WORLDWIDE AIRPORTS LAWYERS ASSOCIATION

WELCOME TO WALA X | London, UK October 15-17, 2018

GROUND HANDLER LIABILITY – AS A PERSONAL DATA PROCESSOR

welcome AIRPORT SERVICES

Michal Jaworski Attorney – at – law

GDPR – introduction (1)

- **The EU General Data Protection Regulation (GDPR) is the most significant change in data privacy regulation in last 25 years.**
- The aim of the GDPR is to protect all EU citizens from privacy and data breaches in today's data-driven world. Although the key principles of data privacy still hold true to the previous directive, many changes have been proposed to the regulatory policies; the key points of the GDPR as well as information on the impacts it will have on business can be found below.

GDPR – introduction (2)

- Arguably the biggest change to the regulatory landscape of data privacy comes with the extended jurisdiction of the GDPR, as it applies to all companies processing the personal data of data subjects residing in the Union, regardless of the company's location. It applies to the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not.
- The GDPR also applies to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU, where the activities relate to: offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behavior that takes place within the EU. Non-EU businesses processing the data of EU citizens also have to appoint a representative in the EU.
- Compliance is needed!

GDPR – introduction (3)

- Why it is so important ?
- Organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater). This is the maximum fine that can be imposed for the most serious infringements e.g. not having sufficient customer consent to process data or violating the core of Privacy by Design concepts.
- There is a tiered approach to fines e.g. a company can be fined 2% for not having their records in order (article 28), not notifying the supervising authority and data subject about a breach or not conducting impact assessment. It is important to note that these rules apply to both controllers and processors – meaning 'clouds' are not exempt from GDPR enforcement.

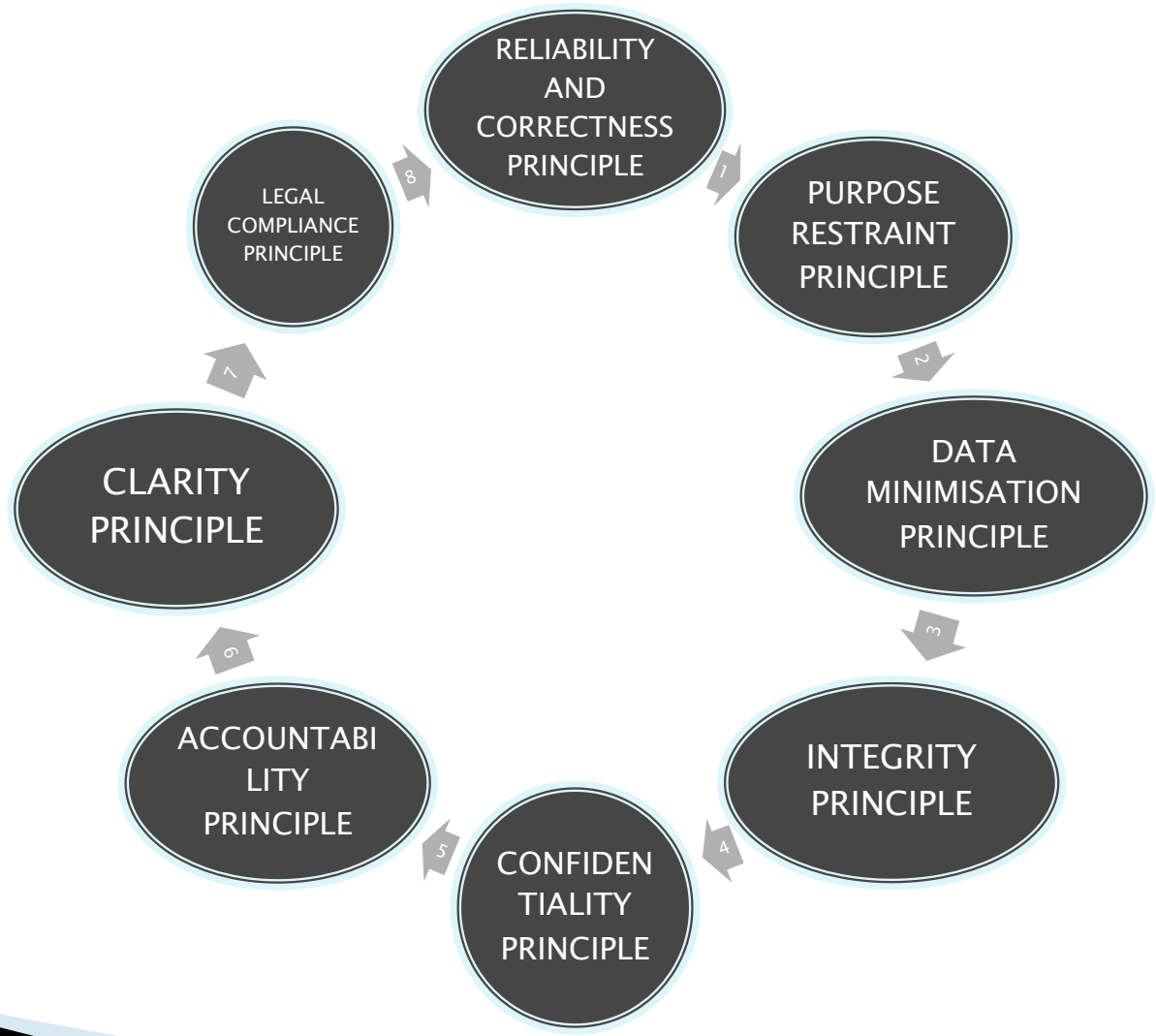
Legal basis

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

DIRECTIVE (EU) 2016/681 of 27 April 2016 of the European Parliament and of the Council on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime

and more than **70 pieces** of legislation that govern data protection around the world (Argentina Personal Data Protection Act (30Oct2000); Canada Federal Personal Information Protection and Electronic Documents Act, S.C. 2000, ch. 5 (PIPEDA) and 3 others; Brazilian Data Protection Act 14Aug2018

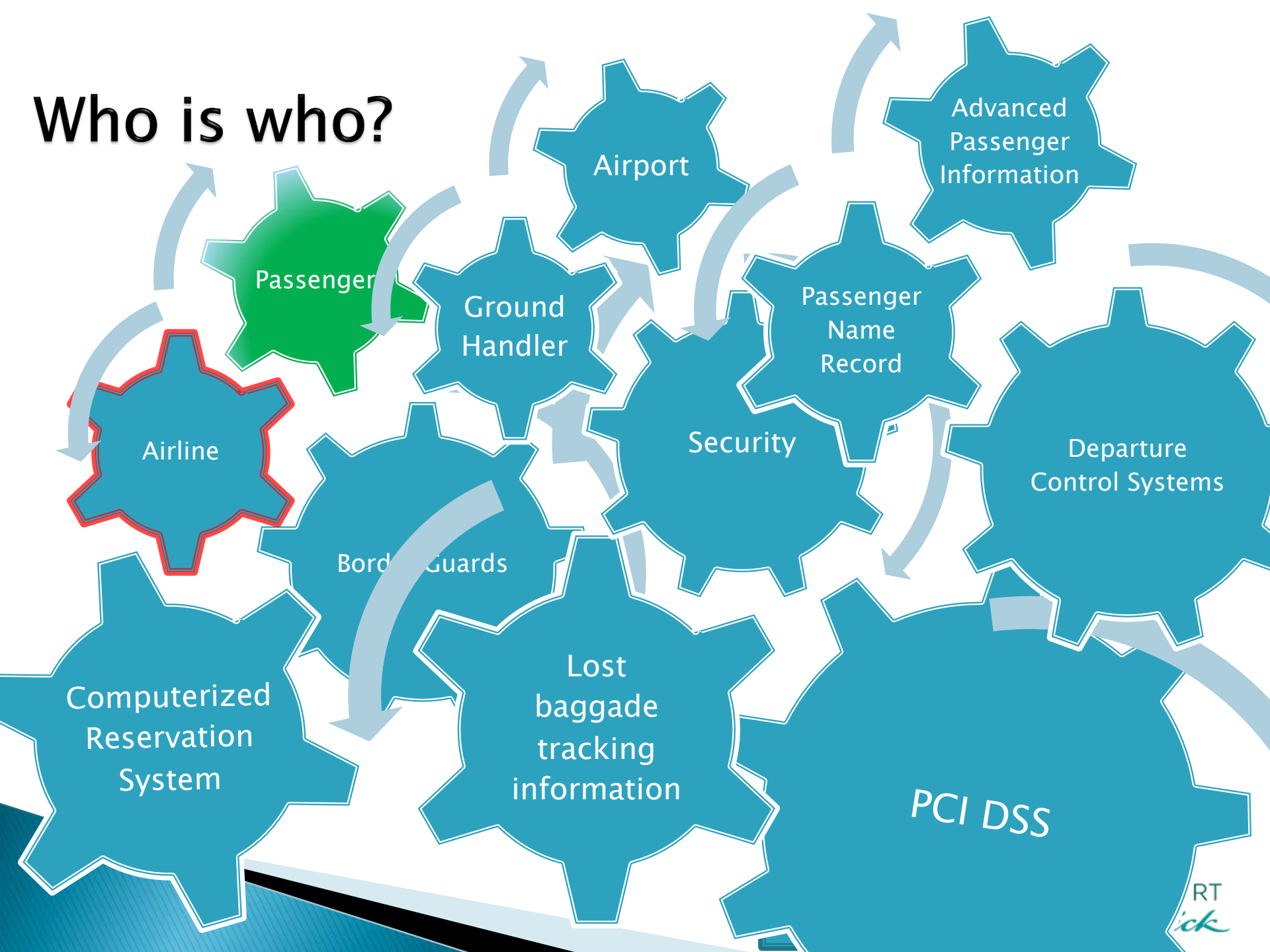
Principles related to processing personal data



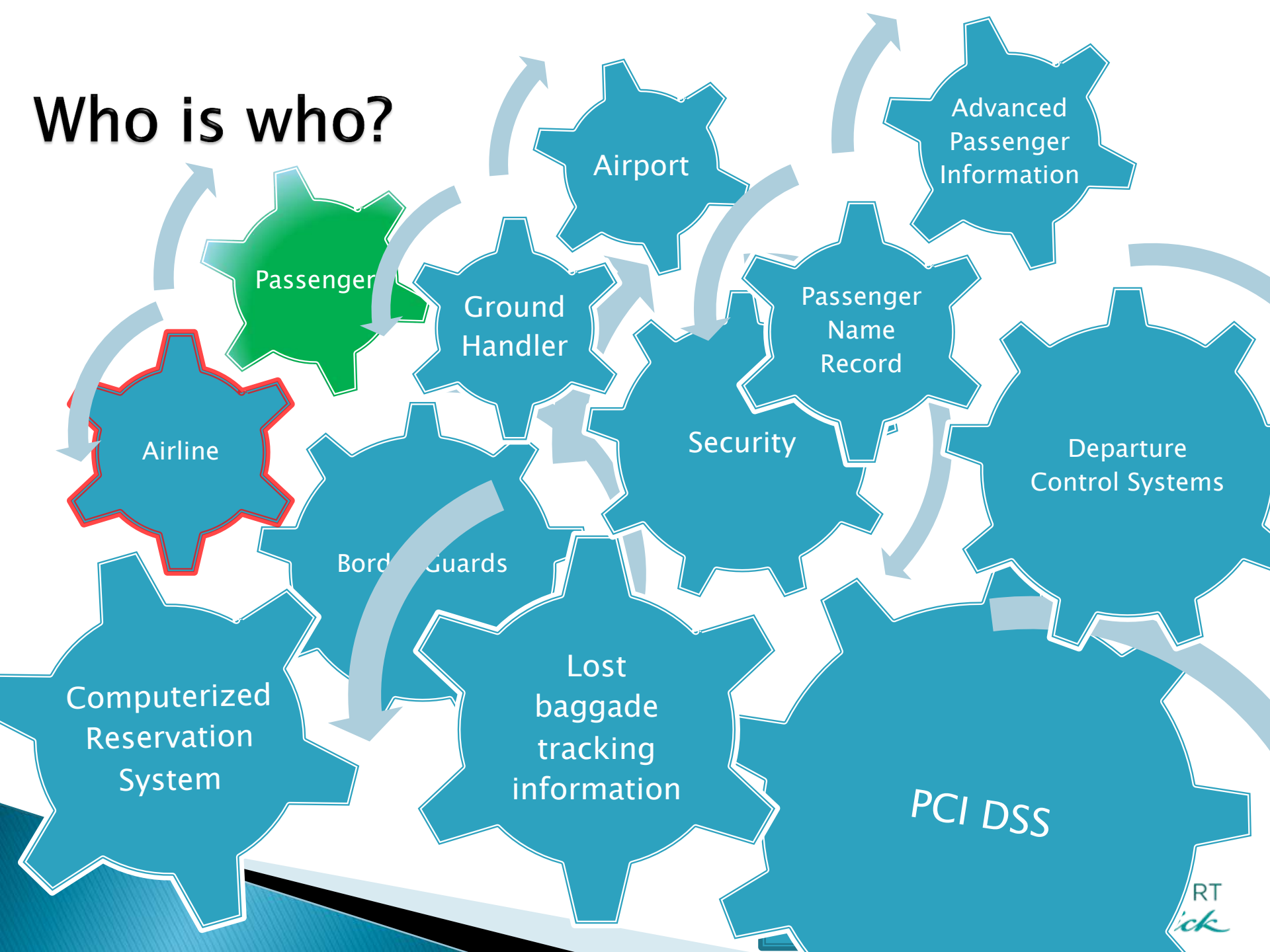
Controllers or Processors Who is who?

‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law

Who is who?


Airport
Advanced Passenger Information
Passenger
Ground Handler
Passenger Name Record
Airline
Security
Departure Control Systems
Bord Guards
Computerized Reservation System
Lost baggade tracking information
PCI DSS

Who is who?


Airport
Advanced Passenger Information
Passenger
Ground Handler
Passenger Name Record
Airline
Security
Departure Control Systems
Bord Guards
Computerized Reservation System
Lost baggade tracking information
PCI DSS

Personal data provided in the “Passenger’ data” section: **gender, first name (names), surname, date of birth, nationality, ID number (Passport number), loyalty programme card number, information on special assistance, email address, telephone number, information on purchasing additional insurance, information on purchasing additional services (e.g. My Favourite Seat, Excess Baggage), destination, etc.**

Airline is a controller of all passenger’s data and information, which determines (alone or jointly with others), the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Handling Agent is a ‘processor’ which means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller; but in many cases Handling Agent can act as a Controller of personal data who determines purposes and means of the data processing.

A border guard of a country is a national security agency that performs border security, i.e., enforces the security of the country's national borders.

Personal data processing agreement (1)

- Processing by the processor is executed on the basis of the contract or other legal instrument that is subject to European Union legislation or legislation of the Member State and are binding for the Processor and Administrator (Article 23, p. 3 GDPR).
- Point 81 of Preamble: Administrator and the Processor may decide to use standard contractual clauses, that have been accepted by the Commision or supervisory authority in accordance with consistency mechanism and the accepted by the Commision.
- The Contract states that the processor:
- Processess personal data solely on documented instruction of the administrator (...) unless such duty stems frim European Union legislation or legislation of the EU member state applicable for the processor; in such case, before initiating the processing processor should inform the administrator about such duty, unless providing such information is forbidden, considering important public interest.
- Undertakes the measures in accordance to article 32.
- Ensures that persons authorized to process personal data are obliged to maintain the confidentiality by the contract or by the law.

Personal data processing agreement (2)

- The Contract states that the processor :
- After the services which were the ground for data processing, depending on the decision of the administrator, processor should either destroy or return all of the personal data that have been processed and destroy all of its remaining copies, unless EU, or EU's member state law require to store personal data.
- Enables administrator access to all of the information necessary to prove that all of the duties stemming form GDPR has been satisfied and enable administrator or the auditor authorized by the administrator to conduct he audit .
- Processor informs the administrator – if in his opinion any order given by the administrator constitutes a breach of any provisions of GDPR or other UE or its member state applicable laws.

Personal data processing agreement – sample

- **PARAGRAPH 21 – DATA PROTECTION**

  - In the event that the Handling Company and its agents are permitted access to personal data (as defined in Article 4.1. of the Regulation 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter referred to in this as **"the Act"**)) held by the Carrier for any reason or are provided or supplied with personal data by the Carrier for any purpose, the Handling Company and its agents will:
  - use and/or hold such personal data only for the purposes and in the manner permitted herein or otherwise directed by the Carrier and shall not otherwise modify, amend or alter the contents of such personal data or disclose or permit the disclosure of such personal data to any third party unless specifically authorised in writing by the Carrier;
  - put in place all such technical and organisational measures as may be necessary to safeguard such personal data and protect it from accidental or unlawful destruction or loss, alteration or unauthorised disclosure or access and maintain adequate security programmes to ensure only authorised personnel have access to the personal data;
  - promptly, if permitted by law, provide the Carrier with all information in its possession concerning any request for disclosure of personal data from either the data subject or a law enforcement agency including the Office of Information Commissioner (hereinafter referred to in this Paragraph 21 as **"OIC"**) and promptly notify and forward to the Carrier any requests received directly, acknowledging that it is not authorised to respond;
  - not do or omit to do anything which would cause any personal data to be transferred to a country, jurisdiction or territory outside of the EEA or Switzerland without the express written consent of the Carrier;
  - comply in all respects with the Act as amended from time to time including maintaining all relevant legally required notifications with the OIC and will not do or permit anything to be done which might jeopardise or contravene the Carrier's compliance with or notification under the Act; and
  - destroy or Return the personal data to the Carrier including any copies thereof on termination of this Agreement or on the Carrier's demand.
  - The Carrier accepts no liability whatsoever for any inaccuracies in the personal data or for the unlawful obtaining and/or processing of personal data unless caused by negligence, intent or recklessness of the Carrier.
  - For the avoidance of doubt, the provisions of this Paragraph 21 shall survive the termination or expiry of this Agreement.

Personal data processing agreement

PARAGRAPH 21 – DATA PROTECTION

- […].6 Notwithstanding any provisions of the Annex […], the Handling Company shall not appoint any third party to process Carrier Personal Data ("Subprocessor") without the Carrier's prior written consent, and subject in all cases to the Handling Company:
- […].6.1 providing reasonable prior notice to the Carrier of the identity and location of the Subprocessor and a description of the intended processing to be carried out by the Subprocessor to enable the Carrier to evaluate any potential risks to Carrier Personal Data; and
- […].6.2 imposing legally binding contract terms on the Subprocessor which are the same as those contained in the Annex […].
- […].7 The Handling Company acknowledges and agrees that it shall remain liable to the Carrier for a breach of the terms of the Annex […] by a Subprocessor and other subsequent third party processors appointed by it with limitation to claims and all direct losses.
- […].8 The Handling Company shall notify the Carrier in the most expedient time possible under the circumstances and in any event within 48 (forty – eight) hours of becoming aware of any accidental, unauthorized, or unlawful destruction, loss, alteration, or disclosure of, or access to, Carrier Personal Data ("Security Breach"). The Handling Company shall also provide the Carrier with a detailed description of the Security Breach, the type of data that was the subject of the Security Breach and (to the extent known to the Handling Company) the identity of each affected person, as soon as such information can be collected or otherwise becomes available, as well as all other information and co-operation which the Carrier may reasonably request relating to the Security Breach.
- […].9 The Handling Company agrees to take action immediately, at its own expense, to investigate the Security Breach and to identify, prevent and mitigate the effects of any such Security Breach and, with the Carrier's prior agreement, to carry out any recovery or other action necessary to remedy the Security Breach.
- […].10 The Handling Company may not issue, publish or make available to any third party any press release or other communication concerning a Security Breach without the Carrier's prior approval, except situations as agreed by the Parties.

Personal data processing agreement

PARAGRAPH 21 – DATA PROTECTION

- […].11 The Handling Company shall ensure that no Carrier Personal Data is processed outside either the European Economic Area (EEA) or any other territory in which restrictions are imposed on the transfer of Carrier Personal Data across borders under the Data Protection Legislation, without the express prior written consent of the Carrier. In which case, the Handling Company shall comply with the requirements of the Carrier to ensure that adequate safeguards are put in place to protect Carrier Personal Data.
- […].12 The Handling Company shall make available to the Carrier all information necessary to demonstrate compliance herewith and allow for and contribute to audits, including physical inspections, conducted by the Carrier or its representatives by appointment bound by appropriate obligations of confidentiality.
- […].13 The Handling Company shall indemnify and keep the Carrier fully and effectively indemnified in respect of all direct claims and losses arising out of or in connection with a breach by the Handling Company hereof to [____] USD for each incident with total limit of [________] USD for the duration of the contract. Nevertheless, the Handling Company's liability shall be limited to:
- [_________] USD for following incidents:
  - attempts of extorsion;
  - incidents related to multimedia activity:
    - infirgment of third partys' moral rights and damages related to such infrigment,
    - infrigment of third partys' intellectual properity,
    - infirgment of third partys' right to privacy;
  - incidents related to disruptions in network functionality at the Airports on which the Handling Company provides services.
- [_______] USD for
  - all claims related to incidents mentioned in this paragraph if such claims are pursued on territory of United States of America or Canada ...
- Nevertheless, the Parties shall endeavour to clarify the circumstances of any such instances, including the respective roles of the Carrier or the Handling Company."

Data security breach

- If the procesor finds that personal data protection has been breached, he notifies the administrator without any delay (Article 33 p. 2 GDPR)
- Such notification should include:
- Description of the charater of the breach, including the category of the data and approximate number of persons that may have been affected by the breach;
- Full name and contact details of Data Protection Officer (DPO);
- Description of the possible consequences of the personal data protection breach;
- Description of the means undertaken, or proposed by the processor in order to mitigate the consequenes of the breach including the means undertaken to minimize the damages.

- Administrator and the Processor should appoint the Data Protection Officer, when :
- a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity
- b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on the a large scale.
- c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 or personal data relating to criminal convictions and offences referred to in Article 10.
- **Notification:**
- Airline (as a controller) and Handling Agent (as a procesor):
- Publication of DPO contact details;
- Notification to supervisory authority about contact details;
- Are obliged to inform about any breach of personal data within 72 hours.

welcome
AIRPORT SERVICES

Thank you!

Michal Jaworski
attorney – at – law
m.jaworski@welcome-as.pl
mjaworski@jmklegal.pl