european regions airline association

GDPR

ERA's summary and advice to members on GDPR

SUMMARY AND BACKGROUND

The much-anticipated General Data Protection Regulation (GDPR) will become rule of law on 25 May 2018. It is compliance-heavy while seeking to harmonise data protection law among EU member states. With regulatory burden recently identified by ERA members as an area of concern, this publication, in conjunction with the ERA GDPR Self-Assessment Checklist (www.eraa.org/policy/eu-initiatives/gdpr) sets out to:

- Clearly identify the differences between the current Directive and the enhanced upcoming GDPR.
- Give members clear and unambiguous information regarding risks of non-compliance.
- Define a structured process improvement methodology to maintain compliance standards for the future.

The implementation of the GDPR is the biggest overhaul of privacy legislation in 20 years. The purpose of this publication is to support ERA members to get, and remain, compliant. Fortunately for aviation, regulatory compliance has always been the foundation of airline policy, experience that will serve ERA members well as they prepare data processing activities for the future.

PRUDENT PROTECTION – KNOW THE DIFFERENCES

Knowing the regulatory upgrades required between the current directive and the replacement GDPR are the first step to prudent protection. Knowing where and how to apply that information has proven to be demanding. Focus points of concern for ERA member airlines are as follows:

- How to continue the commercial use of customer data.
- Legal, reputational and financial impact of a data breach.
- PNR data not being GDPR compliant.
- Partner GDPR compliance.
- Ex-employee data breaches.

Source: ERA member airlines

PROCESSING OF PERSONAL DATA (ARTICLE 5)

How ERA members intend to process personal data collected must now be easily accessible and in a clear format. Transparency is key, where comprehensive information must be given to the data subject detailing what personal data is being collected, why it is being collected, what it will be used for (**purpose limitation**) and how long it will be kept (**storage limitation**). Airlines must also create a **'record of processing activities' (Article 30)**, an internal document that details this information, along with categories of data subject, recipients and security measures that are in place to protect that data, both technical (such as encryption) and organisational (such as restricting who has access to your systems). The data subject must also be informed of these rights under the GDPR. It may not be feasible to present this information in a single document, therefore the use of **'fair processing notices'** can feature on travel documents or communications with data subjects, with directions to a more specific privacy policy.

CONDITIONS FOR CONSENT (ARTICLE 7)

When collecting personal data, one way to do so legally is with the consent of the data subject. The following GDPR terminology should be familiar at this stage, however a reminder that consent must be **'freely given, specific, informed and unambiguous'**. For an airline, data collection is for tracking and safety purposes along with customer experience enhancement, however the airline must ensure the data collected is focused (**data minimisation**).

The request for consent must be shown separately in clear and plain language and it must be as easy to withdraw consent as it is to give it. Data subjects will also have the right to object to the collected data being used for direct marketing purposes. This right to object must be brought explicitly to the attention of the data subject. Any agreements member airlines have in place with car hire, hotels and other ancillary services must be reviewed and an opt-out choice clearly available to the data subject.

You can find the WP29 Guidelines on Consent in the downloads section at **www.eraa.org/policy/eu-initiatives/gdpr**.

RIGHTS OF THE DATA SUBJECT – GENERAL (CHAPTER 3)

Further to the examples mentioned, the GDPR will entitle any data subject to claim damages from the data controller or the data processor where it is deemed they have suffered material and/or non-material damage as a result of a violation of the GDPR provisions (**Article 82 – Right to compensation and liability**), including but not limited to the following:

- Not receiving personal data in a common and structured manner to allow easy transfer from one controller to another (**data portability**).
- The right to be forgotten (**right to erasure**) allows data subjects to request their personal data be erased, where there exists no lawful reason to keep it. Organisations are expected to reply within one month, with complex requests possibly granted an extension. Airlines are also expected to take reasonable steps to inform third parties, (e.g. airport special assistance providers) of the data subject request to be forgotten. As this may be difficult in practical terms, use the recording process to document this '**reasonable effort**'. Under the GDPR, the request shall be processed free of charge unless deemed to be '**manifestly unfounded or excessive**' by the Data Protection Authority (DPA).

You can find the WP29 Guidelines on Data Portability in the downloads section at **www.eraa.org/policy/eu-initiatives/gdpr**.

DATA PROTECTION BY DESIGN AND DEFAULT (ARTICLE 25)

The GDPR places direct '**accountability**' obligations on data controllers and processors to demonstrate compliance. They must maintain certain documentation, conduct impact assessments and implement data protection by design and default. The launch of any new software must be done in compliance with the GDPR, with existing processing activities assessed and defaulted to the same standard.

DATA BREACH NOTIFICATION (ARTICLE 33 & 34)

A data breach within an airline must be reported directly to the DPA if it is likely to result in a risk to the rights and freedoms of individuals (**data security**). Under the regulation, this must be done '**without undue delay**'. The report must be within 72 hours of breach awareness, with failure to do so resulting in the organisation required to produce reasoned justification.

There are circumstances where the controller must inform the data subject. This is dependent on the likelihood of high '**risk to their rights and freedoms**'. It is to be noted that a data breach event can be insured against.

You can find the WP29 Guidelines on Data Breach Notification in the downloads section at **www.eraa.org/policy/eu-initiatives/gdpr**.

A recent example given at the ERA Industry Affairs Group meeting highlighted the loss of a laptop. Is this considered a data breach? Is the laptop password protected? If not – and it allows access to personal data, then yes it is a breach, likely to result in a risk to the rights and freedoms of individuals.

If the laptop is password protected and the personal data is encrypted, then it is unlikely to pose a risk to the rights and freedoms of individuals.

The advice? Ensure the security of company laptops is as risk averse as the data is sensitive.

DATA PROTECTION IMPACT ASSESSMENT (DPIA) (ARTICLE 35)

Although not a new concept, impact assessments have been introduced to better advise organisations how at risk they are if the processing of personal data is '**likely to result in a high risk to the rights and freedoms of natural persons**'. The WP29 does give links to accepted methodologies, along with highlighting the basic criteria.

See the WP29 Guidelines on DPIA in the downloads section at **www.eraa.org/policy/eu-initiatives/gdpr**.

DATA PROTECTION OFFICER (DPO) (ARTICLE 37)

The designation of a DPO is in line with the direct accountability now placed on the data processor. Airlines work with '**large scale**' data and ERA advises its members to appoint a DPO if you have not already done so. The individual must have sufficient expertise, beyond reproach knowledge and understanding of the GDPR and interpersonal skills at all levels. The individual must report directly to the highest level of management and must be facilitated in every way possible carrying out their job function. The details of the airline DPO must be readily available to data subjects.

See the WP29 Guidelines on DPOs in the downloads section at **www.eraa.org/policy/eu-initiatives/gdpr**.

DATA TRANSFERS TO THIRD COUNTRIES (ARTICLE 44)

The GDPR will now apply to third country data controllers and processors whose activities relate to EU data subjects. Members engaging third country processors must be aware that methods used by the contactor are now subject to the EU GDPR when such data relates to EU data subjects. Further, you must ensure that the third country, territory or international organisation is within the Commission finding of adequacy under Directive 95/46. To that end, joint processing or outsourcing of processing should be clearly documented, stating your respective responsibilities. ERA encourages members to implement approved codes of conduct or alternative approved certification measures as best practice.

BINDING CORPORATE RULES (BCRS) (ARTICLE 47)

Addressing the legitimacy of intra-group international data transfers, BCRs must be legally binding. This particular principle may not apply to member airlines currently, however a review of the ERA Brexit publication (published February 2018) highlights how and when it may become relevant for some. Airlines are a multi-jurisdictional operation and there are elements that may differ from one jurisdiction to another.

WP29 Guidelines on Binding Corporate Rules (BCRs) can be found in the downloads section at **www.eraa.org/policy/eu-initiatives/gdpr**.

For example, how long a processor may retain personal data, after a service transaction has been completed, for purposes of potential future claims is not the same in Belgium as in the UK. Key considerations for intra-group international data transfers may be the location of the gathered data and the nationality of the individuals involved.

RISK ANALYSIS REALITY

In addition to other measures including investigations, access to premises, warnings and stop orders to processing or transferring data, the GDPR now provides for fines up to €20m or four percent of the worldwide turnover of a business, whichever the higher.

Along with reputational damage, the GDPR introduces a new two-tiered sanctions regime, shown below. It is worth highlighting that the penalty is based on annual turnover, not annual profit.

Non-compliance obligations: Lower tier – 2% or €10m

- Intergration of data protection by design and by default
- Records of processing activities
- Cooperations with the supervisory authority
- Security of processing data
- Notification of a personal data breach to the supervisory authority/data subject
- Data Protection Impact assessment/prior consultation
- Designation, position or tasks of the Data Protection Officer
- Certification

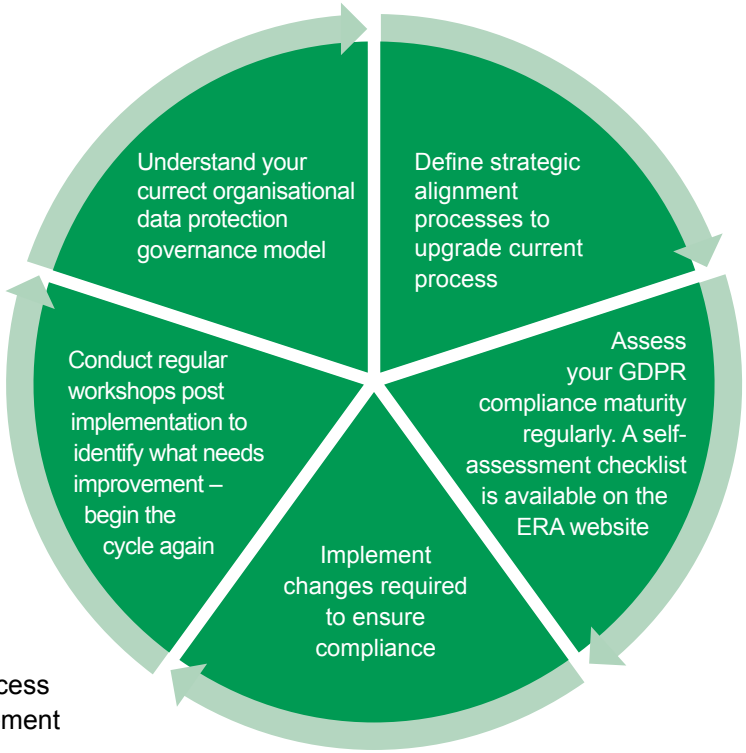
Non-compliance obligations: Upper tier – 4% or €20m

- Violation of the basic principles for processing, including conditions for consent, lawfulness of processing and processing of special categories of personal data
- Violation of the rights of a data subject
- Transfer of personal data to a recipient in a third country or an international organisation in violation of the rules governing cross-border transfer

See downloads section at **www.eraa.org/policy/eu-initiatives/gdpr**.

PROCESS IMPROVEMENT METHODOLOGY

It is not sufficient to implement an irregular pattern of passenger data monitoring. As an airline, you must map out and record your processing activities as an ongoing requirement. Similar to air safety compliance, you are subject to audit without prior notice and must allow access to your 'records of processing activities' upon request to avoid penalty.



Example: Ongoing process monitoring and improvement

Ensure that the proposed compliance solutions are delivering, and change them where they are not. Note: all changes must be recorded to be compliant. Plan routine reviews of the successful process. Gather feedback from staff who work with GDPR, implement the feedback where commensurate with being further compliant, while fostering and promoting a 'just culture' reporting philosophy.

ERA'S FUTURE ACTIONS AND ACTIVITIES

ERA encourages all members to have their GDPR compliance framework developed at this point. If it is not in place, it is well overdue.

ERA Industry Affairs Group (IAG) will continue to monitor developments to best support members. A member airline will present at the next IAG meeting about the airline's experience with its national supervisory authority. A code of conduct for ERA members is currently being researched.

There are further mechanisms being identified for members' benefit, such as a potential 'sharespace' where ERA members can exchange information regarding compliance and audit experiences. Engagement with data protection authorities post regulation launch date is also on the agenda for ERA.

European Regions Airline Association
Park House, 127 Guildford Road, Lightwater, Surrey, GU18 5RA, United Kingdom
Telephone: +44 (0)1276 856495
E-mail: info@eraa.org Website: www.eraa.org
European Regions Airline Association Limited is registered in England & Wales.
Company No: 8766102

era
european regions airline association

May 2018