SAFE SKIES.
SUSTAINABLE FUTURE.

ICAO Middle East Seminar on Advance Passenger Information (API) and Passenger Name Record (PNR) Data

Data Protection and Passenger Data

Steven Waterman, Facilitation Section ICAO

Data Protection and Passenger Data

United Nations Security Council Resolutions

ICAO Annex 9 – Passenger Data Exchange Systems

EU Data Protection Framework:

GDPR and Police Directive

EU Passenger Name Record Directive

Evidence Based Policy Development

Data Protection and Passenger Data

- We only collect personal data we actually need for our specified purposes
- We have sufficient personal data to properly fulfil those purposes
- We periodically review the data we hold, and delete anything we don't need

- WCO/IATA/ICAO API Guidelines – maximum set of data elements that can be included in API PAXLST Messages
- ICAO DOC 9944 Guidelines on Passenger Name Record data

Data Protection and Passenger Data

Personal data must be kept for no longer than is necessary for the purpose for which it is processed

- ICAO Annex 9 - retain PNR data for a set period … necessary and proportionate for the purposes for which the PNR data is used
  - Recommended Practices: five years and then depersonalized after between six months and two years after the transfer of the PNR data

- EU PNR Directive – Five years, plus depersonalized by masking out specific data elements

Appropriate time limits must be established for the periodic review of the need for the continued storage of personal data

Data Protection and Passenger Data

Rules Based Targeting

- The rules and criteria should be specific and reliable enabling the identification of individuals who might be under a ‘reasonable suspicion’ of participation in terrorist offences or serious crime
- The rules should be non-discriminatory and regularly reviewed

Watchlisting

- The databases with which passenger data is cross-checked should be reliable, up to date

Historical Searches

- Requests should be duly reasoned, necessary and proportionate

Data Protection and Passenger Data

- The right to be informed
- The right of access
- The right of rectification
- The right to erasure or restriction of processing

Under what circumstances may these restricts be restricted:

- avoid obstructing an official or legal inquiry, investigation or procedure
- avoid prejudice to the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties
- protect public security
- protect national security

Data Protection and Passenger Data

Data Protection Officers

- Data protection officers (DPOs) assist you to monitor internal compliance, inform and advise on your data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the Information Commissioner
- The DPO should be independent, an expert in data protection, adequately resourced, and report to the highest management level
- A DPO can be an existing employee or externally appointed
- In some cases several organizations can appoint a single DPO between them
- DPOs can help you demonstrate compliance and are part of the enhanced focus on accountability

Data Protection and Passenger Data

Data Protection Supervisory Authority

- Each supervisory authority should be provided with the financial and human resources, premises and infrastructure, which are necessary for the effective performance of their tasks
- Supervisory authorities should be are able to exercise their functions with complete independence from the body responsible for the processing and use of the data
- Each supervisory authority should handle complaints lodged by any data subject and should investigate the matter
- The supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period.

Thank You

ICAO 80