STEPHENSON HARWOOD

# Data protection in the United Kingdom: the GDPR countdown

## What do airlines need to do?

The European General Data Protection Regulation ("**GDPR**") comes in to force on 25 May 2018 and heralds a step change in data protection ("**DP**") law throughout the European Union. What does this mean for the airline industry?

The GDPR is designed to harmonise national data protection laws across Europe, enhance the rights of EU citizens, and reshape the way that organisations approach data privacy.

### The GDPR:

- Has as an increased territorial scope as it applies to all companies processing the personal data of EU citizens, regardless of the company's location.
- Permits fines of up to 4% of annual global turnover or €20 million, whichever is greater.
- Strengthens the conditions for consent, thereby requiring individuals to give unambiguous and informed consent for their data to be processed.
- Imposes a 72 hour timeframe for companies to report a data breach if there is risk to affected individuals.
- Affords individuals the right to access their personal data and the 'right to be forgotten' (data erasure).
- Introduces data portability, namely the right for an individual to receive the personal data concerning them and the right to transmit that data to another controller.
- Implements 'privacy by design', which calls for the inclusion of data protection from the onset of the designing of systems rather than as an afterthought.
- Requires companies that systematically process data to appoint a Data Protection Officer ("**DPO**").

The GDPR will apply to most international airlines as they will be classified as data controllers by virtue of the personal data they hold about their passengers. This means that the GDPR will apply to airlines – both EU and non-EU – that:

- Offer flights, holidays and/or other services to EU-based individuals, including through an EU reservation centre or office or via a website that provides for bookings to be made by EU citizens (whilst providing for the appropriate currency and language during the booking process).
- Monitor the behaviour of EU residents, such as through cookies or by collecting location data for EU passengers in transportation hubs or via mobile devices used to make payments for tickets or to display a boarding pass.

Equally, it will apply to air cargo operators whose documentation such as airway bills, invoices, proof of delivery documents, release notes and manifests contain data relating to EU citizens.

To ensure compliance with GDPR by 25 May 2018, it is vital that airlines:

- Take stock of their current DP practices now.
- Understand the impact of the changes to DP law for them and on their business.
- Take any necessary action.

### Key points for airlines to address in this process are:

- Privacy notices on websites (amendments and additions will be required to ensure they meet the new requirements).
- A review of liability protection in light of the harsher penalties that may apply for non-compliance with DP legal requirements.
- A review of the legal basis adopted for processing personal and sensitive data.
- Shorter timeframes for complying with subject access requests and reporting any data breaches to the UK's Information Commissioner's Office ("**ICO**").
- New and enhanced data subject rights in relation to personal data.
- Reviewing agreements with third party service providers such as airports, ground handlers, and freight and logistics operators to ensure compliance with the new DP requirements.
- Negotiations with third party service providers over the extent of their liability for DP law breaches and any indemnities required.

## Where to start?

Here. This document sets out an essential eight point DP checklist. The starting point for airlines should be a data audit, as this will go some way towards satisfying the new requirements and help identify what other steps need to be taken. This audit should be undertaken as soon as possible to ensure full compliance by May 2018.

Stephenson Harwood can help airlines navigate this initial data audit and address the above points. Full contact details of our team of DP and aviation experts are on the last page of this document should you wish to find out more about our range of DP advice specific for airlines or should you have any general DP queries arising from this document.

## 1. Information held by airlines

Under existing DP law, there is an implicit requirement that data controllers such as airlines know what data they hold and how that data is held. The GDPR makes this explicit, requiring data controllers to record and document details including the data they hold, the purposes of the processing of that data and who the data is shared with. Processors must also document their processing activities.

By doing this, airlines may discover certain DP issues that need to be addressed. For example, controllers may identify certain data that is not necessary – such as data regarding passengers who did not proceed with a flight booking – and make arrangements for its deletion.

**To comply with this new requirement, airlines should consider carrying out a data audit covering:**

- ✓ **the personal data held**
- ✓ **the source of that data**
- ✓ **how the data is stored, where it is stored and how long for**
- ✓ **the reason(s) it is necessary to process that data**
- ✓ **whether it is legitimate to process that data**
- ✓ **who else has access to the data.**

## 2. Communicating privacy information

Data controllers such as airlines should already use privacy notices on their websites and via other booking channels that provide fair processing information to data subjects such as passengers and employees that might also seek express consent to the processing of personal and sensitive personal data.

The GDPR enhances the existing requirements so that it will be necessary for data controllers to communicate:

- The reason(s) and the legal basis which they are relying on to process personal data.
- How long the data will be held for.
- Information about the right to complain to the ICO where individuals think there is a problem with the way their data is being handled.

All notices must be concise, transparent, intelligible and easily accessible.

The definition of personal data is modified and simplified, and the definition of sensitive personal data is extended to cover genetic and biometric data. Sensitive personal data is defined as data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, 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. So if an airline holds data on the PNR (passenger name record) or otherwise relating to special dietary requirements where this might reveal an individual's religion, or a medical condition, a request for special assistance (e.g. mobility) or pregnancy, the individual's consent is necessary for the processing of that data unless lives are at risk (e.g. serious cross-border threats to health) and the individual is unable to give consent.

**Airlines should review their existing privacy notices and policies on their websites and in other documentation, and update them in line with the new requirements. This privacy policy should make clear how the data collected on your website, including passengers' personal data, will be used.**

## 3. Data rights (including subject access requests)


The current DP law already provides certain rights to data subjects (such as employees and passengers) over the personal data that data controller may hold about them. This includes a right to access their personal data and rights to stop certain data processing.

The GDPR makes significant enhancements and additions to these rights, including a new right to delete personal data where continued processing is unnecessary (not just where damage or distress is caused) and a right to "data portability", which is the ability to request that certain data is transferred to a different controller.

In addition, the subject access request ("**SAR**") requirements are being made more onerous, so that:

- The time for compliance with any SAR is reduced from 40 days to one month.
- The ability to charge a £10 fee for any SAR is now much more limited.
- It is possible to refuse, or ask for a reasonable fee for, unfounded or excessive SARs but prescribed information must be provided to the data subject in such circumstances.

**Airlines should consider how their procedures should change to comply with these enhanced rights.**

## 4. Data subject consent

Consent to the processing of personal data will generally become more difficult to obtain. For example, it must be freely given, specific, informed and unambiguous. There must also be a positive opt-in and so it will not be possible to infer consent from silence, pre-ticked boxes or inactivity. Requests for consent that are bundled in with other terms, rather than clearly separated out, will probably not be sufficient.

**Airlines that rely on consent to process data will need to review existing consents to determine whether they would be adequate under GDPR or whether there are more appropriate legal grounds to rely on than consent. Existing privacy notices on websites, and in conditions of carriage and employee contracts may not be adequate and so a new GDPR-compliant consent mechanism may be required.**

Data subjects will have the right to withdraw consent at any time and this could potentially create significant operational issues for controllers. In addition, GDPR-compliant consent may be difficult for employers to obtain from their employees, since the imbalance of power means that consent may not be seen as having been freely-given. As such, controllers may need to look for a different legal basis for processing personal data.

In 2017, the ICO sent a strong message ahead of the GDPR coming into force by fining a UK airline £70,000. This fine related to the airline sending an email to more than three million customers who had previously opted out of receiving communications.

## 5. Legal basis for processing personal data

The legal basis (or bases) adopted for processing personal data will be more of an issue under the GDPR, as some individuals' rights will be modified depending on the legal basis adopted. For example, if controllers rely on consent, data subjects such as passengers will generally have stronger rights, including a right to have their data deleted.

Alternatives to data subject consent for non-sensitive personal data include where processing is necessary for the performance of a contract with the data subject or for the purposes of legitimate interests pursued by the controller (except where those interests are overridden by the interests, rights or freedoms of the data subject).

**Airlines need to determine the legal basis on which personal data of passengers and employees is processed, document this and update the relevant privacy notices on their website and in their documentation to explain it.**

## 6. Accountability – demonstrating compliance

The GDPR includes an accountability principle which effectively means airlines must not only comply with the data protection principles but also demonstrate how they comply.

**Airlines can take a number of steps to help ensure and demonstrate compliance:**

- ✓ Keep records of all data processing activities carried out.
- ✓ Implement (or review existing) technical and organisational measures for achieving compliance, e.g. data protection policies in relation to employee training and internal audits of processing activities regarding passenger data.
- ✓ Undertake a data protection impact assessment ("**DPIA**") where data processing is likely to result in high risk to individuals, e.g. where new technology is being deployed. Data controllers could prepare a DPIA policy/template document.
- ✓ Implement measures that meet the principles of data protection by design and by default, including data minimisation, pseudonymisation, transparency, and improving security features on an ongoing basis.

## 7. Data breaches and fines for breaches


A personal data breach is a breach of security leading to the destruction, loss, alteration or unauthorised disclosure of, or access to, personal data.

There will be a new mandatory requirement for controllers to notify data breaches to the ICO where it is likely to result in a risk to the rights and freedoms of individuals (e.g. where a breach could result in discrimination, damage to reputation or financial loss). Notifications must be made without undue delay and, where possible, within 72 hours of becoming aware of the breach. If the breach is likely to result in a high risk to the rights and freedoms of individuals, the controller must also notify the individuals concerned directly without undue delay.

Failure to notify can result in a fine of up to the higher of €10 million or 2% of annual worldwide turnover. This would be in addition to the fine for the breach itself, which could be up to the higher of €20 million and 4% of annual worldwide turnover (a significant increase to the current maximum fine of £500,000).


Controllers' potential liability is therefore greatly increased. Data processors such as third party suppliers are directly responsible under the GDPR for informing the relevant controller "without undue delay" after becoming aware of a personal data breach, but controllers may wish to make this obligation more onerous under contract, by for example requiring that the processor notifies them within 24 hours, to allow the controller to meet the 72-hour deadline.

**Airlines should ensure they have robust procedures in place to identify, assess, record and, where appropriate, notify data breaches. A register of data breaches should be maintained. Airlines may also wish to revisit the protection from liability they obtain through indemnities in contracts with processors and any liability insurance that covers GDPR fines.**

## 8. Contracts with data processors

The GDPR places direct legal obligations on data processors in relation to things like implementing appropriate data security measures and keeping a record of processing carried out on behalf of a data controller. Data processors are also required to ensure contracts with data controllers contain certain minimum provisions, such as a description of the scope, nature and purpose of processing.

**Airlines should review and update their contracts with their service providers who are acting as data processors to ensure there are appropriate provisions in relation to the data processor's new direct obligations and other relevant matters such as compliance, monitoring and reporting.**

Liability and indemnity clauses in contracts should also be reviewed to ensure the risk allocation remains appropriate given that data processors now have direct legal obligations and given that data controllers and data processors will have the same obligations in areas such as security. Data processors will be directly liable for breaches under the GDPR and so may consider seeking indemnities from controllers in relation to data protection fines caused by the controllers.

If you would like further information on the developments referred to in this guide, our DP advice or any other data protection legal issues relating to airlines, please get in touch with the Stephenson Harwood aviation or commercial, outsourcing and technology teams.


### Paul Phillips
Partner

T: +44 20 7809 2302
M: +44 7734 135 401
E: paul.phillips@shlegal.com

### Chloe Challinor
Senior associate

T: +44 20 7809 2142
M: +44 7702 141 049
E: chloe.challinor@shlegal.com

### Tim Knight
Associate

T: +44 20 7809 2990
M: +44 7808 077 572
E: timothy.knight@shlegal.com

### Jonathan Kirsop
Partner

T: +44 20 7809 2121
M: +44 7554 403 022
E: jonathan.kirsop@shlegal.com

### Chloe Haywood
Associate

T: +44 20 7809 2348
M: +44 7872 112 799
E: chloe.haywood@shlegal.com

### Johnny Champion
Associate

T: +44 20 7809 2358
E: johnny.champion@shlegal.com







BD377-GDPR airlines-0318