White Paper: Data Protection and International Carriage By Air

First Edition - May 2024

Contents

First Edition - 14 June 2024

Foreword

Keeping personal data safe and secure is a shared responsibility of governments and industry, including airlines. Developed in 1980, the Organization for Economic Cooperation and Development (OECD) Privacy Guidelines were the first internationally agreed privacy principles, long before the internet and the highly connected world that we know today. However, since that time, the rapid development of social media platforms, virtual reality, smart devices, and artificial intelligence has forced governments to adapt their legislation to new realities.

The EU's General Data Protection Regulation (GDPR) came into force in 2018, prompting many other countries to introduce or amend their own data protection laws. These laws vary, creating challenges for privacy and data protection, especially when data and personal information crosses borders. In our globalized world, the G7 and others now recognize the need for more international cooperation to prevent fragmentation and promote interoperability and certainty for consumers and businesses.

This White Paper explains some of the specific challenges faced by the airline industry as a truly international sector. These challenges often result from the unique characteristics of the airline operating and regulatory environment- characteristics that were not considered when most privacy and data protection laws were written. The White Paper identifies some high-level recommendations for additional work and dialogue, including some possible options for the short, medium, and long term. Prepared with input from members of the IATA Privacy Law Working Group (PLWG), it is hoped this White Paper will be useful material for the future work of the International Civil Aviation Organization (ICAO) on these issues. I thank each member of the PLWG for their time, contributions, and commitment.

Finally, let me make it clear that airlines are not seeking to avoid their responsibilities under privacy and data protection laws or to protect personal information. On the contrary, the White Paper is an attempt to identify the work necessary to better enable our member airlines to protect personal information while driving the international air connectivity that delivers significant benefits to our communities, economies, and nations. We look forward to working with governments, data protection and privacy experts, international organizations, and other groups in a spirit of openness and cooperation in this important endeavor.

Leslie MacIntosh
Corporate Secretary and Acting General Counsel

1. Executive summary

Air transport is at the heart of the global economy. It creates employment, facilitates trade, enables tourism, and supports sustainable development all around the world. Everyday 12.5 million passengers are safely and securely transported on over 128,000 flights between over 21,000 different city-pairs.

While ensuring the safety and security of their customers is always the top priority for airlines, compliance with data protection laws is also critical. In order to transport our 12 million flying passengers per day, airlines safely and securely share personal data with partners in the aviation value chain, including other airlines, airports, ground handlers, travel agents, and border control authorities.

The air transport sector has long been recognized by the 193 States who are members of the International Civil Aviation Organization (ICAO) as having "special characteristics". Given this, it has also been recognized that governments ought to be particularly careful in avoiding unilateral and extraterritorial measures that may adversely affect the development of international air transport.

Regrettably, today's data protection laws are fragmented and inconsistent, an issue that is exacerbated when multiple laws apply simultaneously to scenarios of international carriage by air.

In addition, data protection laws frequently conflict with other laws such as United Nations (UN) mandated obligations to provide Passenger Name Record (PNR) information for the prevention of serious crime and terrorism. As a result, ICAO member states have taken significant steps to agree Standards and Recommended Practices (SARPs) to facilitate the provision of PNR data (Amendment 28 to Annex 9 of the Chicago Convention). Unfortunately, those steps have only been partially successful, with airlines facing the threat of fines or an inability to provide connectivity due to the conflict between the states requiring such data and those who refuse to allow it to be provided it due to privacy concerns.

These issues can be addressed through greater multilateral intergovernmental collaboration with the objectives of interoperability between data protection laws and overcoming barriers to cross-border data flows.

In September 2023, IATA in cooperation with ICAO, held a seminar on data protection and international air carriage in Montreal, Canada.[1] This collaboration aligns with both ICAO and IATA's missions of ensuring safe and orderly development for aviation.

Following the seminar, there is consensus amongst stakeholders that ICAO should bring together a multi-disciplinary group of experts to review how data protection laws interact with international civil aviation.[2]

However, it is recognised that many of these issues are not specific to aviation, and there is a need for IATA and ICAO to collaborate with other intergovernmental bodies such as the Organization for Economic Cooperation and Development (OECD). As an example, the OECD's "Data Free Flow with

[1] **Available via ICAO TV. See: https://www.icao.tv/data-protection-and-international-carriage-by-air-seminar**
[2] **Conrad Clifford, "Thoughts on ICAO's role in data protection". See: https://www.iata.org/en/pressroom/opinions/thoughts-on-icaos-role-in-data-protection/**

Trust" initiative which IATA has contributed to, aims to overcome barriers to cross-border data flows and is supported by the G20/G7 and the World Economic Forum (WEF).

This White Paper is intended to inform stakeholders of the specific challenges faced by the air transport sector and suggests a series of initiatives that IATA and ICAO could progress - in some cases in collaboration with other intergovernmental bodies such as the OECD.

It sets out information on the types of personal data handled by airlines and the role and regulation of international aviation before going on to explain the key challenges faced by airlines as regards privacy and data protection laws. We then examines the specific challenges to deal with the provision of data to government bodies.

The final part of this White Paper summarizes the key work of IATA to date in this area and suggests next steps for IATA, the proposed ICAO expert group and for further IATA-ICAO engagement with other inter-governmental bodies.

The aim of these endeavors is better protection of personal data and continued compliance with national data protection laws. By working constructively with States, ICAO and other international organizations, IATA believes it is possible to achieve these goals while also facilitating the continued development of air connectivity for the economic and social benefit of governments and their citizens.

2. Privacy, data protection and international aviation

2.1. What is personal data?

"Personal data" refers to any information relating to an identifiable person. It can include names, dates of birth, identification numbers (i.e., passport, ID or visa numbers), location data, online identifiers, payment details and residential or email addresses, and information relating to the physical, physiological, medical, economic, cultural or social characteristics of a person. One characteristic of personal data is its potential to be used, directly or indirectly, to identify an individual, either by itself or when combined with other information.

Privacy and data protection laws regulate the collection, use, retention, and transfer of personal data. These laws specify what airlines and other companies must do when they collect, use, retain or transfer such data.

2.2. What personal data do airlines handle?

In transporting over 12 million passengers per day, airlines safely and securely collect and share personal data with partners in the aviation value chain, including other airlines, airports, ground handlers, travel agents and border control authorities.

Airlines need to collect, process and transfer data to those third parties to ensure that passengers can travel internationally and receive the services they require, as well as to comply with applicable legal requirements.

Key examples are as follows:

- **Bookings:** Personal data is shared when a passenger books air travel and related services either directly with an airline, via another airline (under an interline or codeshare arrangement)[3] or through a travel agent or a travel management company. A passenger (as well as employees assisting them) must be able to access and, if necessary, modify their booking details from any location.

- **Check-in and airport processes:** Personal data is transmitted between airlines and others that may be involved in providing different services to passengers such as check-in, access to airside areas within the airport and for the boarding of the aircraft. Where services are required at a transfer or arrival point, for example, personal information is also required for use in the place of transfer or arrival.

- **Government requirements:** Personal data may be transmitted between airlines and government authorities. This includes information contained in passports or other identity documents ("API" data) and an extract of the information contained in the passenger booking, commonly known as the Passenger Name Record ("PNR" data). This information is needed by government authorities to maintain records of those entering and exiting their countries and to

[3] When two airlines have an **interline agreement**, it allows passengers to book through itineraries on two (or more) airlines with less hassle than booking each segment separately. For example, travellers only have to check in once for all the flights on the itinerary, receive all their boarding passes, and their baggage will be transferred from the first airline to the second airline without having to collect it and drop it off again. A **codeshare flight** is one in which an airline operates a flight but has agreements with other airlines that they can market the same flight as if it were part of their own network giving consumers greater choice.

validate a passenger's entitlement to travel under immigration law. This information may also be used by government authorities to identify if a passenger is a person of interest for other purposes (in relation to serious crime or terrorist activity, for example).

2.3. What personal data do governments require from airlines?

The requirements to provide data to governments flow from state sovereignty and a government's inherent right to control its own borders. Article 13 of the Chicago Convention recognized the right of each country to determine the "entry, clearance, immigration, passports, customs, and quarantine" requirements for persons "upon entrance into or departure from, or while within the territory of that State".

In this White Paper, we not only explore the issues relating to government requests for Advance Passenger Information (API) and Passenger Name Record (PNR) data but we recognize there are others such as law enforcement requests, health data requests and air accident/incident investigations.

What is Advance Passenger Information?

API data is, among other elements, the data contained in the passenger's passport or identity card which is collected at check in (on-line or at airport) or on boarding a flight to the country of departure and/or arrival.

API data is used to validate a **known** passenger entitlement to travel (such as under visa and visa waiver programs) and to identify if a passenger is a known person of interest to border control and law enforcement.

API data is the same data that is collected by border authorities directly from the passenger upon arrival.

What is Passenger Name Record data?

PNR data is an extract from the passenger booking record, the Passenger Name Record. Information contained in a PNR is collected for airline's operational and commercial purposes. PNR data contains a significant amount of personal information that is subject to data protection regulations worldwide.

The purpose of the provision of PNR data is to assist border authorities and law enforcement with the identification of **unknown** persons of interest using that information in combination with other data allowed persons to be identified.

2.3.1 Advance Passenger Information (API)

The requirement to provide API data to government authorities started in the 1980s, with adoption growing slowly initially and wider adoption following the 11 September 2001, attacks on the United

States. In 2014 the UN Security Council, under its Chapter VII powers, passed a resolution (UNSC Resolution 2178, 2014)[4] to require all UN states to implement API systems.

The provision of API data to government authorities has not been viewed as contentious in terms of data protection laws as the same data is ultimately provided by the passengers to border authorities on departure and/or arrival when passports or identity cards are inspected.

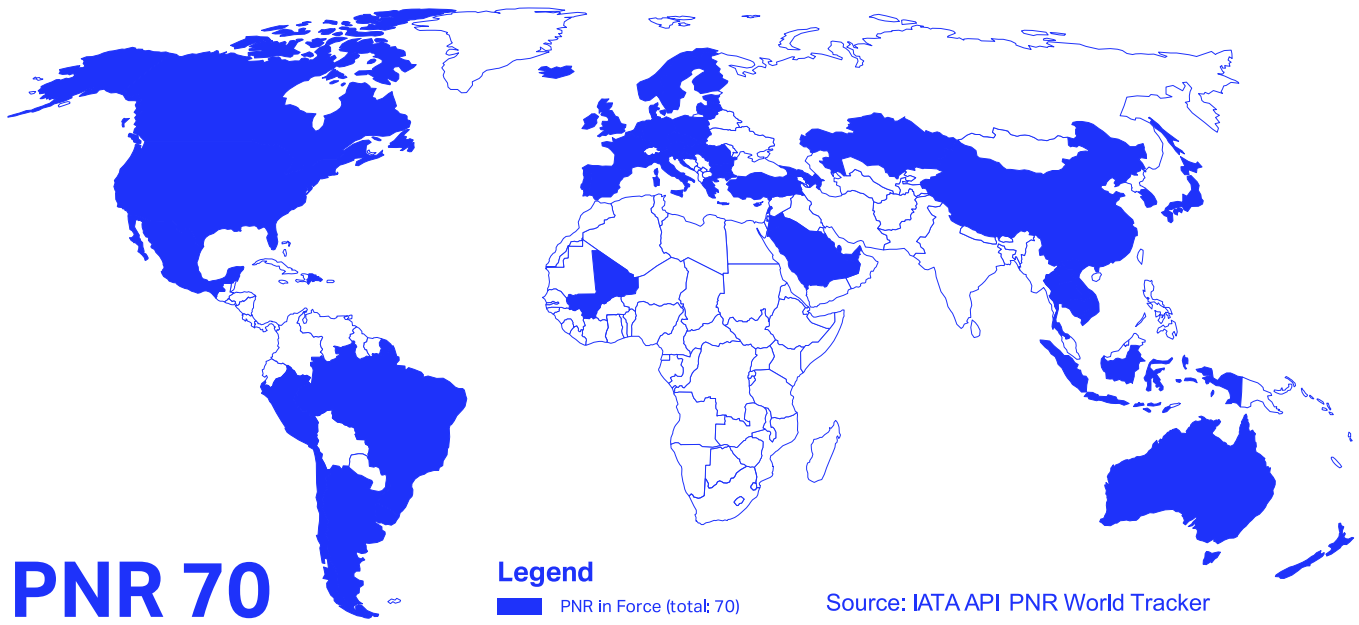
2.3.2 Passenger Name Record (PNR) data

Following the 11 September 2001, attacks on the United States, in October 2001, a requirement to provide PNR data was introduced by the US government.

The requirement to provide PNR data was then adopted by other countries in the following years and that accelerated following the UN Security Council, again under its Chapter VII powers, passed a resolution (UNSC Resolution 2396 (2017)) to require all UN states to implement both PNR and API systems.

At present, some 70 countries have requirements for the provision of PNR data as shown in the graphic below.

Global PNR implementation status



2.3.3 Other types of personal data

It should be noted that many governments require airlines to collect and provide personal information other than API or PNR data. Government legislation can require airlines to collect such information for immigration, public health, customs, law enforcement or other border management

[4] See https://www.un.org/securitycouncil/s/res/2178-%282014%29#:~:text=Decides%20that%20with%20regard%20to,to%20resolution%202161%20(2014)

purposes. In most cases, the failure to collect and transmit this information to the government concerned attracts regulatory liability on the part of the airline.

During the COVID-19 pandemic, for example, many governments required airlines by law to collect personal information relating to the medical condition, test results and vaccination status of passengers and transfer that information to the government before arrival.

3. International air transport and its regulatory and operational characteristics

The 193 Contracting States to the Chicago Convention work through the International Civil Aviation Organization (ICAO) on a multilateral basis to develop standards, practices, and policies to ensure that "international civil aviation may be developed in a safe and orderly manner and that international air transport services may be established on the basis of equality of opportunity and operated soundly and economically"[5].

One of the key objectives of the Chicago Convention and the ICAO regulatory framework is uniformity in both technical and legal standards. It has been recognised that, in order for international air transport activities to be undertaken effectively and efficiently between countries, the rules applicable to these activities need to be either uniform or closely consistent in their substantive content and application. Given the importance of data to the modern processes of international travel, it stands to reason that a similar philosophy should be applied to the data protection aspects of international air transport operations.

The parties to the Chicago Convention have recognized the need to "avoid adopting unilateral and extraterritorial measures that may affect the orderly, sustainable and harmonious development of international air transport and to ensure that domestic policies and legislation are not applied to international air transport without taking due account of its special characteristics".[6]

ICAO member states recognize the need to "avoid adopting unilateral and extraterritorial measures that may affect the [...] development of international air transport."

Airline companies are particularly sensitive to data protection laws that regulate their ability to collect and use personal data required for travel across international borders. Unlike some other industries, the relevant service includes the movement of a person across international borders and therefore also implies the processing of data across international borders. It is axiomatic that, for example, the international handling and transfer of personal data is not a matter of business convenience in the airline context but a matter of obvious practical necessity. In IATA's view, this is essential context that ought to be taken into by governments in the development of domestic policies and legislation on privacy and data protection.

[5] ***Preamble, Chicago Convention***
[6] **Policy and Guidance Material on the Economic Regulation of International Air Transport (Doc 9587), ATConf/5 Declaration of Global Principles for the Liberalization of International Air Transport (5.4), see https://www.icao.int/Meetings/atconf6/Documents/Doc%209587_en.pdf**

4. The challenges for international aviation

The key challenges for international civil aviation regarding data protection laws are as follows:

1. **Data protection laws exist globally but are inconsistent.**
2. **Multiple data protection laws may apply simultaneously.**
3. **Data protection laws increasingly conflict with other laws.**
4. **Data protection laws create barriers to cross-border data flows.**
5. **Data localization requirements are unworkable.**

This section of the White Paper explores each key challenge below.

4.1. Data protection laws exist globally but are inconsistent

Data protection laws now apply in almost every state. As of February 2023, 162 countries have such laws in effect or under consideration, which leaves only 36 UN member states without such laws. It is predicted that all countries will have data protection laws within the next 10 years.[7]

These data protection laws have developed in a fragmented and inconsistent way, with different substantive and procedural requirements applying (or proposed to apply) when comparing different countries and within federal states at the state/province level (e.g., USA/Canada).

For international aviation, the challenge of a patchwork of different requirements is particularly acute. Airlines do not operate in each country in isolation but operate a connected network with aircraft, crew and passengers travelling between multiple locations. The ability to take a consistent approach is therefore not simply a matter of convenience but one of necessity.

The approach to the required legal bases for the processing personal data varies significantly - some laws provide that all processing is permitted unless prohibited and others prohibit processing unless it comes under a specific legal ground or legal basis. There are clear differences on certain requirements, for example, the requirement to obtain consent and what consent means. Further details are set out in Annex A (regarding the available basis for handling personal data) and Annex B (which deals with the requirements for international transfers of data).

The approach to international data transfers also varies widely, including as to when transfers are permitted and under what substantive and procedural requirements. More details are set out below in Section 4.4 and in Annex B.

4.2. Multiple data protection laws may apply simultaneously

The primary basis for the application of data protection laws is the physical or legal presence of the business entity collecting and processing the personal data within the territory or jurisdiction of the state.

However, many data protection laws also apply extra-territorially even when there is no physical or legal presence in that state, some applying based on the relevant act of offering products and

[7] **Global Data Privacy Laws 2023 (2023) 181 Privacy Laws and Business International Report (PLBIR) 1, 2-4, Graham Greenleaf, University of New South Wales, Faculty of Law. Date Written: February 10, 2023. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4426146.**

services to individuals within a state (e.g. EU, Brazil, Vietnam, China and India); and others based on the citizenship of the individuals whose data is being collected or processed (e.g. Nigeria and Philippines).

Differing criteria for application mean that two or more data protections laws may apply at the same time.

4.3. Data protection laws increasingly conflict with other laws

Airlines are subject to requirements to provide data to government authorities, such as border control and law enforcement. Those requirements can come into direct conflict with applicable data protection laws, which may not recognize the law of the other country as a valid legal ground or basis. Airlines may then face the prospect of fines or other regulatory action.

That issue is examined further in Section 5 in the context of requirements to provide booking information, known as PNR (Passenger Name Record) data.

4.4. The laws create barriers to cross-border data flows

In a number of states, there are complex substantive and procedural rules that create barriers to cross-border data flows and in many cases an assessment is required to check if the laws of the other state are "adequate". While the requirement of adequacy is mainly seen as an approach taken under EU GDPR by the 27 EU member states, it has been adopted by many states outside the EU – the adequacy concept is recognized by a total of 61 non-EU countries.[8]

However, the approach to who should be doing the assessment, when it is required and the substantive requirements vary widely and there is at present no mutual recognition or interoperability on adequacy assessments. Where such adequacy decisions are required, they can play one of three roles:

1. Obligations for organizations to make adequacy assessments

Following decisions of the EU courts in the 2020 "Schrems II" judgement, organizations are required to conduct adequacy assessments by organizations even a recognized transfer mechanism is being used - such as standard contractual clauses. The scope of such assessments is detailed and complex and extends to the role of state surveillance laws, the effectiveness of the court system and a whole range of other issues under the laws of the other state. The implication of those requirements was made most visible when in 2023, Meta (Facebook) was ordered to stop data transfers to the US and notified of a proposed fine of USD 1.2 billion as it had relied on the standard contractual clauses mechanism for data transfers between the EU and US but it was determined US law did not provide adequate protection for the data being transferred.

2. Government adequacy decisions to facilitate data transfers

Some data protection laws have a mechanism to enable data transfers by government bodies recognizing other states data protection laws as adequate. The issue with that approach is that

[8] **See *Privacy and/or Trade*", see https://lawreview.uchicago.edu/sites/default/files/02_Chander_ART_Final.pdf. Also see the Council of Europe 2001 publication "*Additional Protocol to Convention 108 regarding supervisory authorities and transborder data flows*", which has been ratified by 44 states and signed by a further 7 states, see https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=181.**

progress has often been slow. For example to date, the EU has only recognized the following states as having adequate data protection laws outside the EEA: Andorra, Argentina, Canada (commercial organizations only), Faroe Islands, Guernsey, Israel, Isle of Man, Japan (private sector only), Jersey, New Zealand, Republic of Korea, Switzerland , the United Kingdom under the EU GDPR and the EU Law Enforcement Directive, the United States (commercial organizations participating in the EU-US Data Privacy Framework) and Uruguay.[9] In addition, there are further limits to the value of those adequacy decisions as they have been subject to successful challenge in the courts, for example the EU recognition of US adequacy is now into its third iteration (EU-US Data Privacy Framework) after being invalidated by the "Schrems II" judgement showing the fragility of these critical mechanisms.

3. Government decisions to block data transfers

There are other examples where the laws approach is that data transfers are generally permitted but there is a mechanism provided, such as under Indian Digital Personal Data Protection Act (2023), to block some or all personal data transfers.

4.5. Data localization requirements are unworkable

The term "data localization" has been interpreted in different ways; in this White Paper it refers to a country requiring data to be hosted within a country and not to restrictions or safeguards for data to be transferred outside that country. Data localization has been suggested at various times by various states including Russia, Vietnam, UAE, Kenya and Indonesia.

However, airline operations require that there is a single record of their inventory and bookings (without that it would result in unintended duplicate bookings for the same flight). The localization concept is unworkable for practical reasons and inconsistent with the approach following the Chicago Convention to "ensure that domestic policies and legislation are not applied to international air transport without taking due account of its special characteristics".

[9] **See** https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

5. Case study: a multilateral approach to PNR data?

It has long been recognized that one solution to the PNR information requirements of governments, as dealt with in section 2.3 above, is a multilateral approach (i.e., agreements between multiple states) rather than a bilateral approach (i.e., agreements between just two states). The EU, for example, first suggested a global multilateral approach to these issues in 2003.[10]

In 2017, pursuant to UNSC Resolution 2396, ICAO was given a mandate to introduce PNR standards and recommended practices for member states. In 2020, ICAO finalized PNR standards and recommended practices as Amendment 28 to Annex 9 of the Chicago Convention for adoption by ICAO members.

ICAO's work was successful in establishing the baseline of a multilateral approach to the provision of PNR data.

5.1. A bilateral approach to PNR and its pitfalls

However, the potential of this work was limited, as following decisions of its courts on PNR data and data transfer more generally (see box below), in 2021 the European Commission directed EU member states to file a "N*otification of Difference*" under Article 38 of the Chicago Convention. The statement provided that "the requirements resulting from [European] Union law in respect of the transfer and processing of PNR data are more exacting than" those under the ICAO proposals.[11]

As a result, there remains an EU requirement to have a bilateral agreement with additional requirements to be met in addition to the multilateral ICAO approach agreed in Amendment 28 of Annex 9 of the Chicago Convention.

[10] Communication from the Commission to the Council and the Parliament - Transfer of Air Passenger Name Record (PNR) Data: A Global EU Approach /* COM/2003/0826 final */, see https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52003DC0826:EN:HTML.
In addition, in 2010: Communication from the Commission of 21 September 2010 on the global approach to transfers of Passenger Name Record (PNR) data to third countries COM(2010) 492 final, see https://eur-lex.europa.eu/EN/legal-content/summary/a-global-approach-to-pnr-data-transfers.html.
[11] See Council Decision (EU) 2021/121 of 28 January 2021: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2021.037.01.0006.01.ENG

Timeline of key events regarding EU Data Transfers (including PNR Agreements)

2000: European Commission grants adequacy for the US Safe Harbor Scheme:2000
2001: US issues requirement to provide PNR data
2004: EU-US PNR Agreement
2006: CJEU invalidates 2004 EU-US PNR Agreement (UE-US enter into interim agreement)
2012: EU - US PNR Agreement
2013: Snowden revelations re US 'Prism' internet communications interception scheme
2015: CJEU invalidates adequacy decision for US Safe Harbor scheme ("Schrems I" case)
2016: European Commission grants adequacy for the EU-US Privacy Shield
2017: CJEU opinion rejects proposed EU-Canada PNR Agreement
2018: EU GDPR and EU PNR Directive enter into effect (replaces earlier legislation)
2020: CJEU invalidates adequacy decision for EU-US Privacy Shield ("Schrems II" case)
2020: ICAO publishes Amendment 28 to Annex 9 of the Chicago Convention
2021: EU files "notification of difference" with ICAO to Amendment 28 to Annex 9
2023: European Commission grants adequacy for the EU-US agree Trans-Atlantic Data Privacy Framework
2023: NOYB/ Max Schrems state they will challenge Privacy Framework at the CJEU.

The issue should however not be seen as a uniquely EU issue, noting that at present 61 states outside the EU have some form of requirement for data protection laws to be adequate before data transfers to those countries.[12] With new laws and amendments to laws there is an increasing prospect of other countries (or their courts) determining that the multilateral approach in Amendment 28 of Annex 9 is not sufficient.

In addition, due to the extra-territorial application of data protection laws transferring data between two countries can be blocked if a third country's laws apply to the relevant airline asked to provide data.

5.2. Where does a bilateral approach leave provision of PNR data?

Without a functioning multilateral approach to the provision of PNR data (as originally envisaged by Amendment 28 to Annex 9), airlines remain caught in a conflict between the requirement to provide PNR data and the requirement to comply with applicable data protection laws. Bilateral efforts seem very unlikely to resolve these issues, because:

1. A bilateral approach is often too slow given the number of counties that need to agree; and
2. A bilateral approach cannot resolve issues relating to third countries.

5.2.1 Bilateral agreements are slow

The issues with the speed of agreeing matters with a bilateral approach can be clearly seen from the EU experience – the EU has agreements or negotiation mandates in place with only 8 of the 47

[12] See *Privacy and/or Trade*" https://lawreview.uchicago.edu/sites/default/files/02_Chander_ART_Final.pdf

countries outside the EU who currently require PNR data (see our box entitled "Status of EU PNR Agreements" below).

Notably, and while the EU has progressed further with recognition of "adequacy", adequacy decisions are not extended to cover PNR data transfers which require a separate agreement.

Status of EU PNR Agreements

United States of America: 2012 Agreement in effect (replacing 2004 agreement invalidated by CJEU in 2006 and the 2006 interim agreement).
Canada: 2006 Agreement. Proposed replacement agreement rejected by CJEU in 2017. Negotiations for a new agreement concluded and revised agreement announced 24 November 2023.
Australia: 2012 Agreement.
UK: 2020 EU-UK Trade and Cooperation Agreement.
Japan: EU PNR negotiation mandate approved in 2020 following the 2019 EU adequacy decision regarding Japan.

5.2.2 A bilateral approach cannot resolve issues relating to third countries

There are some issues bilateral agreements cannot address, as they involve third countries:

- Even if two countries agree terms for the provision of PNR data between them, a third country's laws may still apply to the airline asked to provide the data and may prevent the provision of such data.
- A country sending data may have concerns regarding the onward transfer of PNR data from the original receiving party other countries in addition to the original recipient.

In IATA's view, the best way forward is a re-engagement through ICAO to the multilateral process to find implementable solutions that respect data protection laws while achieving the important objectives to prevent serious organized crime and terrorism.

In addition, where possible, alternative technical solutions that reduce the role of airlines in the transfer of data for these purposes should be actively pursued so that governments take the primary role of collecting data within their own states and then providing it onwards to other states.

6. Moving towards solutions

6.1. Work to date

IATA has been actively working to raise attention to these issues, with the support of the IATA Privacy Law Working Group:

- March 2022: IATA submitted a Working Paper to the ICAO Legal Committee on the issues raised in this White Paper.[13]
- April 2023: IATA contributed to the work for OECD paper "*Moving forward on data free flow with trust - New evidence and analysis of business experiences*".[14]
- October 2023: IATA organized an ICAO-IATA conference on "Data protection and international carriage by air" held in Montreal in October 2023, as reported on by the IATA Deputy Director General[15], and with attendees from ICAO, ICAO government member representatives, IATA airline members and other organizations including the OECD.
- January 2024: IATA worked with ICAO to remind ICAO members of their obligations in relation to Amendment 28 to Annex 9 and the need to (ICAO Election Bulletin 2024/3)
- February 2024: IATA sought to raise awareness of these issues with IATA members at the IATA World Legal Symposium in Vancouver and with an IATA "*Airlines*" magazine article entitled "*A fragmented global approach to data privacy*".[16]

6.2. Next steps

The next phase of work on these issues should move from awareness raising to identifying realistic options with a focus on possible multilateral solutions.

The suggestions below are split as follows: firstly, actions for IATA to lead on and, secondly, areas where IATA believes it needs to work with ICAO and thirdly those where IATA (and potentially ICAO) needs to work with international and regional organizations active in privacy and data protection law enforcement and reforms.

For each objective, the time period suggested for the activity is suggested with short term being within 12 months, medium term being 1-3 years and long term over 3 years.

A. IATA activity

The following are areas that IATA will pursue that do not have a dependency on ICAO or on wider stakeholders:

1. Submit a working paper to the 39th Session of the ICAO Legal Committee (25-28 June 2024), requesting the approval of the ICAO Council to establish a multi-disciplinary group of experts to study the interaction of national data protection laws and international carriage by air.

[13] See https://www.icao.int/Meetings/LC38/Documents/WP/LC38%20WP%207-1%20EN%20Privacy%20laws%20and%20International%20carriage%20by%20air.pdf.
[14] See https://www.oecd-ilibrary.org/science-and-technology/moving-forward-on-data-free-flow-with-trust_1afab147-en.
[15] See https://www.iata.org/en/pressroom/opinions/thoughts-on-icaos-role-in-data-protection/.
[16] See https://airlines.iata.org/2024/02/20/fragmented-global-approach-data-privacy.

B. ICAO related activity

The following are areas that IATA suggests are best pursued in collaboration with ICAO and are focused narrowly on the aviation sector the challenges it faces and informing aviation specific solutions.

1. Creation of a specialist ICAO working group establish a multi-disciplinary group of experts to study the interaction of national data protection laws and international carriage by air. [**Short term**]
2. A review of options to update Amendment 28 to Annex 9 to meet requirements of all ICAO members [**Medium term**].
3. A comparative review of the approach to extra-territoriality in the sphere of data protection law with a focus on international aviation and to develop ICAO policy and guidance on approach to extra-territoriality in context of international civil aviation (such guidance exists already for anti-trust/competition law). That can then inform engagement through ICAO and IATA with other stakeholders as set out below. [**Medium term**]
4. A comparative review of the legal basis for the processing and transfer of data to support interoperability and to inform drafting of legislation and guidance when ICAO members are passing new and updated data protection legislation. [**Medium term**]
5. An ICAO policy position on data localization and the challenges for international aviation [**Medium term**]

C. Privacy organization related activity

The following describes areas where the focus is broader than ICAO/ IATA and the aviation sector:

1. Engagement with the OECD on the Data Free Flow with Trust Community of Experts activity [**Short term**]
2. Broaden engagement with other international organizations such as APEC CBPR system, ASEAN PDP Framework, Ibero-American Data Protection network (RIPD) to help drive cooperation on data flows and awareness of the issues faced by international aviation [**Short Term**]
3. Engagement through relevant stakeholders to explore options for greater inter-operability including through:
   a) alignment of standard contractual clauses, used for data transfers [**Medium term**]
   b) standardization of security requirements [**Medium term**]
   c) standardization of adequacy assessment processes such as transfer impact assessments [**Medium term**]
4. Engagement through relevant stakeholders to explore options to support moves from bilateral to multilateral or plurilateral adequacy recognition on a mutual basis [**Long-term**]

Annex A: Conflicting approaches to the legal requirements to collect and process personal data

The "legal basis" requirement

The legal basis for the collection, processing (and international data transfer) varies between different jurisdictions which presents challenges to effective operation of civil aviation and delivery of services customers expect.

However, in others, where EU GDPR applies or where the local model looks to this standard of law, the "controller" is required to have a legal basis in place to process personal data (which includes onwards data sharing), otherwise the processing is unlawful. By contrast, in the USA, the California Consumer Privacy Act does not require the particular "legal basis" for the initial collection of data to be specified, only to provide transparency on the "business or commercial purpose" for collecting the data.[17]

"The result is an overlapping patchwork of data protection laws with different substantive requirements each of which may interact with or conflict with the data protection and other laws of other states."

When looking at the APAC region, although traditionally there has been a lean towards consent, there have been recent developments in some jurisdictions to shift towards aligning with the European concepts. Processing for performance of a contract and processing necessary to comply with legal obligations are notably being relied upon as a legal basis outside of consent in such jurisdictions such as China, Korea, Malaysia, Philippines and Thailand. Singapore goes further by also recognizing legitimate interests and vital interests.

In the EU GDPR model, there are six legal bases available to process personal data, only one of which is consent which is relied on generally only where no other legal basis is available. Where 'special

[17] The CCPA defines a business purpose as: "the use of personal information for the business's or a service provider's operational purposes, or other notified purposes[…] provided that the use of personal information shall be reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed or for another operational purpose that is compatible with the context in which the personal information was collected." See: https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.140.

category data' is processed (such as health data), an additional (more restricted) lawful basis must be satisfied which has the effect of further limiting the circumstances when that data can be collected or shared.

Legal Basis for Personal Data	Legal Basis for Special Category of Personal Data
• Consent • Legitimate interests • Necessary for the performance of a contract • Legal obligation • Vital interests; and • Public task.	• Explicit consent; • Employment, social security and social protection law; • Protect vital interests; • Not-for-profit bodies; • Made public by the data subject; • Legal claims and judicial acts; • Substantial public interest conditions; • Health or social care; • Public interest in the area of public health, or • Archiving purposes in public interest, scientific or historical research.

The meaning of some of those legal bases is set out in more detail above as they are frequently much more restrictive in how they can be used than they would appear.

Below we examine further the most relied upon legal basis in the airline industry of legitimate interest, compliance with laws, consent and performance of contract.

Legitimate interests

Legitimate interests, where available, is typically relied upon for more commercial data handling reasons. Fueling business purposes as well as interests of the individuals concerned. It is in that context also used for processing where there is a regulatory, public interest context, which does not fall within the strict compliance with laws or public task legal basis. Such as where the processing is undertaken to satisfy legal requirements on a parent company in another country, but the company itself isn't directly subject to that legal requirement.

Legitimate interests are not however recognized as a legal basis on which personal data can be lawfully processed under all privacy laws (e.g. China). Where it does apply some look to the EU GDPR standard of the concept, whilst others treat the concept similarly yet differently or are just developing their approaches. Countries like Brazil for, example, have only recently introduced guidelines on the use of legitimate interest. Even within the EU there are diverging interpretations. Data protection regulators meanwhile are taking a narrower view of when it can be applied in practice to a business purpose, when weighed against the privacy rights of the individual. The paperwork required to adopt this legal basis is greater in some countries, with documented risk assessment required, and individuals' rights (such as a right to object or to erasure) linked to it.

So, whilst an important legal basis for the industry, underpinning a lot of necessary operational processing, and potential adoption of innovative technologies, the absence of a harmonized

approach to interpretation let alone application, means that legitimate interest is used with increasing caution and uncertainty.

Compliance with laws

This legal basis permits the processing of personal data to meet legal and regulatory obligations. However, this may need to be a legal or regulatory rule under the relevant domestic or specific international laws. For example, if personal data has to be disclosed by an airline based in Country A for tax reporting due to underlying local tax law in Country A, this legal basis would apply.

This legal basis also has differing applications and interpretation. Many jurisdictions allow for processing and disclosure of personal data to comply with domestic law requirements. A common example being for the prevention and detection of crime which is often dictated by local security and policing law requirements. Challenges however arise in applying this where the prevailing legal requirement is limited to domestic, particular international laws or otherwise laws which are not directly binding on the controller.

This can lead to some conflict of laws scenarios in air carriage where Airline A needs to request information to comply with legal obligations upon it, but Airline B isn't subject to those laws directly and so cannot rely on compliance with laws to pass on the data requested to Airline A.

Consent

Some jurisdictions are more consent based such as the Latin America ("LATAM") region (for example Argentina, Brazil and Ecuador) and the Asia Pacific ("APAC") region (for example South Korea, Singapore and Indonesia). Canada also generally relies on consent for data collection, use, and disclosure. Consent can take different forms.

In Europe the concept of consent is a high bar and not one that is reflected across the world. It has a very particular meaning and is only valid if it is (amongst others) freely given, specific and informed. It can be withdrawn by the individual at any time.

In APAC, Africa, and LATAM, informed consent is required. Informed consent differs from the EU concept of consent in that it can be achieved by informing the individual under what circumstance their information may be shared with third parties or third parties may have access to their information. Notice also plays a part in this exercise as typically across most regions airlines as well as travel agents are under a requirement to provide a privacy notice, alongside their terms which explains to passengers why they are collecting their personal data and what it will be subsequently used for. What must be contained in this notice differs between jurisdictions, with some being more prescriptive than others.

Reliance on consent creates heavy compliance burdens, in how it is collected, recorded and stored. There are variances and divergences at local country level, as consent and notice in China will look different to consent and notice in Singapore and South Korea, with each jurisdiction will having their own requirements which includes ensuring the consent and notice is in the local language.[18] This creates in turn significant real-world operational barriers to reliance on consent. In the air carriage context when there is a multiplicity of controllers around the globe involved at different stages.

[18] **PDPC | Comparing "Consent" Rules in General Data Protection Laws across Asia-Pacific.**

Performance of a contract

This is an important legal basis for the industry where available, but it isn't available under all privacy laws. Even if it is available interpretations again differ as to the boundaries of its application. For this legal basis to apply under the EU GDPR model the processing of personal data must be "necessary" to deliver an organization's side of the contract with the individual or in order to take steps at the request of the individual prior to entering into a contract. This does not mean that the processing must be essential for the purposes of performing a contract, however it must typically be a targeted and proportionate way of delivering the contractual service. In air carriage with its multiplicity of stakeholders delivering the overall passenger journey experience, and the strong customer desire for frictionless yet secure travel, those perimeters are increasingly difficult to navigate. Especially when viewed against a backdrop of emerging case law in the EU in which its application has been challenged in other sectors.

Legal basis in action

The example below illustrates an airline journey which involves 3 jurisdictions. and how different data is being collected and processed, and what legal basis may apply.

Example

'Passenger A' boards plane in Montreal, with 'Airline 1' travelling to Algiers via Paris.
'Passenger A' is disabled and requires assistance throughout duration of travel, including airports and the interactions involved in the connecting flight from 'Airline 1' to 'Airline 2'.

1. Initial data collection when 'Passenger A' books ticket with 'Airline 1' (Canada consent based)
2. 'Passenger A' discloses disability details – processing sensitive/ special category data to 'Airline 1' (consent).
3. Data is processed by 'Airline 1' and possibly shared onwards with other airlines/ airports (Paris Airport & 'Airline 2') involved in connecting flights (in Canada consent, but in Paris onward sharing may be consent / contract / vital interests) as airport in Paris – EU GDPR legal basis applies.
4. Data processed in airport, data collection and check in. Sensitive / Special category data processing to accommodate the needs of 'Passenger A' (assistance on the ground in airport to get passenger on and off the plane). EU GDPR legal basis applies.
5. Further data processing when 'Passenger A' travels through and connects onto flight with 'Airline 2'.
6. 'Airline 2' collects personal data, and processes 'Passenger A' onto connecting flight.
7. 'Airline 2' lands in Algiers. Processing on landing - Algerian law (similar concepts of consent, contract legal obligation, interests of data subject / vital interests).

As shown in the example above, data collection and processing varies between jurisdictions due to treating data in different ways, for example there can be restrictions on what can be collected from a given passenger and how this might be used. Therefore, what might be collected lawfully under EU GDPR as being necessary to perform a contract (the contract with passenger for the flight) or legitimate interests (used for data sharing) may require consent in the APAC or LATAM regions. This

causes airlines to have to create different customer approaches, to collection and processing of personal data, which rely on different legal basis, and which are not harmonized at a global level.

As flagged at section 4.4 there is a recognized need for greater interoperability and mutual recognition between different data protection laws.

Annex B: International data transfers

Requirements for the International data transfers

Across Europe, APAC, LATAM, the USA, and the UK various data transfer regimes are in place. It is an ever changing, unstable, complex moving landscape. Data Transfer requirements are further complicated due to a growing number of laws with different transfer requirements, and that is further complicated by extra-territorial application of some laws (as seen in section 3 above).

Data transfers and how these are structured can be viewed as 3 models: open, conditional and control.[19] In the open model (e.g. the USA), this has limited rights for individuals, less transfer restrictions and promotes greater free flow of information. However, it has been observed that an increasing number of jurisdictions are now implementing regulations regarding cross-border data transfers, including some that previously emphasized the importance of unrestricted data flow, such as the United States. In the conditional model (e.g. EU), this places greater emphasis on data transfer controls and restrictions (such as SCCs and BCRs) and focuses on the rights of the individual. Whereas in the control model (e.g. Federation of Russia), this places strict restrictions on transfers which includes data localization controls and provides governments with greater control over individuals and access to information. As an example, see below for the different transfer positions in terms of mechanisms and relevant circumstances where data transfers are permitted across the EU, China, Brazil, India and Canada.

EU position	• Adequacy decision • SCCs • BCRs • Derogations • A legally binding and enforceable instrument between public authorities or bodies • An approved code of conduct • Certification under an approved certification scheme • Administrative arrangements between public authorities
China position	• SCCs • Self-security assessment with approval from Cyber Administration of China • Certification • Where there is any stipulation on the condition or any other stipulation for the provision of personal information to a recipient outside the territory of China in any international treaty or agreement concluded or acceded to by China, such stipulation may apply..
Brazil position	• Adequacy decision • SCCs • BCRs • Express consent • Compliance with laws

[19] **Ferracane and van der Marel (2021,) "Regulating personal data: Linking different models to digital services trade | CEPR**

	• Necessary for contract • Necessary for regular exercise of rights in court, administrative or arbitration proceedings • Seals, certificates, and codes of conduct • Necessary for international legal cooperation among public intelligence, prosecution, and enforcement bodies, • Necessary for the protection of the data subject's or third party's life or physical integrity • Necessary for purposes of enforcement of a public policy or a legal duty of public service, being made public
India position	• Enforcing any legal right or claim • Processing of personal data by judicial or regulatory bodies • Processing of personal data in the interest of prevention, detection, investigation, or prosecution of any offense or contravention of any law • Processing personal data in India of individuals outside India pursuant to a contract between an Indian entity and a foreign entity (e.g., outsourcing); or • Processing for court-approved mergers, amalgamations, restructuring, etc.
Canada position	• SCCs • Entering into a data transfer contract (non-SCC) which includes the right of an oversight, monitoring, and a right to audit the services being provided and security measures. • Intragroup agreements • Consent

Adequacy Decisions

In terms of adequacy decisions these are typically based on legal instruments, for example "adequacy regulations" made in country which set out in law that the legal framework in that country, territory, sector or international organization has been assessed as providing 'adequate' protection for individuals' rights and freedoms for their personal data. As mentioned in section 4.4 of this white paper 88 countries across the world have some form of adequacy assessment of other countries data protection laws, with 61 of these being outside of Europe.[20] Although many jurisdictions recognize adequacy they are not aligned, with some countries basing their adequacy decisions on their own views and assessments whilst others default to European decisions – known as mutual adequacy decisions as seen in Japan. Typically, the focus has been on the European model of adequacy and how a third country shapes up to EU GDPR, and whether the third country provides essentially equivalent protection. This presents a conflict of laws, as other regions are not born from this model and differ largely from the EU GDPR which results in widely divergent requirements for data transfers.

Pros

- Where an adequacy decision is in place you do not need to put transfer documentation in place to cover that transfer, although you would need to clearly reference that there is an adequacy decision for the purpose of documenting this in the contract.

Cons

- Adequacy decisions only work for those countries on the given jurisdiction's "safe" list, transfers to countries not on the list will have to employ another transfer mechanism.
- Lack of mutual recognition or interoperability.
- In some instances, the adequacy decision mechanism may not be available under the prevailing law for transfers to governments.

Standard Contractual Clauses (SCCs) & Transfer Risk Assessments

The SCCs are transfer mechanisms used and developed in Europe. The EU Official Journal published two sets of new SCCs which have been available for use since June 4, 2021. Post Brexit, the UK introduced its own set of SCCs and adequacy decisions.

SCCs involve further due diligence considerations before they can be adopted. This follows the decision in the "Schrems II" case ((Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems and intervening parties, Case C-311/18) which considered the validity of Privacy Shield (which governed data transfers as between the USA and Europe) as well as aspects of the SCCs. In the Schrems II judgment, the use of Privacy Shield was invalidated with immediate effect as it was found that Privacy Shield could not ensure the protection of personal data in light of the US' excessive state surveillance powers. The EU-US Privacy Shield Framework had been in place since 2016 and it allowed for transfers to be made outside of the EEA to the US, where an organization has signed up and was a member of the Privacy Shield framework.

The Schrems II ruling also raised questions over the long term viability of the SCCs (particularly in light of any intelligence gathering laws in third countries) and as a result introduced an obligation on organizations to undertake a careful examination of the protection given to personal data transferred out of the EU (save for those countries with adequacy determinations) in order to ensure that the protection was adequate as compared to that provided in the EU. In this case the court stated that organizations need to do more to ensure the security of personal data transferred under the European Commission's SCCs framework. In other words, SCCs, without additional due diligence on the transferee and the country to which data is transferred to satisfy the transferor of the security of the data, are no longer an automatic guarantee of compliance with the rules on international transfers.

Timeline of key events regarding Schrems II case

2000: European Commission grants adequacy for the US Safe Harbor Scheme:2000.
2013: Snowden revelations re US 'Prism' internet communications interception scheme.
2015: CJEU invalidates adequacy decision for US Safe Harbor scheme ("Schrems I" case), Schrems complains to Irish Data Protection Commissioner regarding SCCs.
2016: European Commission grants adequacy for the EU-US Privacy Shield, Privacy Shield certification scheme launched.
2017: Irish Data Protection Commissioner refers the Schrems II complaint to the CJEU.
2020: CJEU invalidates adequacy decision for EU-US Privacy Shield ("Schrems II" case) but SCCs remain valid, but TRA required (and supplementary measures, as needed.

Following the Schrems II decision, companies are now required to assess whether the laws of the country to where personal data is being transferred to provides data subjects with protections that are "essentially equivalent" to those provided by European law. This assessment (known as a Transfer Risk assessment ("TRA") is required even where an adequate safeguard is in place. (e.g. SCCs/IDTA/Addendum). Companies are expected to conduct their own assessments of the third country's laws before such transfer takes place and be able to evidence this assessment has been made.

On May 22, 2023, Meta Ireland (Meta) incurred a historic GDPR fine of €1.2 billion, exceeding the previous record held by Amazon, which amounted to €746 million. The fine was imposed by the Irish Data Protection Commissioner (DPC) following a binding decision issued by the European Data Protection Board (EDPB) in April 2023. The substantial fine was levied against Meta for its transfer of personal data to the U.S. using SCCs since July 16, 2020. Additionally, Meta has been directed to ensure that its data transfers align with GDPR compliance requirements.

Pros

- The SCCs are the most used transfer mechanism, 85% of EU based companies rely on SCCs to transfer data outside of EU, whilst 5% use other mechanisms.[21]
- SCCs can be used for transfers to third parties as well as transfers to other entities within a corporate group.
- SCCs contribute positively to interoperability due to providing a common set of standards, which are fixed.

Cons

- SCCs are not used globally. In many jurisdictions (e.g. most recently India) a valid contract is sufficient but the detailed content of what must be in that contract isn't prescribed. The obligations can be extensive (e.g., in the EU SCCs) so this can be a barrier to adoption.
- The sheer scale of the exercise to adopt and sign for each airline is vast. Intra-group as well as with other airlines and stakeholders, service providers…etc. It is hugely resource draining to pinpoint every transfer where the clauses are needed, and then to document it appropriately.
- They may not be available under the prevailing law as a protective measure for all transfers e.g., if not adopted for transfers to governments.

[21] **See Digital Europe: https://www.digitaleurope.org/resources/data-transfers-in-the-data-strategy-understanding-myth-and-reality/, page 11**

- If there is a change in law (as seen with the introduction of the latest versions of SCCs) the SCCs will need to be updated, this being a timely and costly process in terms of ongoing maintenance.
- There is an expectation on the data exporter (here the exporting airline) to know when to conduct a TRA or TIA, which causes issues in terms of keeping up with fast paced emerging laws or having in depth knowledge of local surveillance and data localization requirements.
- SCCs often include provisions mandating that the data recipient falls under the jurisdiction of EU regulators, a stipulation that has resulted in the reluctance of numerous foreign recipients to engage in such agreements.

Even between jurisdictions the approach to TRAs or TIAs is not aligned as seen with the variances between data protection authorities in terms of different templates and guidance.

Binding Corporate Rules (BCRs)

In the alternative, BCRs are another available mechanism, but these only operate as between companies within the same group and cannot be used as a contract with third party entities. It involves creating a set of rules in the form of a policy which all entities within the business sign up to, using a binding mechanism – such as a power of attorney for the head company or a series of binding resolutions to bind all other companies in the group. BCRs act as global data protection policies subject to regulatory review and approval. The use of these is typically seen with large internal corporates who look to obtaining BCRs as a "gold standard". Whilst BCRs are a European transfer mechanism they are recognized in other jurisdictions, such as Turkey, Nigeria, South Africa and Argentina.

Pros

- BCRs provide a single solution for large/ multi-jurisdictional companies.
- You can create different versions, for example a controller version to manage the data flows as between controllers in the group, and a processor version to cover those entities who process on behalf of other entities in the group.
- Once in place data can freely move around the group without entities having to enter into further agreements with each other in respect of such transfers. BCRs are currently not subject to any challenge.
- BCRs contribute positively to interoperability due to providing a uniformed, binding standardized set of rules.

Cons

- BCRs can only be used for transfers around a corporate group, and will not cover transfers to third parties, and these transfers will need to be covered off by an alternative mechanism.
- To obtain BCRs, this is a project within itself, it is not a quick win and requires time and cost. Time will involve considering how to make the BCRs binding and how to structure liability in the group in terms of where a breach of the BCRs occurs. This will require internal review and audit to understand how the BCRs will reflect and align with the corporate structure in place. BCRs would need sign off at stakeholder level and internal buy in.

Certification Schemes

Certification schemes provide an alternative model whereby organizations can sign up to a scheme and once approved a certification is issued to the organization. Membership in the scheme then demonstrates compliance with specific laws.

In Asia the Asia-Pacific Economic Cooperation ("APEC") Cross-Border Privacy Rules ("CBPR") system is a government-backed data privacy certification that companies can join to demonstrate compliance with internationally recognized data privacy protections. Whilst there are some correlations, it also differs from BCRs, so it isn't a direct read across to adopt both approaches. Whilst the CBPR system was developed by 21 APEC economies and endorsed by APEC Leaders in 2011 to facilitate cross border transfers, it first requires an APEC economy to demonstrate that it can enforce compliance with the CBPR system's requirements before joining. Currently, however only nine economies participate in the system: Australia, Canada, Japan, the Republic of Korea, Mexico, the Philippines, Singapore, Chinese Taipei, and the United States.

The Global Cross-Border Privacy Rules Forum, established in 2022, is an initiative that is seeking to build on the APEC CBPR system as a framework that supports the effective protection and flow of data internationally, and seeks to widen adoption of this framework and certification approach beyond the APEC region. Whilst there are strong global ambitions, at this point only the APEC CBPR signature countries Australia, Canada, Japan, the Republic of Korea, Mexico, the Philippines, Singapore, Chinese Taipei, and the United States, together with the UK as an associate member, are initial members and work continues to set up the relevant infrastructure for businesses to obtain certification. The ASEAN Framework and the Ibero-American data protection network are other examples of non-binding multilateral agreements which also promote interoperability.

Separately in Africa, the African Union ("AU") Data Policy Framework (endorsed by the AU Executive Council in February 2022) is a framework which was released by the AU in July 2022 which seeks to establish and set out AU's digital economy plans which includes (but is not limited to) data governance, data control and cross border data flows. The AU Data Policy Framework highlights that although 32 of 55 African countries have in place or are in the process of getting into place data protection laws[22] many of these countries will not be viewed as a "safe" destination country for data transfers, due to not providing the same level of data protection seen in the exporting country. The Framework flags the need for a unilateral and harmonized adequate legal framework across African countries, managed through a centralized certification authority.

Pros

- Certification Schemes can offer a more practical way of demonstrating compliance to regulators, individuals and other third-party companies.
- Certification is a voluntary model.
- Certification schemes such as APEC and CPBR promote an interoperable model for data governance.

Cons

- Certification mechanisms can be time-consuming and costly to set up.

[22] **See AU Data Policy Framework: https://au.int/sites/default/files/documents/42078-doc-AU-DATA-POLICY-FRAMEWORK-ENG1.pdf ,page 21**

- Certification criteria will vary as between schemes and may not therefore align or be recognized across other schemes in other jurisdictions.
- Certification schemes do not offer a consistent approach for global operating industries such as airlines.

Derogations

In the absence of appropriate safeguards or adequacy decisions the EU GDPR allows for derogations in specific scenarios. These derogations allow transfers to occur where they fall into one of the specific situations described in Article 49 GDPR: (i) explicit consent; (ii) transfer necessary to perform a contract; (iii) necessary to conclude contract; (iv) necessary for important reasons of public interest; (v) for the establishment, exercise or defense of legal claims; (vi) necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or (vii) transfer is made from a public register[23].

Pros

- No additional transfer safeguard is required when relying on a derogation.

Cons

- Reliance on derogations is largely untested, and regulatory guidance on their scope is limited, so there is risk nonetheless associated with a degree of uncertainty as to whether the relevant regulators will regard a derogation as engaged, and whether all of the data processing which will take place (where there is a data transfer) falls within that which is "necessary". It is therefore preferable to use other more tested mechanisms for data transfers.

Consent

In other cases, especially in the LATAM and African regions, cross-border transfer of personal data is possible only with the consent of the subject and appropriate notice having been provided (as seen in places like Chile, Columbia and Costa Rica). In practice, foreign companies tend to include, in the form of consent to the collection and processing of personal data, a section on the consent of the subject to the cross-border transfer of personal data to the territory of foreign states.

Pros

- Gives individuals choice.
- Provides transparency around data transfers.

Cons

- Real world challenges of obtaining and recording in practice in the air carriage context.
- Consent is not interpreted consistently across the globe.

Can be withdrawn/ revoked or challenged at any time by the individual who provided consent.

[23] **See EDPB Guidelines on Derogations: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_en.**

Key touch points for airlines

For international airlines, and other stakeholders engaged in facilitating carriage by air who have global reach due to their service offerings, there are multiple data collection and data transfer touch points. There are many complex considerations at play. Different laws and requirements apply depending on where the data has originated from, in terms of the passenger and the given airlines. There is no one size fits all.

This requires in-depth assessment in terms of what needs to be covered and how for (i) the data processing and ii) the data transfers. This is a complex area which causes issues due to the risk of non-compliance in some jurisdictions for not having appropriate terms in place. This risk is heightened in the airline industry due to the regular and daily processing of high volumes of passenger personal and sensitive data.

Without a general consensus and a lack of appropriate guidance in place, airlines are forced to incorporate and reference multiple data transfer mechanisms to cover those transfers. For example, one contract may include a combination of EU (34 pages) & UK SCCs (9 pages), UK IDTA (36 pages), BCRs, (60-100 pages), China SCCs (18 pages) and Swiss and US DPF regimes (which can be structured as in clause references out to registrations online). As seen in the page numbers provided next to each transfer mechanism (this being an approximate number of pages), where each are included in one contract this has the potential to add 150-200 pages to a given contract. Further to this, the majority of these types of transfer mechanism need to be populated with the details of the specific transfer, including the type of personal data, categories of individual, security that is both in place, and to where it is being transferred.