

Athens International Airport

Some privacy, please!
The untold quest of passenger data



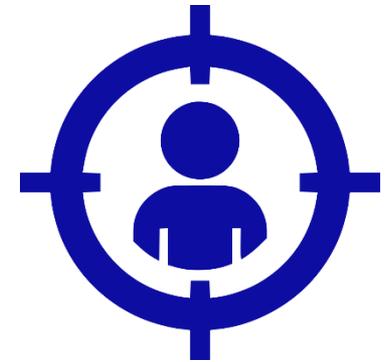
Data Privacy Landscape



**4,5 billion
passengers**



**gathered personal
data is staggering**



**prime target
for potential
malicious
acts**

Data Privacy Landscape



- The EU General Data Protection Regulation (GDPR) has come into force on 25 May 2018, **applying also to companies based outside the EU**, which have an office within the EU, or offer goods or services to **individuals located in the EU**.
- Lawfulness of personal data processing purpose, minimization in volume and retention, security, accuracy, transparency and accountability are some of the basic principles reaffirmed by GDPR

Types of Personal Data

The aviation sector typically holds a considerable amount of information on each passenger, including:

PNR

API

Loyalty
Club

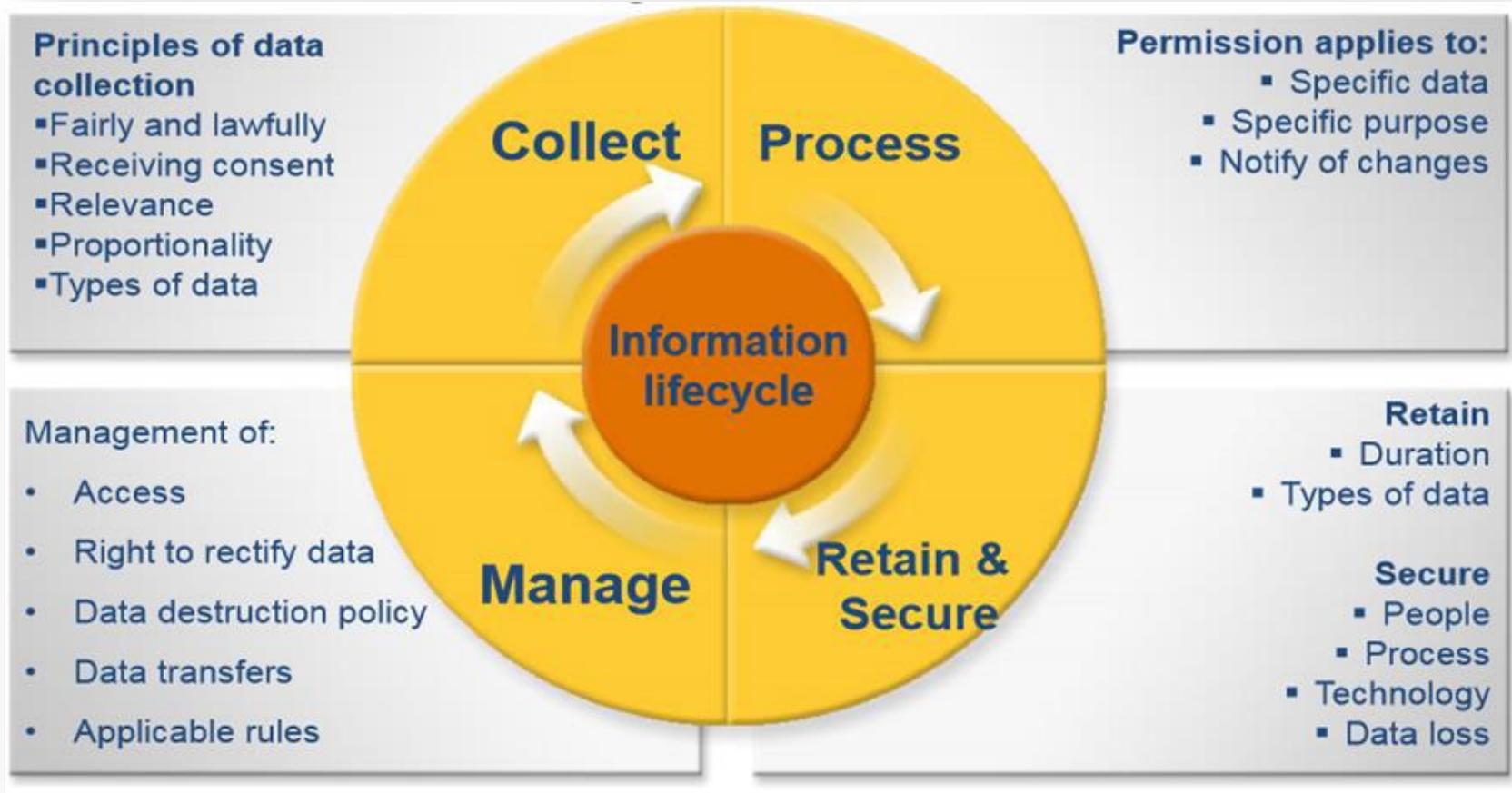
Security related
(e.g. full body
scanners,
biometrics)

Notification of
medical
condition

Preferences
(e.g. choice of
meals)

PRM Assistance

Personal Data Lifecycle



Pre-flight phase processing



Direct sales from Airline website/apps



Sales through Global Distribution Systems (GDS) e.g. "Galileo", "Amadeus"



One - stop - shop platforms (car rentals, hotels, travel agencies etc.) e.g. "Amazon for Travel"

Pre-flight phase processing

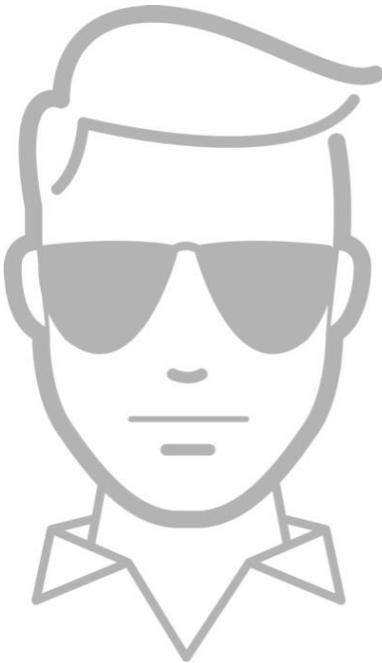
Use of **Data Analytics** for the provision of **personalized services** to the passenger Airlines are hoping that **big data** might prove one **antidote** to the pressures of tight profit margins and intense **competition-**

"Our flight attendants are able to access customer profiles and journey information at their fingertips through their handheld devices, allowing them to better engage with our customers," the company said.

"All of our frontline employees — from flight attendants to gate agents — also have the airline's "In the moment" app, which allows them to compensate customers for accidents such as spillages or delays."

Pre-flight processing

"PREDICTIVE SERVICE" mainly for registered loyalty card holders



Mr. Smith no longer needs to be sitting in first class to qualify for this sort of treatment.

*Airlines are seeking to harness big data to personalize customer experiences for as many travelers as possible — and they have a lot of data. **"We need to be operating at the level of Google,"** said the chief executive of the Airline Passenger Experience Association.*

*"For every **passenger**, we know every detail that serves as a **marketing treasure** trove of personalization. "We have full names, addresses, exact birthdays, seat assignments, credit cards and everything that should make personalization easy" he added*

Pre-flight processing

BLOCKCHAIN for Aviation



Each transaction generates a "hash"; If a transaction is approved by a majority of the nodes then it is written into a block. Each block refers to the previous block and together make the Blockchain. A Blockchain is effective as it is spread over many computers, each of which have a copy of the Blockchain.

Pre-flight processing: Risks

All above examples of collaboration between various business partners **expand the network** in the processing of personal data, **which is as secure, as the weakest link in that network!**

There have been documented instances of proven security protocol vulnerabilities in networks between airlines and their partners, **which put personal data at grave risk of malicious, or accidental loss.**

In 2018 alone, the publicized data breaches in the aviation sector are hugely alarming:

Pre-flight processing: Data Breaches

- **Non-EU legacy carrier admitted in October 2018 that the personal data** of up to **9.4 million people were exposed** due to unauthorized access, claiming that beyond said event there was no conclusive evidence of further data manipulation;
- **EU- based legacy carrier also announced that personal and financial details of nearly 500,000 of customers who made bookings between August 21st and September 5th2018, had been compromised**, exposing payment details including credit card CVV codes in a “*sophisticated and malicious attack*”, as officials explained. As later revealed, thousands of such data had been sold by hackers on the Dark Web.
- **Non-EU legacy carrier publicly admitted a data breach occurring in August 2018 affecting 1% of its mobile app users (approx. 20,000 of its 1.7 million users)**

Pre-flight processing: Data Breaches

As a result of the data breach announcement, **the carrier's parent group share suffered a considerable drop of almost 3%** in stock exchange and the competent national data protection authority is currently investigating the events and may impose the fines foreseen in the GDPR. Further claims on Court by affected individuals may also not be ruled out.

Processing during air-travel operations

- **Passenger Lists: 1944 – Art. 29 of the Chicago Convention** requires every aircraft to carry certain documents, including, for passengers, “a list of their names and places of embarkation and destination”;
- **Computer Assisted Passenger Prescreening System (CAPPS) in the USA, 1990s;**
- **Airline Reservation and Departure Control System (ARS-DCS)**
- **Advanced Passenger Information (API)**
- **Passenger Name Record (PNR)**
- **"Other Service Information" (OSI), like PRM Service**
- **Use of Body Scanners, during Airport Security Checks**

Aviation Security events which lead to tighter passenger controls

- **Metal detectors** for revealing weapons made of metal;
- **The 9/11 strike in New York**, caused the demand by US Authorities to receive PNR data in all incoming flights– PNR Agreements with the EU, Canada and Australia in 2000s, EU Regulation 2016/681;
- Removal of shoes at security checks, following **American Airlines flight 63 from Paris to Miami Shoe bomber (12/2001)**;
- **The 2004 attacks in Madrid** caused the transfer of Advanced Passenger Information (API) in the EU;
- **Liquid explosives in 2006**
- **The 2007 Car bomb attack at Glasgow Airport** caused the launch of PNR checks within E.U;
- **The failed attack on Northwest Airlines Flight 253 from Schiphol to Detroit**, on Christmas Day, 2009 by concealed plastic explosives in a passenger's underwear caused the use of whole-body scanners by certain airports in Europe and the U.S.

PNR – EU Directive 2016/681

1

In addressing these issues in April 2016 “EU Directive 2016/681” was published, regulating the collection and exchange of PNR and API data in both intra and extra EU flights from airlines to police authorities, aiming to prevent, detect and prosecute terrorist acts and serious crime.

2

This Directive has been transposed in the Hellenic legal system by law 4579 in late 2018 and a special “**Passenger Information Unit (PIU)**”, has been established within the Directorate of Data Processing and Analysis of Hellenic Police to accommodate the collection and further transfer and exchange of such data.

Retention of PNR Data by PIU: Five (5) years in total; however six (6) months after submission, the data are totally depersonalized

Further key considerations

- **Data Minimization**
- **Transfer of personal data out of EEA (cloud storage, third party processing)**
- **Hellenic GDPR implementation law is overdue**
- **Data privacy and cybersecurity are intersecting circles**

Conclusion

- **Cyber Security and Passenger data protection** is a **marathon**, rather than a one-time action; Stakeholders can work together in fortifying passenger data security, integrity and confidentiality, thus preserving the wealth of the Industry;
- The adoption and observance of **Codes of Conduct** by ACI/IATA/other involved associations and Privacy Certifications (**Privacy Seal**), when made available, are effective means of demonstrating compliance, working to the benefit of all stakeholders in privacy audits;
- **Passengers need to be fully informed** on the particulars of their personal data processing with appropriate Privacy Notices, **beforehand at first contact (e.g. at ticket/services purchase)** providing info on **personal data processing purpose and legal basis, type, retention, security, data controller & third party processors, transfers, exercise of rights**);
- Passengers will ultimately respond positively and reward those service providers showing to them how their data is respected and how far these entities will go to protect them;
- When **negative incidents** occur, any **brand** takes an instant **blow**,

Thank You !