service string advice shall begin with the upper case characters UNA immediately followed by six characters in the order shown below. The same character shall not be used in more than one position of the UNA.

Default Service Characters		
Name	**Graphic Representation**	**Functionality**
Colon	**:**	Component Data Element Separator
Plus sign	**+**	Data Element Separator
Full stop or Comma	**. or ,**	Decimal Mark
Question mark	**?**	Release Character
Asterisk	*****	Repetition Separator
Apostrophe	**‘**	Segment Terminator

Description	No.	Field Type	Comm Usage	Status	Max Rep	Code Set	Comp.	Values / Comments
COMPONENT DATA ELEMENT SEPARATOR	UNA1	an1	an1	M	1	-	-	
DATA ELEMENT SEPARATOR	UNA2	an1	an1	M	1	-	-	
DECIMAL MARK	UNA3	an1	an1	M	1	-	-	
RELEASE CHARACTER	UNA4	an1	an1	M	1	-	-	
REPETITION SEPARATOR	UNA5	an1	an1	M	1	-	-	
SEGMENT TERMINATOR	UNA6	an1	an1	M	1	-	-	

Note:

1. UNA1 through UNA6 represent the UN notation for positional values as opposed to normal representation using data element numbers. In this case where positional values are used, standard separators for standalone data elements are not used in the UNA segment. The data is simply a string of characters with each position defining a specific delimiter and its use.

Examples:

1. Default characters for UNA service string

   UNA:+.?*‘

2. In this example, the right-parens represents the exception to the default Segment Terminator.

   UNA:+.?*)

3. In this example, default characters have been replaced with specific system service string.

   UNA*(.-#’

4. In this example, Component Data Element Separator and Data Element Separator are unchanged, while Release Character, Repetition Separator and Segment Terminator are changed

   UNA:+.@?$

4.2 UNB: INTERCHANGE HEADER

Function: To start, identify and specify an interchange.

Composite/Data Element	**No.**	**Field Type**	**Comm Usage**	**Status**	**Max Rep**	**Code Set**	**Comp.**	**Values / Comments**
SYNTAX IDENTIFIER	S001	-	-	M	1	-	-	
Syntax identifier	0001	a4	a4	M	1	-	S001	**IATA**
Syntax version number	0002	n1	n1	M	1	-	S001	**1**
INTERCHANGE SENDER	S002	-	-	M	1	-	-	
Sender identification	0004	an..35	an..35	M	1	-	S002	***‘AIRLINE1’*** Sender of the message
Partner identification code qualifier	0007	an..4	-	N/A	-	-	-	
Address for reverse routing	0008	an..14	-	N/A	-	-	-	
INTERCHANGE RECEIVER	S003	-	-	M	1	-	-	
Recipient identification	0010	an..35	an..35	M	1	-	S003	***‘NZCS’*** Receiver of the message
Partner identification code qualifier	0007	an..4	-	N/A	-	-	-	
Routing address	0014	an..14	-	N/A	-	-	-	
DATE AND TIME OF PREPARATION	S004	-	-	M	1	-	-	
Date of preparation	0017	n6	n6	M	1	-	S004	***‘091128’*** The default format is ‘YYMMDD’ (n6)
Time of preparation	0019	n4	n4	M	1	-	S004	***‘0900’*** The default format is ‘HHMM’ (n4)
INTERCHANGE CONTROL REFERENCE	0020	an..14	an..14	M	1	-	-	***‘000000001’*** Will be repeated in UNZ data element 0020
RECIPIENTS REFERENCE PASSWORD	S005	-	-	N/A	-	-	-	
Recipient reference password	0022	an..14	-	N/A	-	-	S005	
Recipient reference password qualifier	0025	an..2	-	N/A	-	-	S005	
APPLICATION REFERENCE	0026	an..14	an..14	C	1	-	-	
PROCESSING PRIORITY CODE	0029	a1	a1	C	1	-	-	
ACKNOWLEDGEMENT REQUEST	0031	n1	n1	C	1	-	-	
COMMUNICATIONS AGREEMENT ID	0032	an.35		C	1	-	-	
TEST INDICATOR	0035	n1		C	1	-	-	

Notes:

1. The conditional status (C) of elements within this segment is used to indicate that Border Control Authorities may establish bilateral requirements for these data elements.
2. Elements 0001/0002 recommendation to use +IATA:1
3. Element 0004 is the airline code and 0010 is the targeted specific State entity.
4. Elements 0017 and 0019 are based on UTC (GMT)
5. For systems hosting multiple carriers and/or Ground Handlers, use composite S002, element 0008 for Carrier or ground handling agent (2 or 3 character airline designator, e.g. BD or full term e.g., AEROGROUND, or a bilaterally agreed code). Additionally S003, data element 0014 may be used for the routing address of the recipient or for hub routing for electronic documents.

Examples:

1. Generic example for PNRGOV file generated on 28th Nov 2009 at 9:00GMT:

   UNB+IATA:1+AIRLINE1+NZCS+091128:0900+000000001’

2. Message header DL Airline to Canadian CBSA for PNRGOV file generated on 12th Jan 2011 at 15:30GMT:

   UNB+IATA:1+DL+CBSAPNRGOV+110112:1530+1234567890’

3. This example is concerned with the push to Australia. QF30 is a flight with the following routing and times:

   HKG - 01 Aug 12 - 18:55 - MEL – 02 Aug 12 – 06:05

   The push will occur at 24h prior Scheduled Departure Time out of HKG

   For the flight departing on 1st Aug at 18:55 (Local Time) from HKG and arriving at MEL at 06:05 on 2nd Aug, the following segment UNB will be sent:

   UNB+IATB:1+1A+AUCBP+120731:1055+0002++PNRGOV+X'

4. United Airlines Flight 1752 - From San Francisco (SFO) to Sydney (SYD)

   Scheduled Departure: 02 Aug 12 14:25 local (22:25 GMT)

UNB segments	Push
UNB+IATA:1+UA+AUCBP+120731:2225+12345678905’	-72
UNB+IATA:1+UA+AUCBP+120801:2225+12345678904’	-24
UNB+IATA:1+UA+AUCBP+120802:2030+12345678903’	-2
UNB+IATA:1+UA+AUCBP+120802:2130+12345678902’	-1
UNB+IATA:1+UA+AUCBP+120802:2240+12345678901’	Wheels Up

4.3 UNE: FUNCTIONAL GROUP TRAILER

Function: To end and check the completeness of a Functional Group.

Composite/Data Element	No.	Field Type	Comm Usage	Status	Max Rep	Code Set	Comp.	Values / Comments
NUMBER OF MESSAGES	0060	n..6	n..6	M	1	-	-	***'1'***
APPLICATION SENDER IDENTIFICATION	0048	an..14	an..14	M	1	-	-	***'000000001'*** Must be equal to UNG data element 0048

Note:

1. Data element 0048 used in the UNE must match 0048 used in UNG

Example:

1. UNE+1+000000001'
2. See UNG example 2.

   UNE+1+1'
3. See UNG example 3.

   UNE+1+901'

4.4 UNG: FUNCTIONAL GROUP HEADER

Function: To head, identify and specify a Functional Group.

Composite/Data Element	No.	Field Type	Comm Usage	Status	Max Rep	Code Set	Comp.	Values / Comments
FUNCTIONAL GROUP IDENTIFICATION	0038	an6	an6	M	1	-	-	**PNRGOV**
APPLICATION SENDER IDENTIFICATION	S006	-	-	M	1	-	-	
Application Sender identification	0040	an..35	an..35	M	1	-	S006	***'AIRLINE1'*** Sending Application
Partner identification code qualifier	0007	an..4	-	N/A	-	-	S006	
APPLICATION RECIPIENT IDENTIFICATION	S007	-	-	M	1	-	-	
Application Recipient identification	0044	an..35	an..35	M	1	-	S007	***'NZCS'*** Receiving Application
Partner identification code qualifier	0007	an..4	-	N/A	-	-	S007	
DATE AND TIME OF PREPARATION	S004	-	-	M	1	-	-	
Date of preparation	0017	n6	n6	M	1	-	S004	***'091128'*** The default format is 'YYMMDD' (n6)
Time of preparation	0019	n4	n4	M	1	-	S004	***'0900'*** The default format is 'HHMM' (n4)
FUNCTIONAL GROUP REFERENCE NUMBER	0048	an..14	an..14	M	1	-	-	'***000000001'*** Will be repeated in UNE data element 0048
CONTROLLING AGENCY	0051	an..2	an..2	M	1	-	-	**IA**
MESSAGE VERSION	S008	-	-	M	1	-	-	
Message Type Version Number	0052	an..3	an..3	M	1	-	S008	**'10'** (for example)
Message Type Release Number	0054	an..3	an..3	M	1	-	S008	***'1'*** See Note 2.
Association assigned code	0057	an..6	an..6.	C	1	-	-	
APPLICATION PASSWORD	0058	an..14	an..14	C	1	-	-	

Notes:

1. The conditional status (C) of elements within this segment is used to indicate that Border Control Authorities may establish bilateral requirements for these data elements.
2. Border Control Authorities may establish bilateral requirements for the value placed in these data elements.
3. Data element 0048 used in the UNE must match 0048 used in UNG

Examples:

1. An example of an airline sending to a State agency

   UNG+PNRGOV+AIRLINE1+NZCS+091128:0900+000000001+IA+10:1'

2. See UNE example 2.

   UNG+PNRGOV+UA+USADHS+070218:1545+1+IA+D:05B'

3. See UNE example 3

   UNG+PNRGOV+AF+USADHS+070218:2100+901+IA+D:05B'

4.5 UNH: MESSAGE HEADER

Function: To head, identify and specify a Functional Group.

Composite/Data Element	No.	Field Type	Comm Usage	Status	Max Rep	Code Set	Comp.	Values / Comments
MESSAGE REFERENCE NUMBER	0062	an..14	an..14	M	1	-	-	***'MSG001'*** Will be repeated in UNT data element 0062
MESSAGE IDENTIFIER	S009	-	-	M	1	-	-	
Message type	0065	an..6	a6	M	1	-	S009	**PNRGOV**
Message version number	0052	an..3	n2	M	1	-	S009	**10**
Message release number	0054	an..3	n1	M	1	-	S009	***'1'*** See Note 2.
Controlling agency, coded	0051	an..2	a2	M	1	-	S009	**IA**
Association assigned code	0057	an..6	-	N/A	-	-	S009	
Code list directory version number	0110	an..6	-	N/A	-	-	S009	
Message type sub-function identification	0113	an..6	-	N/A	-	-	S009	
COMMON ACCESS REFERENCE	0068	an..35	an..35	C	1			Initiator's key. As per ISO 9735:CARF is a Key to relate all subsequent transfers of data to the same business case or file.
STATUS OF THE TRANSFER	S010	-	-	C	1	-	-	
Sequence of transfers	0070	n..2	n..2	M	1	-	S010	
First and last transfer	0073	a1	a1	C	1	-	S010	
MESSAGE SUBSET IDENTIFICATION	S016		-	N/A	-	-		
Message subset identification	0115	an.14	-	N/A	-	-	S016	
Message subset version number	0116	an..3	-	N/A	-	-	S016	

Note:

1. The conditional status (C) of elements within this segment is used to indicate that Border Control Authorities may establish bilateral requirements for these data elements.
2. When used in an ACKRES, the data elements 0068 and 0070 should carry the same values as the UNH of the message for which it is providing acknowledgement.
3. If multiple messages are required to send the PNRs for a given flight push, the following rules shall apply:

   - 0068 should be the same for each message in the series.

   - S010/0070 should contain the sequence number of each message in the series (consecutive numbers starting with 1)

   - S010/0073 should contain an indication of where the message fits into the sequence of multiple messages as one of the following:

   C – Commencing message of a sequence

   F – Final message of a sequence

   For interim messages in a sequence, S010/0073 is not used

Examples:

1. UNH with data element 0068 containing Initiator's key and Responder's key:

   UNH+1+PNRGOV:10:1:IA+0976310900003C'

2. UNH for a flight split across 3 messages.

   First message: UNH+1+PNRGOV:11:1:IA+893133434478201+01:C'

   Second message: UNH+1+PNRGOV:11:1:IA+893133434478201+02'

   Third and final message: UNH+1+PNRGOV:11:1:IA+893133434478201+03:F

3. UNH for PNR Push and ACKRES.

   PNR Push
   UNH+1+PNRGOV:10:1:IA+0976310900003C'

   ACKRES
   UNH+1+ACKRES:10:1:IA+0976310900003C'

4. UNH for PNR Push and ACKRES, where the flight is split across multiple messages, second message.
   PNR Push
   UNH+1+PNRGOV:11:1:IA+893133434478201+02'
   ACKRES
   UNH+1+ACKRES:11:1:IA+893133434478201+02'

4.6 UNT: MESSAGE TRAILER

Function: To end and check the completeness of a message by counting the segments in the message (including UNH and UNT) and validating that the message reference number equates to data element 0062 in the UNH segment (when applicable).

Composite/Data Element	No.	Field Type	Comm Usage	Status	Max Rep	Code Set	Comp.	Values / Comments
NUMBER OF SEGMENTS IN A MESSAGE	0074	n..10	n..10	M	1	-	-	'***2578***'
MESSAGE REFERENCE NUMBER	0062	an..14	an..14	M	1	-	-	'***MSG001***' Must equal UNH data element 0062

Notes:

1. For data element 0074, the number is computed by counting the number of segments used in the message from the UNH to the UNT inclusive.

2. For 0062, the value must be identical to the value in 0062 in the corresponding UNH segment.

Examples:

1. UNT+2578+MSG001´
2. UNT+2578+1'

4.7 UNZ: INTERCHANGE TRAILER

Function: To end and check the completeness of an Interchange.

Composite/Data Element	No.	Field Type	Comm Usage	Status	Max Rep	Code Set	Comp.	Values / Comments
INTERCHANGE CONTROL COUNT	0036	n..6	n..6	M	1	-	-	***'1'***
INTERCHANGE CONTROL REFERENCE	0020	an..14	an..14	M	1	-	-	***'000000001'*** Must be equal to UNB data element 0020

Example:

5. UNZ+1+000000001'

5 PADIS RESERVATIONS SUB-GROUP APPROVED SEGMENTS

This section lists all the segments, in alphabetical order, that are a part of the PADIS PNRGOV EDIFACT Message. For each segment, all composites and elements are listed along with a description, the element or composite number according to the data dictionary, field type, common usage, mandatory or conditional characteristic, number of repetitions, indication of a code set and general comments to assist in better understanding the intent of the composite and/or element.

Always refer to 3.1 Message Segment Descriptions for the context of the segment within the message structure.

5.1 ABI: ADDITIONAL BUSINESS SOURCE INFORMATION (PNRGOV)

Function: To specify additional originator and source information.

Push PNR Data to States - PNRGOV

Composite/Data Element	No.	Field Type	Comm Usage	Stat.	Max Rep.	Code Set	Comments
SOURCE TYPE	C337	- -	- -	M	1	- -	
Sector/subject identification qualifier	7293	an..3	an..3	M	2	Yes	To specify this information is the creator of the history credit.
ORIGINATOR DETAILS	C300	- -	- -	C	1	- -	
Travel agent identification details	9900	n..9	n8	C	1	- -	ATA/IATA ID number or pseudo IATA number.
In-house identification	9902	an..9	an..9	C	1	- -	Identification code assigned to an office/agency by the reservation system. Maybe a pseudo city or city and office number.
In-house identification	9902	an..9	an..9	N/A	1	- -	
In-house identification	9902	an..9	- -	N/A	1	- -	
LOCATION	C328	- -	- -	C	1	- -	
Place/Location Identification	3225	an..25	a3..5	C	1	Yes	The location of the agent making the change.
Place/Location name	3224	an..17	- -	N/A	1	- -	
COUNTRY, CODED	3207	an..3	an..3	N/A	1	- -	
COMPANY IDENTIFICATION	9906	an..35	an..3	C	1	Yes	A 2-3 character airline/CRS code to specify the creator of the change.

Example:

1. The creator of the history credit is a DL agent in Atlanta.

   ABI+4+05FD28:GS+ATL++DL’

5.2 ADD: Address Information (PNRGOV)

Function: To specify passenger address information.

Push PNR Data to States - PNRGOV

Composite/Data Element	No.	Field Type	Comm. Usage	Stat.	Max Rep.	Code Set	Comments
ACTION DETAILS	C031	- -	- --	N/A	1	- -	
Update action code	9858	a1	- -	N/A	1	- -	
Action request/notification, coded	1229	an..3	- -	N/A	9	- -	
ADDRESS DETAILS	C032	- -	- -	M	9	- -	
Address purpose code	3299	an..3	an..3	C	1	Yes	Specifies the purpose of the address information, e.g., contact, payer, billing address
Street and number/P.O. Box	3042	an..35	an..35	C	1	- -	The street number and name
City name	3164	an..35	an..35	C	1	- -	City name
Country sub-entity identification	3229	an..9	an..9	C	1	- -	State or province
Country sub-entity name	3228	an..35	an..35	C	1	- -	
Country, coded	3207	an..3	an..2	C	1	Yes	Use ISO 3166-1-alpha 2 code
Postcode identification	3251	an..17	an..10	C	1	- -	
Free text	4440	an..70	an..70-	C	1	- -	Telephone information
Place/location	3224	an.l7	- -	N/A	1	- -	

Notes:

1. The ADD in GR.1 at level 2 may contain a contact address for the PNR.
2. The ADD in GR.2 at level 3 may contain emergency contact information and or/ UMNR delivery and collection addresses.
3. The ADD in GR.4 at level 5 may contain the address of the payer of the ticket.
4. If the address and/or telephone information cannot be broken down in separate elements, the information may be found in OSIs and SSRs.

Example:

1. The contact address is 4532 Wilson Street, Philadelphia, zip code 34288

   ADD++700:4532 WILSON STREET:PHILADELPHIA:PA::US:34288’

5.3 APD: ADDITIONAL PRODUCT DETAILS (PNRGOV)

Function: To convey additional information concerning an airline flight.

Push PNR Data to States - PNRGOV

Composite/Data Element	No.	Field Type	Comm. Usage	Stat.	Max Rep.	Code Set	Comments
ADDITIONAL PRODUCT DETAILS	C314	- -	- -	C	1	- -	Additional details describing a specific means of transport
Type of Means of Transport	8179	an..8	an3	C	1	Yes	UN/IATA code identifying type of aircraft (747, 737, etc.).
Number of Stops	9924	n..3	- -	N/A	1	- -	
Leg Duration	9926	n..6	- -	N/A	1	- -	
Percentage	5482	n..8	- -	N/A	1	- -	
Days of Operation	9928	an..7	- -	N/A	1	- -	
Date/Time/Period	2380	an..35	- -	N/A	1	- -	
Complexing Flight Indicator	9950	an1	- -	N/A	1	- -	
Place/Location Identification	3225	an..25	- -	N/A	1	- -	
Place/Location Identification	3225	an..25	- -	N/A	1	- -	
Place Location Identification	3225	an..25	- -	N/A	1	- -	
STATION INFORMATION	C348	- -	- -	N/A	1	- -	
Gate Description	9870	an..6	- -	N/A	1	- -	
Related Place/ Location One ID	3223	an..25	- -	N/A	1	- -	
Related Place/ Location Two ID	3233	an..25	- -	N/A	1	- -	
STATION INFORMATION	C348	- -	- -	N/A	1	- -	
Gate Description	9870	an..6	- -	N/A	1	- -	
Related Place/ Location One ID	3223	an..25	- -	N/A	1	- -	
Related Place/ Location Two ID	3233	an..25	- -	N/A	1	- -	
MILEAGE/TIME DETAILS	C317	- -	- -	N/A	1	- -	
Measurement Value	6314	n..18	- -	N/A	1	- -	
Measure Unit Qualifier	6411	an..3	- -	N/A	1	- -	
First Time	9918	n..4	- -	N/A	1	- -	
TRAVELLER TIME DETAILS	C318	- -	- -	N/A	1	- -	
First Time	9918	n..4	- -	N/A	1	- -	
Second Time	9922	n..4	- -	N/A	1	- -	
Check-In Details	9952	an..10	- -	N/A	1	- -	
PRODUCT FACILITIES	C320	- -	- -	N/A	10	- -	
Facility Type, Coded	9932	an..3	- -	N/A	1	- -	
Facility Description, Text	9934	an..70	- -	N/A	1	- -	
Product Details Qualifier	9970	an..3	--	N/A	1	--	
Characteristic Identification	7037	an..17	--	N/A	26	--	

Example:

1. Equipment Type of Boeing 747

   APD+747'

5.4 DAT: DATE AND TIME INFORMATION (PNRGOV)

Function: To convey information regarding estimated or actual dates and times of operational events.

Push PNR Data to States - PNRGOV

Composite/Data Element	No.	Field Type	Comm. Usage	Stat.	Max Rep.	Code Set	Comments
DATE AND TIME DETAILS	C688	- -	- -	C	99	- -	
Date/Time/Period Qualifier	2005	an..3	an ..3	C	1	Yes	To identify the type of date to follow
First Date	9916	an..35	n6	C	1	- -	A date (ddmmyy).
First Time	9918	n..4	n4	C	1	- -	A time (hhmm).
Date/Time/Period Qualifier	2005	an..3	- -	N/A	1	- -	
First Time	9918	n..4	- -	N/A	1	- -	
Movement Type	8335	an..3	- -	N/A	1	- -	
Place/Location Identification	3225	an..25	- -	N/A	1	- -	

Notes:

1. DAT at GR1 can contain ticket issue date and last PNR transaction date/Time
2. DAT at GR6 will be check-in transaction date/time as stored by RES systems holding DC data
3. DAT at GR10 will hold PNR History transaction date/time
4. DAT at Group 6 holds Check-in information. C688/2005 will be used to specify that date/time is in free text format in data element C688/9916.
5. Unless specifically stated otherwise in bilateral agreement, the time is in Universal Time Coordinated (UTC)

Examples:

1. Latest PNR transaction date and time.

   DAT+700:241097:1005'
2. Ticket issuance date and time

   DAT+710:041159:0730'
3. Check-in transaction date/time

   DAT+2:010604:1800’
4. PNR History transaction date/time

   DAT+T:010695:1800'
5. Check-in including date time is expressed as free text

   DAT+3:L FT WW D014357 12AUG121423Z 1D5723'

5.5 EBD: EXCESS BAGGAGE DETAILS (PNRGOV)

Function: To specify information concerning excess baggage charges and the associated baggage details

Push PNR Data to States - PNRGOV

Composite/Data Element	No.	Field Type	Comm. Usage	Stat.	Max Rep.	Code Set	Comments
EXCESS BAGGAGE DETAILS	C674	- -	- -	C	1	- -	
Currency, coded	6345	an..3	an..3	C	1	- -	The currency code per unit
Monetary amount	5004	n..18	n..18	C	1	- -	The rate per unit
Processing indicator, coded	7365	an..3	- -	N/A	1	- -	
BAGGAGE DETAILS	C675	- -	- -	C	3	- -	
Quantity	6060	n..15	n..2	C	1	- -	The total number in excess
Measurement value	6314	n..18	- -	N/A	1	- -	
Allowance or charge qualifier	5463	an..3	an..3	C	1	Yes	Specifies if pieces or weight
Measure unit qualifier	6411	an..3	an..3	C	1	Yes	If weight, specifies if pounds or kilograms.
Processing indicator, coded	7365	an..3	- -	N/A	1	- -	
BAGTAG DETAILS	C358	- -	- -	N/A	99	- -	
Company identification	9906	an..35	- -	N/A	1	- -	
Item number	7140	an..35	- -	N/A	1	- -	
Total number of items	7240	n..15	- -	N/A	1	- -	
Place/location identification	3225	an..25	- -	N/A	1	- -	
Company identification number	9996	an..15	- -	N/A	1	- -	
Data indicator	9988	n..2	- -	N/A	1	- -	
Item characteristic, coded	7081	an..3	- -	N/A	1	- -	
Special requirement type	9962	an..4	--	N/A	1	--	
Measurement value	6314	n..18	--	N/A	1	--	
Measure unit qualifier	6411	an..3	--	N/A	1	--	
Free text	4440	an..70	--	N/A	1	--	

Note:

1. Used to send paid baggage information.

Example:

1. One piece of baggage over the allowance USD 50

   EBD+USD:50.00+1::N’

5.6 EQN: NUMBER OF UNITS

Function: To specify the number of units required.

Push PNR Data to States - PNRGOV

Composite/Data Element	No.	Field Type	Comm. Usage	Stat.	Max Rep.	Code Set	Comments
NUMBER OF UNIT DETAILS	C523	- -	- -	M	9	- -	
Number of Units	6350	n..15	n..3	M*	1	- -	A 1-3 numeric to specify number of PNR or passengers.
Number of Units Qualifier	6353	an..3	- -	N/A	1	- -	

Notes:

1. The EQN at level 0 is used to specify the total number of PNRs being sent for the flight push. In case of full PNR push, the total number of PNRs contained in the full PNR push regardless of the number of messages used for the full push. In the case of update PNR push, the total number of PNRs contained in the update PNR push regardless of the number of messages used for the update push should be used.
2. The EQN at GR8 is used to identify numbers of passengers split from/to PNR.
3. As bilaterally agreed, where there is no PNR to be sent in a specific message, the EQN at level ‘0’ may contain the number zero (“0”).

Examples:

1. Total number of PNRs

   EQN+98'
2. Four passengers split from this PNR.

   EQN+4'MSG

5.7 ERC: APPLICATION ERROR INFORMATION

Function: To identify errors in the message sent to the States

Acknowledgement Response – ACKRES

Composite/Data Element	**No.**	**Field Type**	**Comm. Usage**	**Stat.**	**Max Rep.**	**Code Set**	**Comments**
APPLICATION ERROR DETAIL	C901	- -	- -	M	1	- -	
Application error, coded	9321	an..3	n..3	M	1	Y	
Code list qualifier	1131	an..3	- -	N/A	1	--	
Code list responsible agency, coded	3055	an..3		N/A	1		

Examples:

1. Application Error - Invalid Departure Time

   ERC+103'

2. Invalid flight number.

   ERC+114'

5.8 FAR: FARE INFORMATION (PNRGOV)

Function: To specify fare information details.

Push PNR Data to States - PNRGOV

Composite/Data Element	**No.**	**Field Type**	**Comm. Usage**	**Stat.**	**Max Rep.**	**Code Set**	**Comments**
NUMBER OF UNITS QUALIFIER	6353	an..3	an..3	C	1	Yes	Type of passenger, e.g. adult, child, group, corporate. Used to specify an industry defined pricing passenger type code (PTC).
QUANTITY	6060	n..15	n..3	C	1	- -	Age. To specify age related to a child or senior citizen, etc.
FARE DETAILS	C662	- -	- -	C	1	- -	
Number of units Qualifier	6353	an..3	an..3	C	1	Yes	Discounted fare type, related to each PTC code.
Percentage	5482	n..8	n..3	C	1	- -	The percent of discount. Discount fare.
Country, coded	3207	an..3	an..3	C	1	Yes	ISO country code in lieu of discounted percentage amount.
Fare classification type, coded	9878	an..3	an..3	C	1	Yes	Discounted fare classification type.
IDENTITY NUMBER	7402	an..35	an..35	C	1	- -	In-house fare type/corporate contract number.
FARE TYPE GROUPING INFORMATION	C644	- -	- -	N/A	1	- -	
Pricing Group	5388	an..35	- -	N/A	5	- -	.
RATE/TARIFF CLASS	5242	an..35	an..18	C	9	- -	Fare basis code/ticket designator code.

Examples:

1. The fare is a 20 percent discounted fare type for an 9 year old child.

   FAR+C+9+1:20:US+++YEE3M'

2. The fare is an industry discounted passenger traveling on business with space available.

   FAR+I++764:4::B2+++C'

5.9 FOP: FORM OF PAYMENT (PNRGOV)

Function: To convey details describing the form of payment

Push PNR Data to States - PNRGOV

Composite/Data Element	No.	Field Type	Comm. Usage	Stat.	Max Rep.	Code Set	Comments
FORM OF PAYMENT DETAILS	C641	- -	- -	M	99	- -	
Form of Payment Identification	9888	an..10	an..3	M	1	Yes	Form of payment type
Data Indicator	9988	an..3	an..3	C	1	Yes	To indicate old, new or original form of payment
Monetary Amount	5004	n..18	n..18	C	1	- -	Form of payment amount
Company Identification	9906	an..35	an..3	C	1	- -	Vendor code (CC)
Reference Number	1154	an..35	an..25	C	1	- -	Account number (CC/GR/SGR)
First Date	9916	an..35	n4	C	1	- -	Expiration date (CC) (mmyy)
Approval Identification	9889	an..17	-	N/A	1	- -	
Source, Coded	9890	an..3	-	N/A	1	- -	
Monetary Amount	5004	n..18	-	N/A	1	- -	
Verification, Coded	9891	an..3	-	N/A	1	- -	
Account holder number	3194	an..70	-	N/A	1	- -	
Payment Time Reference, Coded	2475	an..3	-	N/A	1	- -	
Free Text	4440	an..70	-	C	1	- -	
Membership Status, Coded	7453	an..3	-	N/A	1	- -	
Transaction Information	9892	an..35	-	N/A	1	- -	

Note:

1. If payment is via credit card, then the provision of the cardholder name is via the IFT if different from the passenger.

Examples:

1. Paid with an American Express card, with an expiration date of 12/11

   FOP+CC::416.00:AX:373212341234123:1211’

2. Form of payment is cash.

   FOP+CA::731.00'

3. Form of payment is Government receipt.

   FOP+GR::200.00::AB123456'

4. Old form of payment was VISA card with an expiration date of August, 2013

   FOP+CC:2:628.32:VI:4235792300387826:0813’

5.10 FTI: FREQUENT TRAVELLER INFORMATION (PNRGOV)

Function: To specify frequent traveller information.

Push PNR Data to States - PNRGOV

Composite/Data Element	No.	Field Type	Comm. Usage	Stat.	Max Rep.	Code Set	Comments
FREQUENT TRAVELLER IDENTIFICATION	C326	- -	- -	M	9	- -	
Company Identification	9906	an..35	an..3	M	1	Yes	Airline designator, coded
Frequent Traveller Identification	9948	an..25	an..20	M	1	- -	A code to identify a frequent traveller - the frequent traveller number.
Traveller Reference Number	9944	an..10	- -	N/A	1	- -	
Status, coded	4405	an..3	- -	N/A	1	- -	
Membership level	7456	an..35	- -	C	1	- -	Membership Information
Hierarchical ID Number	7164	an..12	- -	N/A	1	- -	
Item Description	7008	an..35	- -	C	1	- -	Tier Description
Company Identification	9906	an..35	- -	C	1	- -	Alliance Code
Passenger Priority Value	9949	n..4	- -	N/A	1	- -	

Examples:

1. A United Airlines Frequent Traveller.

   FTI+UA:12345678964'

2. Passenger is using frequent flyer account on airline ZZ.

   FTI+ZZ:001012693109'

3. Passenger has a British Airways Frequent Traveller number, is a BA GOLD member and description of tier level is GOLD. Passenger also has a One World (code 701) alliance Emerald member.

   FTI+BA:12345678:::GOLD::GOLD+BA:12345678:::EMER::EMERALD:701'

5.11 IFT: INTERACTIVE FREE TEXT (PNRGOV)

Function: To provide free form or coded text information.

Push PNR Data to States - PNRGOV

Composite/Data Element	**No.**	**Field Type**	**Comm. Usage**	**Stat.**	**Max Rep.**	**Code Set**	**Comments**
FREE TEXT QUALIFICATION	C346	- -	- -	C	1	- -	
Text Subject Qualifier	4451	an..3	an..3	M	1	Yes	See code set values.
Information Type	9980	an..4	an..4	C	1	Yes	A code describing data in 4440
Status, coded	4405	an..3	an..3	C	1	Yes	Fare calculation reporting indicator or pricing indicator
Company Identification	9906	an..35	an..3	C	1	- -	Validating carrier airline designator
Language, coded	3453	an..3	- -	N/A	1	Yes	ISO Code for Language of free text.
FREE TEXT	4440	an..70	an..70	C	99	- -	Free text message

Notes:

1. Multiple occurrences of the same type of literal free text should each be contained in a separate IFT segment to avoid confusion regarding where each occurrence begins and ends.
2. If the value in code set 4451 indicates that coded information exists, then this coded data pertains to information in element 9980.
3. Data in fare calculation is positional information within a free text data element. The data should never be truncated or padded by an EDIFACT handler.
4. When data element 4451 is used, it should contain values 1, 3 or 4. All other codes in 4451 code set are SISC codes.

Examples:

1. Fare calculation with fare calculation reporting indicator.

   IFT+4:15:0+DEN UA LAX 01.82 487.27 UA DEN 487.27 USD976.36 ENDXFDEN3LAX+3'

2. OSI information.

   IFT+4:28::KL+CTC 7732486972-U‘

3. Sponsor information.

   IFT+4:43+TIMOTHY SIMS+2234 MAIN STREET ATLANTA, GA 30067+770 5632891‘

5.12 LTS: LONG TEXT STRING (PNRGOV)

Function: To represent a piece of information that contains multiple lines of text as one whole.

Push PNR Data to States - PNRGOV

Composite/Data Element	No.	Field Type	Comm. Usage	Stat.	Max Rep.	Code Set	Comments
TEXT STRING DETAILS	9990	an..9999	an..9999	M	1	- -	Block of free text up to 9999 characters. May include control characters such as carriage return and line feed.

Notes:

1. Carriage returns and line feeds may corrupt commercial parsers and this will need to be agreed through a bilateral agreement
2. Flown segments are to be included in history.

Example:

1. Unstructured PNR history.
   ```
   LTS+ LAX GS WW D006217 2129Z/09DEC 02961B AS DL1314U 19FEB MCOATL NN/SS1
   1130A    105P AS SEAT RS    29F  TRAN/TRINH              DL1314 19FEB MCOATL AS DL1319T
   23FEB ATLMCO NN/SS1   355P  524P¬AS SEAT RS    28A  TRAN/TRINH              DL1319 23FEB
   ATLMCO A$ 4P  A-USD   160.93 TX  33.27          TTL    194.20 WW09DEC AC  A ORL DL
   ATL87.44UA10A0SJ DL ORL73.49TA10X3SJ USD160.93END  ZP MCOATL XF MCO4.5ATL4.5 PS
   LAXADLLAX LAXGSWWUS LAXDL -LAX GS WW D006217 09DEC2129Z 02961B XS DL1314U 19FEB
   MCOATL NN/HK1  1130A  105P  XS SEAT XR/RS 29F  TRAN/TRINH              DL1314 19FEB MCOATL
   XS DL1319T 23FEB ATLMCO NN/HK1   355P  524P XS SEAT XR/RS 28A  TRAN/TRINH              DL1319
   23FEB ATLMCO X$ 4P  A-USD   160.93 TX  33.27          TTL    194.20 WW09DEC XC  A ORL DL
   ATL87.44UA10A0SJ DL ORL73.49TA10X3SJ USD160.93END  ZP MCOATL XF MCO4.5ATL4.5 XE  A-
   USD XF-9.00/ZP-7.20/AY-5.00/US-12.07/ XT TKT-TE/1200N/09DEC    -LAX GS WW D006217
   09DEC2129Z 02961B’
   ```

5.13 MON: MONETARY INFORMATION (PNRGOV)

Function: To specify monetary information details.

Push PNR Data to States - PNRGOV

Composite/Data Element	No.	Field Type	Comm. Usage	Stat.	Max Rep.	Code Set	Comments
MONETARY INFORMATION	C663	- -	- -	M	20	- -	
Monetary amount type qualifier	5025	an..3	an1..3	M	1	Yes	To specify total ticket/document amount
Allowance or Charge number	1230	an..35	an1..18	C	1	- -	Amount or text defined by industry standards Reso 720a para 13
Currency, coded	6345	an..3	an..3	C	1	- -	ISO currency code
Place/location identification	3225	an..25	- -	C	2	- -	

Examples:

1. Ticket/document amount is $0.00 due to an award certificate.

   MON+T:AWARD'

2. Ticket/document amount is 297.50 EUR.

   MON+T:297.50:EUR’

5.14 MSG: MESSAGE ACTION DETAILS (PNRGOV), (ACKRES)

Function: To specify the message type and business function.

Push PNR Data to States - PNRGOV
Acknowledgement Response- ACKRES
PNRGOV Adhoc Request - GOVREQ

Composite/Data Element	No.	Field Type	Comm. Usage	Stat.	Max Rep.	Code Set	Comments
MESSAGE FUNCTION / BUSINESS DETAILS	C302	- -	- -	M*	1	- -	
Business Function, Coded	4025	an..3	an..3	C	1	Yes	A code specifying type of service (air, car, hotel, etc.).
Message Function, Coded	1225	an..3	an..3	C	1	Yes	Identifies what action is requested or has been performed.
Code List Responsible Agency, Coded	3055	an..3	- -	N/A	1	- -	
Message function, coded	1225	an..3	- -	N/A	20	- -	
RESPONSE TYPE, CODED	4343	an..3	an…3	C	1	Yes	Indicates whether request was processed successfully.

Notes:

1. Business Function, Coded (Element 4025) is only used in the MSG Gr9 of PNRGOV to specify the type of service (car, hotel, train, etc.)
2. If MSG is used at Level 0 of PNRGOV or ACKRES, 4025 is not needed
3. Data element 4343 is M* if the MSG is used in the ACKRES message.
4. Data element 4343 is N/A if the MSG is used in the PNRGOV and GOVREQ messages.

Examples:

1. To specify that the TVL is for a hotel segment.

   MSG+8'
2. Push PNR data to States

   MSG+:22’
3. To identify a change PNRGOV message

   MSG+:141’

5.15 ORG: ORIGINATOR OF REQUEST DETAILS (PNRGOV)

Function: To specify the point of sale details.

5.15.1 ORG: Push PNR Data to States - PNRGOV

Composite/Data Element	No.	Field Type	Comm. Usage	Stat.	Max Rep.	Code Set	Comments
SYSTEM DETAILS	C336	- -	- -	M*	1	- -	
Company Identification	9906	an..35	an..3	M*	1	Yes	2-3 character airline/CRS code, or bilaterally agreed code, of the system that delivers the message.
Place/Location identification	3225	an..25	a3..5	C	1	Yes	3 character ATA/IATA airport/city code of the delivering system/ originator of the request.
Place/Location Name	3224	an..17	- -	N/A	1	- -	
ORIGINATOR IDENTIFICATION DETAILS	C300	- -	- -	C	1	- -	
Travel Agent Identification Details	9900	n..9	n8	C	1	- -	ATA/IATA travel agency ID number or pseudo IATA travel agency number.
In-House Identification	9902	an..9	an..9	C	1	- -	Identification code assigned to an office/agency by the reservation system. May be a pseudo city or city and office number.
In-House identification	9902	an..9	an..9	C	1	- -	Identification code that is related to a system key. Access security/entry key into actioning system.
In-House identification	9902	an..9	- -	N/A	1	- -	
LOCATION	C328	- -	- -	C	1	- -	
Place/Location Identification	3225	an..25	a3..5	M*	1	Yes	A 3 character ATA/IATA airport/city code from where the agent initiates the request.
Place/Location Name	3224	an..17	- -	N/A	1	- -	
SYSTEM DETAILS	C336	- -	- -	C	1	- -	
Company Identification	9906	an..35	an..3	C	1	Yes	2-3 character airline/CRS code, or bilaterally agreed code, of the system that originates the message, when different from the delivering system.
Place/Location Identification	3225	an..25	a3..5	C	1	Yes	3 character ATA/IATA airport/city code of the system that originates the message.
Place/Location name	3224	an..17	- -	N/A	1	- -	
ORIGINATOR TYPE CODE	9972	an1	an1	C	1	Yes	One character code for airline agent, travel agent, etc.
ORIGINATOR DETAILS	C354	- -	- -	C	1	- -	
Country, Coded	3207	an..3	an..3	C	1	Yes	ISO country code of the agent.
Currency, Coded	6345	an..3	an..3	C	1	Yes	ISO currency code for currency of originator country.
Language, Coded	3453	an..3	an..3	C	1	Yes	ISO code of language.
ORIGINATOR'S AUTHORITY REQUEST CODE	9904	an..9	an..9	C	1	- -	A reference number/ authority code assigned to the requester as in an agent's initials or logon.

COMMUNICATION NUMBER	3148	an..25	an..6	C	1	- -	LNIATA where LN=line and IA=interchange address and TA=terminal address.
PARTY ID IDENTIFICATION	3039	an..17	an..17	C	1	- -	Group identification such as network id.

Notes:

1. The ORG at level 0 is the sender of the data.
2. The ORG in GR.1 at level 2 is the originator of the booking. For “update” pushes when the push flight/date is cancelled from a PNR or the complete PNR is cancelled or not found, the ORG is sent as an empty segment, i.e., does not contain data.
3. The ORG in GR.6 at level4 is the agent id who checked in the passenger for this flight segment.

Examples:

1. The originator of the message is American Airlines agent in Dallas

   ORG+AA:DFW'

2. The originator of the booking is an LH agent located in Amsterdam hosted on Amadeus.

   ORG+1A:MUC+12345678:111111+AMS+LH+A+NL:NLG:NL+0001AASU’

3. The originator of the booking is an Amadeus travel agent request.

   ORG+1A:NCE+12345678:DDGS+++T'

4. Origination details for a Worldspan travel agent request.

   ORG+1P:HDQ+98567420:IPSU+ATL++T+US:USD+GS'

5. For a cancelled PNR in an “update” push

   ORG’

5.15.1 ORG: PNRGOV Adhoc Request - GOVREQ

Composite/Data Element	No.	Field Type	Comm. Usage	Stat.	Max Rep.	Code Set	Comments
SYSTEM DETAILS	C336	- -	- -	- -	1	- -	
Company Identification	9906	an..35	- -	- -	1	- -	
Place/Location identification	3225	an..25	- -	N/A	1	- -	
Place/Location Name	3224	an..17	- -	N/A	1	- -	
ORIGINATOR IDENTIFICATION DETAILS	C300	- -	- -	N/A	1	- -	
Travel Agent Identification Details	9900	n..9	- -	N/A	1	- -	.
In-House Identification	9902	an..9	- -	N/A	1	- -	
In-House identification	9902	an..9	- -	N/A	1	- -	
In-House identification	9902	an..9	- -	N/A	1	- -	
LOCATION	C328	- -	- -	N/A	1	- -	
Place/Location Identification	3225	an..25	- -	N/A	1	- -	
Place/Location Name	3224	an..17	- -	N/A	1	- -	
SYSTEM DETAILS	C336	- -	- -	N/A	1	- -	
Company Identification	9906	an..35	- -	N/A	1	- -	
Place/Location Identification	3225	an..25	- -	N/A	1	- -	
Place/Location name	3224	an..17	- -	N/A	1	- -	
ORIGINATOR TYPE CODE	9972	an1	- -	N/A	1	- -	
ORIGINATOR DETAILS	C354	- -	- -	M*	1	- -	
Country, Coded	3207	an..3	an..3	M*	1	Yes	ISO country code of the State making the adhoc request for PNRGOV of a specific flight/date..
Currency, Coded	6345	an..3	- -	N/A	1	- -	
Language, Coded	3453	an..3	- -	N/A	1	- -	
ORIGINATOR'S AUTHORITY REQUEST CODE	9904	an..9	- -	N/A	1	- -	
COMMUNICATION NUMBER	3148	an..25	- -	N/A	1	- -	
PARTY ID IDENTIFICATION	3039	an..17	- -	N/A	1	- -	

Examples:

1. The originator of the message is The Australian government.

   ORG++++++AU'

5.16 PTK: PRICING/TICKETING DETAILS (PNRGOV)

Function: To specify pricing/ticketing details.

Push PNR Data to States - PNRGOV

Composite/Data Element	No.	Field Type	Comm. Usage	Stat.	Max Rep.	Code Set	Comments
PRICING / TICKET-ING INFORMATION	C664	- -	- -	C	1	- -	
Price type qualifier	5387	an..3	an..3	C	1	Yes	Ticketing mode indicator
Price type qualifier	5387	an..3	an..3	C	1	Yes	International or domestic sales indicator
Price type qualifier	5387	an..3	an..3	C	1	Yes	Statistical code
Price type qualifier	5387	an..3	an..3	C	1	Yes	Self sale indicator
Price type qualifier	5387	an..3	an..3	C	1	Yes	Net reporting indicator
Price type qualifier	5387	an..3	an..3	C	1	Yes	Tax on commission indicator
Price type qualifier	5387	an..3	an..3	C	1	Yes	Non-endorsable indicator
Price type qualifier	5387	an..3	an..3	C	1	Yes	Non-refundable indicator
Price type qualifier	5387	an..3	an..3	C	1	Yes	Penalty restriction indicator
Price type qualifier	5387	an..3	- -	N/A	1	- -	
Price type qualifier	5387	an..3	- -	N/A	1	- -	
Price type qualifier	5387	an..3	- -	N/A	1	- -	
Price type qualifier	5387	an..3	an..3	C	1	Yes	Non-interlineable indicator
Price type qualifier	5387	an..3	an..3	C	1	Yes	Non-commissionable indicator
Price type qualifier	5387	an..3	- -	N/A	1	- -	
Price type qualifier	5387	an..3	an..3	C	1	Yes	Non-reissuable/non-exchangeable indicator
Price type qualifier	5387	an..3	an..3	C	1	Yes	Carrier fee reporting indicator
Price type qualifier	5387	an..3	an..3	C	1	Yes	Refund calculation indicator
Price type qualifier	5387	an..3	- -	N/A	1	- -	
Price type qualifier	5387	an..3	- -	N/A	11	- -	
PRICE/TARIFF TYPE, CODED	5379	an..3	- -	N/A	1	- -	
PRODUCT DATE/TIME	C310	- -	- -	C	1	- -	
First date	9916	an..35	n6	C	1	- -	Ticketing purchase deadline date. (ddmmyy)
First time	9918	n..4	n4	C	1	- -	Ticketing purchase deadline time. (hhmm)
Second date	9920	an..35	- -	N/A	1	- -	
Second time	9922	n..4	- -	N/A	1	- -	
Date variation	9954	n1	- -	N/A	1	- -	
COMPANY IDENTIFICATION	C306	- -	- -	C	1	- -	
Company identification	9906	an..35	an..3	M	1	Yes	Validating carrier airline code
Company identification	9906	an..35	an..3	C	1	Yes	Ticketing system code
Company identification	9906	an..35	- -	N/A	1	- -	
COMPANY IDENTIFICATION NUMBERS	C665	- -	- -	C	1	- -	
Company identification number	9996	n..15	n3	M	1	- -	Validating carrier accounting code
Company identification number	9996	n..15	n3	C	1	- -	System provider accounting code
LOCATION DETAILS	C666	- -	- -	C	2	- -	
Place/location identification	3225	an..25	a3..5	C	1	- -	Sales/ticketing location city code
Country, coded	3207	an..3	an..3	C	1	Yes	Sales/ticketing location country code
IDENTITY NUMBER	7402	an..35	an..35	C	1	- -	In house fare type/corporate contract number

MONETARY AMOUNT	5004	n..18	- -	- -	N/A	- -	

Example:

1. The pricing/ticketing details: the ticket is non-refundable, the ticketing deadline date and time are 10 pm on 6/15/10, the validating carrier is DL and the sales/ticketing location city code is ATL.
   PTK+NR++150610:2200+DL+006+ATL'

5.17 RCI: RESERVATION CONTROL INFORMATION (PNRGOV)

Function: To specify a reference to a reservation.

Push PNR Data to States – PNRGOV
PNRGOV Adhoc Request - GOVREQ

Composite/Data Element	No.	Field Type	Comm. Usage	Stat.	Max Rep.	Code Set	Comments
RESERVATION CONTROL INFORMATION	C330	- -	- -	M*	9	- -	
Company Identification	9906	an..35	an..3	M*	1	Yes	2-3 character of airline/CRS code of the following record reference (Reservation Control Number)
Reservation Control Number	9956	an..20	an..20	M*	1	- -	Reference to a record
Reservation Control Type	9958	an1	an1	C	1	Yes	Code identifying type of record reference: record locator number, confirmation number, etc.
First Date	9916	an..35	n6	C	1	- -	Date record was created (ddmmyy).
Time	9994	n..9	n4..6	C	1	- -	Time (GMT) record was created, common usage is to minute or second, not millisecond (hhmmss[msmsms]).

Notes:

1. The composite C330 will appear at least once and may be repeated up to eight more times.

2. In case the data is coming from a DCS or ground handling system which does not have access to the reservation system's Record Locator, the following information will be contained in composite C330:
   - 9906 - the operating carrier code
   - 9956 - the locator assigned by DCS in 9956
   - 9958 – a code specifying that the RCI contains a "DCS Reference"

3. The operating carrier's record locator should be included in the RCI if available

Examples:

1. SAS passenger record reference.

   RCI+SK:12DEF'

2. Galileo and SAS record references.

   RCI+SK:123EF+1G:345ABC'

3. Delta is the operating carrier and the PNR was created on 24 February 2010 at 2230 GMT.

   RCI+DL:ABC456789::240210:2230'

4. CX is the operating carrier and no PNR was received from the reservation system at a station handled by a ground handler; therefore the CX reservation PNR locator is not available and "DCS reference" is the Reservation Control Type.

   RCI+CX:89QM3LABML:C'

5.18 REF: REFERENCE INFORMATION (PNRGOV)

Function: To specify an association between references given to travellers, to products, to services.

Push PNR Data to States - PNRGOV

Composite/Data Element	**No.**	**Field Type**	**Comm. Usage**	**Stat.**	**Max Rep.**	**Code Set**	**Comments**
REFERENCING DETAILS	C653	- -	- -	C	99	-	
Reference Qualifier	1153	an..3	- -	N/A	1	- -	
Reference Number	1154	an..35	an..25	C	1	-	Unique passenger identifier assigned for communications with one or more States

Example:

1. The unique passenger reference identifier is 4928506894.

   REF+:4928506894'

5.19 RPI: RELATED PRODUCT INFORMATION (PNRGOV)

Function: To indicate quantity and action required in relation to a product.

Push PNR Data to States - PNRGOV

Composite/Data Element	**No.**	**Field Type**	**Comm. Usage**	**Stat.**	**Max Rep.**	**Code Set**	**Comments**
QUANTITY	6060	n..15	n..3	C	1	- -	Number of passengers associated with the TVL segment.
STATUS, CODED	4405	an..3	an..3	C	10	Yes	ATA/IATA action/advice/status code for this TVL segment.

Example:

1. Flight booking status is holds confirmed for 3 passengers.

   RPI+3+HK'

5.20 SAC: SOURCE AND ACTION INFORMATION (PNRGOV)

Function: To specify information concerning the source and action to be taken.

Push PNR Data to States - PNRGOV

Composite/Data Element	No.	Field Type	Comm. Usage	Stat.	Max Rep.	Code Set	Comments
STATUS INDICATOR, CODED	1245	an..3	- -	N/A	1	- -	
PLACE/LOCATION IDENTIFICATION	3225	an..25	- -	N/A	1	- -	
STATUS, CODED	4405	an..3	an..3	M*	1	Yes	Specifies the status (action) taken on the history item, such as add, cancel, etc.

Notes:

1. Used in conjunction with other segments where the item was actioned. Eg Name Change, flight etc
2. Flown segments are to be included in history.

Examples:

1. The history line contains a cancelled item

   SAC+++X'
2. The history line contains an added item

   SAC+++A’

5.21 SRC: SEGMENT REPETITION CONTROL (PNRGOV)

Function: To indicate the number of segment group repetitions.

Push PNR Data to States - PNRGOV

Composite/Data Element	No.	Field Type	Comm. Usage	Stat.	Max Rep.	Code Set	Comments
SEGMENT REPETITION CONTROL DETAILS	C678	- -	- -	N/A	9	- -	
Quantity	6060	n..15	--	N/A	1	- -	
Number of Units	6350	n..15	- -	N/A	1	- -	
Total number of items	7240	n..15	--	N/A	1	- -	

Note:

1. Used as trigger segment for PNRGOV GR.1 and will repeat for each PNR in the message.

Example:

1. This trigger segment is sent as an empty segment.

   SRC'

5.22 SSD: SEAT SELECTION DETAILS (PNRGOV)

Function: To specify details concerning seat selection and the associated security and processing information.

Push PNR Data to States - PNRGOV

Composite/Data Element	No.	Field Type	Comm. Usage	Stat.	Max Rep.	Code Set	Comments
SPECIFIC SEAT DETAILS	C679	- -	- -	C	1	- -	
Specific seat	9809	an..4	an..4	C	99	- -	The seat number that the passenger has been assigned.
NO SMOKING INDICATOR	9807	a1	- -	N/A	1	- -	
SEAT CHARACTERISTIC DETAILS	C680	- -	C	N/A	1	- -	
Seat characteristics	9825	an..2	--	N/A	99	- -	
SEAT RANGE DETAILS	C681	- -	C	N/A	1	- -	
Seat row number	9830	n..3	--	N/A	1	- -	
Range maximum	6152	n..18	- -	N/A	1	- -	
Seat column	9831	an1	- -	N/A	20	- -	
CABIN CLASS DESIGNATOR	9854	a1	a1	C	1		Used to specify the cabin class
CABIN CLASS OF SERVICE	9873	n1	- -	N/A	1	- -	
FREE TEXT	4440	an..70	- -	N/A	1	- -	
PLACE/LOCATION IDENTIFICATION	3225	an..25	- -	N/A	1	- -	
PLACE/LOCATION IDENTIFICATION	3225	an..25	- -	N/A	1	- -	
PROCESSING INDICATOR	7365	an..3	- -	N/A	1	- -	
SECURITY IDENTIFICATION DETAILS	C682	- -	--	N/A	1	- -	
Security identification	9751	an..5	- -	N/A	2	- -	
PROCESSING INDICATOR	7365	an..3	- -	N/A	1	- -	
SPECIFIC SEAT PURPOSE	C683	- -	- -	N/A	99	- -	
Item characteristic	7081	an..3	- -	N/A	1	- -	
Specific seat	9809	an..4	- -	N/A	1	- -	

Note:

1. 9854 uses individual airlines cabin class designator and not a codeset

Example:

1. The passenger has been assigned seat 24A in coach.

   SSD+24A++++Y’

5.23 SSR: SPECIAL REQUIREMENTS DETAILS (PNRGOV)

Function: To specify special requests or services information relating to a traveller.

Push PNR Data to States - PNRGOV

Composite/Data Element	No.	Field Type	Comm. Usage	Stat.	Max Rep.	Code Set	Comments
SPECIAL REQUIREMENT TYPE DETAILS	C334	- -	- -	M	1	- -	
Special Requirement Type	9962	an..4	an..4	M	1	Yes	Specifies the type of special request (seat, unaccompanied minor, boarding pass, etc.).
Status, coded	4405	an..3	an..3-	C	1	Yes-	Status or action for this SSR, e.g. HK, NN
Quantity	6060	n..15	n..3	C	1	- -	Number of services requested or processed.
Company Identification	9906	an..35	an..3	C	1	Yes	2-3 character airline/CRS code identifying system to which special request is directed.
Processing Indicator	7365	an..3	- -	N/A	1	- -	
Processing Indicator	7365	an..3	- -	N/A	1	- -	
Place/Location Identification	3225	an..25	a3..5	C	1	Yes	Board city of segment to which special service request applies.
Place/Location Identification	3225	an..25	a3..5	C	1	Yes	Off city of segment to which special service request applies.
Free Text	4440	an..70	an..70	C	99	- -	Literal text related to the special service request.
SPECIAL REQUIREMENT DATA DETAILS	C332	- -	- -	C	999	- -	
Special Requirement Data	9960	an..4	an..4	C	1	- -	Identifies specific information (age of unaccompanied minor, seat number, etc.).
Measure Unit Qualifier	6411	an..3	an..3	C	1	Yes	Qualifies 9960 (i.e., years).
Traveller Reference Number	9944	an..10	n..3	C	1	- -	Specifies for which traveller in the TIF segment the special service applies.
Seat Characteristic, coded	9825	an..2	an..2	C	5	Yes	Characteristic of a seat specified in 9960, or for a generic seat assignment (not associated to a particular seat).

Notes:

1. SSR’s in GR.1 apply to all flights and may apply to all passengers or may apply to specific passenger based on the traveler reference number in SSR/9944 and TIF/9944.
2. SSR’s in GR.2 apply to the specific passenger.
3. SSR’s in GR.5 (per TVL) apply to a specific flight and may apply to all passengers or may apply to a specific passenger based on the traveler reference number in SSR/9944 and TIF/9944.
4. The Traveler Reference Number (9944) in the SSR segment in Gr.1 or Gr. 5 may be used to specify for which passenger this SSR applies. This is a reference number assigned by the sending system and should contain the same reference number as that found in the Traveler Reference number in the TIF in Gr.2.

Examples:

1. One passenger is an SSR type unaccompanied minor.

   SSR+UMNR'

2. Passenger number 2 has requested to transport a bike on a DL flight.

SSR+BIKE:HK:1:DL+::2’

3. Passenger has been assigned seat 53C on the AA flight from AMS to JFK.

   SSR+SEAT:HK:1:AA:::AMS:JFK+53C::2:N’

4. DOCS information for a passenger on KL.

   SSR+DOCS:HK:1:KL::::://///05AUG70/F//STRIND/BENITA+::2’

5. Other information about passenger one.

   SSR+OTHS:HK::AF:::::CORP//***CORPORATE PSGR***+::1'

6. A passenger by the name of Mr. John Meeks supplies a United States Redress number for his PNR:
   a. For those systems using automated format:
   SSR+DOCO:HK:1:AA:::JFK:LAX:0001Y28JUN//R/1234567890123///US

   b. For those systems using non-automated format:
   SSR+DOCO:HK:1:AA:::::://R/1234567890123///US

7. Passenger has been assigned seat 22C on the PY flight from AUA to PBM.

   SSR+SEAT:HK:1:PY:::AUA:PBM NOTICKET/TOM:+22C’

8. Passenger is an infant traveling with an adult on PY flight from PBM to MIA and the date of birth is 12Jul09.

   SSR+INFT:HK:1:PY:::PBM:MIA:INFANT/BABY 12JUL09’

9. A bassinet has been confirmed for the PY flight from MIA to PBM.

   SSR+BSCT:HK:1:PY:::MIA:PBM’

10. Passenger has requested a generic seat on the AA flight from DCA to MIA.

    SSR+NSSA:NN:1:AA:::DCA:MIA:MADDOX/MOLLY’

11. Passenger traveling with a British passport and 1st and 2nd given names in separate fields:

    SSR+DOCS:HK::DL:::::/P/GBR/123456789/GBR/12JUL64/M/23AUG19/SMITHJR/JONATHON/ROBERT’

12. Passenger traveling with a British passport and 1st and 2nd given names in same field:

    SSR+DOCS:HK::DL:::::/P/GBR/987654321/GBR/12JUL15/M/15JAN13/COOPER/GARYWILLIAM’

13. Passenger traveling with a British passport and 1st and 2nd given names in same field:

    SSR+DOCS:HK::DL:::::/P/GBR/123456789/GBR/12JUL12/M/23AUG15/WAYNE/JOHNALVA’

5.24 TBD: TRAVELER BAGGAGE DETAILS/Electronic Ticketing (PNRGOV)

Function: To specify the baggage details, including number of bags and serial numbers.

Push PNR Data to States - PNRGOV

Composite/Data Element	No.	Field Type	Comm. Usage	Stat.	Max Rep.	Code Set	Comments
STATUS, CODED	4405	an..3	- -	N/A	1	- -	
BAGGAGE DETAILS	C675	- -	- -	C	2	- -	Checked baggage information
Quantity	6060	n..15	n..3	C	1	- -	Number of pieces
Measurement and value	6314	n..18	n..4	C	1		Weight of checked baggage
Allowance or charge qualifier	5463	an..3	an..3	C	1	Yes	Kilograms or pounds
Measure unit qualifier	6411	an..3	- -	N/A	1	- -	
Processing indicator, coded	7365	an..3	- -	N/A	1	- -	
BAGGAGE REFERENCE DETAILS	C686	- -	- -	C	1	- -	
Processing indicator, coded	7365	an..3	a2	C	1	Yes	Pooled checked bag indicator
Identify number	7402	an..35	an..14	C	1	- -	Baggage pool reference
BAGTAG DETAILS	C358	- -	- -	C	99	- -	
Company identification	9906	an..35	an..3	C	1	- -	Airline designator
Item number	7140	an..35	n..10	M*	1	- -	Bag license plate
Total number of items	7240	n..15	n..3	C	1	- -	Number of consecutive tags serial numbers
Place/location identifier	3225	an..25	a..3	C	1	- -	Place of destination
Company identification number	9996	n..15	n3	C	1	- -	Bag Tag Issuer’s Code (numeric code) as contained in the IATA Airline Coding Directory.
Data indicator	9988	n..2	n1	C	1	Yes	To specify if online or interline
Item characteristic, coded	7081	an..3	a2	C	1	Yes	Indicates manual, auto or limited release bag tag
Special service requirement type	9962	an..4	- -	N/A	1	- -	
Measurement value	6314	n..18	- -	N/A	1	- -	
Measure unit qualifier	6411	an..3	- -	N/A	1	- -	
Free text	4440	an..70	- -	N/A	1	- -	

Note:

1. This segment is for the checked in baggage and not for excess bag details

Examples:

1. Bag pool members with Head of Pool ticket.
2. TBD+++MP:0741234123456’3 bags, weight 84 kilos, Head of Pool, tags 4074902824, 3 in sequence to MSP.
3. TBD++3:84:700++HP+KL:4074902824:3:MSP’Total 5 bags, weight 155 pounds, 2 checked to MSP, 3 short checked to JFK

   TBD++5:155:701+++KL: 8074902824:2:MSP+ KL: 8074902826:3:JFK’
4. Total 2 bags, weight 20 kilos, head of pool, 2 bags in sequence to CPH with the carrier code of the airline issuing the bag tags.

   TBD++2:20:700++HP:5+LH: 3020523456:2:CPH:220’
5. 2 bags, tag QF111111 to Sydney

   TBD++2+++QF: 0081111111:2:SYD’
6. 1 bag, no weight provided

```
TBD++1+++UA:4016722105:1:DOH
```

5.25 TIF: TRAVELLER INFORMATION (PNRGOV)

Function: To specify a traveller(s) and personal details relating to the traveller(s).

Push PNR Data to States - PNRGOV

Composite/Data Element	No.	Field Type	Comm. Usage	Stat.	Max Rep.	Code Set	Comments
TRAVELLER SURNAME INFORMATION	C322	- -	- -	M	1	- -	
Traveller Surname	9936	an..70	a..70	M	1	- -	Specifies passenger surname.
Number of Units Qualifier	6353	an..3	an..3	C	1	Yes	Indicates name qualifier, i.e. group name and same family name, etc.
Quantity	6060	n..15	- -	N/A	1	- -	
Status, coded	4405	an..3	- -	N/A	1	- -	
TRAVELLER DETAILS	C324	- -	- -	C	99	- -	
Traveller Given Name	9942	an..70	a..70	C	1	- -	Specifies passenger given name and title.
Number of Units Qualifier	6353	an..3	an..3	C	1	Yes	Specifies passenger type (adult, frequent traveller, infant, etc.).
Traveller Reference Number	9944	an..10	an..10	C	1	- -	Direct reference of passenger assigned by requesting system. Used as a cross reference between data segments. In GR2 must be unique per passenger within the PNR.
Traveller Accompanied by Infant Indicator	9946	an1	an1	C	1	Yes	Adult passenger is accompanied by an infant without a seat.
Other names	9754	an..70	- -	C	2	- -	

Notes:

1. Only one surname and given name should be sent in one occurrence of the TIF even if there are multiple names for a surname in the PNR.
2. The Traveller Reference Number (9944) is assigned by the sending system and this number in Gr.2 may be used to cross reference an SSR in Gr.1 or Gr.5 or a TRI in Gr.7.

Examples:

1. Passenger Jones/John Mr is an adult.

   TIF+JONES+JOHNMR:A'

2. Passenger has a single letter family name – Miss Moan Y – single letter is doubled where MoanMiss was considered the given name. This rule is as defined in AIRIMP rules and its examples.

   TIF+YY+MOANMISS:A’

3. Adult passenger has a single letter family name – Miss Tuyetmai Van A – all given names are combined with the single letter surname where Miss was considered the given name. This rule is as defined in AIRIMP rules and its examples.

   TIF+ATUYETMAIVAN+MISS:A’

4. The PNR is for a group booking with no individual names.

   TIF+SEETHE WORLD:G’

5. Infant no seat Passenger

   TIF+RUITER+MISTY:IN’

5.26 TKT: TICKET NUMBER DETAILS (PNRGOV)

Function: To convey information related to a specific ticket.

Push PNR Data to States - PNRGOV

Composite/Data Element	**No.**	**Field Type**	**Comm. Usage**	**Stat.**	**Max Rep.**	**Code Set**	**Comments**
TICKET NUMBER DETAILS	C667	- -	- -	M	1	- -	
Document/message number	1004	an..35	an..14	C	1	- -	Ticket document number
Document/ message name, coded	1001	an..3	an..3	C	1	Yes	Document type "1" for ticketless
Total number of items	7240	n..15	n..2	C	1	- -	Total number of booklets issued
Data Indicator	9988	an..3	an..3	C	1	Yes	To specify if in connection with ticket number.
Action request/notification, coded	1229	an..3	- -	N/A	1	- -	
Document/message number	1004	an..35	an..14	C	1	- -	In connection with document number may be an EMD
STATUS, CODED	4405	an..3	- -	N/A	1	- -	

Examples:

1. The ticket number for a passenger

   TKT+0062230534212:T'

2. Conjunctive ticket – 2 booklets

   TKT+0271420067693:T:2'

3. A Ticketless passenger

   TKT+:1'

5.27 TRA: Transport Identifier

Function: To specify transport service(s) or to specify transport service(s) which is/are to be updated or cancelled.

Push PNR Data to States - PNRGOV

Composite/Data Element	No.	Field Type	Comm. Usage	Stat.	Max Rep.	Code Set	Comments
COMPANY IDENTIFICATION	C306	- -	- -	M	1	- -	
Company Identification	9906	an..35	an..3	C	1	Yes	A 2-3 character code to specify the operating airline designator code when different from the marketing airline.
Company Identification	9906	an..35	- -	N/A	- -	- -	
Company Identification	9006	an..35	- -	N/A	- -	- -	
PRODUCT IDENTIFICATION DETAILS	C308	- -	- -	C	1	- -	
Production Identification	9908	an..35	an..4	C	1	- -	The operating flight number
Characteristic Identification	7037	an..17	a1	C	1	- -	Operating reservations booking designator
Product Identification Characteristic	9914	an..3	a1	C	1	- -	An operational suffix related to flight number
Item Description Identification	7009	an..7	- -	N/A	- -	- -	

Example:

1. Flight number 123 operated by Delta
   TRA+DL+123:Y”

2. Gr.5 portion of the message

```
TVL+121210:0915::1230+LHR+JFK+DL+324:B'
TRA+KL+8734:B’                    Operating carrier information
RPI+2+HK’
APD+767’
SSR+SEAT:HK:2:DL:::LHR:JFK+15A::1+15B::2’
DAT+2:111210:0915’
TRI++108:::1’
TIF+SMITHJR+JOHNMR:A:1’
SSD+15A++++Y’
TVL+121210:2200::2330+JFK+YVR+DL+330:B'
RPI+2+HK’
APD+767’
SSR+SEAT:HK:2:DL:::JFK:YVR+15E::1+15F::2’
```

5.28 TRI: TRAVELLER REFERENCE INFORMATION (PNRGOV)

Function: To specify information regarding a traveller or traveller account .

Push PNR Data to States - PNRGOV

Composite/Data Element	No.	Field Type	Comm. Usage	Stat.	Max Rep.	Code Set	Comments
REFERENCE QUALIFICATION	C670	- -	- -	N/A	1	- -	
Identity number qualifier	7405	an..3	- -	N/A	1	- -	
Reference Qualifier	1153	an..3	- -	N/A	1	- -	
TRAVELLER IDENTIFICATION	C671	- -	- -	C	999	- -	
Reference Number	1154	an..35	an..35	C	1	- -	The sequence/boarding number for this flight for a passenger.
Reference Qualifier	1153	an..3	- -	N/A	1	- -	
Specific Seat	9809	an..4	- -	N/A	1	- -	
Traveller Reference Number	9944	an..10	n..3	C	1	- -	Used to indicate which passenger is being checked in and refers to the 9944 assigned in the TIF in GR2 level 2.

Notes:

1. The Traveler Reference Number (9944) in the TRI segment in Gr.7 may be used to specify for which passenger the check-in information applies so that the TIF in this group does not need to be sent. This is a reference number assigned by the sending system and should contain the same reference number as that found in the Traveler Reference number in the TIF in Gr.2.
2. Each occurrence of the TRI handles only one passenger (i.e. one surname and one given name) at a time, thus the Composite C671 does not repeat

Example:

1. The sequence number for this passenger is 108.

   TRI++108'

2. The sequence number for passenger, which has reference number 4, is 220.

   TRI++220:::4'

3. The sequence number for passenger, which has reference number 10, is JFK-058.

   TRI++JFK-058:::10'

4. No sequence number for the passenger, which has reference number 11.

   TRI++:::11'

5.29 TVL: TRAVEL PRODUCT INFORMATION (PNRGOV)

Function: To specify details related to a product.

5.28.1 Flight Details for Passenger data sent

TVL at Level 0

Push PNR Data to States - PNRGOV
PNRGOV Adhoc Request - GOVREQ

Composite/Data Element	No.	Field Type	Comm. Usage	Stat.	Max Rep.	Code Set	Comments
PRODUCT DATE/TIME	C310	- -	- -	M*	1	- -	
First Date	9916	an..35	n6	M*	1	- -	Departure date (ddmmyy)
First Time	9918	n..4	n4	C	1	- -	Departure time (hhmm)
Second Date	9920	an..35	n6	C	1	- -	Arrival date (ddmmyy)
Second Time	9922	n..4	n4	C	1	- -	Arrival time (hhmm)
Date Variation	9954	n1	n1	C	1	- -	Variance between departure and arrival date.
LOCATION	C328	- -	- -	M*	1	- -	
Place/Location Identification	3225	an..25	a3..5	M*	1	Yes	A 3 character code to specify the last IATA airport / city code of departure prior to crossing the border
Place/Location Name	3224	an..17	- -	N/A	1	- -	
LOCATION	C328	- -	- -	M*	1	- -	
Place/Location	3225	an..25	a3..5	M*	1	Yes	A 3 character code to specify the first IATA airport / city code of arrival after crossing the border.
Place/Location Name	3224	an..17	- -	N/A	1	- -	
COMPANY IDENTIFICATION	C306	- -	- -	M*	1	- -	
Company Identification	9906	an..35	an..3	M*	1	Yes	A 2-3 character code to specify the operating airline designator code.
Company Identification	9906	an..35	an..3	N/A	1	- -	
Company Identification	9906	an..35	- -	N/A	1	- -	
PRODUCT IDENTIFICATION DETAILS	C308	- -	- -	M*	1	- -	
Product Identification	9908	an..35	n..4	M	1	- -	Flight number
Characteristic Identification	7037	an..17	- -	N/A	1	- -	
Product Identification Characteristic	9914	an..3	a1	C	1	- -	An operational suffix related to flight number.
Item Description Identification	7009	an..7	- -	N/A	3	- -	
PRODUCT TYPE DETAILS	C309	- -	- -	N/A	1	- -	
Sequence Number	1050	an..6	- -	N/A	9	- -	
LINE ITEM NUMBER	1082	n..6	- -	N/A	1	- -	
PROCESSING INDICATOR, CODED	7365	an..3	- -	N/A	1	- -	
MARRIAGE CONTROL DETAILS	C311	- -	- -	N/A	99	- -	
Relation, coded	5479	an..3	- -	N/A	1	- -	
Group number	9995	n..10	- -	N/A	1	- -	
Line item number	1082	n..6	- -	N/A	1	- -	
Relation, coded	5479	an..3	- -	N/A	1	- -	
Company identification	9906	an..35	- -	N/A	1	- -	

Note:

1. Dates and times in the TVL are in Local Time.
2. Departure and arrival points of the transborder segment for a given country are the ones of the leg which makes the segment eligible for push to a given country.

Examples:

1. The passenger information being sent is for Delta flight 10 from ATL to LGW on 30MAR which departs at 5:00 pm.

   TVL+300310:1700+ATL+DFW+DL+10'

2. The passenger information being sent is for Delta flight 9375 from ATL to AMS on 24 FEB which departs at 9:35 pm.

   TVL+240210:2135+ATL+AMS+DL+9375'

3. This example is only concerned with the push to Canada. While the US will also have a push, the US is not demonstrated in this example. CX888 is a multileg flight with the following routing and times,
   HKG 10May 0100 YVR 09May 2030
   YVR 09May 2230 JFK 10May 0420
   The leg eligible for Canada is HKG YVR. The passenger information to push are for CX888 from HKG YVR (terminate YVR Canada) and HKG to JFK (transit YVR Canada). The push will occur at Scheduled Departure Time out of HKG.
   For the flight departing on 10th May at 0100 (Local Time) from HKG and arriving at YVR at 2030 on 09May, the following segment TVL in PNRGOV level 0 will be sent:

   TVL+100512:0100:090512:2030+HKG+YVR+CX+888

5.28.2 Flight Itinerary

TVL in Gr5 at Level 2 and Gr.12 at Level 4

Push PNR Data to States - PNRGOV

Composite/Data Element	No.	Field Type	Comm. Usage	Stat.	Max Rep.	Code Set	Comments
PRODUCT DATE/TIME	C310	- -	- -	C	1	- -	
First Date	9916	an..35	n6	C	1	- -	Departure date (ddmmyy)
First Time	9918	n..4	n4	C	1	- -	Departure time (hhmm)
Second Date	9920	an..35	n6	C	1	- -	Arrival date (ddmmyy)
Second Time	9922	n..4	n4	C	1	- -	Arrival time (hhmm)
Date Variation	9954	n1	n1	C	1	- -	Variance between departure and arrival date.
LOCATION	C328	- -	- -	C	1	- -	
Place/Location Identification	3225	an..25	a3..5	M*	1	Yes	A 3 character code to specify place of departure.
Place/Location Name	3224	an..17	- -	N/A	1	- -	
LOCATION	C328	- -	- -	C	1	- -	
Place/Location	3225	an..25	a3..5	M*	1	Yes	A 3 character code to specify place of arrival.
Place/Location Name	3224	an..17	- -	N/A	1	- -	
COMPANY IDENTIFICATION	C306	- -	- -	C	1	- -	
Company Identification	9906	an..35	an..3	M*	1	Yes	A 2-3 character code to specify the marketing airline designator code.
Company Identification	9906	an..35	an..3	C	1	Yes	A 2-3 character code to specify the operating airline designator code when different from the marketing airline.
Company Identification	9906	an..35	- -	N/A	1	- -	
PRODUCT IDENTIFICATION DETAILS	C308	- -	- -	M*	1	- -	
Product Identification	9908	an..35	an..4	M	1	- -	Marketing flight number or ARNK or OPEN
Characteristic Identification	7037	an..17	a1	C	1	- -	Marketing reservations booking designator
Product Identification Characteristic	9914	an..3	a1	C	1	- -	An operational suffix related to flight number.
Item Description Identification	7009	an..7	- -	N/A	3	- -	
PRODUCT TYPE DETAILS	C309	- -	- -	N/A	1	- -	
Sequence Number	1050	an..6	- -	N/A	9	- -	
LINE ITEM NUMBER	1082	n..6	- -	N/A	1	- -	
PROCESSING INDICATOR, CODED	7365	an..3	- -	N/A	1	- -	
MARRIAGE CONTROL DETAILS	C311	- -	- -	N/A	99	- -	
Relation, coded	5479	an..3	- -	N/A	1	- -	
Group number	9995	n..10	- -	N/A	1	- -	
Line item number	1082	n..6	- -	N/A	1	- -	
Relation, coded	5479	an..3	- -	N/A	1	- -	
Company identification	9906	an..35	- -	N/A	1	- -	

Notes:

1. Dates and times in the TVL are in Local Time.

2. For OPEN and ARNK segments, the date, place of departure and place of arrival are conditional. For an Airline/ Flight Number / class/ date / segment, the date, place of departure and place of arrival are mandatory.

3. When referring to a codeshare flight, two TVLs are required (one as difined in 5.28.2 for the marketing flight and one providing the operating flight information as defined in 5.28.3). If the marketing and operating carrier/flight are the same, only one TVL is used as defined in 5.28.2.

4. Flown segments are to be included in history.

5. Departure and arrival city/airport codes as contained in the passenger's booked itinerary.

Examples:

1. The flight segment in the passenger's itinerary is Delta flight 10 from ATL to LHR on April 1 which departs at 10:35 p.m. and arrives at noon and the reservation booking designator is K. The operating carrier is KL.

   TVL+010410:2235:020410:1200+ATL+LHR+DL:KL+10:K'

2. An ARNK segment is used to fill a gap in the itinerary.

   TVL+++++ARNK'

3. An OPEN segment is used where the passenger has purchased a ticket between two cities/airports but does not know the flight number or date.

   TVL++LHR+ORD++OPEN'

4. An OPEN segment is used where the passenger has purchased a ticket between two cities/airports and knows the airline on which he will fly but not the flight number or date.

   TVL++LAX+SIN+SQ+OPEN'

5. This example is only concerned with the push to Canada. While the US will also have a push, the US is not demonstrated in this example.
   CX888 is a multileg flight with the following routing and times:
   HKG 10May 0100 YVR 09May 2030
   YVR 09May 2230 JFK 10May 0420
   The leg eligible for Canada is HKG YVR. The passenger information to push are for CX888 from HKG YVR (terminate YVR Canada) and HKG to JFK (transit YVR Canada). The push will occur at Scheduled Departure Time out of HKG.
   For the flight departing on 10th May at 0100 (Local Time) from HKG and arriving at YVR at 2030 on 09May, the following segment TVL in PNRGOV will be sent:

   Level 0 - TVL+100512:0100:090512:2030+HKG+YVR+CX+888

   Grp 5 level 2 for HKG YVR passengers - TVL+100512:0100:090512:2030+HKG+YVR+CX+888

   Grp 5 level 2 for HKG JFK passengers - TVL+100512:0100:100512:0420+HKG+JFK+CX+888

5.28.3 Codeshare information

Second TVL in GR5 at level 2 to send codeshare flight number and RBD.

Push PNR Data to States - PNRGOV

Composite/Data Element	No.	Field Type	Comm. Usage	Stat.	Max Rep.	Code Set	Comments
PRODUCT DATE/TIME	C310	- -	- -	N/A	1	- -	
First Date	9916	an..35	- -	N/A	1	- -	
First Time	9918	n..4	- -	N/A	1	- -	
Second Date	9920	an..35	- -	N/A	1	- -	
Second Time	9922	n..4	- -	N/A	1	- -	
Date Variation	9954	n1	- -	N/A	1	- -	
LOCATION	C328	- -	- -	N/A	1	- -	
Place/Location Identification	3225	an..25	- -	N/A	1	- -	
Place/Location Name	3224	an..17	- -	N/A	1	- -	
LOCATION	C328	- -	- -	N/A	1	- -	
Place/Location	3225	an..25	- -	N/A	1	- -	
Place/Location Name	3224	an..17	- -	N/A	1	- -	
COMPANY IDENTIFICATION	C306	- -	- -	N/A	1	- -	
Company Identification	9906	an..35	- -	N/A	1	- -	
Company Identification	9906	an..35	- -	N/A	1	- -	
Company Identification	9906	an..35	- -	N/A	1	- -	
PRODUCT IDENTIFICATION DETAILS	C308	- -	- -	M*	1	- -	
Product Identification	9908	an..35	an..4	M	1	- -	The operating flight number
Characteristic Identification	7037	an..17	a1	C	1	- -	Operating reservations booking designator
Product Identification Characteristic	9914	an..3	a1	C	1	- -	An operational suffix related to flight number.
Item Description Identification	7009	an..7	- -	N/A	3	- -	
PRODUCT TYPE DETAILS	C309	- -	- -	N/A	1	- -	
Sequence Number	1050	an..6	- -	N/A	9	- -	
LINE ITEM NUMBER	1082	n..6	- -	N/A	1	- -	
PROCESSING INDICATOR, CODED	7365	an..3	- -	N/A	1	- -	
MARRIAGE CONTROL DETAILS	C311	- -	- -	N/A	99	- -	
Relation, coded	5479	an..3	- -	N/A	1	- -	
Group number	9995	n..10	- -	N/A	1	- -	
Line item number	1082	n..6	- -	N/A	1	- -	
Relation, coded	5479	an..3	- -	N/A	1	- -	
Company identification	9906	an..35	- -	N/A	1	- -	

Notes:

1. This TVL is only used in a codeshare situation and provides the code share operating flight number, operational suffix if any and the operating flight RBD.
2. When referring to a codeshare flight, two TVLs are required (one as defined in 5.28.2 for the marketing flight and one providing the operating flight information as defined in 5.28.3). If the marketing and operating carrier/flight are the same, only one TVL is used as defined in 5.28.2.

Examples:

1. The sold as flight (marketing carrier flight) is operated as flight 2345 and the RBD is K. This example only demonstrates the operating information however a preceding TVL would be required for the marketing information

   TVL+++++2345:K'

2. This example contains an illustration of both the operating and the marketing TVLs for a codeshare situation where the marketing carrier is DL and the operating carrier is KL..

   TVL+010410:2235: 020410:1200+ATL+AMS+DL:KL+9362:K'

   TVL+++++972:M'

5.28.4 Non Air Segments

TVL in GR.9 at level 3 is used to carry non-air segments (car, hotel, rail, etc.)

Push PNR Data to States - PNRGOV

Composite/Data Element	No.	Field Type	Comm. Usage	Stat.	Max Rep.	Code Set	Comments
PRODUCT DATE/TIME	C310	- -	- -	M*	1	- -	
First Date	9916	an..35	n6	M*	1	- -	The starting date of the utilization of the service/product, e.g. check-in date, pickup date,
First Time	9918	n..4	n4	C	1	- -	The starting time of the utilization of the service/product, e.g. check-in time, pickup time (hhmm)
Second Date	9920	an..35	n6	C	1	- -	The ending date of the utilization of the service/product, e.g. check-out date, drop-off date.
Second Time	9922	n..4	n4	C	1	- -	The ending time of the utilization of the service/product, e.g. check-out time, drop-off time (hhmm)
Date Variation	9954	n1	- -	N/A	1	- -	
LOCATION	C328	- -	- -	M*	1	- -	
Place/Location Identification	3225	an..25	a3..5	M*	1	Yes	A 3 character code where utilization of the service/product commences, e.g. location of the hotel or rental car company..
Place/Location Name	3224	an..17	an..17-	C	1	- -	May contain the hotel name
LOCATION	C328	- -	- -	C	1	- -	
Place/Location	3225	an..25	a3..5	M*	1	Yes	A 3 character code where utilization of the service/product terminates if different from the first location, e.g. drop-off location
Place/Location Name	3224	an..17	- -	N/A	1	- -	
COMPANY IDENTIFICATION	C306	- -	- -	C	1	- -	
Company Identification	9906	an..35	an..3	M*	1	Yes	Indicates the code of the provider of the service/product, e.g. HH, ZE
Company Identification	9906	an..35	- -	N/A	1	- -	
Company Identification	9906	an..35	- -	N/A	1	- -	
PRODUCT IDENTIFICATION DETAILS	C308	- -	- -	M*	1	- -	
Product Identification	9908	an..35	an..10	M	1	- -	A code identifying the location or other mechanism used by a vendor to offer services/products for sale, e.g. hotel property id
Characteristic Identification	7037	an..17	an..17	C	1	- -	The classes related to the service/product, e.g. hotel room type, car type
Product Identification Characteristic	9914	an..3	- -	N/A	1	- -	
Item Description Identification	7009	an..7	- -	N/A	3	- -	
PRODUCT TYPE DETAILS	C309	- -	- -	N/A	1	- -	
Sequence Number	1050	an..6	- -	N/A	9	- -	
LINE ITEM NUMBER	1082	n..6	- -	N/A	1	- -	
PROCESSING INDICATOR, CODED	7365	an..3	- -	N/A	1	- -	
MARRIAGE CONTROL DETAILS	C311	- -	- -	N/A	99	- -	
Relation, coded	5479	an..3	- -	N/A	1	- -	
Group number	9995	n..10	- -	N/A	1	- -	
Line item number	1082	n..6	- -	N/A	1	- -	

Relation, coded	5479	an..3	- -	N/A	1	- -	
Company identification	9906	an..35	- -	N/A	1	- -	

Examples:

1. Car segment.

   TVL+290110:1050:310110:0900+ATL++ZE+:FCAR’

2. Hotel segment.

   TVL+100910:1600:120910+MCI:HYATT REGENCY CROWN++HY+918W2:ROH’

5.30 TXD: TAX DETAILS (PNRGOV)

Function: To specify all details related to taxes

Push PNR Data to States - PNRGOV

Composite/Data Element	No.	Field Type	Comm. Usage	Stat.	Max Rep.	Code Set	Comments
DUTY/TAX/FEE CATEGORY, CODED	5305	an..3	an..3	C	1	- -	Special tax indicator
TAX DETAILS	C668	- -	- -	C	99	- -	
Duty/Tax/Fee rate	5278	an..17	n..17	C	1	- -	Tax Amount.
Country, coded	3207	an..3	an..3	C	1	Yes	ISO code identifying country.
Currency, coded	6345	an..3	an..3	C	1	Yes	ISO code identifying currency.
Duty/Tax/Fee type, Coded	5153	an..3	an..3	C	1	Yes	Tax designator code to specify individual taxes of a group.
Duty/tax/fee rate	5278	an..17	an..11	C	1		Tax filed amount
Currency, coded	6345	an..3	an..3	C	1	Yes	Tax filed ISO currency code
Duty/Tax/Fee type, Coded	5153	an..3	an..3	C	1	Yes	Tax filed type code
Monetary amount	5004	an..18	an..3	C	1	- -	Filed conversion rate
Monetary function, coded	5007	an..3	an..3	C	2	Yes	Tax qualifier

Notes:

1. The tax code and country code should be in data elements 5153 and 3207 respectively.

Examples:

1. Tax details for departure taxes for Great Britain.

   TXD++5:GB::9'

2. Tax information related to the given fare.

   TXD++6.27::USD'

6 CODE SETS

For all codesets utilized in the PNRGOV message, please refer to the **PADIS EDIFACT AND XML Code set Directory** available on the PADIS Extranet

This document will not contain any codeset breakdown to ensure that all relevant codes available now and in the future are available for use should they be required. This will ensure that no codeset is presented incorrectly in this document.

If additional codes are required, they should be submitted to the PADIS Working Group for approval prior to being submitted to a PADIS Board vote for inclusion in the standards.

7 BUSINESS CASE EXAMPLES

The following business case examples are provided to illustrate the variety of data and potential differences in where specific data is contained in a message based on the system sending the message, where and how data is stored in that system and based on the original source of the information.

Because of the volume of data that would be sent for entire flight, the examples only contain information for one complete PNR with indication that the message is partial data for entire flight.

All examples placed in the Implementation Guide have been reviewed and agreed by the PNRGOV working group

Scenarios – Two Passengers traveling internationally:

A PNRGOV message sent 24 hours prior to departure for Delta flight 324 with routing LHR > JFK > YVR. This flight requires four separate messages to 3 separate governments (UK, US and Canadian). The first message is for DL flight 324 out of London (LHR) and is sent to UK and US. The partial message contains two PNRs with the following characteristics:

PNR 1 – Two Passengers booked and paid by 3rd party, credit card payment. PNR has been split, the full itinerary has had a change in flight, SSR meals and seats for all passengers. Passengers are ticketed and due to a change in the itinerary, the ticket had to be exchanged and repriced. Also included are elite frequent flier, Secure Flight Passenger Data, and hotel. Two bags were paid for fees. Passenger John Smith has checked in at 24 hours prior to departure.

PNR 2 – Two passengers, booked on a round trip by a GDS. The name has been changed.

UNA:+.*	
UNB+IATA:1+DL+??+101209:2100+020A07’	Interchange header segment
UNH+1+PNRGOV:10:1:IA+F6C2C268'	Message header
MSG+:22'	
ORG+DL:ATL+52519950’	
TVL+121210:0915+LHR+JFK+DL+324'	PNR data for DL324/12DEC10 LHR
EQN+2'	Number of PNRs being sent in the message
SRC’	<<< Start of PNR 1 >>>
RCI+DL:MFN4TI'	
SSR+AVML:HK:2:DL’	
DAT+700:061210:1010+710:061210:1200’	
IFT+4:28::DL+THIS PASSENGER IS A VIP’	
IFT+4:28::DL+CTCR 00115555555555’	
ORG+DL:ATL+52519950:LON+++A+GB:GBP+D050517’	Booked by DL call center agent in UK
ADD++702:45 HIGH STREET:SLOUGH:BERKSHIRE::GB:SL1AA:00441753637285’	Phone in free text
EBD+GBP:40.00+4::N’	Total for 4 bags
TIF+SMITHJR+JOHNMR:A:1’	Adult passenger, Mr. John Smith Jr.
FTI+DL:1234567890:::ELITE’	
IFT+4:15:9+LHR DL X/JFK DL YVR GBP/IT END ROE0.618831 XT3.10AY6 8.50YQ3.40+YC4.30XY3.10XA2.80XFATL4.5’	
REF+:38739393AN8739P’	
FAR+N+++++MIL24’	Military Fare
SSR+DOCS:HK::DL::::/P/GBR/123456789/GBR/12JUL64/M/23AUG19/SMITH JR/JONATHON/ROBERT’	
TKT+0062120234533:T:1'	
MON+B:2888.00:GBP+T:2957.94:GBP'	
PTK+NR++061210:1010+DL+006+LON'	
TXD++3.10:::AY6+8.50:::YQ+3.40:::YC+4.30:::XY+3.10:::XA+2.80:::XF'	
DAT+710:061210:1200’	
FOP+CC:::VI:XXXXXXXX1186:0211'	
IFT+4:43+TIMOTHY SIMS+2234 MAIN STREET ATLANTA, GA 30067+770 5632891’	Sponsor
TIF+JONES+WILLIAMMR:A:2’	Adult passenger, Mr. William Jones
FTI+AF:0093789865:::ELITE’	
IFT+4:15:9+ LHR DL X/JFK DL YVR GBP/IT END ROE0.618831 XT3.10AY6 8.50YQ3.40+YC4.30XY3.10XA2.80XFATL4.5’	
REF+:38739393AN8780P’	
FTI+AF:0093789865:::ELITE’	
FAR+A+++++YN324N’	Normal Advance Booking Fare
SSR+DOCS:HK::DL:::://///GBR/12JUL64/M//JONES/WILLIAMNEVELL’	
TKT+0062120234534:T:1'	
MON+B:2888.00:GBP+T:2957.94:GBP'	
PTK+NR++061210:1010+DL+006+LON'	
TXD++3.10:::AY6+8.50:::YQ+3.40:::YC+4.30:::XY+3.10:::XA+2.80:::XF'	
DAT+710:081210:1200’	

FOP+CC:::VI:XXXXXXXX1186:0211'	
IFT+4:43+TIMOTHY SIMS+2234 MAIN STREET ATLANTA, GA 30067+770 5632891’	Sponsor
TVL+121210:0915::1230+LHR+JFK+DL+324:B'	First flight in itinerary
APD+767’	
SSR+SEAT:HK:2:DL:::LHR:JFK+15A::1+15B::2’	Seats for both passengers
DAT+2:111210:0915’	Check-in info starts here
TRI++108:::1’	Boarding/Check-in #108
TIF+SMITHJR+JOHNMR:A:1’	Adult passenger, Mr. John Smith Jr.
SSD+15A++++Y’	Seat and cabin check-in info
TVL+121210:2200::2330+JFK+YVR+DL+330:B'	Second flight in itinerary
RPI+2+HK’	
APD+767’	
SSR+SEAT:HK:2:DL:::JFK:YVR+15E::1+15F::2’	Seats for both passengers
EQN+1’	
RCI+DL:ABCDEF'	
MSG+8’	Hotel segment
TVL+121210:1500:151210+YVR:VANCOUVER ARMS++VN+67576:ROH’	Hotel info
ABI+1+:LHRRR+LON++DL’	Start First History Item
DAT+ZT:071210:1010’	
SAC+++X’	
TVL+101210:0915::1230+LHR+JFK+DL+324:B'	Cancel Flight #1
RPI+2+K’	
SAC+++X’	
SSR+AVML:HK:2:DL’	Cancel AVML for both passengers
SAC+++X’	
SSR+SEAT:HK:2:DL:::LHR:JFK+15A::1+15B::2’	Cancel Seats for both passengers
SAC+++X’	
TVL+101210:2200::2330+JFK+YVR+DL+330:B'	Cancel Flight #2
RPI+2+K’	
SAC+++X’	
SSR+AVML:HK:2:DL’	Cancel AVML for both passengers
SAC+++X’	
SSR+SEAT:HK:2:DL:::JFK:YVR+15E::1+15F::2’	Cancel Seats for both passengers
SAC+++A’	
TVL+121210:0915::1230+LHR+JFK+DL+324:B'	Add flight #1
RPI+2+K’	
SAC+++A’	
SSR+AVML:HK:2:DL’	Add AVML for both passengers
SAC+++A’	
SSR+SEAT:HK:2:DL:::LHR:JFK+15A::1+15B::2’	Add Seats for both passengers
SAC+++A’	
TVL+121210:2200::2330+JFK+YVR+DL+330:B'	Add flight #2
RPI+2+K’	
SAC+++A’	
SSR+AVML:HK:2:DL’	Add AVML for both passengers
SAC+++A’	
SSR+SEAT:HK:2:DL:::JFK:YVR+15E::1+15F::2’	Add Seats for both passengers
SRC’	<<< Start of PNR 2 >>>
RCI+1A:23456'	
DAT+700:061210:1010+710:061210:1200’	
ORG+1A:MUC+12345678:F31+LON++T+GB:GBP+A78987’	
ADD++702:351 LANDSDOWN ROAD:SLOUGH:BERKSHIRE::GB::SL1AA’	Booked by 1A travel agent in UK
EBD+GBP:20.00+2::N’	Total for 2 bags
TIF+WAYNE+JOHNMR:A:1’	Adult passenger, Mr. John Wayne
FTI+DL:1234567893:::ELITE’	
IFT+4:15:9+LHR DL X/JFK DL YVR GBP/IT END ROE0.618831 XT3.10AY6 8.50+YQ3.40YC4.30XY3.10XA2.80XFATL4.5’	
REF+:38739393AN8740P’	
FAR+A+++++YN324N’	Normal advance booking fare
SSR+DOCS:HK::DL:::::/P/GBR/123456789/GBR/12JUL12/M/23AUG15/WAYNE/JOHNALVA’	
TKT+0062120234535:T:1'	
MON+B:2888.00:GBP+T:2957.94:GBP'	
PTK+NR++061210:1010+DL+006+LON'	
TXD++3.10:::AY6+8.50:::YQ+3.40:::YC+4.30:::XY+3.10:::XA+2.80:::XF'	
DAT+710:061210:1200’	
FOP+CC:::VI:XXXXXXXX1186:0211'	
TIF+COOPER+GARYMR:A:2’	Adult passenger, Mr. Gary Cooper
FTI+AF:0093789830:::ELITE’	
IFT+4:15:9+ LHR DL X/JFK DL YVR GBP/IT END ROE0.618831 XT3.10AY6 8.50+YQ3.40YC4.30XY3.10XA2.80XFATL4.5’	
REF+:38739393AN8793P’	
FAR+A+++++YN324N’	Normal Advance Booking Fare
SSR+DOCS:HK::DL:::::/P/GBR/987654321/GBR/12JUL15/M/15JAN13/COOPER/GARYWILLIAM’	
TKT+0062120234536:T:1'	
MON+B:2888.00:GBP+T:2957.94:GBP'	
PTK+NR++061210:1010+DL+006+LON'	
TXD++3.10:::AY6+8.50:::YQ+3.40:::YC+4.30:::XY+3.10:::XA+2.80:::XF'	
DAT+710:061210:1200’	
FOP+CC:::DC:XXXXXXXX3578:0211'	
TVL+121210:0915::1230+LHR+JFK+DL+324:B'	First flight in itinerary
RPI+1+HK’	
APD+767’	
SSR+SEAT:HK:2:DL:::LHR:JFK++17A::1+17B::2’	Seats for both passengers

DAT+2:111210:0915’	Check-in info starts here
TRI++2:::1’	Boarding/Check-in #2
TIF+COOPER+GARYMR:A:2’	Adult passenger, Mr. Gary Cooper
SSD+15A++++Y’	Seat and cabin check-in info
TVL+121210:2200::2330+JFK+YVR+DL+330:B'	Second flight in itinerary
RPI+1+HK’	
APD+767’	
SSR+SEAT:HK:2:DL:::JFK:YVR+17E::1+17F::2’	Seats for both passengers
ABI+1+:LHRRR+LON++DL’	Start First History Item
DAT+ZT:071210:1010’	
SAC+++X’	
TIF+WAYNE+JONMR:A:1’	Cancel Name
SAC+++A’	
TIF+WAYNE+JOHNMR:A:1’	Add Name
UNT+135+1	
UNZ+1+020A07’	

Further Business Case examples are provided in the Appendix B.

8 ADDITIONAL IMPLEMENTATION GUIDELINES

8.1 Types of Push and PNR Cancellations

The control of which type of push is used between a government and a given carrier is defined in the bilateral agreement between that government and that carrier. In these paragraphs, the term cancellation refers to either the pushed flight being cancelled from the PNR itinerary or the entire PNR being cancelled.

8.1.1 Full PNR Push (PNRGOV)

Under this concept, a full PNR Push is used to send all active PNRs to the government each time a push is required from that government. In all cases, PNRs no longer containing the pushed flight segment are omitted from subsequent pushes. For a full push, the MSG on level 0 will contain 22 (Push PNR data to States) in C302/1225.

8.1.2 Update PNR Push (PNRGOV)

Under this concept, the initial push to a given government sends a full PNR Push as defined in paragraph 8.1.1.
Intermediate pushes may contain only those PNRs that have been modified, added to, or removed from the flight since the previous push. The Update push will contain 141 (Update) in MSG C302/1225.

- If a PNR is included in a push, all PNR data is sent.
- For cancellations, only the SRC (empty), the RCI with the record locator information and an empty ORG are included.

Example:

- PNR for passenger APPLE booked 7 days prior to departure
- PNR for passenger PEAR booked 2 months prior to departure
- PNR for passenger BANANA booked 1 month prior to departure
- PNR for passenger MINT booked 36 hours prior to departure.
- PNR for passenger ORANGE booked 2 weeks prior to departure and changed 50 hours and changed 20 hours prior to departure.
- PNR for passenger LIME booked 10 days prior to departure and segment cancelled 18 hours prior to departure.
- PNR for passenger PINEAPPLE booked 12 days prior to departure and PNR cancelled 30 hours prior to departure
- A particular government requires five pushes. The above PNRs will be included as follows:
- 72 hours prior to departure – APPLE, PEAR, BANANA, ORANGE, LIME, PINEAPPLE
- 48 hours prior to departure - ORANGE
- 24 hours prior to departure – MINT, PINEAPPLE (only SRC/RCI/ORG)
- 12 hours prior to departure – ORANGE, LIME (only SRC/RCI/ORG)
- 1 hour prior to departure – No PNRs sent.

For any push in which there are no PNRs, the EQN on level 0 contains a “0” in C523/6353.

8.1.3 Adhoc PNR Push (GOVREQ/PNRGOV)

The Adhoc push is used by bilateral agreement.

- If the Adhoc request is for an entire flight, a full push as defined in 7.1 above is sent. The MSG on level 0 of the GOVREQ message will contain 43 (Flight report) in C302/1225. The MSG on level 0 of the PNRGOV message will contain 22 (PNR Data to Government) in C302/1225.

- If the request is for a specific PNR locator, the MSG on level 0 of the GOVREQ message will contain 77 (Record locator request) in C302/1225.

- All PNR data is sent for an active and relevant PNR. The MSG on level 0 of the PNRGOV message will contain 22 (PNR Data to Government) in C302/1225.

- If the PNR is not found or if the PNR itinerary is not relevant to the government (no active itinerary to or from the requesting country), then ACKRES is returned with the appropriate ERC error code.

8.2 Error Handling

Acknowledgement of the receipt and/or processing of a PNRGOV or GOVREQ message by the destination application, if bilaterally agreed, should be accomplished using a functional message whenever possible. The functional message may be an ACKRES in response to a PNRGOV, or may be either an ACKRES or PNRGOV in response to a GOVREQ as is explained in section 2 of this document. However, there may be business cases in which the PNRGOV or GOVREQ message is not able to reach the destination application in a timely manner or at all. In these cases, it is appropriate to use a CONTRL message to provide automated advice to the sender of that message regarding the status of processing.

The following table briefly summarizes the recommendations for acknowledgement of receipt and/or processing of a message based on the standard PADIS interactive process. For more background and detailed recommendations, please see the document entitled **PADIS EDIFACT Message Processing - Background for PNRGOV Users**.

Message	Use Case	Recommended Response Message
PNRGOV	Successful Receipt & Processing	ACKRES
PNRGOV or GOVREQ	Successful Receipt, Functional Data Errors	ACKRES with ERC
PNRGOV or GOVREQ	Received containing syntax errors rendering it unable to parse	CONTRL
PNRGOV or GOVREQ	Received with incorrect header information or unsupported message type or version	CONTRL
PNRGOV or GOVREQ	Received, but destination application is not available	CONTRL
GOVREQ	Successful Receipt & Processing – Response returned immediately	PNRGOV
GOVREQ	Successful Receipt & Processing – response to follow	ACKRES

For details, refer to the Appendix C: **PADIS EDIFACT Message Processing - Background for PNRGOV Users**

APPENDIX A – CONTRL MESSAGES

SYNTAX AND SERVICE REPORT (CONTRL) MESSAGE

Introduction

This specification provides the definition of the IATA EDIFACT Syntax and Service Report (CONTRL) message to be used in Electronic Data Interchange (EDI) between partners involved in administration, commerce and transport.

Functional Definition

Purpose:

CONTRL is a message syntactically acknowledging or rejecting, with error indication, a received interchange, functional group or message.

References:

UNTDID, Part 4, Section 2.5
UN/ECE UNSM General introduction, Section 1

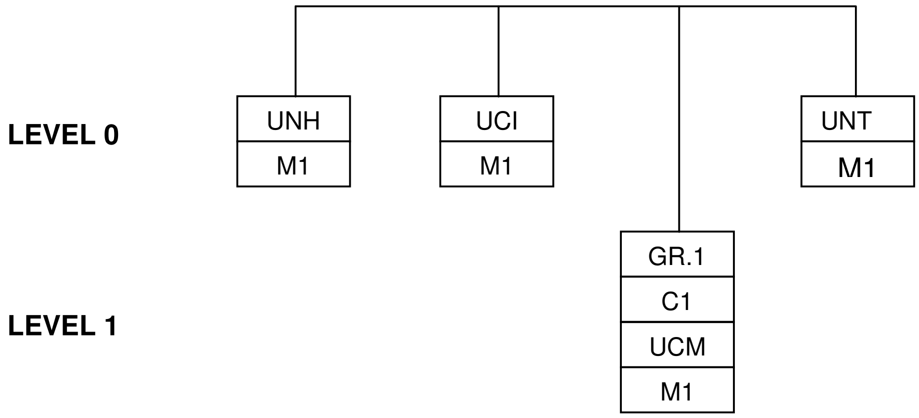
Principles:

See Trade/WP.4/R.1010

CONTRL Segment Table

TAG	NAME	STATUS	REPETITIONS
UNH	MESSAGE HEADER	M	1
UCI	INTERCHANGE RESPONSE	M	1
UCM	MESSAGE RESPONSE	C	1
UNT	MESSAGE TRAILER	M	1

CONTRL Message Branching Diagram



CONTRL Supporting Batch Segments

The following batch segments (taken from the Trade/WP.4/R.1010/Corr.1) are detailed to support the CONTRL message.

UCI INTERCHANGE RESPONSE

Function: To identify the subject interchange and to indicate acknowledgement or rejection (action taken) of the UNA, UNB and UNZ segments, and to identify any error related to these segments.
Depending on the action code, it may also indicate the action taken on the functional groups and messages within that interchange.

Name -ISO 9735	No.	Field Type	Status	IATA Status	Remarks IATA Implementation
INTERCHANGE CONTROL REFERENCE	0020	an..14	M	M	As per ISO 9735
INTERCHANGE SENDER	S002		M	M	As per ISO 9735
Sender identification	0004	an..35	M	M	As per ISO 9735
Partner identification code qualifier	0007	an..4	C	C	As per ISO 9735
Address for reverse routing	0008	an..14	C	C	As per ISO 9735
INTERCHANGE RECIPIENT	S003		M	M	As per ISO 9735
Recipient identification	0010	an..35	M	M	As per ISO 9735
Partner identification code qualifier	0007	an..4	C	C	As per ISO 9735
Routing address	0014	an..14	C	C	As per ISO 9735.
ACTION, CODED	0083	an..3	M	M	As per ISO 9735
SYNTAX ERROR, CODED	0085	an..3	C	C	As per ISO 9735
SEGMENT TAG	0013	a3	C	C	As per ISO 9735
DATA ELEMENT IDENTIFICATION	S011		C	C	As per ISO 9735
Erroneous data element position in segment	0098	n..3	M	M	As per ISO 9735
Erroneous component data element position	0104	n..3	C	C	As per ISO 9735

UCM MESSAGE RESPONSE

Function: To identify a message in the subject interchange, and to indicate that message's acknowledgement or rejection (action taken), and to identify any error related to the UNH and UNT segments.

Name -ISO 9735	No.	Field Type	Status	IATA Status	Remarks IATA Implementation
MESSAGE REFERENCE NUMBER	0062	an..14	M	M	As per ISO 9735
MESSAGE IDENTIFIER	S009		M	M	As per ISO 9735
Message type identifier	0065	an..6	M	M	As per ISO 9735
Message type version number	0052	an..3	C	C	As per ISO 9735
Message type release number	0054	an..3	M	M	As per ISO 9735
Controlling agency	0051	an..2	M	M	As per ISO 9735
Association assigned code	0010	an..6	C	C	As per ISO 9735
ACTION, CODED	0083	an..3	M	M	As per ISO 9735
SYNTAX ERROR, CODED	0085	an..3	C	C	As per ISO 9735
SEGMENT TAG	0013	a3	C	C	As per ISO 9735
DATA ELEMENT IDENTIFICATION	S011		C	C	As per ISO 9735
Erroneous data element position in segment	0098	n..3	M	M	As per ISO 9735
Erroneous component data element position	0104	n..3	C	C	As per ISO 9735

APPENDIX B – Business Examples

All amounts have been *neutralized* to ensure there is no hint of price sensitivity. All personally identifiable information is fictitious.

1 Example of PNRs with Infant, Reservation and Check-in data and unformatted history

UNA:+.*'	Interchange header segment
UNB+IATA:1+1A+KRC+130527:0649+0003'	Message header
UNH+1+PNRGOV:11:1:IA+270513/0649/SQ/602'	
MSG+:22'	22 used for 'Push PNR data to States'
ORG+1A:MUC'	Information about the sender of this message
TVL+270513:1430:270513:2205+SIN+ICN+SQ+602'	Leg information for which passenger data is being sent
EQN+1'	Number of PNRs being sent in the message
SRC'	
RCI+1A:3PGZOV::190313:1354'	PNR Record information, PNR creation date and time
DAT+700:270513:0559'	Latest PNR transaction date
ORG+1A:MUC+32393340:SINSQ08AA+NCE+SQ:NCE+A+SG+ELPD+CFDE59+9	Originator of request details
TIF+BELT:I+ISABELLE MRS:A:2:1'	Passenger last and first name
FTI+SQ:8794285757'	Passenger Frequent Flyer number
IFT+4:63::SQ'	63 : Go show indicator
REF+:001C451486DFF0CC'	Unique passenger id
SSR+DOCS:HK:1:SQ:::::/P/GBR/512731999/GBR/20SEP12/FI/25OCT17/BELT/SOPHY OLIVIA/'	Passport information of the infant
SSR+DOCS:HK:1:SQ:::::/P/GBR/509229987/GBR/01JUL78/F/12NOV22/BELT/ISABELLE RUTH/'	Passport information of the parent
TIF+BELT:I+SOPHY:IN:3'	Infant last and first name
IFT+4:63::SQ'	63 : Go show indicator
TVL+270513:1430:270513:2205+SIN+ICN+SQ+602:D'	Segment booked information
RPI+1+HK'	Flight booking status
APD+333'	Aircraft type
SSR+INFT:HK:1:SQ:::SIN:ICN:BELT/SOPHY 20SEP12+::2'	SSR INFT information
SSR+DOCS:HK:1:SQ:::SIN:ICN:/P/GBR/512731999/GBR/20SEP12/FI/25OCT17/BELT/SOPHY OLIVIA/+::2'	Passport information of the infant
SSR+DOCS:HK:1:SQ:::SIN:ICN:/P/GBR/509229987/GBR/01JUL78/F/12NOV22/BELT/ISABELLE RUTH/+::2'	Passport information of the parent
RCI+1A:3PGZOV::190313:1354'	Passenger record locator specific to this flight
DAT'	
	Check-in information of the parent:
ORG+SQ++++A'	Check-in Agent information
TRI++SIN-168:::2'	Sequence/boarding number
TIF+BELT:I+ISABELLE MRS:A:2'	Check-in passenger last and first name
SSD+011D++++J'	Seat number assigned
TBD++3:33:700++HP:SIN-168+618:0123456789:2:ICN+618:0123456788:3:ICN+618:0123456787:722356:IC	Checked in Baggage information
DAT'	
	Check-in information of the infant:
ORG+SQ++++A'	Check-in Agent information
TRI++SIN-169:::3'	Sequence/boarding number
TIF+BELT:I+SOPHY:IN:3'	Check-in passenger last and first name
SSD+011D++++J'	Seat number assigned
LTS+0/O/NM/BELT/ISABELLE MRS(ADT)(INF/SOPHY/20SEP12)'	**Unformatted history information**
LTS+0/O/SS/SQ 602 D 27MAY 1 SINICN LK1 1430 2205/NN *1A/E* /SQ/SG/C/I/CAB J//1///// /Y 1625/B 153//AY 1838/EY 1685/SINICN/D'	
LTS+0/O/SR/SSR INFTSQNN1 BELT/SOPHY 20SEP12/SQ 602 D 27MAY SINICN/BELT/ISABELLE MRS(ADT)(INF/SOPHY/20SEP12)'	
LTS+0/O/SR/SSR FQTVSQHK/ SQ8794285757 S/KFES/BELT/ISABELLE MRS(ADT)(INF/SOPHY/20SEP12)'	
LTS+0/O/SR/SSR FQTSSQHK1 SQ8794285757 S/KFES/SQ 602 D 27MAY SINICN/BELT/ISABELLE MRS(ADT)(INF/SOPHY/20SEP12)'	
LTS+0/O/SR/SSR DOCSSQHK1 P/GB/509229987/GB/01JUL78/F/12NOV22/BELT/ISABELLE//H/SQ 602 D 27MAY SINICN/BELT/ISABELLE MRS(ADT)(INF/SOPHY/20SEP12)'	
LTS+0/Z/AMADEUS E RETAIL CR-SINSQ08AA 32393340 SU 0001AA/DS-9CCFDE59 19MAR1354Z'	
LTS+0/1/R/SR/SSR INFTSQKK1 BELT/SOPHY 20SEP12/HN/SQ 602 D 27MAY SINICN/BELT/ISABELLE MRS(ADT)(INF/SOPHY/20SEP12)'	
LTS+1/Z/1AINV RM SQ 191354 CR-1AINV RM SQ 0000 19MAR1354Z'	
LTS+2/P/QE/SINSQ0100/1C15D4'	
LTS+2/Z/1AINV RM SQ 191354 CR-1AI NV R 19MAR1354Z'	
LTS+3/Z/ -SQ/WSSQSAA CR-SINSQ08AA 32393340 GS 9999WS/RO-9C404C04 SAAW330SQ 00000000 19MAR1354Z'	
LTS+4/Z/1AINV RM SQ 191354 CR-1AINV RM SQ 0000 19MAR1354Z'	
LTS+0/5/C/5/AP AMADEUS-H'	
LTS+0/5/C/27/TKXL 20MAR/0004/SINSQ08AA'	
LTS+5/A/27/TKOK 19MAR/SINSQ08AA'	
LTS+5/6/R/27/TKOK 19MAR/SINSQ08AA'	
LTS+6/Z/AA CR-SINSQ08AA 32393340 SU 0001AA/DS-9CCFDF66 19MAR1359Z'	
LTS+7/Z//DCS-SYNCUS CR-SINSQ00CO 00000000 PD 6160MC/DS-9CBABA44 23MAY1240Z'	

LTS+0/8/C/SR/SSR FQTVSQHK/ SQ8794285757 S/KFES/BELT/ISABELLE MRS(ADT)(INF/SOPHY/20SEP12)'	
LTS+0/8/C/SR/SSR FQTSSQHK1 SQ8794285757 S/KFES/SQ 602 D 27MAY SINICN/BELT/ISABELLE MRS(ADT)(INF/SOPHY/20SEP12)'	
LTS+8/A/SR/SSR FQTVSQHK/ SQ8794285757 G/QPPS/BELT/ISABELLE MRS(ADT)(INF/SOPHY/20SEP12)'	
LTS+8/A/SR/SSR FQTSSQHK1 SQ8794285757 G/QPPS/SQ 602 D 27MAY SINICN/BELT/ISABELLE MRS(ADT)(INF/SOPHY/20SEP12)'	
LTS+8/Z/CSXAPU CR-NCE1A0SQ0 SU 0001AA 24MAY2009Z'	
LTS+9/Z/1AINV RM SQ 242009 CR-1AINV RM SQ 0000 24MAY2009Z'	
LTS+1/10/R/SR/SSR INFTSQHK1 BELT/SOPHY 20SEP12/KK/SQ 602 D 27MAY SINICN/BELT/ISABELLE MRS(ADT)(INF/SOPHY/20SEP12)'	
LTS+4/10/R/SR/SSR BSCTSQHK1/KK/SQ 602 D 27MAY SINICN/BELT/ISABELLE MRS(ADT)(INF/SOPHY/20SEP12)'	
LTS+10/Z/ETK-ISSBOE CR-SINSQ01W0 32391122 GS 1916VV/RO-9CB39093 MUCPI2SQ1 00000000 25MAY0309Z'	
LTS+11/A/SK/SK LKPX SQ HK1 Z8OWIE-P1/SQ 602 D 27MAY SINICN/BELT/ISABELLE MRS(ADT)(INF/SOPHY/20SEP12)'	
LTS+11/Z/ISSBOE CR-SINSQ01W0 32391122 GS 1916VV/RO-9CB39093 MUCPI2SQ1 00000000 25MAY0313Z'	
LTS+12/Z/MRS BELT CR-SINSQ01W0 32391122 GS 1916VV/RO-9CB39093 MUCPI2SQ1 00000000 25MAY0315Z'	
LTS+13/Z/1AINV RM SQ 250315 CR-1AINV RM SQ 0000 25MAY0315Z'	
LTS+14/A/7/RX ******** ATTN SINKKXH SINKDXH SINKNXH PLS ASSIST PAX WITH TKT 618-2402058077 AND 618-2402241436 TO BE SEATED TOGETHER FLT'	
LTS+14/A/7/RX SQ602 D SIN - ICN 27MAY13 14\:30 ON BSCT SEAT X MANY THANKS SINRRRSQ'	
LTS+14/A/7/RX MS BELT CALLED TO UPDATE SEAT RQST X ADDED SEAT / MEAL X TELEX SENT X NIL SEATS AND MEALS X MOBILE CONTACT NUMBER UPDATED'	
LTS+14/A/7/RX X VIAN / 8\:48 IST 25/5/2013'	
LTS+14/Z/MRS BELT CR-SINSQ01W0 32391122 GS 1916VV/RO-9CB39093 MUCPI2SQ1 00000000 25MAY0320Z'	
LTS+15/A/SR/SSR DOCSSQHK1 P/GBR/512731999/GBR/20SEP12/FI/25OCT17/BELT/SOPHY OLIVIA//BELT/ISABELLE MRS(ADT)(INF/SOPHY/20SEP12)'	
LTS+15/A/SR/SSR DOCSSQHK1 P/GBR/512731999/GBR/20SEP12/FI/25OCT17/BELT/SOPHY OLIVIA//SQ 602 D 27MAY SINICN/BELT/ISABELLE MRS(ADT)(INF/SOPHY/20SEP12)'	
LTS+15/Z//DCS-IREQ CR-SINSQ00VW 00000000 GS 9743EC/DS-9CBCCB00 27MAY0422Z'	
LTS+0/16/C/SR/SSR DOCSSQHK1 P/GB/509229987/GB/01JUL78/F/12NOV22/BELT/ISABELLE//H/SQ 602 D 27MAY SINICN/BELT/ISABELLE MRS(ADT)(INF/SOPHY/20SEP12)'	
LTS+16/A/SR/SSR DOCSSQHK1 P/GBR/509229987/GBR/01JUL78/F/12NOV22/BELT/ISABELLE RUTH//SQ 602 D 27MAY SINICN/BELT/ISABELLE MRS(ADT)(INF/SOPHY/20SEP12)'	
LTS+16/Z//DCS-IREQ CR-SINSQ00VW 00000000 GS 9743EC/DS-9CBAB9B5 27MAY0423Z'	
LTS+17/A/SR/SSR DOCSSQHK1 P/GBR/509229987/GBR/01JUL78/F/12NOV22/BELT/ISABELLE RUTH//BELT/ISABELLE MRS(ADT)(INF/SOPHY/20SEP12)'	
LTS+17/Z//DCS-IREQ CR-SINSQ00VW 00000000 GS 9743EC/DS-9CBAB9D5 27MAY0423Z'	
LTS+18/Z//DCS-SYNCUS CR-SINSQ00VW 00000000 GS 9743EC/DS-9CBABA1D 27MAY0423Z'	
LTS+19/Z//DCS-SYNCUS CR-SINSQ00VW 00000000 GS 9743EC/DS-9CBCCB14 27MAY0423Z'	
LTS+20/Z//DCS-SYNCUS CR-SINSQ00CO 00000000 PD 2092EL/DS-9CBAB94B 27MAY0559Z'	
LTS+21/Z//DCS-SYNCUS CR-SINSQ00CO 00000000 PD 2092EL/DS-9CBABA1A 27MAY0559Z'	
UNT+85+1'	Number of segments
UNZ+1+0003'	Interchange trailer

2 Example of Codeshare PNRs with Reservation and Check-in data and unformatted history

UNA:+.*'	Interchange header segment
UNB+IATA:1+1A+KRC+130527:0754+0003'	Message header
UNH+1+PNRGOV:11:1:IA+270513/0754/SQ/609'	
MSG+:22'	22 used for 'Push PNR data to States'
ORG+1A:MUC'	Information about the sender of this message
TVL+270513:1640:270513:2200+ICN+SIN+SQ+609'	Leg information for which passenger data is being sent
EQN+2'	Number of PNRs being sent in the message
SRC'	**1st PNR**
RCI+1A:2LS6KP::200513:0439+KE:EDP2RW'	PNR Record information, PNR creation date and time
DAT+700:270513:0718'	Latest PNR transaction date
ORG+1A:MUC+:HDQKE2400+NBE+KE:NBE+A+KR+GNPD+003956+94'	Originator of request details
TIF+PARK:I+SEJOONMR::1'	Passenger last and first name
FTI+SQ:314655277:::::G'	Passenger Frequent Flyer number
IFT+4:63::SQ'	63 : Go show indicator
REF+:001435199A918A76'	Unique passenger id
SSR+DOCS:HK:1:SQ:::::/P/KR/JR3364288/KR/10SEP72/M/05JUL16/PARK/SE JOON'	Passport information
TVL+270513:1640:270513:2200+ICN+SIN+KE:SQ+609:B'	Segment booked information
RPI+1+HK'	Flight booking status
APD+333'	Aircraft type
SSR+NSSA:HN:1:SQ:::ICN:SIN+::1'	Seat request information
SSR+CKIN:HK:1:SQ:::ICN:SIN:10KG EXBG WAIVER AUTH BY MDPRM+::1'	SSR information
SSR+DOCS:HK:1:SQ:::ICN:SIN:/P/KOR/JR3364288/KOR/10SEP72/M/05JUL16/PARK/SE JOON/+::1'	Passport information
RCI+1A:2LS6KP::200513:0439+KE:EDP2RW'	Passenger record locator specific to this flight
TVL+++++303:Y'	Operating flight number
DAT'	
ORG+SQ++++A'	Check-in Agent information
TRI++ICN-188:::1'	Sequence/boarding number
TIF+PARK:I+SEJOONMR::1'	Check-in passenger last and first name
SSD+039G++++Y'	Seat number assigned
TBD++2:34:700++MP+618:1026000001:2:MPM+618:1026000002:3:MPM'	Checked in Baggage information
LTS+0/O/NM/PARK/SEJOONMR'	**Unformatted history information**
LTS+0/O/SS/SQ 609 E 27MAY 1 ICNSIN LK1 1640 2200/LK *1A/E*/KE/KR/C/I/CAB Y//2/0001//// /Y 621/B 3//AY 914/EY 908/ICNJNB/E'	
[…]	
LTS+14/A/SR/SSR DOCSSQHK1 P/KR/JR3364288/KR/10SEP72/M/05JUL16/PARK/SE JOON/PARK/SEJOONMR'	
LTS+14/Z/SELRMKE 210921 CR-SEL RM KE 21MAY0921Z'	
[…]	
LTS+47/Z//DCS-SYNCUS CR-ICNSQ00CS 00000000 PD 6017GN/DS-9CBABA8A 27MAY0718Z'	
SRC'	**2nd PNR**
RCI+1A:X49V9U::210113:0411+OZ:2OX5VV'	PNR Record information, PNR creation date and time
DAT+700:270513:0726'	Latest PNR transaction date
ORG+1A:MUC+32393340:SINSQ08AA+NCE+SQ:NCE+A+SG+HJGS+CFDEA9+9	Originator of request details
TIF+KIM:I+KONG CHUN MRS:A:3'	Passenger last and first name
FTI+SQ:223422444'	Passenger Frequent Flyer number
IFT+4:63::SQ'	63 : Go show indicator
REF+:0010350E7830159A'	Unique passenger id
SSR+DOCS:HK:1:SQ:::::/P/KOR/M17072944/KOR/15FEB57/F/23MAR19/KIM/KONG CHUN/'	Passport information
TVL+270513:1640:270513:2200+ICN+SIN+OZ:SQ+609:Z'	Segment booked information
RPI+1+HK'	Flight booking status
APD+333'	Aircraft type
SSR+RQST:HK:1:SQ:::ICN:SIN+14A::3'	Seat request information
SSR+DOCS:HK:1:SQ:::ICN:SIN:/P/KOR/M17072944/KOR/15FEB57/F/23MAR19/KIM/KONG CHUN/+::3'	Passport information
RCI+1A:X49V9U::210113:0411+OZ:2OX5VV'	Passenger record locator specific to this flight
TVL+++++752:D'	Operating flight number
DAT'	
ORG+SQ++++A'	Check-in Agent information
TRI++ICN-229:::3'	Sequence/boarding number
TIF+KIM:I+KONG CHUN MRS:A:3'	Check-in passenger last and first name
SSD+014A++++J'	Seat number assigned
TBD++2:29:700++MP+618:0000290138:1:SIN+618: 0000290139:3:SIN'	Checked in Baggage information
LTS+0/S/PARK/KWANG SOO MR(ADT) -YHD2DT'	Unformatted history information
LTS+0/Z/PARK HYUNJU CR-SELSQ01G0 17381302 GS 5477EK/RO-9CB3A23D MUCPI2SQ1 00000000 21JAN0411Z'	
[…]	
LTS+65/Z//DCS-SYNCUS CR-ICNSQ00CI 00000000 GS 6058HJ/DS-9CBAB945 27MAY0726Z'	
UNT+336+1'	Number of segments
UNZ+1+0003'	Interchange trailer

3 Simple PNR booked in another system (no PNR history)

UNA:+.*'	Interchange header segment
UNB+IATA:1+1A+CBSAPNRGOV+130527:1414+0001++PNRGOV'	Message header
UNH+1+PNRGOV:11:1:IA+LH474/270513/0000'	
MSG+:22'	22 used for 'Push PNR data to States'
ORG+1A:MUC'	Information about the sender of this message
TVL+270513:1550:270513:1820+MUC+YUL+LH+474'	Leg information for which passenger data is being sent
EQN+3'	Number of PNRs being sent in the message
SRC'	**1st PNR**
RCI+1A:3MZVP2::210513:1526+AC:P46KA5'	GDS code, RLOC within the GDS code, PNR creation date and time, other GDS where the booking is as well present + RLOC within this other GDS
DAT+700:270513:1354'	Latest PNR transaction date
ORG+1A:MUC+:MUC1A1TTY++1A++DE+LHSU'	Originator of request details
TIF+JACKS:I+JAMES::1'	Passenger last and first name
REF+:00243519B9209183'	Unique passenger id
SSR+DOCS:HK:1:LH::::://///21APR66/M//JACKS/JAMES'	Passport information
TKT+3537321830:T:1'	Ticket number and total number of booklets issued
TVL+270513:1550:270513:1820+MUC+YUL+AC:LH+9099:U'	Segment booked information
RPI+1+HK'	Flight booking status
APD+343'	Aircraft type
RCI+1A:3MZVP2::210513:1526+AC:P46KA5'	Passenger record locator specific to this flight
TVL+++++474:U'	Operating flight number
SRC'	**2nd PNR**
RCI+1A:33O6DK::070513:0837+1G:MS6HXI'	GDS code, RLOC within the GDS code, PNR creation date and time, other GDS where the booking is as well present + RLOC within this other GDS
DAT+700:270513:1354'	Latest PNR transaction date
ORG+1A:MUC+:SWI1G2400++1G++IT+LHSU+0401C0+94'	Originator of request details
TIF+CARRERA:I+MARCUSMR::1'	Passenger last and first name
FTI+LH:992223782028813'	Frequent traveler number
REF+:002015188BD5A2F7'	Unique passenger id
SSR+DOCS:HK:1:LH:::::/P/IT/YA0196755/IT/17APR80/M/11JAN20/CARRERA/MARCUS'	Passport information
TKT+3909508960:T:5'	Ticket number and total number of booklets issued
DAT+710:100513'	Ticket issue date
TVL+270513:1300:270513:1405+VCE+MUC+LH:EN+9457:Z'	Segment booked information
RPI+1+HK'	Flight booking status
RCI+1A:33O6DK::070513:0837+1G:MS6HXI'	Passenger record locator specific to this flight
TVL+++++8203:Z'	Operating flight number
TVL+270513:1550:270513:1820+MUC+YUL+LH+474:Z'	Segment booked information
RPI+1+HK'	Flight booking status
APD+343'	Aircraft type
RCI+1A:33O6DK::070513:0837+1G:MS6HXI'	Passenger record locator specific to this flight
SRC'	**3rd PNR**
RCI+1A:35K2IO::150213:0149+1S:EVFSDI'	GDS code, RLOC within the GDS code, PNR creation date and time, other GDS where the booking is as well present + RLOC within this other GDS
DAT+700:270513:1354'	Latest PNR transaction date
ORG+1A:MUC+:DFW1S4100++1S++CA+LHSU+7E5AA8+9B'	Originator of request details
TIF+DORON:I+NINA MS::2'	Passenger1 last and first name
REF+:00183511D94292CC'	Unique passenger id
SSR+DOCS:HK:1:LH::::://///05FEB53/F//DORON/NINA'	SSR DOCS information
TKT+3204694511:T:4'	Ticket number and total number of booklets issued
DAT+710:150213'	Ticket issue date
TIF+LENDROT:I+CHARLOTTE MS::1'	Passenger2 last and first name
REF+:00183511D94292CD'	Unique passenger id
SSR+DOCS:HK:1:LH::::://///14FEB52/F//LENDROT/CHARLOTTE'	SSR DOCS information
TKT+3204694509:T:4'	Ticket number and total number of booklets issued
DAT+710:150213'	Ticket issue date
TVL+270513:1550:270513:1820+MUC+YUL+LH+474:W'	Segment booked information
RPI+2+HK'	Flight booking status
APD+333'	Aircraft type
RCI+1A:35K2IO::150213:0149+1S:EVFSDI'	Passenger record locator specific to this flight
UNT+55+1'	Number of segments
UNZ+1+0001'	Interchange trailer

4 Example with three PNRs containing ticket information

Three PNRs:

- one single passenger, ticketless, registered passenger with customer ID,
- one single passenger, with a IATA ticket,
- one Group PNR with some names

UNB+IATA:1+TZ+AUCBPS+130523:2210+00102181551362'	
UNG+PNRGOV+TZ+AUCBPS+130523:2210+00102181551362+IA+11:1'	
UNH+00102181551362+PNRGOV:11:1:IA+AUTZ000623052013221001SIN20130528'	
MSG+:22'	PNR Data to State (Australia)
ORG+TZ:MSP+++TZ:SYS+++HOLMESS'	Sent by TZ agent HOLMESS
TVL+280513:2225:290513:0750+SIN+OOL+TZ+0006'	For flight TZ 0006 from SIN to OOL
EQN+3'	3 PNRs on flight
SRC'	**1st PNR**
RCI+TZ:W9TEND::230513:181348'	Airline locator W9TEND, created 23 May 2013 at 18:13Z
DAT+700:230513:2125+710:230513:2124'	Last modified 23 May 2013 at 21:25Z
	Payment made 23 May 2013 at 21:24Z
ORG+TZ:SYS+++++:SGD'	Booking originated by a TZ system user
ADD++700:123 ANY STREET:LAKE TOWN:MN::US:55123:H5555555555 W 1 555 555 5555 '	Reservation contact information including address and telephone numbers
TIF+VANDENBERG+KEVINMICHAELMR:A:43576'	Adult passenger name and unique ID
REF+:43576'	Security-related unique ID
FAR+A+32++++SFLY+SFLY'	Adult fare with fare basis code SFLY
SSR+DOCS:HK:1:TZ:::::/P/USA/548721687/USA/04JUL80/M/12JAN19/VANDENBERG/KEVIN/MICHAEL+::43576'	Passport details
TKT+:700'	Ticketless payment
MON+B:999.00:SGD+T:1999.99:SGD'	Base and total fare
TXD++99.99::SGD:BK+99.99::SGD:OO+99.90::SGD:SG+99.99::SGD:WY+99.99::SGD:OP+99.99::SGD:AU+99.99::SGD:WG+99.99::SGD:WY'	Tax details
DAT+710:230513:2124'	Date of payment
FOP+CA::1999.99'	Cash form of payment
TVL+280513:2225:290513:0750+SIN+OOL+TZ+0006:S'	First flight (TZ006 SIN-OOL 28MAY13)
RPI+1+HK'	1 passenger confirmed
TVL+310513:0900:310513:1500+OOL+SIN+TZ+0005:S'	Second flight (TZ005 OOL SIN 31MAY13)
RPI+1+HK'	1 passenger confirmed
ABI+4++++TZ'	History item #1 by TZ user/system
DAT+T:230513:1813'	Action taken 23MAY 18 :13Z
SAC+++X'	Action was cancellation
IFT+4:19+XF MC 0 VANDENBERG KEVIN 20 00'	History item system-specific details
ABI+4++++TZ'	History Item #2 by TZ user/system
DAT+T:230513:1829'	Action taken 23MAY 18:29Z
SAC+++X'	Action was cancellation
IFT+4:19+ F 28MAY13 SIN OOL 2225 0750 TZ 6 HK SFLY 590 82'	History item system-specific details
TVL+280513::290513+SIN+OOL+TZ+0006:S'	Canceled item was flight TZ006 in S class
RPI+1+HK'	For a party of 1
SAC+++X'	Action was cancellation
IFT+4:19+ F 31MAY13 OOL SIN 0900 1500 TZ 5 HK SFLY 582 81'	History item system-specific details
TVL+310513::310513+OOL+SIN+TZ+0005:S'	Canceled item was flight TZ005 in S class
RPI+1+HK'	For a party of 1
ABI+4++++TZ'	History item #3 by TZ user/system
DAT+T:230513:2124'	Action taken 23MAY13 at 21:24Z
SAC+++A'	Action to add content
IFT+4:19+ P CA 1 173 63 SGD'	History item system-specific details
SAC+++A'	Action to add content
IFT+4:19+ F 28MAY13 SIN OOL 2225 0750 TZ 6 HK SFLY 590 82'	History item system-specific details
TVL+280513::290513+SIN+OOL+TZ+0006:S'	Added item was flight TZ006 in S class
RPI+1+HK'	For a party of 1
SAC+++A'	Action to add content
IFT+4:19+ F 31MAY13 OOL SIN 0900 1500 TZ 5 HK SFLY 582 81'	History item system-specific details
TVL+310513::310513+OOL+SIN+TZ+0005:S'	Added item was flight TZ005 in S class
RPI+1+HK'	For a party of 1
SRC'	**2nd PNR**
RCI+TZ:D1RGHI::230513:183845'	Airline locator D1RGHI, created 23 May 2013 at 18:38Z
DAT+700:230513:1838+710:230513:1838'	Last modified 23 May 13 at 18:38Z
	Paid 23 May 13 at 18:38
ORG+TZ:SYS+++++:SGD'	Booking originated by a TZ system user
ADD++700:9874 HILLY DRIVE:ST LOUIS:MO::US:63124:H5555551212 '	Reservation contact information including address and telephone numbers
TIF+DYE+DOLANMR:A:43577'	First Passenger (Adult) name and Unique ID
FTI+RI:438QZ99'	Frequent traveler information
REF+:43577'	Security related unique ID
FAR+A+23++++SFLY+SFLY'	Adult fare with fare basis codes
SSR+DOCS:HK:1:TZ:::::/P/USA/159264375/USA/01FEB90/M/20NOV19/DYE/DOLAN+::43577'	Passport details
SSR+DOCA:HK:1:TZ:::::/D/AUS/13 SHORE AVENUE/BROADBEACH/QLD/4215+::43577'	Destination address
TKT+:702'	Externally Issued E-ticket
MON+B:999.99:SGD+T:1999.99:SGD'	Base and Total fare
TXD++99.99::SGD:BK+99.99::SGD:OO+99.99::SGD:SG+99.99::SGD:WY+99.99::S	Tax details

D:OP+99.99::SGD:AU+99.99::SGD:WG+99.99::SGD:WY'	
DAT+710:230513:1838'	Date of most recent payment
FOP+CA::9999.99'	Payment was in cash
TIF+DYE+KAYLAMS:A:43578:1'	Second Passenger (Adult) name and Unique ID. Passenger is accompanied by an infant in lap
REF+:43578'	Security related unique ID
FAR+A+20++++SFLY+SFLY'	Adult fare with fare basis codes
SSR+DOCS:HK:1:TZ:::::/P/USA/345678901/USA/07APR93/F/15DEC18/DYE/KAYLA+::43578'	Passport details
SSR+DOCA:HK:1:TZ:::::/D/AUS/13 SHORE AVENUE/BROADBEACH/QLD/4215+::43578'	Destination address details
TKT+:702'	Externally Issued E-ticket
MON+B:999.99:SGD+T:1999.99:SGD'	Base and Total fare
TXD++99.99::SGD:BK+99.99::SGD:OO+99.99::SGD:SG+99.99::SGD:WY+99.99::SGD:OP+99.99::SGD:AU+99.99::SGD:WG+99.99::SGD:WY'	Tax details
DAT+710:230513:1838'	Date and time of payment
TIF+DYE+ARCHER:IN:43578I'	Third passenger (infant) name and unique ID
REF+:43578I'	Security related unique ID
FAR+IN+1'	Infant fare was applied
SSR+DOCS:HK:1:TZ:::::/P/USA/654321987/USA/15APR12/MI/31DEC19/DYE/ARCHER+::43578I'	Passport details
TKT+:702'	Externally Issued E-ticket
TVL+270513:1915:280513:1505+LHR+SIN+BA+0011:L'	First Flight (BA 0011 in L class) (informational)
RPI+2+HK'	Confirmed for 2 seats
TVL+280513:2225:290513:0750+SIN+OOL+TZ+0006:S'	Second Flight (TZ0006 in S class)
RPI+2+HK'	Confirmed for 2 seats
SSR+SEAT:HK:1:TZ:::SIN:OOL+54A::43577:N'	Passenger 1 is in seat 54A
SSR+SEAT:HK:1:TZ:::SIN:OOL+54B::43578:N'	Passenger 2 is in seat 54B
SSR+TKNE:HK:1:TZ:::SIN:OOL:9631270001234C2+::43577'	Passenger 1 e-ticket and coupon numbers
SSR+TKNE:HK:1:TZ:::SIN:OOL:9631270001235C2+::43578'	Passenger 2 e-ticket and coupon numbers
SSR+TKNE:HK:1:TZ:::SIN:OOL:INF9631270001236C2+::43578I'	Infant e-ticket and coupon numbers
SSR+SPEQ:HK:1:TZ:::SIN:OOL+::43577'	Passenger 1 has sports equipment
SSR+IFET:HK:1:TZ:::SIN:OOL+::43578'	Passenger 2 ordered In-Flight entertainment
SSR+INFT:HK:1:TZ:::SIN:OOL:DYE/ARCHER 15APR12+::43578'	Passenger 2 has an infant in arms on this flight
TVL+050613:0900:050613:1500+OOL+SIN+TZ+0005:S'	Third flight (TZ0005 in S class)
RPI+2+HK'	Confirmed for 2 seats
SSR+SEAT:HK:1:TZ:::OOL:SIN+54A::43577:N'	Passenger 1 is in seat 54A
SSR+SEAT:HK:1:TZ:::OOL:SIN+54B::43578:N'	Passenger 2 is in seat 54B
SSR+TKNE:HK:1:TZ:::OOL:SIN:9631270001234C3+::43577'	Passenger 1 e-ticket and coupon numbers
SSR+TKNE:HK:1:TZ:::OOL:SIN:9631270001235C3+::43578'	Passenger 2 e-ticket and coupon numbers
SSR+TKNE:HK:1:TZ:::OOL:SIN:INF9631270001236C3+::43578I'	Infant e-ticket and coupon numbers
SSR+SPEQ:HK:1:TZ:::OOL:SIN+::43577'	Passenger 1 has sports equipment
SSR+IFET:HK:1:TZ:::OOL:SIN+::43578'	Passenger 2 ordered in-flight entertainment
SSR+INFT:HK:1:TZ:::OOL:SIN:DYE/ARCHER 15APR12+::43578'	Passenger 2 has an infant in arms on this flight
TVL+050613:2255:060613:0500+SIN+LHR+BA+0012:D'	Fourth flight (BA 0012 in D class) (informational)
RPI+2+HK'	Confirmed for 2 seats
SRC'	**3rd PNR**
RCI+TZ:GBFKSK::230513:184819'	Airline locator GBFKSK, created 23MAY13 at 18:48Z
DAT+700:230513:1849'	Last modified 23 May 2013 at 18:49
	No payments received
ORG+TZ:SYS+++++:SGD'	Originated by a TZ System user
ADD++700:2431 MOPAC EXPRESSWAY:AUSTIN:TX::US:78750:H5125551212 '	Booking contact address and phone number
TIF+ACME TEAM PARTY:G'	Group Name for Group PNR
TIF+CAPSON+LISALMS:A:43579'	First name received. Adult passenger with Unique ID
REF+:43579'	Security-related unique ID
FAR+A+++++ZSCTBIZ+SFLY'	Adult fare will be used with included fare basis codes
TKT+:700'	No ticket information is received
MON+B:999.99:SGD+T:1999.99:SGD'	Base and total fare to be collected
TXD++99.99::SGD:BK+99.99::SGD:OO+99.99::SGD:SG+99.99::SGD:WY+99.99::SGD:OP+99.99::SGD:AU+99.99::SGD:WG+99.99::SGD:WY'	Tax details
TIF+CAPSON+HUNTER:A:43580'	Second name received. Adult passenger with Unique ID
REF+:43580'	Security-related unique ID
FAR+A+21++++ZSCTBIZ+SFLY'	Adult fare will be used with included fare basis codes
SSR+DOCS:HK:1:TZ::::://///27APR92/M//CAPSON/HUNTER+::43580'	Secure Flight Passenger Data
TKT+:700'	No ticket information is received
MON+B:999.99:SGD+T:1999.99:SGD'	Base and total fare to be collected
TXD++99.99::SGD:BK+99.99::SGD:OO+99.99::SGD:SG+99.99::SGD:WY+99.99::SGD:OP+99.99::SGD:AU+99.99::SGD:WG+99.99::SGD:WY'	Tax details
TIF+ALLEN+SETH:A:43581'	Third name received. Adult passenger with Unique ID
REF+:43581'	Security related unique ID
FAR+A+++++ZSCTBIZ+SFLY'	Adult fare will be used with included fare basis codes
TKT+:700'	No ticket information is received
MON+B:999.99:SGD+T:1999.99:SGD'	Base and total fare to be collected
TXD++99.99::SGD:BK+99.99::SGD:OO+99.99::SGD:SG+99.99::SGD:WY+99.99::SGD:OP+99.99::SGD:AU+99.99::SGD:WG+99.99::SGD:WY'	Tax details
TIF+TBA+C:A:43582'	Fourth name TBA
REF+:43582'	
FAR+A+++++ZSCTBIZ+SFLY'	Adult fare quote
TKT+:700'	No ticket information is received
MON+B:999.99:SGD+T:1999.99:SGD'	Base and total fare to be collected
TXD++99.99::SGD:BK+99.99::SGD:OO+99.99::SGD:SG+99.99::SGD:WY+99.99::SGD:OP+99.99::SGD:AU+99.99::SGD:WG+99.99::SGD:WY'	Tax details
TIF+TBA+D:A:43583'	Fifth name TBA
REF+:43583'	
FAR+A+++++ZSCTBIZ+SFLY'	Adult fare quote
TKT+:700'	No ticket information is received

MON+B:999.99:SGD+T:1999.99:SGD'	Base and total fare to be collected
TXD++99.99::SGD:BK+99.99::SGD:OO+99.99::SGD:SG+99.99::SGD:WY+99.99::SGD:OP+99.99::SGD:AU+99.99::SGD:WG+99.99::SGD:WY'	Tax details
TIF+TBA+E:A:43584'	Sixth name TBA
REF+:43584'	
FAR+A+++++ZSCTBIZ+SFLY'	Adult fare quote
TKT+:700'	No ticket information is received
MON+B:999.99:SGD+T:1999.99:SGD'	Base and total fare to be collected
TXD++99.99::SGD:BK+99.99::SGD:OO+99.99::SGD:SG+99.99::SGD:WY+99.99::SGD:OP+99.99::SGD:AU+99.99::SGD:WG+99.99::SGD:WY'	Tax details
TIF+TBA+F:A:43585'	Seventh name TBA
REF+:43585'	
FAR+A+++++ZSCTBIZ+SFLY'	Adult fare quote
TKT+:700'	No ticket information is received
MON+B:999.99:SGD+T:1999.99:SGD'	Base and total fare to be collected
TXD++99.99::SGD:BK+99.99::SGD:OO+99.99::SGD:SG+99.99::SGD:WY+99.99::SGD:OP+99.99::SGD:AU+99.99::SGD:WG+99.99::SGD:WY'	Tax details
TIF+TBA+G:A:43586'	Eighth name TBA
REF+:43586'	
FAR+A+++++ZSCTBIZ+SFLY'	Adult fare quote
TKT+:700'	No ticket information is received
MON+B:999.99:SGD+T:1999.99:SGD'	Base and total fare to be collected
TXD++99.99::SGD:BK+99.99::SGD:OO+99.99::SGD:SG+99.99::SGD:WY+99.99::SGD:OP+99.99::SGD:AU+99.99::SGD:WG+99.99::SGD:WY'	Tax details
TIF+TBA+H:A:43587'	Ninth name TBA
REF+:43587'	
FAR+A+++++ZSCTBIZ+SFLY'	Adult fare quote
TKT+:700'	No ticket information is received
MON+B:999.99:SGD+T:1999.99:SGD'	Base and total fare to be collected
TXD++99.99::SGD:BK+99.99::SGD:OO+99.99::SGD:SG+99.99::SGD:WY+99.99::SGD:OP+99.99::SGD:AU+99.99::SGD:WG+99.99::SGD:WY'	Tax details
TVL+280513:2225:290513:0750+SIN+OOL+TZ+0006:Z'	First flight (TZ0006 in Z class)
RPI+9+HK'	Confirmed for 9 passengers
TVL+170613:0900:170613:1500+OOL+SIN+TZ+0005:S'	Second flight (TZ0005 in S class)
RPI+9+HK'	Confirmed for 9 passengers
ABI+4++++TZ'	History credit by TZ system/user
DAT+T:230513:1849'	Action taken on 23 May 2013 at 18:49
SAC+++C'	Action taken was to Change
IFT+4:19+GN FROM NONE TO ACME TEAM PARTY'	System-specific details
UNT+173+00102181551362'	
UNE+1+00102181551362'	
UNZ+1+00102181551362'	

5 Example with one adult and an Infant

In this example the PNRGOV message is sent 24 hours prior to departure for AM flight (MTY-LAS), containing one PNR booked by AM.

Assumptions:

- Mexico requires PNRGOV messages both for outbound and inbound flights
- 24h trigger used- no check-in data present
- No history and ticketing data (only TKNE SSRs) present-Phase 2

UNA:+.?*'	
UNB+IATA:1+AM+MXPNRGOV+130522:1540+13052210400995+PNRGOV'	Interchange header-sender/receiver/date
UNG+PNRGOV+AM+MXPNRGOV+130522:1540+13052210400995+IA+11:1'	Functional group header
UNH+13052210400995+PNRGOV:11:1:IA+AM498/230513/1142'	Message header
MSG+:22'	Code to specify the message function
ORG+AM'	The originator of the request is AM
TVL+230513:1039:230513:1142+MTY+LAS+AM+498'	PNR data for AM498/23MAY13 MTY LAS
EQN+1'	Total numbers of PNRs
SRC'	
RCI+AM:XXXYET::300413:115500'	Passenger record reference
SSR+OTHS::::::: ADV TKT NUMBER BY 03MAY13 1800CO OR WILL CANCEL'	Special requirements /general information-applies to all
SSR+OTHS::::::: IF THE FARE RULE TL DIFFERS FROM THE AUTOMATIC'	Flights and all passengers
SSR+OTHS::::::: TL THE MOST RESTRICTIVE TL WILL APPLY'	
DAT+700:180513:1502'	Ticket issue / last PNR transaction date/Time
ORG+AM:BOG'	Booked by AM, BOG agent
TIF+TESTSURNAMEONE+TESTNAMEONE MRS:A:1.1:1'	Adult passenger's name & surname
SSR+INFT:NN:1:AM:::::TESTSURNAMETWO/TESTNAMETWO/10AUG11+::1.1'	Infant information: surname/name/DOB
SSR+INFT:NN:1:AM:::::TESTSURNAMETWO/TESTNAMETWO/10AUG11+::1.1'	Infant information: surname/name/DOB
SSR+TKNE:HK:1:AM:::MEX:CUN:1392178947000C2+::1.1'	Ticketing details for adult MEX CUN
SSR+TKNE:HK:1:AM:::CUN:BOG:1392178947000C3+::1.1'	Ticketing details for adult CUN BOG
SSR+TKNE:HK:1:AM:::MEX:CUN:INF1392178947000C2+::1.1'	Ticketing details for infant MEX CUN
SSR+TKNE:HK:1:AM:::CUN:BOG:INF1392178947000C3+::1.1'	Ticketing details for infant CUN BOG
SSR+DOCS:HK:1:AM:::::/P/CO/52263000/CO/30MAY76/F/31OCT15/TESTSURNAMEONE/TESTNAMEONE MRS+::1.1'	Passport information for adult
SSR+DOCS:HK:1:AM:::::/P/COL/AO234000/COL/10AUG11/FI/21DEC22/TESTSURNAMETWO/TESTNAMETWO+::1.1'	Passport information for infant
TIF+TESTSURNAMETWO+TESTNAMETWO:IN:2.1'	Infant passenger's name & surname
IFT+4:28+AM INF'	OSI free text information
TVL+150513:0105:150513:0557+BOG+MEX+AM+709:R'	PNR data for AM709/15MAY13 BOG MEX
RPI+1+YG'	Flight booking status for 1 adult passenger
APD+737'	Equipment Type- Boeing 737
RCI+AM:XXXYET::300413:115500'	AM passenger record reference
TVL+190513:1500:190513:1710+MEX+CUN+AM+445:S'	PNR data for AM445/19MAY13 MEX CUN
RPI+1+HK'	Flight booking status for 1 adult passenger
APD+738'	Equipment Type
SSR+INFT:NN:1:AM:::::TESTSURNAMETWO/TESTNAMETWO/10AUG11'	Infant information: surname/name/DOB
SSR+TKNE:HK:1:AM:::MEX:CUN:1392178947000C2'	Ticketing details for adult MEX CUN
SSR+TKNE:HK:1:AM:::MEX:CUN:INF1392178947000C2'	Ticketing details for infant MEX CUN
RCI+AM:XXXYET::300413:115500'	AM passenger record reference
TVL+230513:0135:230513:0500+CUN+BOG+AM+718:Q'	PNR data for AM718/23MAY13 CUN BOG
RPI+1+HK'	Flight booking status for 1 passenger
APD+737'	Equipment Type
SSR+INFT:NN:1:AM:::::TESTSURNAMETWO/TESTNAMETWO/10AUG11'	Infant information: surname/name/DOB
SSR+TKNE:HK:1:AM:::CUN:BOG:1392178947000C3'	Ticketing details for adult CUN BOG
SSR+TKNE:HK:1:AM:::CUN:BOG:INF1392178947000C3'	Ticketing details for infant CUN BOG
RCI+AM:XXXYET::300413:115500'	AM passenger record reference
UNT+42+13052210400995'	Message trailer corresponding UNH segment
UNE+1+13052210400995'	Functional group trailer corresponding UNG
UNZ+1+13052210400995'	Interchange trailer

6 PNR with Frequent Traveler (2 adults) and PNR split

In this example the PNRGOV message is sent 24 hours prior to departure for AM flight (MTY-LAS).

Assumptions:

- Mexico requires PNRGOV messages both for outbound and inbound flights
- 24h trigger used- no check-in data present
- No history and ticketing data (only TKNE SSRs) present-Phase 2

UNA:+.?*'	
UNB+IATA:1+AM+MXPNRGOV+130522:1540+13052210400995+PNRGOV'	Interchange header-sender/receiver/date
UNG+PNRGOV+AM+MXPNRGOV+130522:1540+13052210400995+IA+11:1'	Functional group header
UNH+13052210400995+PNRGOV:11:1:IA+AM498/230513/1142'	Message header
MSG+:22'	A code to specify the message function
ORG+AM'	The originator of the request is AM
TVL+230513:1039:230513:1142+MTY+LAS+AM+498'	PNR data for AM498/23MAY13 MTY LAS
EQN+2'	Total numbers of PNRs
SRC'	
RCI+AM:ICOXXX::120413:175500'	AM passenger record reference
DAT+700:120413:2044'	Ticket issue / last PNR transaction date/Time
IFT+4:28+AM 045 81 8396 0000/TESTNAMEONE TESTSURNAMEONE'	OSI free text information- contact details
IFT+4:28+AM PNR UNDER AM TRAVEL UNIT LT Q/000'	
IFT+4:28+AM CTCP MEX1800 002 5200 DOMESTIC TOLL FREE'	
IFT+4:28+AM CTCP MEX1866 252 5200 USA AND CAN TOLL FREE'	
IFT+4:28+AM CTCP MEX52 55 4446 0000 FAX'	
IFT+4:28+AM CTCH MEX01 81 8336 6900 H'	
IFT+4:28+AM CTCP MEX045 81 8396 1000 M'	
ORG+AM:TTY'	Booked by AM, TTY agent
TIF+TESTSURNAMEONE+TESTNAMEONE MRS:A:1.1'	1st adult passenger's name & surname
FTI+AM:511650000'	Frequent traveler information (airline/no.)
SSR+TKNE:HK:1:AM:::MTY:LAS:1393207166000C1+::1.1'	Ticketing details for 1st adult MTY LAS
SSR+TKNE:HK:1:AM:::LAS:MTY:1393207166000C2+::1.1'	Ticketing details for 1st adult LAS MTY
TIF+TESTSURNAMEONE+TESTNAMETWO MR:A:2.1'	2nd adult passenger's name & surname
SSR+TKNE:HK:1:AM:::MTY:LAS:1393207166000C1+::2.1'	Ticketing details for 2nd adult MTY LAS
SSR+TKNE:HK:1:AM:::LAS:MTY:1393207166000C2+::2.1'	Ticketing details for 2nd adult LAS MTY
TVL+230513:1039:230513:1142+MTY+LAS+AM+498:A'	PNR data for AM498/23MAY13 MTY LAS
RPI+2+HK'	Flight booking status for 2 adult passengers
APD+738'	Equipment Type
SSR+SEAT:DK:2:AM:::MTY:LAS:.03BN03AN'	Seat information for MTY LAS for 2pax
SSR+TKNE:HK:1:AM:::MTY:LAS:1393207166000C1'	Ticketing details for MTY LAS
SSR+TKNE:HK:1:AM:::MTY:LAS:1393207166000C1'	Ticketing details for MTY LAS
RCI+AM:ICOXXX::120413:175500'	AM passenger record reference
TVL+260513:1311:260513:1800+LAS+MTY+AM+499:A'	PNR data for AM499/26MAY13 LAS MTY
RPI+2+HK'	Flight booking status for 2 adult passengers
APD+738'	Equipment Type
SSR+SEAT:DK:2:AM:::LAS:MTY:.03BN03AN'	Seat information for LAS MTY for 2 passengers
SSR+TKNE:HK:1:AM:::LAS:MTY:1393207166000C2'	Ticketing details for MTY LAS
SSR+TKNE:HK:1:AM:::LAS:MTY:1393207166000C2'	Ticketing details for MTY LAS
RCI+AM:ICOXXX::120413:175500'	AM passenger record reference
SRC'	
RCI+AM:BJOXXX::110513:114800'	AM passenger record reference
DAT+700:190513:0521'	Ticket issue / last PNR transaction date/Time
IFT+4:28+AM CTCBOG 571-600 5820-A-COTOURIST COLOMBIA'	OSI free text information
IFT+4:28+AM CTCT BOG 571 600 5830 A'	
IFT+4:28+AM CTCP BOG 571 600 5820 A PBX'	
IFT+4:28+AM RLOC HDQ1SYDIXXZ'	
ORG+AM:TTY'	Booked by AM, TTY agent
TIF+TESTSURNAMETHREE+TESTNAMETHREE MR:A:1.1'	Adult passenger's name & surname
SSR+TKNE:HK:1:AM:::BOG:CUN:.1393534576000C1+::1.1'	Ticketing details for BOG CUN
SSR+TKNE:HK:1:AM:::CUN:BOG:.1393534576000C2+::1.1'	Ticketing details for BOG CUN
SSR+DOCS:HK:1:AM:::::/P/CO/AO589000/CO/14OCT94/M/08MAY23/TESTSURNAMETHREE/TESTNAMETHREE+::1.1'	Passport information
SSR+CKIN:NN:1::::::WEBCHKIN+::1.1'	Check-in information SSR data
SSR+CKIN:NN:1::::::BAGS TO CHECK 1+::1.1'	Check-in information SSR data
TVL+190513:0700:190513:1030+BOG+CUN+AM+719:V'	PNR data for AM719/19MAY13 BOG CUN
RPI+1+HK'	Flight booking status for 1 adult passenger
APD+738'	Equipment Type
SSR+TKNE:HK:1:AM:::BOG:CUN:.1393534576000C1'	Ticketing details for BOG CUN
RCI+AM:BJOXXX::110513:114800'	AM passenger record reference
TVL+230513:0135:230513:0500+CUN+BOG+AM+718:V'	PNR data for AM718/23MAY13 CUN BOG
RPI+1+HK'	Flight booking status for 1 passenger
APD+737'	Equipment Type
SSR+TKNE:HK:1:AM:::CUN:BOG:.1393534576000C2'	Ticketing details CUN BOG
RCI+AM:BJOXXX::110513:114800'	AM passenger record reference-new PNR
EQN+1'	Split
RCI+AM:ZLMXXX::110513:114800'	AM passenger record reference-original (split from)PNR
UNT+64+13052210400995’	Message trailer corresponding UNH segment
UNE+1+13052210400995’	Functional group trailer corresponding UNG
UNZ+1+13052210400995’	Interchange trailer

7 Examples with different data in EQN segment

All amounts have been *neutralized* to ensure there is no hint of price sensitivity. All passenger and address data is fictitious.
The following examples indicate the combination of MSG and EQN Segments in PNRGOV messages:

- Data element 1225 of composite C302 in the MSG segment is used to indicate whether the transmission is a Full transmission of all PNR data for a flight (22), or changed PNRs only (141).
- Data element 6350 of composite C523 in the EQN segment is used to indicate the number of PNRs transmitted in the message

The combination of the values in these two elements can be used to indicate several conditions:

Example 1: A transmission is made for a flight that has no passengers (no PNRs)

UNB+IATA:1+TZ+AUCBPS+130523:2210+00102181551362'	
UNG+PNRGOV+TZ+AUCBPS+130523:2210+00102181551362+IA+11:1'	
UNH+00102181551362+PNRGOV:11:1:IA+AUTZ000623052013221001SIN2013052	
MSG+:22'	PNR Data to State (full push)
ORG+TZ:MSP+++TZ:SYS+++HOLMESS'	
TVL+280513:2225:290513:0750+SIN+OOL+TZ+0006'	For flight TZ 0006 from SIN to OOL
EQN+0'	No PNRs on flight
UNT+6+00102181551362'	
UNE+1+00102181551362'	
UNZ+1+00102181551362'	

Example 2: There are no updated PNRs since the previous transmission for this flight

UNB+IATA:1+TZ+AUCBPS+130523:2210+00102181551362'	
UNG+PNRGOV+TZ+AUCBPS+130523:2210+00102181551362+IA+11:1'	
UNH+00102181551362+PNRGOV:11:1:IA+AUTZ000623052013221001SIN2013052	
MSG+:141'	PNR Data to State (update)
ORG+TZ:MSP+++TZ:SYS+++HOLMESS'	
TVL+280513:2225:290513:0750+SIN+OOL+TZ+0006'	For flight TZ 0006 from SIN to OOL
EQN+0'	0 PNRs updated
UNT+6+00102181551362'	
UNE+1+00102181551362'	
UNZ+1+00102181551362'	

Example 3: A single PNR has been updated since the previous transmission for this flight (multiple PNRs exist)

UNB+IATA:1+TZ+AUCBPS+130523:2210+00102181551362'	
UNG+PNRGOV+TZ+AUCBPS+130523:2210+00102181551362+IA+11:1'	
UNH+00102181551362+PNRGOV:11:1:IA+AUTZ000623052013221001SIN20130528'	
MSG+:141'	PNR Data to State (update)
ORG+TZ:MSP+++TZ:SYS+++HOLMESS'	
TVL+280513:2225:290513:0750+SIN+OOL+TZ+0006'	For flight TZ 0006 from SIN to OOL
EQN+1'	1 PNR updated
SRC'	Start of 1st PNR
RCI+TZ:W9TEND::230513:181348'	Airline locator W9TEND, created 23 May 2013 at 18:13Z
DAT+700:230513:2125+710:230513:2124'	Last modified 23 May 2013 at 21:25Z
	Payment made 23 May 2013 at 21:24Z
ORG+TZ:SYS+++++:SGD'	
ADD++700:123 ANY STREET:LAKE TOWN:MN::US:55123:H5555555555 W 1 555 555 5555 '	
TIF+VANDENBERG+KEVINMICHAELMR:A:43576'	
REF+:43576'	
FAR+A+32++++SFLY+SFLY'	
SSR+DOCS:HK:1:TZ:::::/P/USA/548721687/USA/04JUL80/M/12JAN19/VANDENBERG/KEVIN/MICHAEL+::43576'	
TKT+:700'	
MON+B:999.00:SGD+T:1999.99:SGD'	
TXD++99.99::SGD:BK+99.99::SGD:OO+99.90::SGD:SG+99.99::SGD:WY+99.99::SGD:OP+99.99::SGD:AU+99.99::SGD:WG+99.99::SGD:WY'	
DAT+710:230513:2124'	
FOP+CA::1999.99'	
TVL+280513:2225:290513:0750+SIN+OOL+TZ+0006:S'	
RPI+1+HK'	
TVL+310513:0900:310513:1500+OOL+SIN+TZ+0005:S'	
RPI+1+HK'	
ABI+4++++TZ'	History item #1 by TZ user/system
DAT+T:230513:1813'	Action taken 23MAY 18 :13Z

SAC+++X'	Action was cancellation
IFT+4:19+XF MC 0 VANDENBERG KEVIN 20 00'	History item system-specific details
ABI+4++++TZ'	History Item #2 by TZ user/system
DAT+T:230513:1829'	Action taken 23MAY 18:29Z
SAC+++X'	Action was cancellation
IFT+4:19+ F 28MAY13 SIN OOL 2225 0750 TZ 6 HK SFLY 590 82'	History item system-specific details
TVL+280513::290513+SIN+OOL+TZ+0006:S'	Canceled item was flight TZ006 in S class
RPI+1+HK'	For a party of 1
SAC+++X'	Action was cancellation
IFT+4:19+ F 31MAY13 OOL SIN 0900 1500 TZ 5 HK SFLY 582 81'	History item system-specific details
TVL+310513::310513+OOL+SIN+TZ+0005:S'	Canceled item was flight TZ005 in S class
RPI+1+HK'	For a party of 1
ABI+4++++TZ'	History item #3 by TZ user/system
DAT+T:230513:2124'	Action taken 23MAY13 at 21:24Z
SAC+++A'	Action to add content
IFT+4:19+ P CA 1 173 63 SGD'	History item system-specific details
SAC+++A'	Action to add content
IFT+4:19+ F 28MAY13 SIN OOL 2225 0750 TZ 6 HK SFLY 590 82'	History item system-specific details
TVL+280513::290513+SIN+OOL+TZ+0006:S'	Added item was flight TZ006 in S class
RPI+1+HK'	For a party of 1
SAC+++A'	Action to add content
IFT+4:19+ F 31MAY13 OOL SIN 0900 1500 TZ 5 HK SFLY 582 81'	History item system-specific details
TVL+310513::310513+OOL+SIN+TZ+0005:S'	Added item was flight TZ005 in S class
RPI+1+HK'	For a party of 1
UNT+50+00102181551362'	
UNE+1+00102181551362'	
UNZ+1+00102181551362'	

APPENDIX C – PADIS EDIFACT Message Processing - Background for PNRGOV Users

1 INTRODUCTION

This document is intended to provide guidance to airlines, System Suppliers and States who are implementing the PNRGOV message. The information contained in this document should be utilized in conjunction with the current PNRGOV implementation Guide. This document is a living document and will be updated for any future requirements / principles as agreed by the Working Group.

The PNRGOV message is designed to comply with States' Legislation for the provision of PNR data from Carriers. Its receipt and processing by a State may be acknowledged with an ACKRES message. However there are certain cases when it is appropriate to return a CONTRL message.

1.1 Purpose

The purpose of this document is to clearly define the recommended method for handling the interchange of PNRGOV messages including the use of ACKRES and CONTRL messages for the acknowledgement of message transfer and processing status.

1.2 Scope

The scope of this document is to provide relevant information in conjunction with the implementation guide to ensure a consistent approach to implementation. It will also identify, where necessary, any bilateral agreements that need to be implemented for the usage of the PNRGOV, ACKRES and CONTRL messages.

1.3 Background

The PNRGOV message has been developed under the auspices of the PADIS Board. The message structure and the contents of the message are designed to provide a consistent approach for all Carriers required to provide PNR information to States. In order to provide a mechanism to acknowledge receipt and/or processing of a message, the ACKRES message has also been defined. This message may be sent by a State to a Carrier by bilateral agreement.

The basis for the PNRGOV messages is PADIS EDIFACT, which in turn is based on UN EDIFACT (ISO 9735). PADIS EDIFACT also defines the CONTRL message as a mechanism that can be used to acknowledge receipt and indicate processing status of a message interchange.

This document discusses common use of CONTRL as opposed to functional response messages (e.g. ACKRES) in the airline industry, and makes recommendations for handling PNRGOV interchanges in a consistent manner.

1.4 References

PADIS Codeset Directory
PADIS Message Standards
ISO 9735

1.5 Assumptions and Constraints

1.5.1 Assumptions

It is assumed that PNRGOV processing will be handled largely asynchronously based on exchange with a queuing technology. However other technologies may be used for message exchange (transport), such as web services, IATA Host-to-Host, etc. It is equally possible that completion of the message exchange indicates only receipt of the message, or also its processing.

Any technology used for transport of messages may or may not provide message delivery assurance / acknowledgement outside of the EDIFACT layer. Any such delivery assurance provided by those layers may be acceptable (as per bilateral agreement between the Carrier and the State) and is beyond the scope of this document.

If message interchange acknowledgement and processing status is desired in lieu of or in addition to that provided by the underlying transport, it is recommended that it is handled as described in this document.

1.5.2 Constraints

- The protocol for message delivery depends on the capability of the States and Carriers. The protocol to be used is agreed on a bilateral basis.

- The software architecture used by each Carrier and State may vary in its handling of each layer of the EDIFACT messages. Variances in architectures may contribute to an organization's ability to generate specific acknowledgement types.
- Individual State legislation may drive specific functional requirements for handling of acknowledgements. Acknowledgment of *Receipt* may or may not indicate Successful *Processing* of the message. Definitions of Receipt, Processing Status and Rejection must be clear such that the Carrier can react appropriately.

1.6 Document Overview

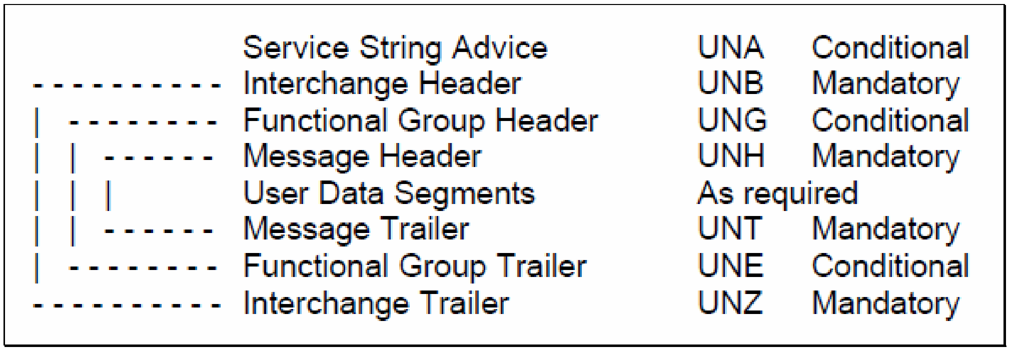
This document addresses 3 key areas for the acknowledgement of receipt/processing. These are:

1. **EDIFACT Envelope Structure** – This section provides a brief overview of the EDIFACT envelope structure and the purpose of each envelope.
2. **Parsing & Processing Steps** – This section identifies the steps that should be taken to parse and process an incoming EDIFACT message as the envelopes are opened.
3. **Acknowledgement Recommendations –** This section provides recommendations for acknowledgement of receipt or rejection and processing status using CONTRL and ACKRES.

2 EDIFACT Envelope Structure

ISO 9735 defines EDIFACT message structure as a combination of:

1. A conditional **Service String Advice (UNA)** - a fixed length structure required at the beginning of the message only if non-standard delimiter characters are used.
2. **Service Segments (UNB-UNZ)** – a set of segments used to envelope the interchange itself, functional groups of messages within an interchange, and each individual message.
3. **User Data Segments** – functional segments as required comprising each individual message.



```
                       Service String Advice       UNA   Conditional
- - - - - - - - - -    Interchange Header          UNB   Mandatory
|   - - - - - - - -    Functional Group Header     UNG   Conditional
|   |   - - - - - -    Message Header              UNH   Mandatory
|   |   |              User Data Segments          As required
|   |   - - - - - -    Message Trailer             UNT   Mandatory
|   - - - - - - - -    Functional Group Trailer    UNE   Conditional
- - - - - - - - - -    Interchange Trailer         UNZ   Mandatory
```

Figure 1 - EDIFACT Interchange Structure

2.1 The Interchange Envelope

An Interchange begins with an Interchange Header (UNB) segment and ends with an Interchange Trailer (UNZ) segment, providing the outermost envelope in an EDIFACT interchange. The purpose of the Interchange Envelope is to identify the transmission attributes of the entire interchange unit. These attributes include:

- The Syntax and Version of the Interchange
- The sender and receiver of the interchange
- The date/time of preparation
- An Interchange Control Reference

The interchange itself may contain multiple independent messages (using the same syntax and version), which may be placed into one or more interchange groups.

For PNRGOV, each interchange is expected to contain a single message. Therefore no message group identification is required.

2.2 The Functional Group Envelope

Within an interchange, multiple individual messages may be grouped by function. When such grouping is required, the Functional Group Header (UNG) and Functional Group Trailer (UNE) form an envelope around a related group of individual messages. Since PNRGOV indicates only a single message per interchange, grouping is not required. Therefore these segments are not used.

2.3 The Message Envelope

Each message in an interchange consists of a set of functional data segments wrapped in a Message Envelope.

- The Message Header segment (UNH) precedes the first functional segment in the message and indicates the message type (e.g. PNRGOV), version and release (e.g. 11:1) and controlling agency (e.g. IA). It also may contain a common access reference (CARF) that can be used to communicate a relationship among messages.

- The Message Trailer segment (UNT) follows the last functional segment in the message and indicates the number of segments in the message (both functional and envelope).

3 Parsing & Processing Steps

The service segments that comprise the interchange, group and message envelopes are versioned on a separate scheme from the functional segments of the EDIFACT message. The syntax and version of the Interchange itself is contained in the UNB segment. The structure (and version) of these segments rarely changes. This allows an application receiving an EDIFACT interchange to be architected in a modular fashion in which common, non-functional logic may be used to handle the service segments and determine the type, version and release of the message(s) contained within. Once the message type, version and release have been determined, the message can be handed off to the appropriate logic module for parsing and processing of the functional segments within the message.

After receipt of the interchange from the chosen transport layer, the receiving handler should process the interchange in the following manner:

1. Determine if the interchange begins with a Service String Advice (UNA) segment.

   This segment is used by a sender to define the characters selected for use as delimiters and indicators in the rest of the interchange that follows (ISO 9735). If present, the 6 characters following the UNA tag should be used by the receiving handler to parse the interchange. If not present, default delimiters and indicators should be used.

   a. If there is an error processing the UNA and the receiving handler can identify the sender of the interchange based on the transport, configuration or other means, it may elect to return a CONTRL message to the sender. This CONTRL message would have to be quite generic (or hard-coded), as no part of the interchange could actually be parsed or interpreted in order to properly populate a corresponding CONTRL.

   b. Note: Once the effective delimiter set has been determined, the handler may elect to parse the entire interchange into a collection of segments, composites and elements. This allows validation of the envelopes as well as the general structure of the interchange before invocation of functional logic.

2. Using the selected (default or modified by UNA) delimiters, parse the Interchange Header (UNB).

   a. If there is a failure to parse a valid UNB, and the receiving handler can identify the sender of the interchange as mentioned in 1.a. above, it may elect to return a CONTRL message to the sender.

   b. Upon successful parsing of the UNB, the receiving handler can identify the interchange syntax and version, interchange sender, interchange receiver, interchange generation date/time, and Interchange Sender's reference. These values may be validated against those obtained from configuration or transport layer, or used to identify the sending and receiving systems for the interchange in order to continue processing.

3. Continue parsing the Functional Group Header (UNG).

   Although the PNRGOV implementation guide and message structure does not indicate the use of the Functional Group envelope, the interchange headers may be processed on a messaging tier that handles various incoming message types, others of which do use functional group headers.

   a. If this is the case, then the handler may use values obtained from this functional group header for further validation/processing.

   b. If this is not the case, then the application may choose to ignore the UNG, or may choose to generate a CONTRL message if one is encountered. When generating a CONTRL message in this case, the Interchange envelope in the CONTRL message should contain values corresponding to the Interchange envelope from the message received.

4. Continue parsing the Message Header (UNH).

   This header will provide information about the message payload including its type (e.g. PNRGOV) version and release (e.g. 11:1) as well as a common access reference. The handler should determine that the message type, version and release are supported and message-type-specific handlers are available. It may also optionally determine if the message type, version and release are expected from this interchange sender for this interchange recipient (obtained from the UNB).

   a. If the specific message type cannot or should not be processed or is otherwise unexpected, a CONTRL message should be returned to the sender indicating the reason the message is being rejected (e.g. version not supported, etc.)

5. Continue parsing the functional segments comprising the message.

   A handler for the message-type-specific segments should be invoked on each segment encountered until the Message Trailer (UNT) segment. Some architectures include message-specific parsing and structural validation at the EDIFACT handler tier, while others defer that processing until a later phase or on another tier.

   The UNT contains an element indicating the number of segments in the message (inclusive of UNH/UNT). This value may be validated against the number of functional segments received.

   a. Any errors in locating the UNT or *parsing* the functional segments due to delimiter/structural issues should result in a CONTRL message being returned to the interchange sender. Code set 0085 includes a number of specific errors that may be returned in the UCI and UCM segments. The UCI and UCM segments also include elements in which the context of the error may be specified (e.g. tag name and ordinal number of the segment having in which the error was encountered, etc.).

   b. Please note that a CONTRL is not generally appropriate for indication of ***functional*** errors encountered while processing the functional segments of message. If functional processing of the message is invoked in-process, functional errors should return a functional response (e.g. ACKRES). Errors in validation of syntax or structure (e.g. data type or field length violations) of the functional segments may result in a CONTRL.

6. Hand the parsed data to the functional processing modules appropriate for the message.

   This hand-off may be in-process or may be via a message queuing technology, etc. as architected by the State.

   a. These modules may perform detailed transformation of the data into internal structures, and if they encounter a ***structural*** error, may also return a CONTRL message to the interchange sender.

   b. If no structural error is encountered, a CONTRL message indicating receipt or successful processing of the interchange *may* be returned to the sender. However, this is not common practice if a functional response message is available (ACKRES). It should only be considered if the EDIFACT handler tier is handing off the message content for later processing by the application, and a more immediate confirmation of receipt is required. In this case, the CONTRL message should only be considered as acknowledgement of *receipt*, not of *processing*.

   c. If no structural error is encountered and functional processing is expected to commence and complete within a reasonable time frame, an ACKRES may be returned to the sender as a result of processing. The ACKRES should indicate the processing status, such as having completed successfully or that the message was rejected due to one or more specific errors.

   d. The State may elect to send no acknowledgement at all. This may be appropriate if it has established other means by which acknowledgement and status may be communicated (e.g. email, web site, etc.)

7. Process the next message in the interchange.

   For PNRGOV, only one message per interchange is expected. However an inbound interchange being processed by a common handler may contain additional messages.

8. Process the next functional group in the interchange.

   For PNRGOV, functional groups are not applicable or expected. However an inbound interchange being processed by a common handler may contain functional groups.

9. Wrap-up processing of the Interchange.

   When all messages in all functional groups have been successfully parsed and handed off for processing, interchange processing is complete.

   a. Generation of a CONTRL message indicating an error may have been already performed due to one of the error conditions mentioned above.

   b. Generation of a CONTRL message indicating receipt and/or processing of the message may be performed, but is not generally used for PADIS.

4 Acknowledgement Recommendations

PADIS standards deal with interactive messaging, in which a request/response pair of messages are exchanged synchronously. The requesting application transmits the request message and synchronously waits for a response message or an eventual time-out. It is always preferred to receive some form of response message rather than to require the application to wait for a timeout period to expire.

Generally speaking, if there are any errors encountered in processing the service segments, the non-functional logic can produce a CONTRL message indicating that there was a failure to hand the functional content off to the functional logic module. However, if there are no errors in processing the envelope and the message is handed off to the functional logic, then it is the responsibility of the functional logic to return an appropriate response message. In the case of PNRGOV, that functional response message would be ACKRES.

While it is possible to use a CONTRL message to positively acknowledge receipt and/or processing of a PNRGOV message, this practice is not commonly used in PADIS, especially when a functional response message is available. This is particularly true in interactive scenarios since a 1:1 request/response pair is expected. If a CONTRL is sent as a positive response, then the requesting system would have to receive a 2nd message containing the functional results from the processing application. This practice results in redundant processing, extra I/O, increased bandwidth usage, etc.

PNRGOV, however, may not be handled as an *interactive* exchange. A State may not elect to send a functional response in the form of an ACKRES, but still wish to convey acknowledgement of *receipt* of the PNRGOV message above and beyond any acknowledgement provided by the transport layer. If the acknowledgment of receipt is strictly from a State's messaging tier, use of CONTRL may be acceptable. However if acknowledgement of receipt is from the State's application tier, use of ACKRES is still recommended.

4.1 Types of Acknowledgements

It is generally accepted that an interchange sender (Carrier) wishes to receive, and States wish to send message acknowledgements in order to track processing and ensure interchanges are being processed as expected. However, there are two main types of events that may be acknowledged. Acknowledgement of *receipt* of a message indicates that a State has received the message for processing. Acknowledgement of *Processing* of the message implies receipt but also indicates the status of functional processing.

4.1.1 Acknowledgement of Receipt

Acknowledgement of receipt of a message (or interchange) indicates a State has received the Carrier's message. However the architecture of the State's system may take several forms. Therefore it is possible for receipt to need further clarification. Receipt could mean a message has simply arrived at the facility, has passed validation of the envelope and queued for functional processing, or has actually been received by the destination application. Any or all of these status values may be of interest to the Carrier and State based on bilateral agreement.

4.1.2 Acknowledgement of Processing

Acknowledgement of Processing indicates that the State has processed the Carrier's message. The acknowledgement itself may indicate a processing status (e.g. success, warning, or failure). In order to be processed, the message has to have been first received by the application. Therefore an acknowledgement of processing implies receipt of the message. However, the definition of *processing* itself may be ambiguous. In this document, *processing* means any functional processing performed by the State on the data received in the PNRGOV message.

4.2 Recommendations

The following table summarizes the recommendations for acknowledgement of receipt and processing in various scenarios. Final decisions are up to each Carrier and State and should be bilaterally agreed upon. However these recommendations provide guidance to Carriers and States looking to implement acknowledgment procedures.
Please note that although architectures vary, conceptually the EDIFACT message must first be received, parsed, recognized and structurally validated. Then the message must be functionally processed. Although some States may choose to do this in a single application, while others may separate the work, the table below separates the two functions logically. Whichever application is handling the functions described in the second column of the table should generate the recommended response.

Acknowledgement Type	Processing Phase	Status	Recommendation
Receipt	Transport	All	Facilities available in the selected transport layer (e.g. WebSphere MQ, S/FTP, Web Service, etc.) can be used to acknowledge receipt of a message interchange by the State. Such acknowledgment indicates only that the message has been received. It does should not imply that it is valid (can be parsed or processed) or has been parsed or processed.
Receipt	Message Router / EDIFACT Handler	Invalid Structure (cannot be parsed)	• A CONTRL message should be returned to the message sender assuming the sender can be determined. • To the extent possible, include any information from the service segments of the received message in the service segments of the CONTRL • Populate the UCI with the most appropriate ACTION,CODED and SYNTAX ERROR, CODED values from code sets 0083 and 0085 respectively. • If the Message Header (UNH) of the message received was successfully parsed, include a UCM segment with S009 populated accordingly from the UNH of the received message. Populate elements 0083 and 0085 as appropriate based on the code sets. Generally 0083 should contain a value of 4 (rejected). If possible also include: • The tag of the invalid segment (e.g. TVL) in element 0013 o The position of the invalid element or composite in S011 • Return of a CONTRL message with a value of 4 in element 0083 of a UCI or UCM indicates that the destination application has not received or processed the message.
Receipt	Message Router / EDIFACT Handler	Invalid Request or Interchange partner	• If the Interchange and Message envelopes are able to be parsed, but the message type or version is not supported or authorized for the interchange partner, a CONTRL message should be returned. This condition should only occur due to a system misconfiguration or disagreement between Carrier and State. • Populate the service segments of the CONTRL based on the values contained in the service segments of the received message • Include a UCI segment containing the most appropriate values for elements 0083 and 0085. The UCI should indicate Interchange-level errors, if any. These include invalid interchange recipient or sender. • Include a UCM segment containing S009 populated based on the corresponding fields from the UNH of the message received. Populate elements 0083 and 0085 as appropriate to indicate message-level errors. These include any syntax or version errors, invalid control totals, etc. • The UCM should contain a value of 4 in element 0083, indicating that the message has been rejected and not processed by the application.

Receipt	Message Router / Handler	Delivered to Application	• If the State's architecture separates the message router from the processing application, and business process dictates that the State's router should acknowledge that the message has been received and forwarded to the application, a CONTRL message should be returned to the sender. • Populate the service segments of the CONTRL based on the values contained in the service segments of the received message. • Include a UCI segment with element 0083 populated with the value 8 – Interchange received. Element 0085 should not be populated. • Include a UCM segment containing S009 populated based on the corresponding fields from the UNH of the message received. Element 0083 should be populated with a 7 (or 8), and element 0085 should not be populated. Note: This procedure should be considered an exception case, as a functional response message (ACKRES) upon completion of functional processing is preferred. (See next item.)
Receipt	Functional Processing (Destination Application)	Success	• Once the inbound message has been handed off to the application, an application-level acknowledgement is recommended. The application should return an ACKRES to the sender to acknowledge receipt of the message. • The service segments of the ACKRES should be populated based on the service segments of the PNRGOV for which it is associated. This includes echo back of the Common Access Reference (CARF) in element 0068 • Populate the MSG Segment as follows: o Element 1225 in Composite C302 should contain 23 to indicate it is an ACKRES o Element 4343 should contain a value of 2 to indicate the message has been received but not yet processed.
Processing Status	Functional Processing (Destination Application)	Successfully Completed	• Once functional processing has begun on the inbound message, an application-level response is recommended. The application should return an ACKRES to the sender to indicate the processing status. • The service segments of the ACKRES should be populated based on the service segments of the PNRGOV for which it is associated. This includes echo back of the Common Access Reference (CARF) in element 0068 • Populate the MSG Segment as follows: o Element 1225 in Composite C302 should contain 23 to indicate it is an ACKRES o Element 4343 should contain a value of 3 to indicate the message has been successfully processed.

Processing Status	Functional Processing (Destination Application)	Not Processed	• If the destination application determines that the message does not require processing, an ACKRES response should be generated. • The service segments of the ACKRES should be populated based on the service segments of the PNRGOV for which it is associated. This includes echo back of the Common Access Reference (CARF) in element 0068 • Populate the MSG Segment as follows: o Element 1225 in Composite C302 should contain 23 to indicate it is an ACKRES o Element 4343 should contain a value of 7 to indicate the message has been received, but not processed. • Optionally, an ERC segment may be included if an appropriate reason for not processing is defined in code set 9321. • Note: This status may not be applicable and the State may only choose to return an Error status.
Processing Status	Functional Processing (Destination Application)	Error / Rejected	• If the destination application determines that the message cannot be processed, an ACKRES response should be generated. • The service segments of the ACKRES should be populated based on the service segments of the PNRGOV for which it is associated. This includes echo back of the Common Access Reference (CARF) in element 0068 • Populate the MSG Segment as follows: o Element 1225 in Composite C302 should contain 23 to indicate it is an ACKRES o Element 4343 should contain a value of 8 to indicate the message has been received and rejected. • One or more ERC segments should be included with appropriate reason(s) for rejection as defined in code set 9321.

5 Examples

Scenario	Message	Sample Content
Not able to parse envelope	CONTRL	UCI+00000000000000+XX+YY+4+18
Able to parse UNB/UNH, Interchange sender XX is invalid or unexpected.	CONTRL	UCI+99999999999999+XX+YY+4+23 UCM+1432+PNRGOV:11:1:IA+4
Message/version not supported	CONTRL	UCI+99999999999999+XX+YY+8 UCM+1432+PNRGOV:93:2:IA+4+2
Parsing error, functional segments out of order (e.g. found an ABD segment when not expected)	CONTRL	UCI+99999999999999+XX+YY+8 UCM+1432+PNRGOV:93:2:IA+4+15+ABD
Received and queued by message router for functional processing, which may be delayed	CONTRL	UCI+99999999999999+XX+YY+8 UCM+1432+PNRGOV:93:2:IA+7
Received by functional processing logic	ACKRES	MSG+:23+2
Received by functional processing logic, but will not be processed	ACKRES	MSG+:23+7
Successfully processed	ACKRES	MSG+:23+3
Error in processing / rejected (e.g. invalid departure date)	ACKRES	MSG+:23+8 ERC+102

JOINT COMMENTS OF
AIRLINES FOR AMERICA,
THE INTERNATIONAL AIR TRANSPORT ASSOCIATION,
THE REGIONAL AIRLINE ASSOCIATION, AND
THE NATIONAL AIR CARRIER ASSOCIATION

Docket CDC-2020-0013

ATTACHMENT 29

Air Transport & Travel Industry

Message Modifications: Approved Revision Process
PNRGOV

Version 12.1.

Date 1 August 2012

Montreal - Geneva

Version	Description of Change	Author	Date
11.1	Initial Publication of document. Numbering corresponds to EDIFACT version message it is based upon.	M. Zitkova	25 Jul 11
12.1	Changed the version number to match the new release of the Implementation Guide	M. Zitkova	30 Jul 12

PNRGOV Message Modifications: Approved Revision Process

Under an agreement between IATA and the World Customs Organization (WCO), maintenance of the PNRGOV message format, and control over the authorization of modifications to that message structure, will be assumed by the WCO. Coordination of actual amendments of the message structure itself will fall under the remit of the WCO API Contact Committee, which meets normally once or twice per year.

The API Contact Committee is currently chaired by Ed Broekema (NL), and comprised of representatives from the US, the UK, Canada, the Netherlands, ICAO and IATA, as well as interested States.

PNRGOV is not a UN/CEFACT approved message. Instead, the PNRGOV EDIFACT message is designed based on the IATA PADIS Message Standard Directory and its associated code sets in accordance with ISO 9735 syntax rules and UN/EDIFACT interactive message design rules. As a result, IATA PADIS will administer the physical message modification process itself, in accordance with the WCO DMR approval process and based upon the WCO API Contact Committee's direction.

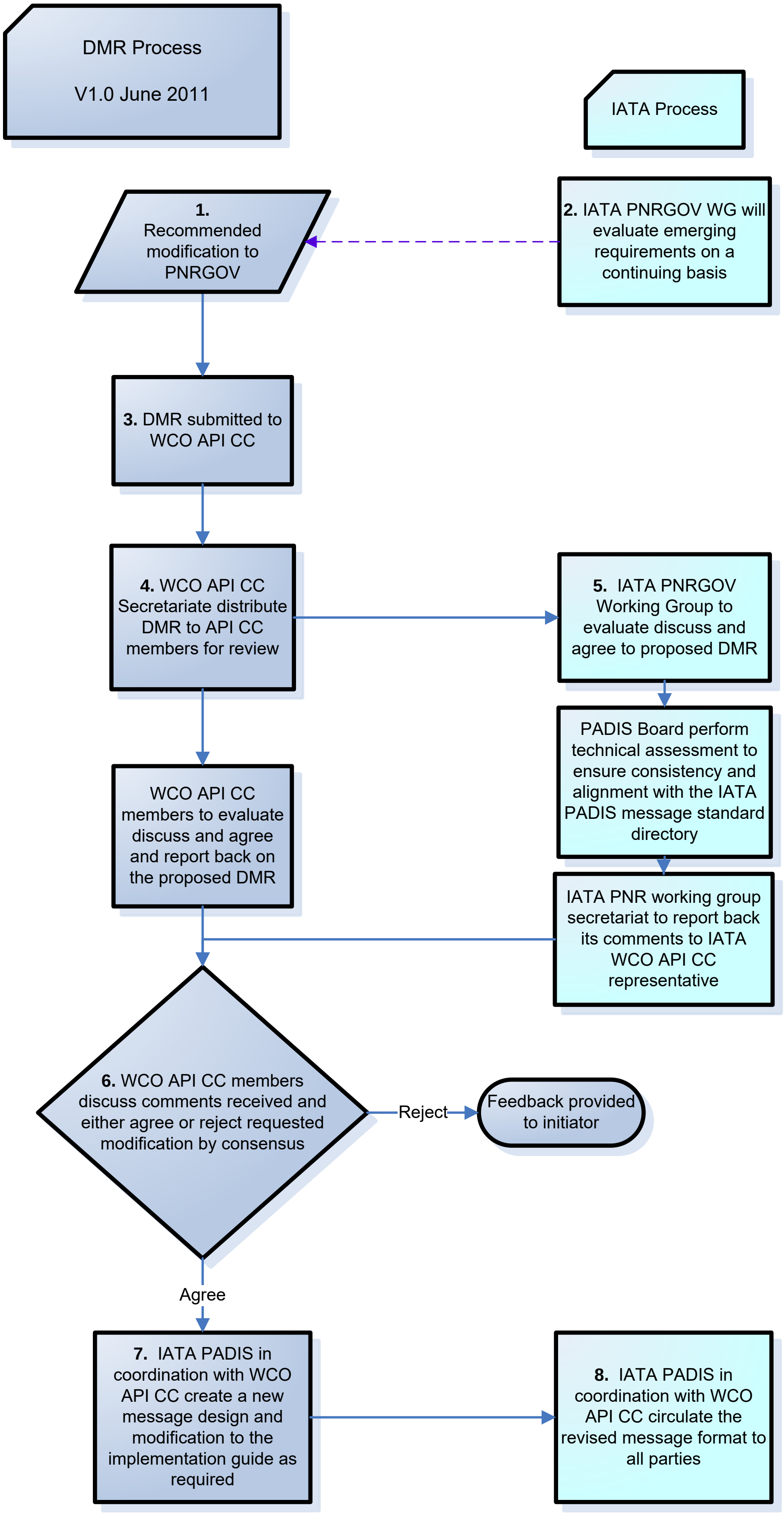

DMR Process
V1.0 June 2011
IATA Process
1. Recommended modification to PNRGOV
2. IATA PNRGOV WG will evaluate emerging requirements on a continuing basis
3. DMR submitted to WCO API CC
4. WCO API CC Secretariate distribute DMR to API CC members for review
5. IATA PNRGOV Working Group to evaluate discuss and agree to proposed DMR
PADIS Board perform technical assessment to ensure consistency and alignment with the IATA PADIS message standard directory
WCO API CC members to evaluate discuss and agree and report back on the proposed DMR
IATA PNR working group secretariat to report back its comments to IATA WCO API CC representative
6. WCO API CC members discuss comments received and either agree or reject requested modification by consensus
Reject
Feedback provided to initiator
Agree
7. IATA PADIS in coordination with WCO API CC create a new message design and modification to the implementation guide as required
8. IATA PADIS in coordination with WCO API CC circulate the revised message format to all parties

Figure 1: Amendment process

Amendment Process:

1. Any interested party may recommend modifications to the PNRGOV message structure, by use of the existing WCO Data Modification Request, or (DMR), process.

2. The IATA PNRGOV Working Group will evaluate the existing PNRGOV message on a regular basis and develop recommendations for modifications as conditions or emerging requirements warrant.

3. DMR's, once completed by the request originator, would be submitted to the WCO API Contact Committee secretariat via a WCO Member. Currently only WCO Members are permitted to initiate a request, except in exceptional cases where the WCO API CC Secretariat can raise a DMR on behalf of IATA. It is expected that a WCO Member who is part of the IATA PNRGOV Working Group would submit the request on behalf of the Working Group members as required.

4. Upon receipt of an appropriately detailed DMR form, the WCO API Secretariat would then distribute the request to all members of the API Contact Committee for their review ahead of the next scheduled meeting, as well as to the IMSC for the purposes of ensuring the request and the suggested formats for changes to the IATA PADIS PNRGOV EDIFACT message are consistent with UN/EDIFACT construction and conventional use from a technical perspective.

5. The IATA WCO API CC Representative will forward the details of any proposed modifications to the IATA PNRGOV Working Group secretariat for review. All proposed changes will be evaluated, discussed and agreed within the IATA PNRGOV Working Group. This review would include a technical assessment by the PADIS Board to ensure consistency and alignment with the IATA PADIS Message Standard Directory. The IATA PNRGOV Working Group secretariat will report back its comments to the IATA WCO API CC representative.

6. The WCO API Contact Committee, taking into account comments received from various interested parties and the results of the IMSC and the PNRGOV WG/IATA PADIS Board review would then discuss the matter and would either agree with or reject the requested modification by consensus.

7. If agreed by the WCO API Contact Committee, and wholly supported by current UN/EDIFACT construction rules (i.e. consistent with syntax) and the IATA PADIS Standard Message Directory (i.e. elements already approved, etc.), the IATA PADIS group in coordination with the WCO API CC (through the WCO Secretariat) would generate a new message design with modifications to the Message Implementation Guide as required.

8. The revised message format would be circulated to all parties, and in particular with IATA to ensure that a new message release and effective date is coordinated among all parties.

JOINT COMMENTS OF
AIRLINES FOR AMERICA,
THE INTERNATIONAL AIR TRANSPORT ASSOCIATION,
THE REGIONAL AIRLINE ASSOCIATION, AND
THE NATIONAL AIR CARRIER ASSOCIATION

Docket CDC-2020-0013

ATTACHMENT 30

Get Email Updates | Contact Us | Comunicarse con Nosotros

Search

About CBP Newsroom Travel Trade Border Security Careers

HOME >> TRAVEL >> TRAVEL INDUSTRY PERSONNEL

Travel
- Advisories and Wait Times
- Biometrics
- Clearing CBP
- Customer Service
- For Canadian Citizens and Mexican Nationals
- For International Visitors
- For Travel Industry Personnel
  - APIS: Advance Passenger Information System
    - Final Rule Requirement
  - Carrier Liaison

Advance Passenger Information System (APIS) Final Rule Requirement

In response to industry concerns regarding the October 4, 2005 APIS Final Rule implementation date, CBP has developed an implementation plan of informed and enforced compliance that balances compliance goals with flexibility built in to aid carriers demonstrating a good faith effort to comply. CBP is already working with carriers individually to address the October 4, 2005 deadline. During the implementation process, CBP may employ both informed (outreach) and enforced (penalties) compliance as appropriate; however, even once the enforced compliance stage is reached, CBP has mechanisms in place to work with and mitigate penalties assessed against carriers on a case-by-case basis. CBP already has designated, national account managers who work directly with carriers on APIS implementation and compliance issues on a full-time basis.

- Carriers and other affected parties who are already doing so, should continue to utilize resources such as their industry associations and CBP APIS national account managers to obtain up-to-date information on APIS compliance. CBP is also posting the full text of APIS Final Rule for easier reference.
- The APIS Final Rule implementation plan may be described broadly as follows:
  - The first stage will focus on achieving technical compliance - the ability to transmit data timely using the prescribed format and data interchanges;
  - The second stage will focus on achieving technical and content (complete and accurate data) compliance; and
  - The third stage will require full technical and content compliance.

Address

- CBP is required to collect address information by the Enhanced Border Security and Visa Entry Reform Act of 2002.

Program

Private Aircraft

For U.S. Citizens/Lawful Permanent Residents

Pleasure Boats and Private Flyers

Preventing International Child Abduction

Search Authority

Trusted Traveler Programs

- Address information, in the larger context of passenger information, is central to risk assessment and targeting.

Carriers should make every effort to ensure the address information they collect and submit to CBP via APIS, is identical to the U.S. destination address declared to CBP by the passenger upon application for entry (for I-94 purposes). Carriers should also make every effort to ensure the address submitted in the APIS manifest appears to be a valid address.

Below is clarification on what information should be included on the manifest for those passengers who are: (1) visiting the US; (2) joining a cruise ship; (3) picking up a rental car or; (4) those not knowing their address while in the United States:

- Visiting the U.S., and the **passenger has a known address**.
  Example:
  Street Address: 1300 Pennsylvania Ave
  City: Washington
  State: D.C.
  ZIP Code: 20229

  - **Transit to a cruise ship**: CBP will accept, "transit to Cruise Line and Vessel/Cruise Name" in the address field. The city of cruise embarkation should be included.
    Example:
    Street Address: Transit to MV Princess of the Seas
    City: Miami
    State: FL
    ZIP Code: 99999

  - **Rental car pickup**: CBP will accept if the first night stay is **NOT known**, the general itinerary of the traveler. If for example the traveler will be touring, the general itinerary city, state and zip code (if known).
    Example:
    Street address: Touring the Grand Canyon
    City: Grand Canyon
    State: AZ
    ZIP Code: 99999

  - Hotel: For those passengers who are **destined to a hotel and do not know the street address** for the hotel, CBP will accept, Hotel name (if known), City (of first night stay), State. ZIP Code should be provided if known.
    Example:
    Street Address: Downtown Hotel Hilton - (be as specific as possible)

City: Houston
State: Texas
ZIP Code: 99999

CBP will continue to conduct outreach with the carrier organizations and post information to cbp.gov regarding the phased implementation schedule and the requirements for the address field.

Last modified: May 23, 2014

Share This Page.

JOINT COMMENTS OF
AIRLINES FOR AMERICA,
THE INTERNATIONAL AIR TRANSPORT ASSOCIATION,
THE REGIONAL AIRLINE ASSOCIATION, AND
THE NATIONAL AIR CARRIER ASSOCIATION

Docket CDC-2020-0013

ATTACHMENT 31

Electronic Advance Passenger Information System

CUSTOMS & BORDER PROTECTION
U.S. DEPARTMENT OF HOMELAND SECURITY

News Legal Notices [!]

Help

< BACK

What is eAPIS?

The Electronic Advance Passenger Information System (eAPIS) is a U.S. Customs and Border Protection (CBP) Web-based application that provides for the collection of electronic traveler manifest information for international travel both into and out of the United States. eAPIS collects and transmits electronic manifests to CBP's Advance Passenger Information System (APIS).

back to top

How do I enroll in eAPIS?

To participate in eAPIS, you must first enroll by following these simple steps:

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1</td><td>Access the eAPIS Welcome page at https://eapis.cbp.dhs.gov; select <b>Enroll</b>.</td></tr>
<tr><td>2</td><td>Agree to the Terms and Conditions for eAPIS; select <b>Next</b>.</td></tr>
<tr><td>3</td><td>Select the type of account you desire, either Commercial or Private; select <b>Next</b>.</td></tr>
<tr><td>4</td><td>Enter the information requested, including the person who will be the Point of Contact regarding manifest submissions.</td></tr>
<tr><td>5</td><td>Create a password that:
<ul>
<li>starts with a number and</li>
<li>is between eight and twelve characters in length and</li>
<li>contains at least one of the following special characters:</li>
</ul>
<table>
<tr><th>Name</th><th>Character</th></tr>
<tr><td>Tilde</td><td>~</td></tr>
<tr><td>Exclamation Point</td><td>!</td></tr>
<tr><td>At</td><td>@</td></tr>
<tr><td>Number</td><td>#</td></tr>
</table>
</td></tr>
</table>

Dollar	$
Percent	%
Caret	^
Ampersand	&
Asterisk	*
Open Parenthesis	(
Close Parenthesis	)
Hyphen	-
Underscore	_
Plus	+
Equals	=
Open Curly Brace	{
Close Curly Brace	}
Vertical Bar	|
Backslash	\
Open Square Bracket	[
Close Square Bracket	]
Colon	:
Semi Colon	;
Forward Slash	/
Question Mark	?
Period	.

No character can be repeated consecutively more than two times.

6	Re-enter your password; select **Next**.
7	Review your entries; select **Complete Enrollment** to submit your enrollment request.

After successfully completing the eAPIS enrollment application, you will:

1. Receive an email with your sender ID and activation key. **Your confirmation e-mail will not arrive immediately**.
2. Return to the eAPIS Web site. Enter your sender ID and password, then select **Log In**.

Be sure that you provide the correct contact information when you enroll in eAPIS. The activation email message is sent to the email address you provide as the primary Point of Contact. If you do not receive your activation email, contact the system administrator for assistance.

Note: Your activation email may not arrive immediately. Be sure that you have provided the correct contact information when you enrolled with eAPIS. The activation email message is sent to the email address you provided for the primary point of contact.

back to top

How do I know whether to choose a Commercial or Private Aviation eAPIS account?

CBP definitions of private and commercial aircraft are found in Title 19 of the Code of Federal Regulations, section 122.1:

> (d) Commercial aircraft. A "commercial aircraft" is any aircraft transporting passengers and/or cargo for some payment or other consideration, including money or services rendered.
>
> (h) Private aircraft. A "private aircraft" is any aircraft engaged in a personal or business flight to or from the U.S. which is not:
>
> 1. Carrying passengers and/or cargo for commercial purposes;
> 2. Leaving the U.S. carrying neither passengers nor cargo in order to lade passengers and/or cargo in a

foreign area for commercial purposes; or

3. Returning to the U.S. carrying neither passengers nor cargo in ballast after leaving with passengers and/or cargo for commercial purposes;

Select the type of account you need according to the criteria described above. Some users may need both account types.

back to top

What if I don't receive the activation email after I enroll in eAPIS?

If you do not find the activation email in your inbox, check your junk email in case it was blocked by your spam settings. The activation email will come from donotreply@dhs.gov with the subject line "You have successfully enrolled."

For this eAPIS Account Type...	You should receive the activation email within...	If you do not receive an activation email...	Then...
Commercial	5-7 days	after 5-7 days	contact the system administrator for assistance
Private Aviation	24 hours	within 24 hours	contact the system administrator for assistance

back to top

How do I log in to eAPIS?

Enter your Sender ID and password in the designated boxes on the eAPIS Welcome page. If this is your first time logging in with this Sender ID, you will be prompted to enter an Activation Key. The Activation Key is included along with your Sender ID in the enrollment confirmation email message.

The Activation Key is valid for a period of 30 days from the date of your email confirmation message. If you do not activate your account within this timeframe, your Activation Key will expire and you will have to re-enroll in eAPIS.

If you do not have a working sender ID or password, you will need to enroll with eAPIS. Select **Enroll** on the eAPIS Welcome page.

back to top

What if I have lost my Activation Key, or if it has expired, or I am unable to activate my account?

If you have lost your activation key, or if it has expired prior to activating your account, or if it has expired prior to activating your account, or you are unable to activate your account, e-mail the system administrator for assistance.

back to top

What if I have lost my Sender ID?

If you have lost your Sender ID, e-mail the system administrator for assistance.

back to top

What if I have forgotten my password?

If you forget your password, you can reset it from the eAPIS Welcome page. Resetting your password de-activates your eAPIS account. You will not be able to access eAPIS until you receive your new Activation Key and reactivate your account.

Follow these steps to reset your eAPIS password:

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1</td><td>From the eAPIS Welcome page, select the <b>Reset your password</b> link. The Reset Password page appears.</td></tr>
<tr><td>2</td><td>Enter your Sender ID and primary contact e-mail address.</td></tr>
<tr><td>3</td><td>Enter your new password. Your password:
<ul>
<li>must start with a number and be between eight and twelve characters in length, and</li>
<li>must contain at least one of the following special characters:
<table>
<tr><th>Name</th><th>Character</th></tr>
<tr><td>Tilde</td><td>~</td></tr>
<tr><td>Exclamation Point</td><td>!</td></tr>
<tr><td>At</td><td>@</td></tr>
<tr><td>Number</td><td>#</td></tr>
<tr><td>Dollar</td><td>$</td></tr>
<tr><td>Percent</td><td>%</td></tr>
<tr><td>Caret</td><td>^</td></tr>
<tr><td>Ampersand</td><td>&</td></tr>
<tr><td>Asterisk</td><td>*</td></tr>
<tr><td>Open Parenthesis</td><td>(</td></tr>
<tr><td>Close Parenthesis</td><td>)</td></tr>
<tr><td>Hyphen</td><td>-</td></tr>
<tr><td>Underscore</td><td>_</td></tr>
<tr><td>Plus</td><td>+</td></tr>
<tr><td>Equals</td><td>=</td></tr>
<tr><td>Open Curly Brace</td><td>{</td></tr>
<tr><td>Close Curly Brace</td><td>}</td></tr>
<tr><td>Vertical Bar</td><td>|</td></tr>
<tr><td>Backslash</td><td>\</td></tr>
<tr><td>Open Square Bracket</td><td>[</td></tr>
<tr><td>Close Square Bracket</td><td>]</td></tr>
<tr><td>Colon</td><td>:</td></tr>
<tr><td>Semi Colon</td><td>;</td></tr>
<tr><td>Forward Slash</td><td>/</td></tr>
<tr><td>Question Mark</td><td>?</td></tr>
<tr><td>Period</td><td>.</td></tr>
</table>
</li>
<li>Cannot include your Sender ID, and</li>
<li>Cannot repeat any character consecutively more than two times.</li>
</ul>
</td></tr>
<tr><td>4</td><td>Re-enter your new password in the <b>Re-enter New Password</b> box exactly as you entered it in the previous box; select <b>Save</b>.</td></tr>
<tr><td>5</td><td><b>Remember your password because it cannot be retrieved from the system.</b></td></tr>
</table>

Using your new password:

After changing your password, you should receive an email message containing your Sender ID and a new Activation Key. To reactivate your account, log in with your Sender ID and new password. Enter your new Activation Key when prompted.

Note: The Activation Key is valid for a period of thirty days from the date on your email confirmation message. If you do not reactivate your account within this timeframe, your Activation Key will expire and you will have to contact the system administrator for assistance.

back to top

How do I change my password without having to reactivate my account?

Follow these steps to change your eAPIS password:

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1</td><td>Log in to eAPIS using your Sender ID and current password.</td></tr>
<tr><td>2</td><td>Select the <b>Update your password</b> link in the Manage Account section of the Manifest Options page.</td></tr>
<tr><td>3</td><td>Enter your new password. Your password:
<ul>
<li>must start with a number and be between eight and twelve characters in length, and</li>
<li>must contain at least one of the following special characters:
<table>
<tr><th>Name</th><th>Character</th></tr>
<tr><td>Tilde</td><td>~</td></tr>
<tr><td>Exclamation Point</td><td>!</td></tr>
<tr><td>At</td><td>@</td></tr>
<tr><td>Number</td><td>#</td></tr>
<tr><td>Dollar</td><td>$</td></tr>
<tr><td>Percent</td><td>%</td></tr>
<tr><td>Caret</td><td>^</td></tr>
<tr><td>Ampersand</td><td>&</td></tr>
<tr><td>Asterisk</td><td>*</td></tr>
<tr><td>Open Parenthesis</td><td>(</td></tr>
<tr><td>Close Parenthesis</td><td>)</td></tr>
<tr><td>Hyphen</td><td>-</td></tr>
<tr><td>Underscore</td><td>_</td></tr>
<tr><td>Plus</td><td>+</td></tr>
<tr><td>Equals</td><td>=</td></tr>
<tr><td>Open Curly Brace</td><td>{</td></tr>
<tr><td>Close Curly Brace</td><td>}</td></tr>
<tr><td>Vertical Bar</td><td>|</td></tr>
<tr><td>Backslash</td><td>\</td></tr>
<tr><td>Open Square Bracket</td><td>[</td></tr>
<tr><td>Close Square Bracket</td><td>]</td></tr>
<tr><td>Colon</td><td>:</td></tr>
<tr><td>Semi Colon</td><td>;</td></tr>
<tr><td>Forward Slash</td><td>/</td></tr>
<tr><td>Question Mark</td><td>?</td></tr>
<tr><td>Period</td><td>.</td></tr>
</table>
</li>
<li>Cannot include your Sender ID, and</li>
<li>Cannot repeat any character consecutively more than two times.</li>
</ul>
</td></tr>
<tr><td>4</td><td>Re-enter your new password in the <b>Re-enter New Password</b> box exactly as you entered it in the previous box; select <b>Save</b>.</td></tr>
<tr><td>5</td><td><b>Remember your password because it cannot be retrieved from the system.</b></td></tr>
</table>

Using your new password:

You can use your new password the next time you log in to eAPIS. Your account does not need to be re-activated.

back to top

What do I do if I get locked out of eAPIS?

The eAPIS system has a 10-minute lock-out period for mistaken password attempts. If you wait 10 minutes, the system will allow you try again.

If you have forgotten your password, you can reset it on the Welcome page. You'll then receive an Activation Key delivered to your email.

The 10-minute lock-out period still applies.

back to top

What happens if I have to log out or if eAPIS times out while I am completing my manifest?

eAPIS is designed to save manifest information within the web site while it is being entered. The manifest is automatically saved for each Sender ID while you enter data.

eAPIS is designed to log off users after 10 minutes of system inactivity. If you were in the process of building a manifest, you will be prompted to finish the Saved Manifest the next time you log in to the system. If you leave a page partially completed and you do not select NEXT, that page may not be saved the next time you log in.

back to top

How do I upload a manifest I created offline?

You can use eAPIS to upload a manifest to CBP if the file meets the following criteria:

Commercial accounts:	**Private Aviation accounts:**
Must be a text file (.txt) no greater than two megabytes.	Must be an XML file (.xml) no greater than two megabytes.
Must be in UN/EDIFACT format.	Must be in valid XML format, based on the eAPIS Private Aviation schema. You can download the schema from the Upload Manifest section of the Manifest Options page.

Follow these steps to upload a file to CBP using eAPIS:

Step	**Action for Commercial accounts**	**Action for Private Aviation accounts**
1	Select **Upload Manifest** from the Manifest Options page.	Select **Upload a General Aviation XML compliant document** from the Upload Manifest section of the Manifest Options page.
2	Select **Browse** to locate the file.	Select **Browse** to locate the file.
3	Select a file when prompted; then select **Next**.	Select a file when prompted; then select **Next**.
4	Preview the content of the file to verify that it is the correct file; then select **Submit**.	Preview the content of the file to verify that it is the correct file; then select **Submit**.

Submission Number: When your manifest data has been successfully submitted, eAPIS responds with an on-screen submission message and a submission number. Print this screen for your records and for future reference.

back to top

How can I be sure that CBP has received my traveler manifest data?

After successful submission of a new APIS manifest, eAPIS responds with an on-screen submission message and a submission number. Print this screen for your records. The submission number represents successful manifest submission; it does not confirm the manifest's accuracy, completeness, or validity.

eAPIS sends your manifest data to the CBP Advance Passenger Information System (APIS) for processing. When APIS has processed your data, an email message is sent to the email address for your primary Point of Contact. The email confirms CBP's receipt of the data transmission; it does not confirm the manifest's accuracy, completeness, or validity.

back to top

How do I contact CBP with questions regarding eAPIS?

Email the system administrator to contact CBP regarding eAPIS. Commercial carriers can contact their National APIS Account Manager directly.

If you have a...	And your Sender ID begins with...	Then email the...
Commercial Air account	APIS	Commercial Air system administrator at eapissupport@cbp.dhs.gov
Private Aviation account	APGA	Private Aviation system administrator at privateaircraftsupport@cbp.dhs.gov

back to top

Is the eAPIS application Section 508 compliant?

eAPIS is Section508 compliant and therefore accessible to everyone. Federal law mandates that government applications and web sites meet a certain level of standards to allow users to employ special technologies such as screen readers. The following design requirements have been included in the development of this application:

- Hidden navigation shortcuts
- Hidden text
- Alt text for all images
- Unique page titles
- The ability to complete the process without JavaScript enabled

For more information regarding Section508 compliance and Web accessibility, visit http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards.

back to top

JOINT COMMENTS OF
AIRLINES FOR AMERICA,
THE INTERNATIONAL AIR TRANSPORT ASSOCIATION,
THE REGIONAL AIRLINE ASSOCIATION, AND
THE NATIONAL AIR CARRIER ASSOCIATION

Docket CDC-2020-0013

ATTACHMENT 32

APPENDIX IIA

ADVANCE PASSENGER INFORMATION GUIDELINES

Appendix IIA :

Guide de mise en oeuvre du message PAXLST

(DISPONIBLE EN ANGLAIS UNIQUEMENT)

Pour les modifications apportées aux lignes directrices de mise en œuvre de message, s'il vous plaît voir la version anglaise.

WCO/IATA/ICAO PASSENGER LIST MESSAGE (PAXLST) IMPLEMENTATION GUIDE

November 2016

Version 6.0

As this Guide is considered to be a living document, potential developers and users of the PAXLST message are recommended to confirm with the WCO, IATA or ICAO that they are in possession of the latest version.

PASSENGER LIST MESSAGE (PAXLST) IMPLEMENTATION GUIDE

TABLE OF CONTENTS

Change log

	Description	Date	Remarks
1.	Update of the PAXLST MIG	25/02/2013	Based on Data Maintenance Requests received in the 5th and the 6th meetings of the API Contact Committee
2	Update of the PAXLST MIG	31/10/2013	Based on discussions at the 7th meeting of the API Contact Committee and follow-up work
3	Update of the PAXLST MIG	10/10/2014	Based on discussions at the 8th meeting of the API Contact Committee and follow-up work
4	Update of the PAXLST MIG	07/10/2015	Based on discussions at the 9th meeting of the API Contact Committee and follow-up work
5	Update of the PAXLST MIG	22/11/2016	Based on discussions at the 10th meeting of the API Contact Committee and follow-up work

PASSENGER LIST MESSAGE (PAXLST) IMPLEMENTATION GUIDE

This Document includes all the data requirements agreed by the WCO, IATA and ICAO and should be used as a basis for development of the air mode PAXLST message.

The WCO Council formally adopted the Advanced Passenger Information Guidelines and this Implementation Guide in July 2017.

IATA formally adopted the revised PAXLST message in TBD.

ICAO approved the revised PAXLST message in TBD.

1.0 INTRODUCTION

The first edition of the Advanced Passenger Information Guidelines was published in 1993 and included the data requirements that carriers were required to provide when reporting Advanced Passenger Information (API) to Border Control Agencies.

The Guideline also contained the specifications for the WCO/IATA subset of the UN/EDIFACT PAXLST message that had been designed as multi-modal, multi-functional message.

In October 2002, the WCO and IATA jointly updated the API Guidelines and reached agreement on a revised set of API data requirements.

This finalized set, adopted jointly by the WCO, IATA and ICAO in 2010, and last revised in 2016 includes additional data elements, in response to heightened security concerns within the air travel industry based on Data Maintenance Request (DMRs) submitted and approved by Members of the WCO/IATA/ICAO API-PNR Contact Committee (Contact Committee). This document represents the maximum number of data elements that carriers may be required to provide when reporting Advanced Passenger Information (API) to Border Control Agencies.

Carriers need to be aware that some Border Control Agencies may not require all elements contained within each message set.

The set of requirements have been mapped into the WCO/IATA/ICAO subset of the UN/EDIFACT PAXLST and CUSRES messages and this detailed Message Implementation Guide has been developed by the Contact Committee.

The purpose of this Guide is to aid border control Agencies and carriers in understanding the UN/EDIFACT PAXLST and CUSRES messages before beginning detailed development and implementation.

This Guide contains the necessary message branching diagrams and describes the function and use of each segment within its relative position within the message sets.

Examples on a segment basis and on a message basis are also included.

2.0 MESSAGE RELATIONSHIPS

The UN/EDIFACT PAXLST message set may be implemented as a standalone batch message for which there is no direct response message, or implemented within a bi-directional, interactive API message exchange process incorporating both UN/EDIFACT PAXLST and CUSRES message sets

The agreed data requirements for the WCO/IATA/ICAO PAXLST message are defined in Section 8 of the Advanced Passenger Information Guidelines and for the purpose of message design are reproduced as follows:

Flight Information (Header Data)
(Please see Section 8.1.4)

Airline Code and Flight Number

Last Place/Port of Call for Aircraft

Place/Port of Initial Arrival for Aircraft

Scheduled Local Departure Dates/Times

Scheduled Local Arrival Dates/Time

Subsequent Place(s)/Port(s) of Call within the Country (for Progressive Flights)

Place/Port of Final Destination within the Country (for Progressive Flights)

Number of Passengers and Number of Crew Members

Data relating to each individual passenger or crew member:

- Core Data Elements as may be found in the Machine Readable Zone of the Official Travel Document (See Section 8.1.5(a))

  Official Travel Document Number

  Issuing State or Organization of the Official Travel Document

  Official Travel Document Type

  Expiration Date of Official Travel Document

  Surname/Given Name(s)

  Nationality

  Date of Birth

  Gender

- Additional Data elements as available in the airline system (see 8.1.5(b))

  Seat Assignment
  Bag Tag Identification
  Checked Bag Quantity

  Traveller’s Status

  Place/Port of Original Embarkation

  Place/Port of Clearance

  Place/Port of Onward Foreign Destination

  Passenger Name Record Locator Number (or unique identifier)

- Additional data not normally found in Airline systems and which must be collected by, or on behalf of the Airline (See Section 8.1.5(c))

  Visa Number

  Issue Date of the Visa

  Place of Issuance of the Visa

  Other Document Number Used for Travel

- Type of Other Document Used for Travel
- Primary Residence
  - Address
  - City
  - State/Province/County
  - Postal Code
  - Country
- Destination Address
  - Address
  - City
  - State/Province/County
  - Postal Code
- Place of Birth
- Country of Primary Residence

- Contact Information for the person or entity responsible for the message content
- Passenger Reference Number (supplement to Passenger Name Record Locator)
- Information Verified indicator
- Passenger Contact information

Accordingly, provisional allowance is made for inclusion of these data consistent with UN/EDIFACT construction rules.

3.0 MESSAGE STRUCTURE FOR THE PAXLST MESSAGE

This message specification is based on the UN/EDIFACT Passenger List (PAXLST) Message and is specific to the air mode. It permits the transfer of passenger and crew member data from an airline to a Border Control Authority or other designated authority in the country of arrival (or departure) of the means of transport.

The basic concept of the PAXLST message is that there is one message for all passengers on the specified flight (or individual interactive PAXLST messages on a passenger-by-passenger basis) and a separate message used to report all crew members on that flight.

3.1 APPLICATION SEGMENTS USED IN THE WCO/IATA/ICAO PAXLST MESSAGE

The segments included in the air mode implementation of PAXLST are:

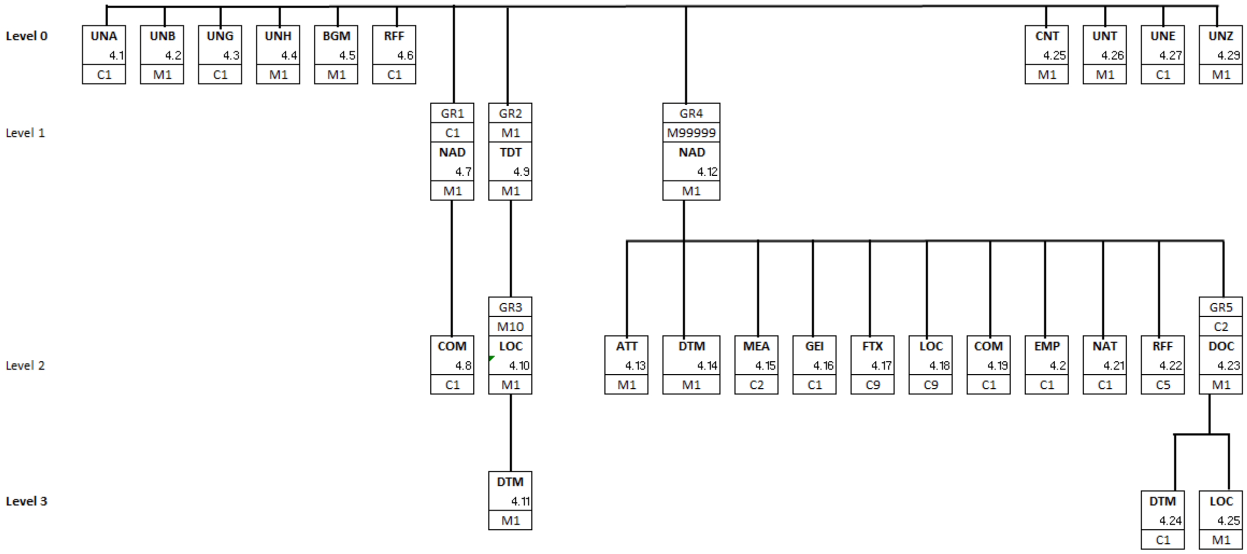
ATT	Attribute
BGM	Beginning of Message
CNT	Control Total
COM	Communication Contact
EMP	Employment Detail
DOC	Document/Message Details
DTM	Date/Time/Period
FTX	Free Text
GEI	Processing Information
LOC	Place/Location Identification
MEA	Measurements
NAD	Name and Address
NAT	Nationality
RFF	Reference
TDT	Details of Transport
UNA	Service Segment Advice
UNB	Interchange Header
UNE	Functional Group Trailer
UNG	Functional Group Header
UNH	Message Header
UNT	Message Trailer
UNZ	Interchange Trailer

It should be noted that the UN/EDIFACT PAXLST message includes other segments not included above.

3.2 UNITED NATIONS SERVICE SEGMENTS

The UN Service Segments UNA, UNB and UNZ should be implemented as they are described in ISO 9735 Application Level Syntax Rules - Version 4. The use of the UNG and UNE segment pair is optional within UN/EDIFACT message syntax, based upon bilateral agreement.

Data requirements for these segments are determined on a bilateral basis between individual carriers and respective Border Control Agencies.


Level 0
UNA 4.1 C1
UNB 4.2 M1
UNG 4.3 C1
UNH 4.4 M1
BGM 4.5 M1
RFF 4.6 C1
CNT 4.25 M1
UNT 4.26 M1
UNE 4.27 C1
UNZ 4.29 M1
Level 1
GR1 C1
NAD 4.7 M1
GR2 M1
TDT 4.9 M1
GR4 M99999
NAD 4.12 M1
Level 2
COM 4.8 C1
GR3 M10
LOC 4.10 M1
ATT 4.13 M1
DTM 4.14 M1
MEA 4.15 C2
GEI 4.16 C1
FTX 4.17 C9
LOC 4.18 C9
COM 4.19 C1
EMP 4.2 C1
NAT 4.21 C1
RFF 4.22 C5
GR5 C2
DOC 4.23 M1
Level 3
DTM 4.11 M1
DTM 4.24 C1
LOC 4.25 M1

4.0 SEGMENT DETAILS FOR USE IN THE PAXLST MESSAGE

This Section provides a detailed table of each segment, in their relative position within the message that may be required for the air mode PAXLST message.

Each table contains the UN/EDIFACT composite element and data element names, numbers and formats.

The table also contains the PAXLST format and status (Mandatory, Conditional or Not Applicable) of the elements within the segment, the number of repetitions, and the indication of a code set.

The elements that may be used in each segment are indicated by **bolding** the element name.

M or **C** in the Status column indicates a Mandatory or Conditional element.

N/A in the Status column indicates that there is no requirement to populate this field.

Additional comments on the use of the elements are also provided.

Code set values that may be used in each segment are provided in **BOLD** text.
Examples of other values are provided in ***BOLD ITALICISED*** text.

4.1 UNA: SERVICE STRING ADVICE

Function: The Service String Advice (UNA) is Conditional and provides the capability to specify the service characters (delimitation syntax) used within the interchange. The UNA service string advice ***must*** be used if the service characters differ from the defaults as identified in ISO 9735 EDIFACT Syntax Rules. The UNA is optional if the default characters are used.

When used, the service string advice shall appear immediately before the interchange header segment. The service string advice shall begin with the upper case characters UNA immediately followed by six characters in the order shown below. The same character shall not be used in more than one position of the UNA.

Default Service Characters

Name	**Graphic Representation**	**Functionality**
Colon	**:**	Component Data Element Separator
Plus sign	**+**	Data Element Separator
Period	**.**	**Decimal mark**
Question mark	**?**	Release Character
Asterisk	*****	Repetition Separator
Apostrophe	**‘**	Segment Terminator

Composite/Data Element	**No.**	**Field Type**	**Comm Usage**	**Status**	**Max Rep**	**Code Set**	**Comp.**	**Values / Comments**
COMPONENT DATA ELEMENT SEPARATOR	UNA1	n1	n1	M	-	-	-	
DATA ELEMENT SEPARATOR	UNA2	n1	n1	M	-	-	-	
DECIMAL MARK	UNA3	n1	n1	M	-	-	-	
RELEASE CHARACTER	UNA4	n1	n1	M	-	-	-	
REPETITION SEPARATOR	UNA5	n1	n1	M	-	-	-	
SEGMENT TERMINATOR	UNA6	n1	n1	M	-	-	-	

Example: UNA:+.?*) In this example, the right-parens represents the exception to the default Segment Terminator.

4.2 UNB: INTERCHANGE HEADER

Function: To start, identify and specify an interchange.

The conditional Status (C) of elements within this segment is used to indicate that Border Control Agencies may establish bilateral requirements for these data elements.

Composite/Data Element	No.	Field Type	Comm Usage	Status	Max Rep	Code Set	Comp.	Values / Comments
SYNTAX IDENTIFIER	S001	-	-	M	1	-	-	
Syntax identifier	0001	a4	a4	M	1	-	S001	**UNOA**
Syntax version number	0002	n1	n1	M	1	-	S001	**4**
INTERCHANGE SENDER	S002	-	-	M	1	-	-	
Sender identification	0004	an..35	an..35	M	1	-	S002	***'AIRLINE1'*** Sender of the message
Partner identification code qualifier	0007	an..4	N/A	C	-	-	-	
Address for reverse routing	0008	an..14	N/A	C	-	-	-	
INTERCHANGE RECEIVER	S003	-	-	M	1	-	-	
Recipient identification	0010	an..35	an..35	M	1	-	S003	***'NZCS'*** (for example) Receiver of the message. (This value is assigned by the implementing agency).
Partner identification code qualifier	0007	an..4	N/A	C	-	-	-	
Routing address	0014	an..14	N/A	C			-	
DATE AND TIME OF PREPARATION	S004	-	-	M	1	-	-	
Date of preparation	0017	n6	n6	M	1	-	S004	***'130628'*** The default format is 'YYMMDD' (n6)
Time of preparation	0019	n4	n4	M	1	-	S004	***'0900'*** The default format is 'HHMM' (n4)
INTERCHANGE CONTROL REFERENCE	0020	an..14	an..14	M	1	-	-	'***000000001'*** Will be repeated in UNZ data element 0020
RECIPIENTS REFERENCE PASSWORD	S005	-	N/A	C	-			
Recipient reference password	0022	an..14	N/A	M			S005	
Recipient reference password qualifier	0025	an..2	N/A	C			S005	
APPLICATION REFERENCE	0026	an..14		C				
PROCESSING PRIORITY CODE	0029	a1		C				

Composite/Data Element	No.	Field Type	Comm Usage	Status	Max Rep	Code Set	Comp.	Values / Comments
ACKNOWLEDGEMENT REQUEST	0031	n1		C				
COMMUNICATIONS AGREEMENT ID	0032	an..35		C				
TEST INDICATOR	0035	n1		C				

Example

```
UNB+UNOA:4+AIRLINE1+NZCS+130628:0900+000000001’
```

4.3 UNG: FUNCTIONAL GROUP HEADER

Function: To head, identify and specify a Functional Group.

The conditional Status (C) of elements within this segment is used to indicate that Border Control Agencies may establish bilateral requirements for these data elements.

Composite/Data Element	No.	Field Type	Comm Usage	Status	Max Rep	Code Set	Comp.	Values / Comments
FUNCTIONAL GROUP IDENTIFICATION	0038	an6	an6	M	1	-	-	**PAXLST**
APPLICATION SENDER IDENTIFICATION	S006	-	-	M	1	-	-	
Application Sender identification	0040	an..35	an..35	M	1	-	S006	***‘AIRLINE1’*** Sending Application
Partner identification code qualifier	0007	an..4	N/A	C	-	-	S006	
APPLICATION RECIPIENT IDENTIFICATION	S007	-	-	M	1	-	-	
Application Recipient identification	0044	an..35	an..35	M	1	-	S007	***‘NZCS’*** (for example) Receiving Application (This value is assigned by the implementing agency).
Partner identification code qualifier	0007	an..4	N/A	C	-	-	S007	
DATE AND TIME OF PREPARATION	S004	-	-	M	1	-	-	
Date of preparation	0017	n6	n6	M	1	-	S004	***‘130628’*** The default format is ‘YYMMDD’ (n6)
Time of preparation	0019	n4	n4	M	1	-	S004	***‘0900’*** The default format is ‘HHMM’ (n4)
FUNCTIONAL GROUP REFERENCE NUMBER	0048	an..14	an..14	M	1	-	-	‘***000000001’*** Will be repeated in UNE data element 0048
CONTROLLING AGENCY	0051	an..2	an..2	M	1	-	-	**UN**
MESSAGE VERSION	S008	-	-	M	1	-	-	
Message Type Version Number	0052	an..3	an..3	M	1	-	S008	***‘D’ (for example)***
Message Type Release Number	0054	an..3	an..3	M	1	-	S008	***‘15B’*** **See Note.**
Association assigned code	0057	an..6		C				
APPLICATION PASSWORD	0058	an..14		C				

Example

UNG+PAXLST+AIRLINE1+NZCS+130628:0900+000000001+UN+D:15B'

Note: Border Control Agencies may establish bilateral requirements for the value placed in this data element.

4.4 UNH: MESSAGE HEADER

Function: To identify and specify the PAXLST message.

The conditional Status (C) of elements within this segment is used to indicate that Border Control Agencies may establish bilateral requirements for these data elements.

Composite/Data Element	No.	Field Type	Comm Usage	Status	Max Rep	Code Set	Comp.	Values / Comments
MESSAGE REFERENCE NUMBER	0062	an..14	an..14	M	1	-	-	‘***MSG001***’ Will be repeated in UNT data element 0062
MESSAGE IDENTIFIER	S009	-	-	M	1	-	-	
Message type	0065	an..6	a6	M	1	-	S009	**PAXLST**
Message version number	0052	an..3	a1	M	1	-	S009	**D**
Message release number	0054	an..3	an2	M	1	-	S009	***‘15B’*** **See Note2.**
Controlling agency, coded	0051	an..2	a2	M	1	-	S009	**UN**
Association assigned code	0057	an..6	a4	M	1	-	S009	**IATA** See Note1
Code list directory version number	0110	an..6		C			S009	
Message type sub-function identification	0113	an..6		C			S009	
COMMON ACCESS REFERENCE	0068	an..35		C	1			
STATUS OF THE TRANSFER	S010			C	1			
Sequence of transfers	0070	n..2		M			S010	
First and last transfer	0073	a1		C			S010	
MESSAGE SUBSET IDENTIFICATION	S016			C	1			
Message subset identification	0115	an..14		M			S016	
Message subset version number	0116	an..3		C			S016	
Message subset release number	0118	an..3		C			S016	
Controlling agency, coded	0051	an..3		C			S016	
MESSAGE IMPLEMENTATION GUIDELINE IDENTIFICATION	S017			C	1			
Message implementation guideline identification	0121	an..14		M	1		S017	
Message implementation guideline version number	0122	an..3		C			S017	
Message implementation guideline release number	0124	an..3		C			S017	
Controlling agency, coded	0051	an..3		C			S017	
SCENARIO IDENTIFICATION	S018			C	1			
Scenario identification	0127	an..14		M			S018	
Scenario version number	0128	an..3		C			S018	
Scenario release number	0130	an..3		C			S018	
Controlling agency, coded	0051	an..3		C			S018	

Example

UNH+MSG001+PAXLST:D:15B:UN:IATA´

Note1

The use of code value ‘IATA’ in data element 0057 is used to indicate that airport and airline codes are IATA assigned codes.

Note2:

These Guidelines refer to the latest available publication of the PAXLST message of the UN/EDIFACT Directory. Border Control Agencies may already have existing guidelines based upon a previously published API Guideline version.

4.5 BGM: BEGINNING OF MESSAGE

Function: To indicate whether the PAXLST message is a passenger or crew list message.

Composite/Data Element	No.	Field Type	Comm. Usage	Status	Max Rep.	Code Set	Comp.	Values / Comments
DOCUMENT/ MESSAGE NAME	C002	-	-	M	1	-	-	
Document name code	1001	an..3	n3	M	1	Yes	C002	**250**, **745, 266, 336, 655**
Code list identification code	1131	an..17	-	N/A	-	-	-	
Code list responsible agency code	3055	an..3	-	N/A	-	-	-	
Document name	1000	an..35	-	N/A	-	-	-	
DOCUMENT/MESSAGE IDENTIFICATION	C106							
Document identifier	1004	an..35	an..4	C				See examples below in Table 4.5.1
Version identifier	1056	an..9		N/A				
Revision identifier	1060	an..6		N/A				
MESSAGE FUNCTION CODE	1225	an..3		N/A				
RESPONSE TYPE CODE	4343	an..3		N/A				

Example

BGM+745' Indicates passenger list
BGM+250' Indicates crew list declaration
BGM+266' **Indicates change in flight status@**
BGM+336' Indicates master crew list declaration
BGM+655' Indicates Gate Pass*
*Note: A gate pass is an authorization for a non-travelling person to access the sterile area of airports for the purpose of accompanying a ticketed traveller. (Presently used only in the United States.)
@ used in interactive API messages only.

Table 4.5.1

Document Name Code	Document Identifier Code	Meaning	Example
745	CP	Change Passenger Data	BGM+745+CP
745	XR	Cancel Reservation	BGM+745+XR
745	RP	Reduction in Party	BGM+745+RP
266	CL	Flight Close (only)	BGM+266+CL
266	CLNB	Flight Close w/ identified Passengers *not* on-board	BGM+266+CLNB
266	CLOB	Flight Close w/ identified Passengers on-board	BGM+266+CLOB
266	XF	Cancel Flight	BGM+266+XF
266	CF	Change Flight/Itinerary	BGM+266+CF

250	CL	Crew Flight Close (only)	BGM+250+CL
250	CLNB	Crew Flight Close w/ identified Crew *not* on-board	BGM+250+CLNB
250	CLOB	Crew Flight Close w/ identified Crew on-board	BGM+250+CLOB

Note:
Crew flight close process may not be implemented by aircraft operators.
Flight close process is normally implemented in iAPI system instead of batch, and associated with Departure Control Systems where seats are assigned to passengers.
It should also be noted that some states require pre and post departure Crew messaging, for example the UK.

4.6 RFF: REFERENCE

Function: To specify a transaction reference number.

Composite/Data Element	No.	Field Type	Comm. Usage	Status	Max Rep.	Code Set	Comp.	Values / Comments
REFERENCE	C506			M	1	-	-	
Reference code qualifier	1153	an..3	a3	M	1	Yes	C506	**TN**
Reference identifier	1154	an..70	an..25	M	1	-	C506	'***BA123456789***'
Document line identifier	1156	an..6	-	N/A	-	-	-	
Version identifier	1056	an..9	-	N/A	-	-	-	
Revision identifier	1060	an..6	n..3	C	-	-	-	***'2'***

Example

RFF+TN:BA123456789' Indicates transaction reference number BA123456789 assigned by an airline system.

RFF+TN:OZ56789034:::2' Indicates transaction reference number OZ56789034 assigned by an airline system. The Revision Identifier may optionally be used to identify this passenger data submission as the second submission for this passenger (i.e updated passenger data).

Notes :
For *States operating Interactive PAXLST messaging (iAPI), the inclusion of the RFF, Transaction Reference Number and its Revision Identifier may be declared Mandatory.*

4.7 NAD: NAME AND ADDRESS - GR. 1

Function: To specify a contact responsible for the message content.
This may either be an assigned profile or the name of the contact person.

If the 'name' (data elements 3036) is used, then contact details must be provided in the following COM (Communication Contact) segment.

Composite/Data Element	No.	Field Type	Comm. Usage	Status	Max Rep.	Code Set	Comp.	Values / Comments
PARTY FUNCTION CODE QUALIFIER	3035	an..3	a2	M	1	Yes	- -	**MS**
PARTY IDENTIFICATION DETAILS	C082	-	-	C	1	-	-	Used if a Profile has been assigned
Party identifier	3039	an..35	an..35	M	1	-	C082	***'ABC9876'***
Code list identification code	1131	an..17	-	N/A	-	-	-	
Code list responsible agency code	3055	an..3	-	N/A	-	-	-	
NAME AND ADDRESS	C058			N/A				
Name and address description	3124	an..35		N/A				
Name and address description	3124	an..35		N/A				
Name and address description	3124	an..35		N/A				
Name and address description	3124	an..35		N/A				

Composite/Data Element	No.	Field Type	Comm. Usage	Status	Max Rep.	Code Set	Comp.	Values / Comments
Name and address description	3124	an..35		N/A				
PARTY NAME	C080	-	-	C	1	-	-	Used if profile has not been established.
Party Name	3036	an..35	an..35	M	1	- -	C080	'***WILLIAMS***' Contact Surname
Party Name	3036	an..35	an..35	M	1	-	C080	'***JANE***' Contact First Name
Party Name	3036	an..35	-	N/A	-	-	-	
Party Name	3036	an..35	-	N/A	-	-	-	
Party Name	3036	an..35	-	N/A	-	-	-	
Party name format code	3045	an..3		N/A	-	-	-	
STREET	C059			N/A				
Street and number or post office box identifier	3042	an..35		N/A				
Street and number or post office box identifier	3042	an..35		N/A				
Street and number or post office box identifier	3042	an..35		N/A				
Street and number or post office box identifier	3042	an..35		N/A				
CITY NAME	3164	an..35		N/A				
COUNTRY SUB-DIVISION DETAILS	C819			N/A				
Country sub-division name code	3229	an..9		N/A				
Code list identification code	1131	an..17		N/A				
Code list responsible agency code	3055	an..3		N/A				
Country sub-entity name	3228	an..70		N/A				
POSTAL IDENTIFICATION CODE	3251	an..17		N/A				
COUNTRY IDENTIFIER	3207	an..3		N/A				

Examples

1.	NAD+MS+ABC9876'	Indicates that a profile has been established for this contact with this assigned identification
2.	NAD+MS+++WILLIAMS:JANE'	Indicates the name of the contact person

4.8 COM: COMMUNICATION CONTACT - GR. 1

Function: To specify the communication number(s) of the person responsible for the message content. Up to 3 communication numbers can be provided.

Data must be provided if no contact profile has been established.

Composite/Data Element	No.	Field Type	Comm Usage	Status	MaxRep.	Code Set	Comp.	Values / Comments
COMMUNICATION CONTACT	C076	-	-	M	3	-	-	
Communication address identifier	3148	an..512	an..35	M	1	-	C076	‘**202 628 9292’**
Communication address code qualifier	3155	an..3	a2	M	1	Yes	C076	**EM**, **FX**, **TE**

Notes

1. The contact details for the ‘physical transmitter’ of the message may be supplied in data element 0004 in the UNB segment.

Example

COM+202 628 9292:TE+202 628 4998:FX+davidsonr.at.iata.org:EM’

Indicates telephone number, fax number and email address of the message sender/contact.

Note: When reporting email addresses, special consideration should be give to any special characters appearing in the email address and potential impact to the syntax delimitation defined in the UNA segment.

4.9 TDT: DETAILS OF TRANSPORT- GR. 2

Function: To identify the flight by IATA airline designator and flight number.

Composite/Data Element	No.	Field Type	Comm. Usage	Status	Max Rep	Code Set	Comp	Values / Comments
TRANSPORT STAGE CODE QUALIFIER	8051	an..3	n2	M	1	Yes	-	**20 – For arriving or departing flight** **34 – For Over-flight**
MEANS OF TRANSPORT JOURNEY IDENTIFIER	8028	an..17	an..8	M	1	-	-	‘***DL123***‘
MODE OF TRANSPORT	C220			N/A				
Transport mode name code	8067	an..3		N/A				
Transport mode name	8066	an..17		N/A				
TRANSPORT MEANS	C001			N/A				
Transport means description code	8179	an..8		N/A				
Transport means description	8178	an..17		N/A				
CARRIER	C040			N/A				
Carrier identifier	3127	an..17	an..3	C				‘***DL***‘
Code list identification code	1131	an..17		N/A				
Code list responsible agency code	3055	an..3		N/A				
Carrier name	3126	an..35		N/A				
TRANSIT DIRECTION INDICATOR CODE	8101	an..3		N/A				
EXCESS TRANSPORTATION INFORMATION	C401			N/A				
Excess transportation reason code	8457	an..3		N/A				
Excess transportation responsibility code	8459	an..3		N/A				
Customer shipment authorisation identifier	7130	an..17		N/A				
TRANSPORT IDENTIFICATION	C222			N/A				
Transport means identification name identifier	8213	an..35		N/A				
Code list identification code	1131	an..17		N/A				
Code list responsible agency code	3055	an..3		N/A				
Transport means identification name	8212	an..70		N/A				

Composite/Data Element	No.	Field Type	Comm. Usage	Status	Max Rep	Code Set	Comp	Values / Comments
Transport means nationality code	8453	an..3		N/A				
TRANSPORT MEANS OWNERSHIP INDICATOR CODE	8281	an..3		N/A				
POWER TYPE	C003			N/A				
Power type cod	7041	an..3		N/A				
Code list identification code	1131	an..17		N/A				
Code list responsible agency code	3055	an..3		N/A				
Power type description	7040	an..17		N/A				

Example

TDT+20+DL123+++DL' Indicates flight identification DL123, Carrier Code DL
TDT+20+EK456’ Indicates flight identification EK456, Carrier Code not required
TDT+34+AF986+++AF’ Indicates flight identification AF986, Carrier Code AF, Over-flight.

4.10 LOC: PLACE/LOCATION IDENTIFICATION - GR.3

Function: To identify the arrival and departure airports relating to the specified flight. Airport codes are published in the IATA Airline Coding Directory.

Composite/Data Element	No.	Field Type	Comm Usage	Status	MaxRep	Code Set	Comp.	Values / Comments
LOCATION FUNCTION CODE QUALIFIER	3227	an..3	n..3	M	1	Yes	-	**87**, **92**, **125**, **130**
LOCATION IDENTIFICATION	C517	-	-	M	1	-	-	IATA Location Identifiers (Airport Codes)
Location name code	3225	an..35	a3	M	1	-	C517	'***YUL***'
Code list identification code	1131	an..17	-	N/A	-	-	-	
Code list responsible agency code	3055	an..3	-	N/A		-	-	
Location name	3224	an..256	-	N/A		-	-	
RELATED LOCATION ONE IDENTIFICATION	C519			N/A				
First related location identifier	3223	an..35		N/A				
Code list identification code	1131	an..17		N/A				
Code list responsible agency code	3055	an..3		N/A				
First related location name	3222	an..70		N/A				
RELATED LOCATION TWO IDENTIFICATION	C553			N/A				
Second related location identifier	3233	an..35		N/A				
Code list identification code	1131	an..17		N/A				
Code list responsible agency code	3055	an..3		N/A				
Second related location name	3232	an..70		N/A				
RELATION CODE	5479	an..3		N/A				

Examples

1. For a single sector progressive flight departing Brussels to New York, the following data would be provided.

LOC+125+BRU'	Indicates the last airport of departure from a foreign country, i.e. Brussels National
LOC+87+JFK'	Indicates the first airport of arrival in the country of destination, i.e. John F Kennedy International, New York

2. For a multi-sector progressive flight departing Heathrow to Vancouver via Montreal and Ottawa, the following data would be provided.

LOC+125+LHR'	Indicates the last airport of departure from a foreign country, i.e. London Heathrow
LOC+87+YUL'	Indicates the first airport of arrival in the country of destination, i.e. Montreal Dorval

LOC+92+YOW' Indicates the next airport in the country of destination,
i.e. Ottawa International

LOC+130+YVR' Indicates the final destination airport in the country of destination, i.e. Vancouver International

4.11 DTM: DATE/TIME/PERIOD - GR. 3

Function: To specify the departure and arrival dates for a flight.
If required, departure and arrival times may also be specified.

All dates and times will be provided in LOCAL time.

Composite/Data Element	**No.**	**Field Type**	**Comm Usage**	**Status**	**MaxRep.**	**Code Set**	**Comp**	**Values / Comments**
DATE/TIME/ PERIOD	C507	-	-	M	1	-	-	
Date or time or period function code qualifier	2005	an..3	n3	M	1	Yes	C507	**189**, **232**
Date or time or period value	2380	an..35	n6 or n10	M	1	-	C507	The default format is 'YYMMDD' (n6) '***130628***' Other format is 'YYMMDDHHMM' (n10). '***1306281205*'**
Date or time or period format code	2379	an..3	n3	C	1	Yes	C507	'**201'** If time (HHMM) is included in data element 2380

Examples

1. **DTM+189:*1306281205*:201'** Indicates the scheduled departure date and time of the flight, (i.e. June 28, 2013 at 12:05 hrs)
Code 201 is used to indicate a YYMMDDHHMM format.

2. **DTM+232:*130628*'** Indicates the scheduled arrival date of flight (i.e June 28, 2013)

4.12 NAD: NAME AND ADDRESS - GR. 4

Function: To specify the names of passengers and crew aboard a specified flight.

The segment may also be used to specify either the address details of the country of residence or the address details while in a specific country.

Composite/Data Element	No.	Field Type	Comm. Usage	Status	MaxRep.	Code Set	Comp.	Values / Comments
PARTY FUNCTION CODE QUALIFIER	3035	an..3	a..3	M	1	Yes	-	**DDT, DDU, FL**, **FM, ZZZ**
PARTY IDENTIFICATION DETAILS	C082			N/A				
Party identifier	3039	an..35		N/A				
Code list identification code	1131	an..17		N/A				
Code list responsible agency code	3055	an..3		N/A				
NAME AND ADDRESS	C058			N/A				
Name and address description	3124	an..35		N/A				
Name and address description	3124	an..35		N/A				
Name and address description	3124	an..35		N/A				
Name and address description	3124	an..35		N/A				
Name and address description	3124	an..35		N/A				
PARTY NAME	C080	-	-	M	1	-	-	Passenger or Crew Names
Party Name	3036	an..35	an..35	M	1	-	C080	‘***SMITH***’ Last name
Party Name	3036	an..35	an.. 35	C	1	-	C080	***‘JOAN’*** First given name (or initial)
Party Name	3036	an..35	an.. 35	C	1	-	C080	‘***A***’ Second given name (or initial)
Party Name	3036	an..35	-	N/A	-	-	-	
Party Name	3036	an..35	-	N/A	-	-	-	
Party name format code	3045	an..3	-	N/A	-	-	-	
STREET	C059	-	-	C	-	-	-	Street Address
Street and number or post office box identifier	3042	an..35	an…35	M	1	-	C059	‘***235 WESTERN ROAD SUITE 203’***
Street and number or post office box identifier	3042	an..35	-	N/A	-	-	-	
Street and number or post office box identifier	3042	an..35	-	N/A	-	-	-	
Street and number or post office box identifier	3042	an..35	-	N/A	-	-	-	
CITY NAME	3164	an..35	an..35	C	1	-	-	‘***SLEAFORD***’

Composite/Data Element	No.	Field Type	Comm. Usage	Status	MaxRep.	Code Set	Comp.	Values / Comments
COUNTRY SUB-ENTITY DETAILS	C819	-	-	C	1	-	-	State/Province/County Either a code in data element 3229 or a name in data element 3228
Country sub-entity name code	3229	an..9	an..9	C	1	-	C819	'***FL***'
Code list identification code	1131	an..17	-	C	1	-	C819	No value required but element must be accounted for if data element 3228 included
Code list responsible agency code	3055	an..3	-	C	1	-	C819	No value required but element must be accounted for if data element 3228 included
Country sub-entity name	3228	an..70	an..35	C	1	-	C819	***'LINCS'***
POSTAL IDENTIFICATION CODE	3251	an..17	an..17	C	1	-	-	'***PE22 4T5'***
COUNTRY NAME CODE	3207	an..3	a3	C	1	-	-	'***GBR***' ICAO codes in Doc 9303/ISO 3166

Examples

1. **NAD+FL+++SMITH:JOAN:A'** Indicates passenger with last name Smith, first name Joan and initial A

2. **NAD+FL+++WILLIAMS:JOHN:DONALD+235 WESTERN ROAD SUITE 203+ SLEAFORD+:::LINCS+PE22 4T5+GBR'**
Indicates passenger with last name Williams, first name John, and second name Donald and with country of residence address.

3. **NAD+DDT+++BARRET:TODD '** Indicates an 'In Transit' Crew member.

4. **NAD+FM+++CALIBRE:STEPHAN:T '** Indicates a Crew Member.

5. **NAD+DDU+++SORENSEN:YNGVAR:L '** Indicates an 'In Transit' Passenger.

4.13 ATT: ATTRIBUTE - GR. 4

Function: To identify the gender of the passenger or crew member.

Composite/Data Element	**No.**	**FieldType**	**Comm Usage**	**Status**	**Max Rep.**	**Code Set**	**Comp.**	**Values / Comments**
ATTRIBUTE FUNCTION CODE QUALIFIER	9017	an..3	a1	M	1	Yes	-	**2**
ATTRIBUTE TYPE	C955			N/A			-	
Attribute type description	9021	an..17		N/A				
Code list identification code	1131	an..17		N/A				
Code list responsible agency code	3055	an..3		N/A				
Attribute type description	9020	an..70		N/A				
ATTRIBUTE DETAIL	C956	-	-	M	1	-	C956	
Attribute description code	9019	an..17	a1	M	1	Yes	C956	**F**, **M**, **X**, **U**
Code list identification code	1131	an..17	-	N/A	-	-	-	
Code list responsible agency code	3055	an..3	-	N/A	-	-	-	
Attribute description	9018	an256	-	N/A	-	-	-	

Example

ATT+2++F'	Indicates a female passenger or crew member
ATT+2++M'	Indicates a male passenger or crew member
ATT+2++X'	
ATT+2++U'	Indicates when a passenger or crew member does not wish to divulge gender and the Machine Readable Zone of a document has no value (i.e. **<**). X is the official code according to document 9030

4.14 DTM: DATE/TIME/PERIOD - GR. 4

Function: To specify the date of birth of a passenger or crew member.

Composite/Data Element	No.	Field Type	Comm Usage	Status	Max Rep.	Code Set	Comp.	Values / Comments
DATE/TIME/ PERIOD	C507	-	-	M	1	-	-	
Date or time or period function code qualifier	2005	an..3	a3	M	1	Yes	C507	**329**
Date or time or period value	2380	an..35	n6	M	1	-	C507	'***640217'*** Format is always 'YYMMDD'
Date or time or period format code	2379	an..3	-	N/A	-	-	-	

Examples

DTM+329:640217' Indicates the date of birth of the passenger or crew member (i.e. February 17, 1964.)

4.15 MEA: Measurements - GR. 4

Function: To specify physical measurements.

This segment used to report number of Checked Bags.

Composite/Data Element	**No.**	**Field Type**	**Comm Usage**	**Status**	**Max Rep.**	**Code Set**	**Comp.**	**Values / Comments**
MEASUREMENT PURPOSE CODE QUALIFIER	6311	an..3	an..2	M	1	Yes	-	**‘CT’ for the number of the baggage.** **‘WT’ for the weight of the baggage.**
MEASUREMENT DETAILS	C502	-	-	N/A	1	-	-	
Measured attribute code	6313	an..3	-	N/A	-	-	C502	
Measurement significance code	6321	an..3	-	N/A	-	-	C502	
Non-discrete measurement name code	6155	an..17	-	N/A	-	-	C502	
Non-discrete measurement name	6154	an..70	-	N/A	-	-	C502	
VALUE / RANGE	C174	-	-	C	-	-		
Measurement Unit Code	**6411**	**an..8**	**a3**	**C**	**-**	**-**	**C174**	**‘KGM’ for Kilograms** **‘LBR’ for Pounds**
Measure	6314	an..18	an..3	M			C174	**‘2’**
Range minimum quantity	6162	an..18	-	N/A	-	-	C174	
Range maximum quantity	6152	an..18	-	N/A	-	-	C174	
Significant digits quantity	6432	an..2	-	N/A	-	-	C174	
SURFACE OR LAYER CODE	7383	an..3	-	N/A	-	-	-	

Examples

MEA+CT++:2'	Indicates that this passenger checked two bags at pre-flight check-in.
MEA+WT++KGM:28'	Indicates that this passenger checked 28 Kgs bags at pre-flight check-in.

4.16 GEI: Processing Information - GR. 4

Function: To identify that information for this passenger has been validated.

Composite/Data Element	No.	Field Type	Comm Usage	Status	Max Rep.	Code Set	Comp.	Values / Comments
PROCESSING INFORMATION CODE QUALIFIER	9649	an..3	an..1	M	1	Yes	-	**4**
PROCESSING INDICATOR	C012	-	-	M	1	-	-	
Processing indicator description code	7365	an..3	an..3	M	1	-	C012	**'173' for information verified** **'174' for information not verified**
Code list identification code	1131	an..17		N/A				
Code list responsible agency code	3055	an..3		N/A				
Processing indicator description	7364	an..35		N/A				
PROCESS TYPE DESCRIPTION CODE	7178	an..17		N/A				

Examples

GEI+4+173' Indicates that the information contained for this passenger has been verified.

4.17 FTX: FREE TEXT - GR. 4

Function: To indicate the description and bag tag numbers of the passenger or crew effects.

Composite/Data Element	**No.**	**Field Type**	**CommUsage**	**Status**	**Max Rep.**	**Code Set**	**Comp.**	**Values / Comments**
TEXT SUBJECT CODE QUALIFIER	4451	an..3	An3	M	1	YES	-	**BAG**
FREE TEXT FUNCTION CODE	4453			N/A				
TEXT REFERENCE	C107			N/A				
Free text description Code	4441	an..17		N/A				
Code list identification code	1131	an..17		N/A				
Code list responsible agency code	3055	an..3		N/A				
TEXT LITERAL	C108	-	-	M	1	-	-	
Free Text	4440	an.512	an.35	M	1		C108	***‘BA123456’***
Free Text	4440	an.512	n..3	C	1		C108	***‘3’***
Free Text	4440	an.512		N/A				
Free Text	4440	an.512		N/A				
Free Text	4440	an.512		N/A				
LANGUAGE NAME CODE	3453	an..3		N/A				
FREE TEXT FORMAT CODE	4447	an..3		N/A				

Example

1. **FTX+BAG+++BA987654’** - Single Bag Tag reference
2. **FTX+BAG+++AF012345:3’** - Indicates 3 bags checked beginning with a sequential reference of AF012345.

4.18 LOC: PLACE/LOCATION IDENTIFICATION - GR. 4

Function: To identify the place of birth, the airports related to the journey, and the country of residence of passengers or crew members.

Composite/Data Element	**No.**	**Field Type**	**Comm Usage**	**Status**	**MaxRep.**	**Code Set**	**Comp.**	**Values / Comments**
LOCATION FUNCTION CODE QUALIFIER	3227	an..3	n..3	M	1	Yes	-	**22, 174, 178, 179, 180**
LOCATION IDENTIFICATION	C517	-	-	M	1	-	-	Either Airports related to the journey, Place of Birth or Country of Residence
Location name code	3225	an..35	a3	C	1	Yes	C517	'***LIS***' Airport related to journey Or '***CAN***' Country of residence
Code list identification code	1131	an..17	-	C	1	-	C517	No value required but element must be accounted for if data element 3224 included
Code list responsible agency code	3055	an..3	-	C	1	-	C517	No value required but element must be accounted for if data element 3224 included No value required
Location name	3224	an..256	an..35	C	1	-	C517	***'AMBER HILL GBR'*** Place of Birth
RELATED LOCATION ONE IDENTIFICATION	C519			N/A				
First related location name code	3223	an..25		N/A				
Code list identification code	1131	an..17		N/A				
Code list responsible agency code	3055	an..3		N/A				
First related location name	3222	an..70		N/A				
RELATED LOCATION TWO IDENTIFICATION	C553			N/A				
Second related location name code	3233	an..25		N/A				
Code list identification code	1131	an..17		N/A				
Code list responsible agency code	3055	an..3		N/A				
Second related location name	3232	an..70		N/A				
RELATION CODE	5479	an..3		N/A				

Examples

1. **LOC+178+LIS'** Indicates the airport where a passenger or crew member began their journey, i.e. Lisbon

2. **LOC+179+ORD'** For intransit passengers or crew members or for progressive clearance flights, indicates the airport where a passenger or crew member will end their journey, i.e. Chicago O'Hare.

3. **LOC+22+BOS'** For intransit passengers or crew members or for progressive clearance flights, indicates the airport where a passenger or crew member will complete clearance procedures, i.e. Boston Logan.

4. **LOC+180+:::AMBER HILL GBR'**
   Indicates the place of birth as per ICAO Document 9303.

5. **LOC+174+CAN'**
   Indicates the country of residence as per ICAO Document 9303 ISO 3166 (3 alpha).

4.19 COM: COMMUNICATION CONTACT - GR. 4

Function: To specify the communication number(s) of the passenger. Up to 3 Communication numbers can be provided.

Composite/Data Element	**No.**	**Field Type**	**Comm Usage**	**Status**	**MaxRep.**	**Code Set**	**Comp.**	**Values / Comments**
COMMUNICATION CONTACT	C076	-	-	M	3	-	-	
Communication address identifier	3148	an..512	an..35	M	1	-	C076	**202 628 9292**
Communication address code qualifier	3155	an..3	a2	M	1	Yes	C076	**EM**, **TE, FX**

Example

COM+202 628 9292:TE+202 628 4998:FX+davidsonr.at.iata.org:EM’
Indicates telephone number, fax number and email address of the traveller.

Note: When reporting email addresses, special consideration should be given to any special characters appearing in the email address and potential impact to the syntax delimitation defined in the UNA segment.

4.20 EMP: EMPLOYMENT DETAILS - GR. 4

Function: to indicate the occupation of a passenger or the rank of crew.

Composite/Data Element	**No.**	**FieldType**	**Comm Usage**	**Status**	**MaxRep**	**Code Set**	**Comp**	**Values / Comments**
EMPLOYMENT DETAILS CODE QUALIFIER	9003	an..3	an..1	M	1	-	-	**1**
EMPLOYMENT CATEGORY	C948	-	-	C	1	-	-	
Employment category description code	9005	an..3	an3	M	1	Yes	C948	‘**CR1**’ for cockpit crew or individuals inside cockpit ‘**CR2**’ for cabin crew **‘CR3’** for airline operation management with cockpit access **‘CR4’** for cargo non cockpit crew and/or non-crew individuals. **‘CR5’** pilots on board but not on duty
Code list identification code	**1131**	**an..17**	**an3**	**C**	**-**	**-**	C948	
Code list responsible agency code	**3055**	**an..3**	**-**	**C**	**-**	**-**	C948	
Employment category description	9004	an..35	-	N/A	-	-	-	
OCCUPATION	C951	-	-	N/A	-	-	-	
Occupation description code	9009	an..3	-	N/A				
Code list identification code	1131	an..17	-	N/A				
Code list responsible agency code	3055	an..3	-	N/A				
Occupation description	9008	an..35	-	N/A				
Occupation description	9008	an..35	-	N/A				
QUALIFICATION CLASSIFICATION	C950			N/A	-			
Qualification classification description code	9007	an..3	-	N/A				
Code list identification code	1131	an..17	-	N/A				
Code list responsible agency code	3055	an..3	-	N/A				
Qualification classification description	9006	an..35	-	N/A				
Qualification classification description	9006	an..35	-	N/A				
PERSON JOB TITLE	3480	an..35	-	N/A	-			

Composite/Data Element	No.	FieldType	Comm Usage	Status	MaxRep	Code Set	Comp	Values / Comments
QUALIFICATION APPLICATION AREA CODE	9035	an..3	-	N/A	-			

Example

EMP+1+**CR1**:110:111'   Indicates current passenger is a cockpit crew

4.21 NAT: NATIONALITY - GR. 4

Function: To specify the nationality of the passenger or crew member.

Composite/Data Element	No.	FieldType	CommUsage	Status	Max Rep	Code Set	Comp	Values / Comments
NATIONALITY CODE QUALIFIER	3493	an..3	n1	M	1	Yes	1	**2**
NATIONALITY DETAILS	C042	-	-	M	1	-	-	ICAO 9303/ISO 3166 codes
Nationality name code	3293	an..3	a3	M	1	-	C042	‘***CAN***’
Code list identification code	1131	an..17	-	N/A	-	-	-	
Code list responsible agency code	3055	an..3	-	N/A	-	-	-	
Nationality name	3292	an..35	-	N/A	-	-	-	

Example

NAT+2+CAN’	Indicates current nationality as a Canadian

4.22 RFF: REFERENCE - GR. 4

Function: To specify the passenger reservation reference number. To specify the passenger reservation number, unique passenger reference, and other reference information related to this traveler. Up to 5 occurrences of this segment may be present

Composite/Data Element	No.	Field Type	Comm. Usage	Status	Max Rep.	Code Set	Comp.	Values / Comments
REFERENCE	C506			M	1	-	-	
Reference code qualifier	1153	an..3	a3	M	1	Yes	C506	**AVF, ABO, SEA , AEA, CR**
Reference identifier	1154	an..70	an..35	M	1	-	C506	'***WWHPDS***'
Document line identifier	1156	an..6	-	N/A	-	-	-	
Version identifier	1056	an..9	-	N/A	-	-	-	
Revision identifier	1060	an..6	-	N/A	-	-	-	

Example

RFF+AVF:WWHPDS'	Indicates passenger reservation reference number
RFF+ABO:BA1321654987'	Indicates Unique Passenger Reference
RFF+SEA:22A'	Indicates assigned Seat identification
RFF+AEA:123456789'	Government agency reference number (Optionally issued by a state to facilitate booking and travel).
RFF+CR:ABC123'	Customer Reference Number. Frequent flyer or frequent traveler reference.

4.23 DOC: DOCUMENT/MESSAGE DETAILS - GR. 5

Function: To identify the official travel document and/or other document used for travel.

Composite/Data Element	**No.**	**Field Type**	**CommUsage**	**Status**	**Max Rep.**	**Code Set**	**Comp.**	**Values / Comments**
DOCUMENT/ MESSAGE NAME	C002	-	-	M	1	-	-	Document types as per ICAO 9303
Document name code	1001	an..3	a..2	M	1	Yes	C002	**P**, **V, I** *See Notes*
Code list identification code	1131	an..17	-	N/A	-	-	-	
Code list responsible agency code	3055	an..3	-	N/A	-	-	-	
Document name	1000	an..35	-	N/A	-	-	-	
DOCUMENT/ MESSAGE DETAILS	C503	-	-	M	1	-	-	Document number
Document identifier	1004	an..35	an..9	M	1	-	C503	***‘98764312’***
Document status code	1373	an..3	-	N/A	-	-	-	
Document source description	1366	an..70	-	N/A	-	-	-	
Language name code	3453	an..3	-	N/A	-	-	-	
Version identifier	1056	an..9	-	N/A	-	-	-	
Revision identifier	1060	an..6	-	N/A	-	-	-	
COMMUNICATION MEDIUM TYPE CODE	3153	an..3		N/A				
DOCUMENT COPIES REQUIRED QUANTITY	1220	n..2		N/A				
DOCUMENT ORIGINALS REQUIRED QUANTITY	1218	n..2		N/A				

Example

DOC+P+98764312' Indicates that the document type is a passport and its number.
DOC+V+9891404' Indicates that the document type is a visa and its number.
DOC+I+G123456' Indicates that the document type is state issued document of identity and its number.

Notes

ICAO 9303 document types also include the characters **A**, **C**, **I** and may be used to indicate an Identity Card. The exact use will be defined by the Issuing State.

One additional character may be used after P, V, A, C, I to further identify the document at the discretion of the Issuing State. The exact use will be defined by the Issuing State.

Document Type ‘**AC**’ is reserved for use as ’Crew Member Certificate’ and Document Type ‘**IP**’ is reserved for use as ‘Passport Card’.

States may approve other documents as identification for travel use.
Document type codes will be assigned by the Issuing State.

Certain States have agreed to assign code ‘**F**’ to identify ‘approved non-standard identity documents used for travel’.

4.24 DTM: DATE/TIME/PERIOD - GR. 5

Function: To specify the expiry date of the official travel document or the issue date of the other document used to travel.

Composite/Data Element	No.	FieldType	Comm Usage	Status	Max Rep	Code Set	Comp.	Values / Comments
DATE/TIME/ PERIOD	C507	-	-	M	1	-	-	
Date or time or period function code qualifier	2005	an..3	n..3	M	1	Yes	C507	**36**, **182**
Date or time or period value	2380	an..35	n6	M	1	-	C507	'***150723***' Format is always 'YYMMDD'.
Date or time or period format code	2379	an..3	-	N/A	-	-	-	

Examples

1. **DTM+36:150723'** Indicates the expiry date of the official travel document (i.e. July 23, 2015).
2. **DTM+182:121006'** Indicates the issue date of the other document used for travel (i.e. October 6, 2012).

4.25 LOC: PLACE/LOCATION IDENTIFICATION - GR. 5

Function: To identify either the country of issue of the official travel document or the place of issue of the other document used for travel.

Composite/Data Element	No.	Field Type	Comm Usage	Status	Max Rep.	Code Set	Comp.	Values / Comments
LOCATION FUNCTION CODE QUALIFIER	3227	an..3	n2	M	1	Yes	-	**91**
LOCATION IDENTIFICATION	C517	-	-	M	1	-	-	Either Country of Issue of official travel document (data element 3225) or Place of Issue of other document (data element 3224)
Location name code	3225	an..35	a3	C	1	Yes	C517	'***CAN***' ICAO 9303/ISO 3166 codes
Code list identification code	1131	an..17	-	C	1	-	-	No value required but element must be accounted for if data element 3224 included
Code list responsible agency code	3055	an..3	-	C	1	-	-	No value required but element must be accounted for if data element 3224 included
Location name	3224	an..256	an..35	C	1	-	-	**'*MONTREAL*'**
RELATED LOCATION ONE IDENTIFICATION	C519			N/A				
First related location name code	3223	an..35		N/A				
Code list identification code	1131	an..17		N/A				
Code list responsible agency code	3055	an..3		N/A				
First related location name	3222	an..70		N/A				
RELATED LOCATION TWO IDENTIFICATION	C553			N/A				
Second related location name code	3233	an..25		N/A				
Code list identification code	1131	an..17		N/A				
Code list responsible agency code	3055	an..3		N/A				
Second related location name	3232	an..70		N/A				
RELATION CODE	5479	an..3		N/A				

Examples

1. **LOC+91+CAN'** Indicates the State responsible for issuing the passport; i.e. Canada

2. **LOC+91+:::MONTREAL'**
Indicates the city where a travel document was issued

4.26 CNT: CONTROL TOTAL

Function: To provide message control total.

Composite/Data Element	No.	Field Type	CommUsage	Status	Max Rep.	Code Set	Comp.	Values / Comments
CONTROL	C270	-	-	M	1	-	-	
Control total type code qualifier	6069	an..3	n2	M	1	Yes	C270	**41, 42**
Control total value	6066	n..18	n..4	M	1	-	C270	'***160***'
Measurement unit code	6411	an..3	-	N/A	-	-	-	

Notes

1. The single occurrence of CNT is used to designate the total number of passengers or the total number of crew on a specified flight.

2. If more than one passenger (or crew) message is to be transmitted, the number reported in CNT in each message is the total number of passengers (or crew) on the flight.

   It is **NOT** the number of passengers (or crew) being reported in each message.

Example

CNT+42:160'	Indicates a total of 160 passengers on the flight.
CNT+41:8'	Indicates a total of 8 crew members on the flight.

4.27 UNT: MESSAGE TRAILER

Function: To end and check the completeness of a message by counting the segments in the message (including UNH and UNT) and validating that the message reference number equates to data element 0062 in the UNH segment.

Composite/Data Element	No.	Field Type	Comm Usage	Status	Max Rep	Code Set	Comp.	Values / Comments
NUMBER OF SEGMENTS IN A MESSAGE	0074	n..10	n..10	M	1	-	-	‘***2578***’
MESSAGE REFERENCE NUMBER	0062	an..14	an..14	M	1	-	-	‘***MSG001***’ Must be equal to UNH data element 0062

Example

UNT+2578+MSG001´

4.28 UNE: FUNCTIONAL GROUP TRAILER

Function: To end and check the completeness of a Functional Group.

Composite/Data Element	No.	Field Type	Comm Usage	Status	Max Rep	Code Set	Comp.	Values / Comments
NUMBER OF MESSAGES	0060	n..6	n..6	M	1	-	-	***‘1’***
APPLICATION SENDER IDENTIFICATION	0048	an..14	an..14	M	1	-	-	***‘000000001’*** Must be equal to UNG data element 0048

Example

UNE+1+000000001’

4.29 UNZ: INTERCHANGE TRAILER

Function: To end and check the completeness of an Interchange.

Composite/Data Element	**No.**	**Field Type**	**Comm Usage**	**Status**	**Max Rep**	**Code Set**	**Comp.**	**Values / Comments**
INTERCHANGE CONTROL COUNT	0036	n..6	n..6	M	1	-	-	***‘1’***
INTERCHANGE CONTROL REFERENCE	0020	an..14	an..14	M	1	-	-	***‘000000001’*** Must be equal to UNB data element 0020

Example

UNZ+1+000000001’

NOTES:

1.) The UNG Segment is optional for use on the PAXLST message. Use of this segment will be determined by Border Control Agencies.
2.) The use of the label ‘CUSTOMS’ in the examples is for illustrations purposes only. The actual value appearing in the UNB *Interchange Receiver ID* and UNG *Application Reciever ID* will be established by Border Control Agencies in their bilateral agreements with the Carriers.

5.1 Single Sector Flight - Passenger

This sample PAXLST illustrates the sum of all segments and many segment examples shown in Section 4 of this Appendix. This PAXLST message identifies a single, non-progressive flight and a single passenger.

```
UNB+UNOA:4+ZZAIRLINE+CUSTOMS+130620:0900+000000001’
UNG+PAXLST+ZZAIRLINE+CUSTOMS+130620:0900+000000001+UN+D:15B’
UNH+PAX001+PAXLST:D:15B:UN:IATA’
BGM+745’
RFF+TN:1234567890’
NAD+MS+++DAVIDSON:ROBERT’
COM+202 628 9292:TE+202 628 4998:FX+DAVIDSONR.AT. IATA.ORG:EM’
TDT+20+ZZ123+++ZZ’
LOC+125+SYD’
DTM+189:1306210900:201’
LOC+87+HNL’
DTM+232: 1306212200:201’
NAD+FL+++WILLIAMS:JOHN:DONALD+235 WESTERN ROAD SUITE 203+
                SLEAFORD+:::LINCS+PE224T5+GBR’
ATT+2++M’
DTM+329:720907’
MEA+CT++:2’
GEI+4+174’
FTX+BAG+++ZZ012345:3’
LOC+22+HNL’
LOC+174+GBR’
LOC+178+SYD’
LOC+179+HNL’
LOC+180+:::AMBER HILL GBR’
COM+44 188 84 14151:TE’
NAT+2+GBR’
RFF+AVF:TYR123’
RFF+ABO:ABC123’
DOC+P+MB140241’
DTM+36:151231’
LOC+91+GBR’
CNT+42:160’
UNT+30+PAX001’
UNE+1+000000001’
UNZ+1+000000001’
```

5.2 Sample Crew Reporting Message

This sample PAXLST identifies as single flight with a Crew Member clearing at the destination.

```
UNB+UNOA:4+ZZAIRLINE+CUSTOMS+130620:0900+QF00321’
UNG+PAXLST+ZZAIRLINE+CUSTOMS+130620:0900+81+UN+D:15B’
UNH+PAX001+PAXLST:D:15B:UN:IATA’
BGM+250’
NAD+MS+USD090746’
TDT+20+ZZ123+++ZZ’
LOC+125+SYD’
DTM+189:1306210900:201’
LOC+87+HNL’
DTM+232: 1306212200:201’
NAD+FM+++CLARK:MICHAEL+ 2365 KAANAPALI HIGHWAY
          +LAHAINA+HI+ 96761’
ATT+2++M’
DTM+329:720907’
NAT+2+CAN’
LOC+22+HNL’
LOC+174+CAN’
LOC+178+SYD’
LOC+179+HNL’
DOC+P+MB140241’
DTM+36:151021’
LOC+91+CAN’
CNT+41:8’
UNT+20+PAX001’
UNE+1+81’
UNZ+1+QF00321’
```

5.3 Progressive Flight with Domestic Continuance – Passenger

This sample identifies a PAXLST message with two passengers arriving in one country and continuing to another destination within the same country.

```
UNB+UNOA:4+ XYZAIRLINES+CUSTOMS+140708:0601+123456789’
UNG+PAXLST+XYZAIRLINES+CUSTOMS+140708:0601+12345+UN+D:15B’
UNH+123+PAXLST:D:15B:UN:IATA’
BGM+745’
RFF+TN:BART34567890:::1’
NAD+MS+++XYZ PSGR SYSTEMS’
COM+703-555-1212:TE+703-555-4545:FX’
TDT+20+XZ877+++XZ’
LOC+92+BCN’
DTM+189:1407081100:201’
LOC+92+IAD’
DTM+232:1407081700:201’
TDT+20+ZX877+++XZ’
LOC+92+IAD’
DTM+189:14070811930:201’
LOC+92+SFO’
DTM+232:14070812330:201’
NAD+FL+++MARTINEZ:JULIO:XAVIER’
ATT+2++M’
DTM+329:680223’
LOC+22+IAD’
LOC+178+BCN’
LOC+179+SFO’
LOC+174+ESP’
NAT+2+ESP’
RFF+AVF:GJO3RT’
RFF+ABO:XZ877001’
DOC+P+YY3478621’
DTM+36:181230’
LOC+91+ESP’
NAD+FL+++MARTINEZ:SORINA:MARIA’
ATT+2++F’
DTM+329:690606’
LOC+22+IAD’
LOC+178+BCN’
LOC+179+SFO’
LOC+174+ESP’
NAT+2+ESP’
RFF+AVF:GJO3RT’
RFF+ABO:XZ877002’
DOC+P+TRQWE9980’
DTM+36:170916’
LOC+91+ESP’
CNT+42:2’
UNT+43+123’
```

```
UNE+1+12345’
UNZ+1+123456789’
```

5.4 Sample PAXLST using UNA Service String Advice Segment

This sample illustrates a PAXLST message that begins with a UNA segment to specify the service characters (delimitation syntax) used within the interchange.
The UNA segment is required when characters other than the default service characters are used in the message.

```
UNA:(.) -
UNB(UNOA:4(QCAIR(CUSTOMS(131221:0100(160415-
UNG(PAXLST(QCAIR(CUSTOMS(131221:0100(0834343434(UN(D:15B-
UNH(1115(PAXLST:D:15B:UN:IATA-
BGM(745-
NAD(MS(((QC OPERATIONS-
COM(88 65414646:TE(88 65458341:FX-
TDT(20(QC0211(((QC-
LOC(125(ICN-
DTM(189:1311221740:201-
LOC(87(SFO-
DTM(232:1312211115:201-
NAD(FL(((CHARLES:JOHNATHAN:T-
ATT(2((M-
DTM(329:570619-
LOC(22(SFO-
LOC(174(IND-
LOC(178(HYD-
LOC(179(SFO-
NAT(2(CAN-
RFF(AVF:L6RESU-
RFF(ABO:000000001L6RESU-
DOC(P(T6735770-
DTM(36:160705-
LOC(91(CAN-
CNT(42:129-
UNT(23(1115-
UNE(1(0834343434-
UNZ(1(160415-
```

5.5 Flight Close-Out PAXLST Message

This sample illustrates a PAXLST message that may be used to report a Flight Close-Out message that identifies all passengers who boarded the flight identified in the message. In this example, passengers are identified only by Passenger Record Locator and Unique Passenger Reference (RFF qualifiers 'AVF' and 'ABO' respectively). The expectation, in this example is that the passenger names (travel documentation, etc.) were collected through previously transmitted PAXLST API submissions.

```
UNB+UNOA:4+XYZ+CUSTOMS+130322:0335+0000001++API'
UNG+PAXLST+XYZ AIRLINES+CUSTOMS+130322:0335+1+UN+D:15B'
UNH+5755176+PAXLST:D:15B:UN:IATA'
BGM+266+CLOB'
RFF+TN:ABC1234:::2'
TDT+20+YZ567+++AA'
LOC+125+LHR'
DTM+189:1303221615:201'
LOC+87+LAX'
DTM+232:1303221905:201'
NAD+ZZZ'
RFF+AVF:TYR123’
RFF+ABO:TYL001’
NAD+ZZZ'
RFF+AVF:TYR123’
RFF+ABO:TYL002’
NAD+ZZZ'
RFF+AVF:TYR123’
RFF+ABO:TYL003’
NAD+ZZZ'
RFF+AVF:TYR123’
RFF+ABO:TYL004’
NAD+ZZZ'
RFF+AVF:AABD55’
RFF+ABO:MCO001’
NAD+ZZZ'
RFF+AVF:AABD55’
RFF+ABO:MCO002’
NAD+ZZZ'
RFF+AVF:ZMJO6O’
RFF+ABO:VEF001’
CNT+42:7’
UNT+31+5755176'
UNE+1+1'
UNZ+1+0000001’
```

APPENDIX A – Data Element List

This Section provides data element codes lists that are used in the air mode PAXLST message. For a complete data element code list, refer to the UN Code Set Directory.

1001 Document name code

Desc: Code specifying the document name.
Repr: an..3

250 Crew list declaration
Declaration regarding crew members aboard the conveyance

745 Passenger list
Declaration to Customs regarding passengers aboard the conveyance; equivalent to IMO FAL 6.

266 Transport equipment status change report
Report on one or more changes of status associated with an item or items of transport equipment. (This code value is used to indicate change in flight status).

336 Customs crew and conveyance
Document/message contains information regarding the crew list and conveyance.

655 Gate pass
Document/message authorizing goods specified therein to be brought out of a fenced-in port or terminal area.

ICAO 9303 Document Types

P	Passport	
V	Visa	
A	Identity Card	(exact use defined by the Issuing State)
C	Identity Card	(exact use defined by the Issuing State)
I	Identity Card	(exact use defined by the Issuing State)
AC	Crew Member Certificate	
IP	Passport Card	

Other Document Types

F Approved non-standard identity documents used for travel
(exact use defined by the Issuing State).

1153 Reference code qualifier

Desc: Code qualifying a reference.
Repr: an..3

AVF Passenger reservation reference number
Number assigned by the travel supplier to identify the passenger reservation

ABO Unique originating passenger reference
Reference to supplement the passenger reference number

AEA Government agency reference number
Optionally issued by a controlling agency state to facilitate booking and travel for a passenger.

CR Customer reference number
Frequent flyer or frequent traveler reference.

SEA Allocated seat

Reference to a seat allocated to a passenger.

2005 Date or time or period function code qualifier
Desc: Code qualifying the function of a date, time or period.
Repr: an..3

36 Expiry date
Date of expiry of the validity of a referenced document, price information or any other referenced data element with a limited validity period

182 Issue date
Date when a document/message has been or will be issued.

189 Departure date/time, scheduled
Date (and time) of scheduled departure of means of transport

232 Arrival date/time, scheduled
Date (and time) of scheduled arrival of means of transport

329 Birth date/time
Date/time when a person was born.

2379 Date or time or period format code
Desc: Code specifying the representation of a date, time or period.
Repr: an..3

201 YYMMDDHHMM
Calendar date including time without seconds
Y = Year; M = Month; D = Day; H = Hour; M = Minute.

3035 Party function code qualifier
Desc: Code giving specific meaning to a party.
Repr: an..3

DDT In transit crew member
The movement of a crew member from one country to another via the territory of an intermediate country for which no entry is intended.

DDU In transit passenger
The movement of a passenger from one country to another via the territory of an intermediate country for which no entry is intended.

FL Passenger
A person conveyed by a means of transport, other than the crew.

FM Crew member
A person manning a means of transport.

MS Document/message issuer/sender
Issuer of a document and/or sender of a message.

ZZZ Flight Close reporting

3155 Communication address code qualifier
Descr: Code qualifying the communication address.
Repr: an..3

EM Electronic mail
Exchange of mail by electronic means.

FX Telefax
Device used for transmitting and reproducing fixed graphic material (as printing) by means of signals over telephone lines or other electronic transmission media.

TE Telephone
Voice/data transmission by telephone.

3225 Place/Location Identification

Refer to ATA/IATA defined three letter airport codes as published in the IATA Airline Coding Directory. For States responsible for issuing official documents, refer to ICAO Doc 9303/ISO 3166.

3227 Location function code qualifier

Desc: Code identifying the function of a location.
Repr: an..3

22 Customs office of clearance
Place where Customs clearance procedure occur.

87 Place/port of conveyance initial arrival
Place/port in the country of destination where the conveyance initially arrives from the "Last place/port of call of conveyance" (125)

91 Place of document issue
The place or location where a document is issued

92 Routing
Indication of a routing place
[PAXLST: Other places/ports within the same State or Country where the referenced flight is scheduled to land (i.e. a progressive flight)].

125 Last place/port of call of conveyance
Conveyance departed from this last foreign place/port of call to go to "Place/port of conveyance initial arrival" (87).

130 Place of ultimate destination of conveyance
Seaport, airport, freight terminal, rail station or other place to which a means of transport is ultimately destined
[PAXLST: Place of ultimate destination of conveyance" within the same State/Country for progressive flight]

174 Place of residence
A place where a party lives
[PAXLST: Country of Primary Residence]

178 Port of embarkation
Port where the person embarks onto the conveyance
[PAXLST: Place where passenger began the current journey]

179 Port of disembarkation
Port where the person disembarks from the conveyance
[PAXLST: Place where passenger will terminate the current journey]

180 Place of birth
Place where the person was born.

3493 Nationality code qualifier

Desc: Code qualifying a nationality.
Repr: an..3

2 Current nationality
Current nationality

4451 Text Subject code qualifier

Desc: Code qualifying the subject of the test.
Repr: an..3

BAG Passenger baggage information
Information related to baggage tendered by a passenger, such as odd size indication, tag

6069 Control total type code qualifier

Desc: Code qualifying the type of control of hash total.
Repr: an..3

41 Total number of crew
The total number of crew.

42 Total number of passengers
The total number of passengers aboard the conveyance.

6311 Measurement purpose code qualifier
Desc: Code qualifying the purpose of the measurement.
Repr: an..3

CT Counts

WT Weights

6411 Measurement purpose code qualifier
Desc: Code qualifying the purpose of the measurement.
Repr: an..8

KGM Kilograms

LBR Pounds

7365 Processing indicator description code
Desc: Code specifying a processing indicator.

173 Information, verified
The information has been verified.

174 Information, not verified
The information has not been verified.

8051 Transport stage code qualifier

Desc: Code qualifying a specific stage of transport
Repr: an..3

20 Main-carriage transport
The primary stage in the movement of cargo from the point of origin to the intended destination
[PAXLST: The flight for which API is applicable.]

34 Overflight
The movement of a conveyance through the airspace over the territories of a country without landing within the territories of the country
[PAXLST: The flight for which over-flight API is applicable.]

9005 Employment category description code
Desc: Code qualifying Employment Category
Repr: an3

CR1 cockpit crew or individuals inside cockpit
CR2 cabin crew
CR3 airline operation management with cockpit access
CR4 for cargo non cockpit crew and/or non-crew individuals
CR5 pilots on board but not on duty

9017 Attribute function code qualifier
Desc: Code qualifying an attribute function.
Repr: an..3

2	Person Attribute refers to a person

9019 Attribute Description Code

Desc: Code specifying an attribute.
Repr: an..3

ICAO 9303 Sex Types

M	Male
F	Female
X	Unknown

Other Sex Types

U	Unknown

— — — END — — —