

# Data Protection & International Carriage

**Leslie MacIntosh**

Corporate Secretary and  
Acting General Counsel



- We have heard a lot today about digitalisation in the aviation industry. Now I want to highlight an important compliance issue relevant to digitalisation and such innovation in the civil aviation industry.
- In this week in which we celebrate the 80<sup>th</sup> anniversary of the Chicago convention, this is a compliance issue facing the sector that was certainly not contemplated when the drafters of the Chicago Convention set out the framework for consistent regulations to promote the safe and orderly development of international air transport services.
- However, this compliance issue is disrupting efficient and orderly connectivity and is becoming increasingly a significant issue for IATA's airline members.
- We now all have an expectation that our personal data and privacy will be taken care of when we share it with businesses and governments for any reason.
- So what do we mean when we talk about personal data and its protection. In fact, personal data is defined in various ways by various local regulations. Generally, personal data refers to any information that can be used to identify an individual, such as your email address, home address, passport number, date of birth, and similar details.
- In some regulations, some types of personal data, such as health information, receive even more protections – this is referred to as “sensitive” data

# What personal data do airlines need to transfer internationally to facilitate air travel?

## Data sent by airlines to governments

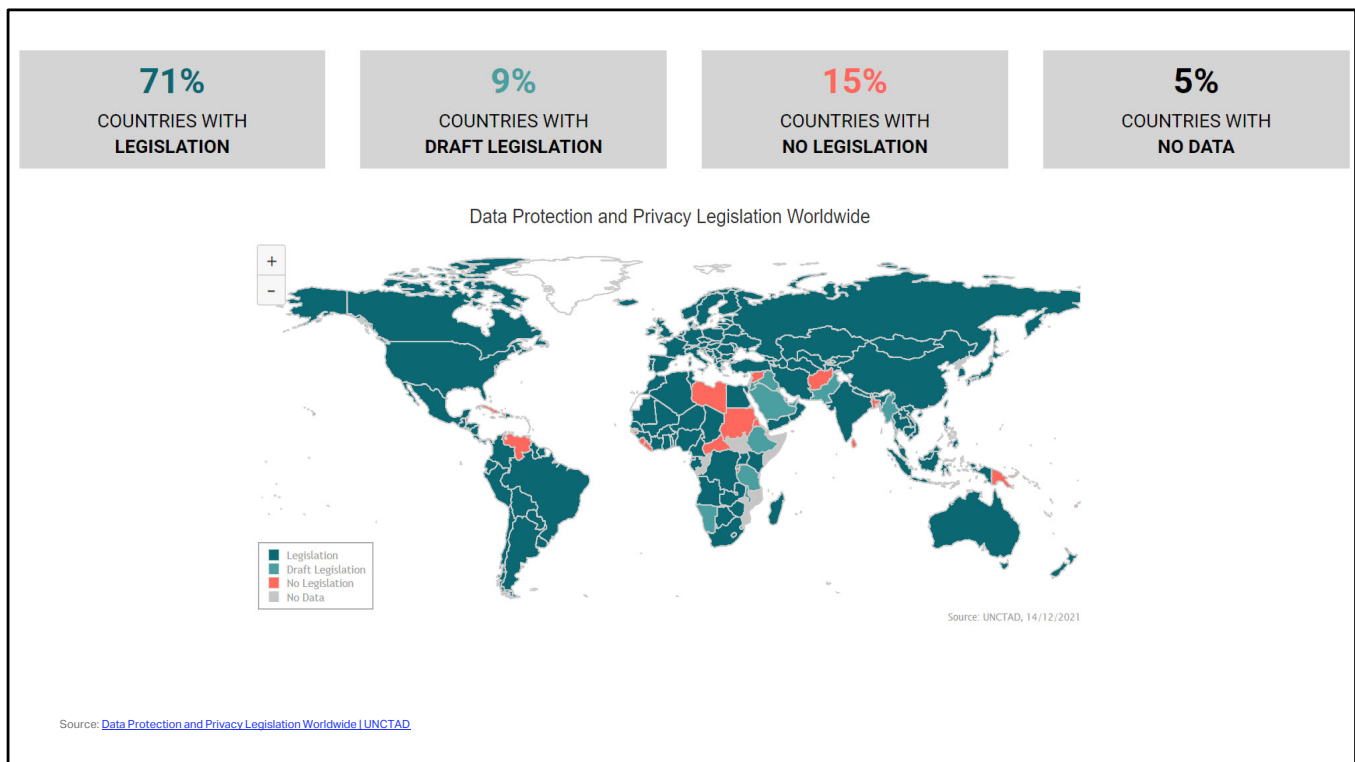
- Advance Passenger Information (API)
- Passenger Name Record (PNR)
- Health Data (notably during Covid)

## Other data sent by airlines

- to other airlines (interline/codeshare bookings)
- to/from travel agents
- to ground handlers and others involved in services
- to airport authorities



- Most of you likely travelled to Geneva by air. To make this journey possible, airlines will have had to collect, process and, in some cases, transfer your personal data outside your home country.
- But what specific data is collected and by whom? To illustrate, think of an iceberg. Above the surface lies the personal data that must be shared with governments.
- For instance, your passenger name record (PNR) data may have been sent to the Swiss government before your arrival; flight crew licences and medical certification may have been shared.
- You will of course remember that during the COVID 19 pandemic, sensitive health information was also collected by airlines and shared.
- However, there's a vast amount of other data required to support your journey, much of which is less visible – below the waterline of our iceberg.
- For example, if you were on a codeshare flight, or if you requested a special meal from the airline or special assistance such as a wheelchair, your personal data would have been shared with the relevant parties such as caterers and airports.
- In fact a special meal request or wheelchair request could involve sensitive data about religion or medical conditions.
- All of these transfers need to be done in compliance with data protection laws across different countries.
- With over 4bn passengers traveling each year, you can imagine the sheer volume of data involved and the significant compliance efforts required to manage it all.



- The introduction of regulations enshrining privacy rights and obligations to protect personal information legislation has history rooted in the social changes that started after World War 2 and gained momentum in the 1960s and 70s.
- Focus on those rights and “regulatory activity” to ensure protection of those rights accelerated over the early 2000s in large part due to the rise of social media. (e.g. Facebook founded in 2004).
- Currently, more than 140 countries have established data protection laws.
- The EU General Data Protection Regulation or GDPR became effective in 2018 - setting a significantly higher protection obligations on third parties, individual rights to control the use of personal data and introducing extraterritorial rights for EU citizens and residents wherever they are – or travel to in the world.
- This led other countries to think about data privacy and protection in a new way. Some implementing or amending their regulations to align with GDPR, some taking steps to impose measures even more significant.
- This has made the landscape increasingly complex and challenging for airlines to navigate. More on this in a moment.
- This regulatory “fever” in the wake of growing and more intrusive social was developed without considering the special characteristics of international civil aviation, that under the Chicago Convention states agreed to take into account when implementing regulations that impact civil aviation. One of those innate characteristics is that in order to transport a person across borders by air, their data needs to travel with them!

## Key challenges



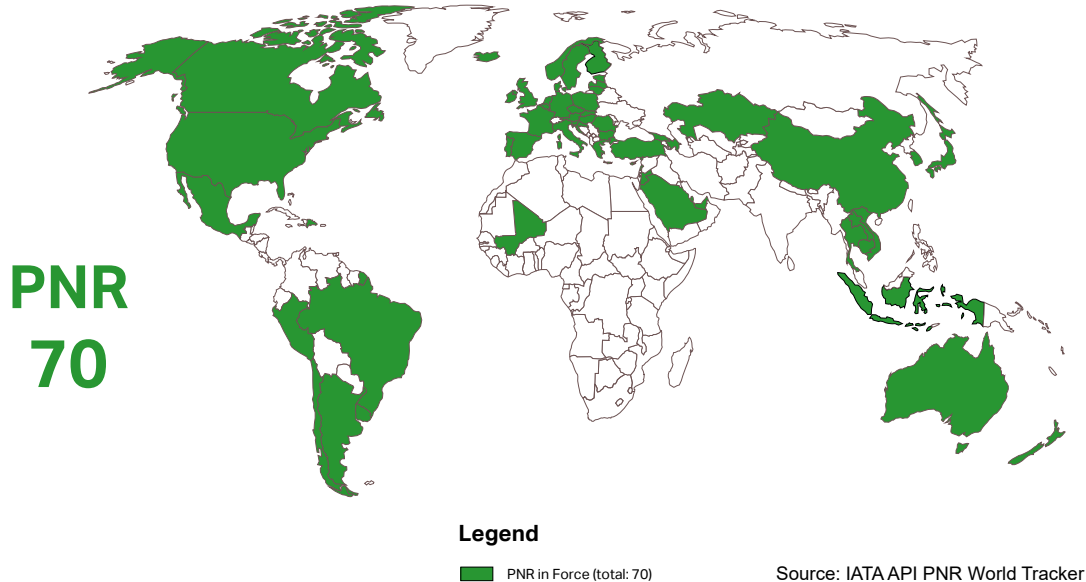
1. Multiple laws may apply simultaneously
2. Laws increasingly conflict with other laws
3. Inconsistent laws create a barrier to cross-border transfers
4. Data localization requirements are unworkable for airlines

There are several key challenges impacting airlines. Let me highlight a few of them:

- Laws are inconsistent – the legal basis for collection and use can be different - for example under EU GDPR, explicit consent is prioritised, and individuals are empowered to make decisions on the use of their data with full knowledge of its potential use. In contrast, the Canadian law, PIPEDA, allows for organisations to infer consent in certain situations and places more emphasis on the actions of the organisation using personal data.
- As we saw in the video, extraterritoriality means that multiple laws may apply to a passenger's itinerary – this makes it difficult to determine which law applies and it also creates confusion for consumers as they do not know who is ultimately responsible for protecting their data. Not all countries have data protection regimes that apply extraterritorially – the PIPEDA in Canada for example does not.
- Laws increasingly create conflicting and inconsistent obligations on airlines – creating barriers to cross border transfers and ultimately connectivity. I'll explain this in more detail on the next slide.

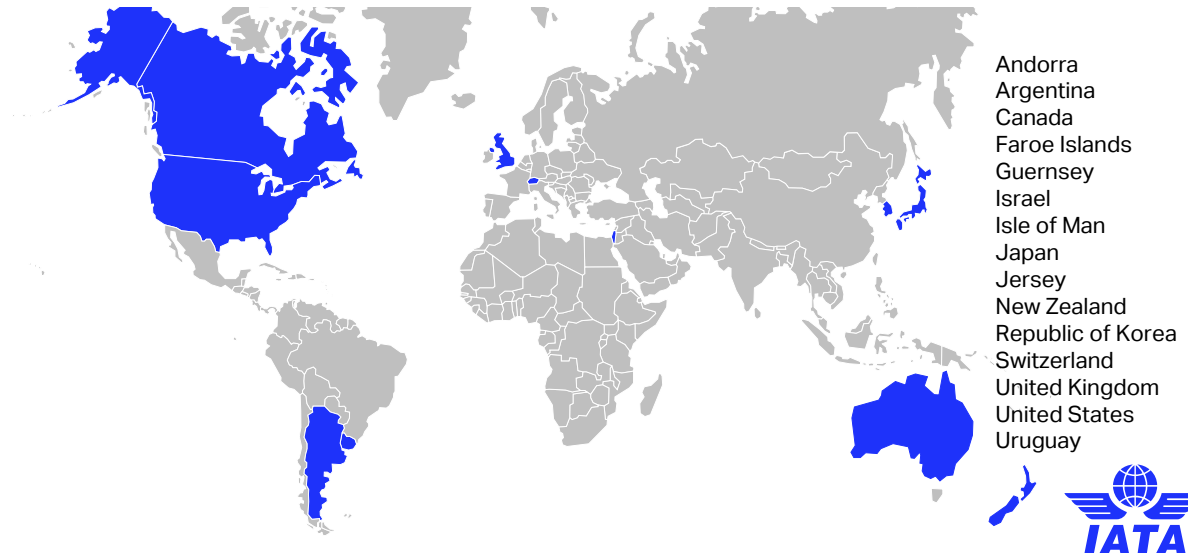
Let's look at probably one of the best examples of the issues facing airlines and how these issues manifest in practice.

## Global PNR Implementation Status



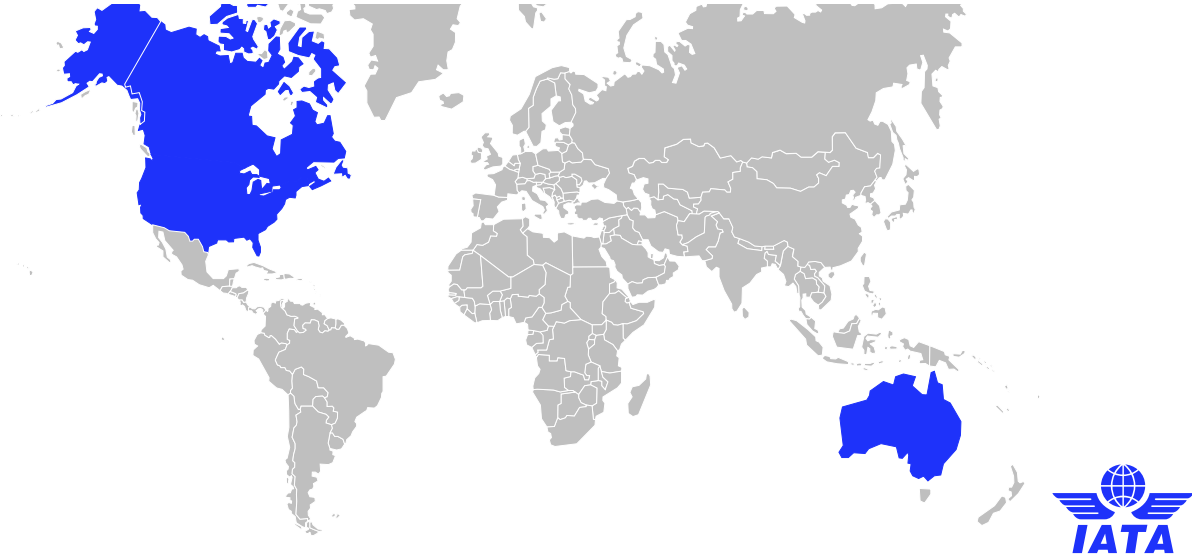
- The UN Security Council mandates that States collect PNR data - UN Security Council Resolution 2396 in response to the threat of returning terrorist fighters. The International Civil Aviation Organisation, agency has established guidance for states regarding the collection of PNR. In 2018, 25 countries had PNR programs; today the number has risen to 70 and it is expected to increase further.
- Now let's say a country implements a PNR system and requires all carriers flying to and from cities in that country to provide PNR data. If airlines fail to submit the information in a timely manner, they may face fines or penalties for non-compliance.

## Only 15 states are deemed by the EU to have 'adequate' data protection laws



- Now carriers from the European Union and EEA States have a problem. The GDPR does not recognize a legal obligation in other jurisdictions as a valid legal basis for the transfer of personal information – even PNR data implemented by States in accordance with the UN Security Council Resolution. . For such transfers to occur, there must be an EU legal requirement or EU must deem the data protection laws in a jurisdiction to be “adequate”, meaning they must meet the same standards as the GDPR. Currently only 15 countries have been granted “adequate” status by Brussels.

## Only 3 states have agreements with EU for sharing PNR data



- But this alone is not enough, there also needs to be a bilateral agreement in place specifically for sharing PNR data! Currently, the EU has such agreements with only three countries - Australia, Canada and the US.
- So of a potential 70 states that require PNR data, only 3 actually have an agreement with the EU to share data from EU citizens traveling to their country.
- Now, the object is not to criticise the EU GDPR or any one particular approach here.
- The challenge lies in the fact that carriers must determine whether to comply with the requirements to transfer PNR data in their home State or risk fines or even the loss of operating approvals because of non-compliance. These fines can be substantial –up to \$50,000 US dollars per flight. We even had one carrier report that the captain of an aircraft was threatened with imprisonment for failing to provide PNR data upon landing.

## Adverse impacts are a daily reality for airlines

- Huge complexity means increased **risks of non-compliance** (e.g. EU GDPR 4% of global revenues or EUR20 million)
- Massive **compliance burden** to try and determine which laws apply
- **Constant threat of fines or loss of operating approvals** due to conflicts between national laws



- Airlines have to comply and manage multiple data privacy and protection regimes across their networks.
- This is a significant logistical and operational challenge.
- There is also a risk that information cannot be shared for critical safety and security reasons and this is a concern for States.
- Aviation requires personal information to be shared to ensure all of our safety.
- It is not clear how these adverse impacts balance with the important right we all have to the protection of our personal information.



# Significant achievement

- ICAO member states recognize the importance of the issue and its relevance to civil aviation
- In early November, the Council of ICAO approved the addition of this topic to the ICAO Legal Committee Work program
- Task force to consider the challenges and options with a view to potentially developing aviation-informed guidance materials.

- I want to highlight what for me is a "WOW" moment in the work we have been doing over the past 3 years to make this issue known to civil aviation regulators and our colleagues at ICAO.
- Over the past three years, IATA has been making the case for ICAO to study the interaction of national data protection laws and civil aviation.
- In November, the ICAO Council approved an update to the Work Programme of the ICAO Legal Committee to include the establishment of a multidisciplinary working group to study the issue and its impact on civil aviation.
- You may be saying to yourself – that doesn't sound particularly exciting or ground breaking ---
- I assure you it is.
- Firstly, the Legal Committee Work programme is rarely added to over the years.
- Secondly, the airlines have been heard by States who agree something must be done
- Thirdly we have a very important opportunity - airlines and states – with their experts on data privacy and civil aviation will work together to ensure the special characteristics of civil aviation will be taken into account in this challenging compliance area that is impacting the safety, security and efficiency of global connectivity.
- Just in the way the drafters of the Chicago Convention would have wanted.