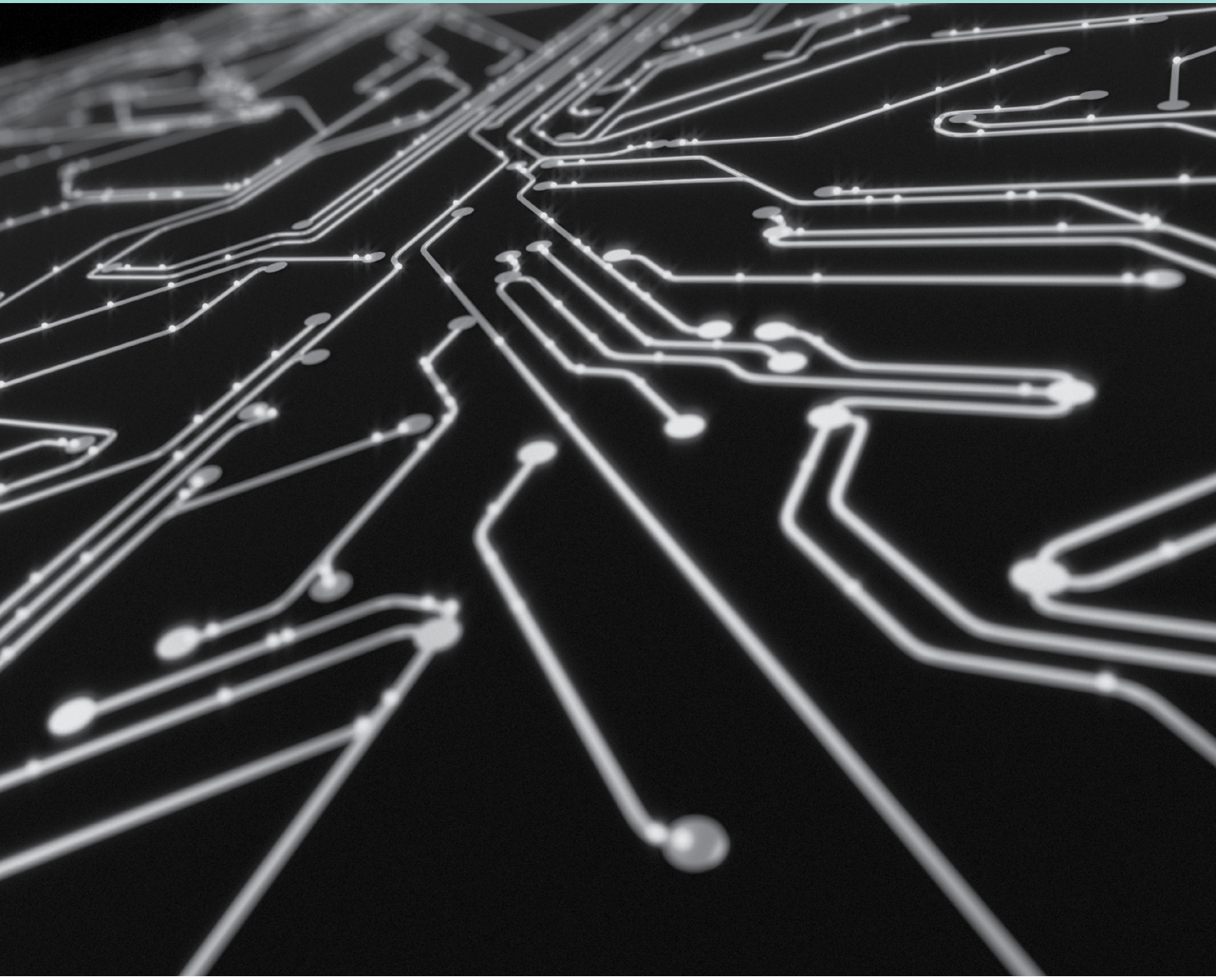


THE EU GENERAL DATA PROTECTION REGULATION AND INTERNATIONAL AIRLINES

SPECIAL UPDATE

The EU General Data Protection Regulation (GDPR) becomes effective across the European Economic Area (EEA), including in the UK, from 25 May 2018. It overhauls a data protection regime dating from 1995. It will also apply to a large number of businesses established outside of the EEA. Airlines now have less than eight months to make the necessary changes to their systems and policies in order to be prepared when the GDPR "goes live". The clock is ticking.

“The penalties for getting this wrong are potentially very high. EEA supervisory authorities will have the power to impose fines of up to €20 million, or four percent of the total worldwide turnover of a business in the preceding financial year, whichever is higher.”

Why do international airlines need to comply with the GDPR?

Privacy rules around the world are tightening. The GDPR is just one example of a regime change which aims to put the rights of the individual first. Many of the principles are similar in privacy regimes around the world, but the GDPR is often stricter. Although compliance with the GDPR will not guarantee compliance with all privacy regimes across the globe, it will help to reduce global risks.

An airline which safeguards the privacy rights of its passengers (and employees) will also be more likely to attract and retain customers. Marketing efforts will be more effective when reaching only the individuals who consented to be contacted for marketing purposes. The airline will be better able to gain and maintain the trust of customers and employees alike.

The penalties for getting this wrong are potentially very high. EEA supervisory authorities will have the power to impose fines of up to €20 million, or four percent of the total worldwide turnover of a business in the preceding financial year, whichever is higher. EEA member states are also required to impose penalties that are *“effective, proportionate and dissuasive”*. A draft UK Data Protection Bill, which will implement the GDPR in the UK, allows for prosecution of directors.

In addition to the potential for high-profile reputational damage involved in breaching data protection law, there is also a heightened risk of complaints and even claims from unhappy customers.

What will change?

Under the GDPR, the obligations on data controllers will substantially increase and, importantly, data processors will also now have data protection obligations. For example, in accordance with a new focus on accountability, data controllers and processors alike will now be required to keep records of their processing. Contracts with processors will need to be updated with new mandatory provisions. Privacy notices will need to be updated. “Consent” will be more difficult to obtain and may need to be refreshed. Principles of “privacy by design” mean that organisations must look at their processing and assess whether it is imperative. We discuss below some of the key elements that require action now.

We are not an EEA airline, why do we have to comply?

The GDPR will relate to organisations based outside of the EEA if certain conditions apply. The GDPR applies to a non EEA organisation if it has a presence in the EEA, or it monitors the behaviour of individuals within the EEA (for example via cookies), or it offers services to individuals within the EEA. It also applies where EEA member state law applies in accordance with international law. The GDPR is likely to relate to most international airlines. Particular factors to consider when determining whether the GDPR will apply are:

- Does your website refer to an EEA reservation centre or office?
- Does your business have a registered establishment in the EEA?
- Is your website directed towards individuals based in the EEA, for example by giving an option to choose a “UK” setting, or a particular language?
- Is your business currently registered with an EEA data protection authority, such as the UK’s Information Commissioner’s Office (the ICO)?
- Do you monitor the behaviour of any individuals within the EEA (irrespective of their nationality or habitual residence)? For example if your website uses tracking cookies then you are “monitoring

individuals" for the purposes of the GDPR.

- Can your flights be bought from within the EEA and can they be sold as a return package whereby the outgoing flight departs from the EEA and the inbound flight returns to the EEA?

If any of these factors apply, then it is likely that the GDPR refers to your business.

Eight key provisions of the GDPR which require action now

Having established that the GDPR will apply to your business, consider the following eight provisions in particular which require priority action. Key terms to understand are as follows:

- "Data controllers" make the decisions on how and why personal data is processed, whereas "data processors" only process data on the instructions of the data controller.
- "Processing" means essentially any action involving personal data (including merely storing it).
- "Personal data" means any information relating to an identified or identifiable natural (living) person. Note that under the new definition of personal data, online identifiers such as cookies and IP addresses can make an individual "identifiable".

1. Reporting of personal data breaches

This is a key change. The current EU directive does not generally require data controllers to notify data protection authorities about security breaches. In the UK, the ICO currently recommends that data controllers notify it if the breach poses a high risk to individuals but there is no legal requirement to do so (except for telecommunications service providers). Under the GDPR notification is mandatory and, as explained above, the timelines for compliance are short.

- A data controller must notify a personal data breach to the relevant supervisory authority within 72 hours after becoming aware of a personal data security breach.
- The exception to this is where the personal data breach is *"unlikely to result in a risk to the rights and freedoms of natural persons"*.
- Where there is such a risk, a delay beyond 72 hours must be accompanied by reasons for the delay.

Notification to the individuals concerned:

- When the personal data breach is *"likely to result in a high risk to the rights and freedoms of natural persons"* the data controller must also notify the data subject *"without undue delay"*. This could be a notification window smaller than 72 hours.

Data controllers will also need to keep a register of any personal data breaches, including details of what happened and what was done to resolve the issue. This will be subject to inspection by the relevant supervisory authority.

Action required

- Create and maintain a register of data breaches.
- Update or create a cyber security breach procedure to take into account the short timelines for notification under the GDPR.
- In the event of a security breach, there will be very little time - to determine the extent of the damage, the individuals affected, the security arrangements which will need to be either changed or strengthened, and whether or not the breach requires notification to the national data protection authority and/

or individuals concerned. It would be prudent to establish parameters for making such decisions, and designate people who will be responsible for making them.

- Consider taking out a cyber insurance policy and lining up public relations advisors who can help you reduce the potential damage to your reputation in the event of a personal data breach.

2. Grounds for processing – beware "consent"

Currently, the processing of personal data is prohibited under the GDPR unless a data controller has one or more of the legal grounds set out in the legislation for processing those data. For standard personal data, the most useful of these grounds from an airline's point of view are that:

- The processing is necessary for the purposes of the "legitimate interests" of the data controller or a third party.
- The processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
- The processing is necessary for compliance with a legal obligation; or
- The individual has given his or her consent to the processing.

The grounds for processing "sensitive personal data" are more limited. Sensitive personal data is defined as data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data uniquely used to identify a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. This includes, for example, information on dietary requirements where these might reveal an individual's religion or a medical condition, requests for special assistance, pregnancy and in some cases a copy of an individual's passport where the combination of the name and photograph reveal the individual's religion or ethnicity. With some exceptions, the individual's consent is necessary unless lives are at risk and the individual is not able to give consent.

Airlines should often be able to rely on the "legitimate interest" or "necessary for the performance of a contract" grounds for processing standard personal data, which will constitute the majority of their processing. If processing sensitive personal data or otherwise relying on the "consent" ground, which is tighter under the GDPR, controllers must be able to demonstrate that an individual has consented to the processing of his or her data. Consent provisions cannot be buried in the middle of a long piece of text and must be a clear indication of the individual's wishes and they must be able to be withdrawn at any time.

Action required

- Review whether and how "sensitive personal data" is collected and held. If you are currently relying on consent for processing any type of data you should check whether there are other applicable grounds that you can rely on instead, and document these.
- Check that each individual (natural person, sole trader or unlimited liability partnership) on your marketing databases has either explicitly consented to receive electronic marketing, or, if they are existing customers, that they were given the opportunity to opt out from such marketing when their contact details were first collected and that their wishes have been respected.
- For business contacts ensure that each communication includes a mechanism to "opt out" of future unsolicited marketing, so that they can easily exercise their right to object to their personal data being processed for marketing purposes.

3. Data audit and record keeping requirements

Record keeping requirements will be more stringent under the GDPR. It will require data controllers (and processors) to keep records of the personal data they process and there will be no phased implementation of the record keeping requirements. Records must be updated regularly and must include information about the purposes of processing, the data subjects and categories of personal data involved, details of personal data transferred outside of the EEA, the envisaged time limits for deletion of different categories of data and a general description of the technical and organisational security measures it uses to keep personal data safe. These records must be available for inspection by a relevant EU data protection authority on request.

Action required

- Audit your personal data processing now. What personal data do you process? Why were they collected? Why and how are you using the data? Where are the data kept? Are there extensive personal data in archive? Do you still need all of them? Do you use the data for the purpose they were collected or do you use them for new purposes?
- If personal data are out of date, update them. If personal data are no longer needed, delete them. This will minimise your risk and ensure that you are in compliance with the GDPR aim of personal data minimisation.

4. Fair processing notices

Data subjects must be kept informed about the processing of their personal data. The GDPR increases the amount of information which must be included in these notices. A key change is that if the data controller is relying on its legitimate interests to process the personal data, the particular legitimate interests should be listed in the privacy notice.

"Sensitive personal data is defined as data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data used to uniquely identify a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation."

Action required

- Add a privacy policy to your website, if you have not done so already, to make clear how you use data collected on your website, and also to make it clear to passengers how their personal data will be used.
- Consider "just in time" notices (that is a box of text which appears when a mouse hovers over a particular box in a collection form) when collecting personal data such as email addresses to say how that information will be used.
- If you collect information on individuals from third parties then make sure that the individuals are aware that you are processing their data. Consider exploring contractual options to ensure that the individuals have been made aware that you will be processing the data, how and why, as well as how to contact you to enforce their rights.

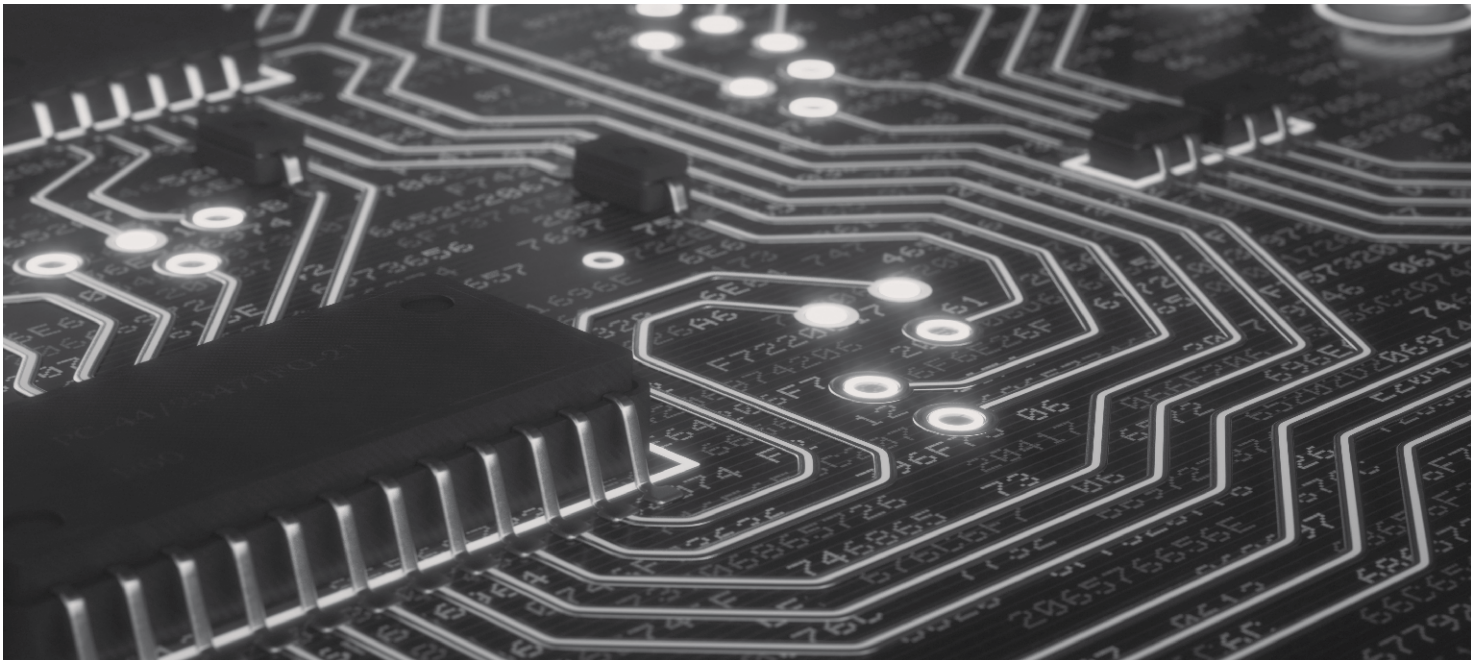
5. Additional and strengthened rights for individuals

The GDPR strengthens and increases individuals' rights. Some examples are as follows:

- Shorter time to respond to subject access requests and more detail required. The current response period for a subject access request is 40 days. The GDPR requires that the response must be "without delay" or at least within one month. The information which must be provided to an individual who makes a genuine subject access request must now include a notification of the right to lodge a complaint with the supervisory authority, and information about transfers of the data outside of the EEA.
- Right to request deletion. The controversial "right to be forgotten" has been strengthened, specifying the circumstances where the data controller must on request erase personal data without "undue delay".
- Data portability. A new right to "data portability" will in many cases entitle individuals to have their personal data transferred to alternative service providers in a structured, commonly used and machine-readable format. This only applies where data processing is carried out by automated means (ie on computers).
- Rights to object to processing and to request restriction. The GDPR gives subjects more rights to object to their data being processed (for example where the data subject believes that his or her legitimate interests outweigh the data controller's) or to request "restriction" of their personal data (for example because the original purposes for processing no longer apply). The burden will be on the controller to demonstrate that it is legally entitled to process the personal data.
- Right to object to direct marketing. Individuals will have an absolute right to object to their personal data being processed (including storage) for direct marketing purposes. This is much stronger than the current right to object to receiving direct marketing materials, because it affects what data about individuals is stored, not just what can be done with them.

Action required

- Put processes in place to deal with requests from individuals seeking to enforce their rights within the shorter period permitted for response, including a designated team to deal with such requests. On receipt of a request from an individual, the quicker that you



can make a decision the sooner you can resume business and minimise waste of company time and resources.

6. Contracts with processors

Contracts between data controllers and data processors are already mandatory. The GDPR prescribes specific new clauses which must be included in such contracts, for example, an obligation on the data processors to act only on the documented instructions of the data controller, to impose confidentiality obligations on the staff who will be processing the data and to delete or return all of the personal data at the end of the provision of services related to the processing.

Action required

- Consider which of your service providers are acting as data processors and which are acting as controllers.
- Make sure that your contracts reflect the position and contain the necessary GDPR elements.

7. "Privacy by design" and Data Privacy Impact Assessments

An important new concept is that of "privacy by design" and by default. When introducing new products, services, or processes, data controllers will need to show that the impact of such products, services or processes has been considered, and that steps have been taken to minimise any negative impact on individuals' rights and freedoms. Data should be pseudonymised where possible and should not be collected unless it is really needed.

Action required

- For new projects, do not collect personal data unless you can justify your purposes for doing so and you have conducted, and documented, privacy impact assessments. These should, amongst other things, determine how you will keep personal data safe and how high risk the proposed project is to individuals' privacy.
- Make sure that your data protection policies are up to date and that your data processing is transparent.

8. Appointment of Data Protection Officers

There will no longer be a need to register as a data controller in an EU member state. However, data controllers and processors must designate a "data protection officer" in certain circumstances, including where:

- *"The core activities" of the controller or the processor consist of "processing operations which… require regular and systematic monitoring of data subjects on a large scale";* or
- The *"core activities"* of the controller or the processor consist of "processing on a large scale" of *"special categories of data"* (ie "sensitive personal data") and "personal data relating to criminal convictions and offences".

These circumstances may not apply to all airlines. However, a controller or processor can also choose to appoint a data protection officer voluntarily, or a member state can require it under local law. Given the increasing importance of data protection, it can be useful to dedicate resources to ensuring compliance with applicable data protection laws. However, be aware that there are mandatory minimum requirements under the

"Given the increasing importance of data protection, it can be useful to dedicate resources to ensuring compliance with applicable data protection laws. However, be aware that there are mandatory minimum requirements under the GDPR for data protection officers, for example the data protection officer should have expertise on both local data protection law and on the GDPR."

GDPR for data protection officers, for example the data protection officer should have expertise on both local data protection law and on the GDPR.

Action required

- Assess whether you should appoint a data protection officer, and make arrangements accordingly. Note that the data protection officer should have expertise on both local data protection law and on the GDPR.

HFW can help you create a plan to ensure compliance with the GDPR. If you are interested in working with us to get ready for the GDPR, we will be happy to discuss your current systems and policies and provide a fee estimate for a bespoke GDPR compliance project.

For further information, please contact the authors of this briefing:

ANTHONY WOOLICH
Partner, London
T +44 (0)20 7264 8033
E anthony.woolich@hfw.com

GILES KAVANAGH
Partner, London
T +44 (0)20 7264 8778
E giles.kavanagh@hfw.com

FELICITY BURLING
Associate, London
T +44 (0)20 7264 8057
E felicity.burling@hfw.com

HFW has over 500 lawyers working in offices across Australia, Asia, the Middle East, Europe and the Americas. For further information about our EU, competition and regulatory trade capabilities, please visit hfw.com/EU-Competition-and-Regulatory

hfw.com

© 2017 Holman Fenwick Willan LLP. All rights reserved.
Whilst every care has been taken to ensure the accuracy of this information at the time of publication, the information is intended as guidance only. It should not be considered as legal advice. Holman Fenwick Willan LLP is the Data Controller for any data that it holds about you. To correct your personal details or change your mailing preferences please contact Souhir Jemai on +44 (0)20 7264 8415 or email souhir.jemai@hfw.com

Beirut Brussels Dubai Geneva Hong Kong Houston Kuwait London Melbourne Paris Perth Piraeus Riyadh São Paulo Shanghai Singapore Sydney