Bird & Bird &

GDPR Two Years On: What are the lessons learnt for the aviation industry?

June 2020

25 May 2020 marked the second anniversary of the EU General Data Protection Regulation ("GDPR"), the EU's cornerstone data protection law that changed the regulatory landscape in Europe and exerts a far-reaching global impact.

Last year limited GDPR enforcement actions were reported throughout its first year of application; this year, we have seen increasing activity from regulators in the field of data protection enforcement and the investigation of high-profile cases, some of which have been within the aviation sector.

The GDPR has extra-territorial effect which affects many organisations in the aviation industry. The GDPR applies to these organisations where personal data is processed either (i) in the context of the activities of their establishments within the European Economic Area ("EEA") (e.g. an airline having a sales office or branch in the EEA), or (ii) in respect of non-EEA establishments, where they process personal data in relation to offering goods or services to individuals in the EEA or monitoring the behaviour of individuals within the EEA (e.g. a non-EEA airline operating a website targeting the EEA market). Read our article for more information on how the GDPR applies to your organisation.

Airlines, airport operators and their service providers, such as ground handling companies, routinely process large amounts of personal data: information about passengers, crew and other employees as well as personal data relating to suppliers and other business contacts. The highly regulated environment in which aviation players operate and the international character of their operations add another layer of complexity in respect of data protection compliance.

In this article, we examine how the GDPR affects the aviation industry and we focus in particular on:

I. Recent data breaches and enforcement action in the aviation sector;
II. Key aspects of data protection compliance for aviation organisations; and
III. The impact of Brexit on data protection compliance.

I. Data breaches and enforcement in the Aviation Industry

During the past couple of years, we have seen a significant increase in security incidents that affect personal data. This is partly because reporting of personal data breaches is now mandatory under the GDPR; but also, because security attacks are becoming more and more sophisticated and are having a larger scale effect.

In line with this trend, the aviation sector has recently suffered a spate of high profile security incidents which have exposed large amounts of personal data and have drawn the attention of data protection regulators in Europe. Some examples of types of data breaches and enforcement actions are summarised below:

Organisation	Data breach	Enforcement action
Airports, airlines, etc.	The most high-profile of these incidents have been caused by malicious external attacks which have compromised personal data such as customers' contact details, travel information and in some instances payment card information. Other incidents – which tend to be the most common in practice – have an internal source and are caused by human error, negligent or rogue behaviour of employees (these include for example an employee losing a USB stick containing personal data or allowing unauthorised access to the company's booking application).	Where data protection regulators have found that the companies suffering the breach did not have appropriate security measures in place or did not otherwise comply with the GDPR, they imposed or published their intention to impose significant fines on those companies. In the meantime, such security incidents have exposed or risk exposing companies to consumer class actions.

II. Key aspects of data protection compliance

The GPDR established a two-tier fine system. For certain violations companies can be fined by data protection regulators up to €10 million or 2% of their global annual turnover, whichever is higher; for the most significant infringements of the GDPR, regulators can impose fines of up to €20 million or 4% of an organisation's global annual turnover, whichever is higher. Of course, the impact of non-compliance extends beyond the fines, and organisations risk being exposed to reputational damage, loss of customer trust, fall of share price and consumer or employee class actions.

In this landscape, it is important to strengthen data protection compliance. We examine below how key data protection aspects can be operationalised within the aviation industry.

i. Interactions with your passengers and employees

1. Customer and employee facing documentation

Privacy notices are the most typical customer and employee facing documents that you need to have in place in order to explain to passengers, flight bookers, crew members and other employees how you process their personal information. The GDPR sets out specific information requirements relating to such documentation, for example:

- The details of your data processing activities (for example, who you are, why you process personal information, on what legal basis you rely under data protection laws, with whom you share personal information and how long you keep it for);

- Individuals' rights in respect of their personal data (for example, their right to get a copy of their data, to have incorrect data rectified or to object to direct marketing); and
- If you take fully automated decisions about individuals (e.g. certain targeted advertising with differential pricing): relevant information, such as information on the process you follow to reach decisions and the effects on such decisions on individuals.

  You must assess how best to provide this information to your customers and employees and ensure that you use clear language that is easy for people to understand.

  Remember, for the users of your websites, you also need to inform them about how you use cookies and to seek their consent.

2. High standards for valid consent

Under the GDPR, it is not always appropriate to rely on consent; however, when you choose to do so, you need to obtain consent in a way that meets GDPR's high bar. GDPR requires that consent is *"freely given, specific, informed and unambiguous"*. Also, individuals have the right to refuse consent or withdraw it at any time, without detriment.

Consent of passengers or employees could be appropriate in certain limited circumstances, for example in order to:

- collect and process information about a passenger's medical condition or their dietary requirements that could reveal their religion or state of health;
- use cookies or similar tracking technologies on your websites; or
- to send electronic marketing communications (unless specific exemptions apply).

3. Dealing with individuals' rights

The GDPR gives individuals certain rights in respect of the processing of their personal data: the right to access their data, have incorrect data about them rectified, receive a portable copy of some of their data, and in some instances object to the processing of their data, request its erasure or request the restriction of processing. When it comes to fully automated decision making, including profiling, individuals have additional rights. In principle, companies have one month to respond to such requests and should do so free of charge.

With the collection and processing of large amounts of passengers'/employees' personal data, you should ensure that you have appropriate processes in place to be able to meet your obligations in respect of individuals' requests.

ii. Engagement with third parties

The GDPR sets out specific requirements in relation to arrangements with data processors and other (joint) controllers. To the extent they haven't already, aviation companies should review their arrangements with third parties to ensure they meet such requirements. In this context, you should consider the following:

- Do you have written data processing agreements with your data processors incorporating GDPR-mandatory terms?
- Do your processors have similar agreements in place with their sub-processors?
- Do you carry out joint processing activities and are joint controller with your partners? If so, have you allocated data protection responsibilities between you and the other party?

Air carriers in codeshare agreements could possibly be deemed as joint controllers for the processing of passengers' personal data – if this is the case, they will be required to arrange between them their respective responsibilities for compliance with the GDPR.

The assessment of a third party as processor, independent or joint controller is crucial in order to determine what terms you should include in your contracts. However, this is not always straightforward.

iii. Accountability

Accountability is a key principle under the GDPR – it essentially requires organisations not only to comply with the GDPR, but also to be able to demonstrate such compliance. The measures outlined below reflect some of an organisation's accountability requirements:

1. **Record of processing activities**

Under the GDPR, you are required to keep a record of your data processing activities. Such record should include details of your processing operations, including, what data you process, for what purposes, to whom the data relates (e.g. passengers, crew members, etc.), with whom you share the data, how long you keep it for and what security measures you use to protect it.

2. **DPO and GDPR Representative**

The GDPR requires organisations to appoint a Data Protection Officer ("DPO") if their core activities consist of large-scale processing of special categories of personal data (for example, health information, trade union membership or biometric data used to uniquely identify individuals) and of data relating to criminal offences or regular and systematic monitoring of individuals on a large scale. Organisations in the aviation industry that meet these conditions would need to designate a DPO.

Organisations that are based outside the EEA and are subject to the GDPR are required to appoint an EEA-based "GDPR Representative". For example, this would be the case for airlines which does not have EEA establishments but provide flight tickets and services to EEA customers.

3. **Data Protection Impact Assessment (DPIA)**

A DPIA is an assessment through which organisations identify and mitigate risks to individuals arising out a data processing activity. The GDPR requires organisations to carry out a DPIA before commencing any "high risk" processing activity.

In the aviation sector, the use of biometric data in the boarding process or the processing of Covid-19 related information is likely to trigger the need to conduct a DPIA.

4. **Privacy by design and by default**

Aviation companies must ensure that their websites, mobile apps, and other information systems are designed to achieve compliance with the GDPR.

5. **Other accountability requirements**

- **Internal policies and procedures**

Aviation companies should have data protection policies and procedures in place to demonstrate compliance with the GDPR. For example, a data breach management policy, a policy for complying with individuals' requests, a direct marketing policy, etc.

- **Training**

It is very important that aviation companies provide data protection training to their staff, in particular to employees who regularly process personal data as part of their tasks (e.g. HR, Finance, Customer services and customer-facing ground handling staff).

iv. Data security and data breach notification obligations

Security is one of the most significant requirements under the GDPR. Organisations have an obligation to put in place appropriate technical and organisational measures to protect the

personal data they process. This requirement extends both to computerised systems and manual records and includes any processes relating to personal data.

The large number of information systems used by aviation companies and the wide range of data points used make this requirement even more important in the aviation industry.

In the event of a data breach, companies are required to report the data breach to the relevant supervisory authority within **72 hours** of becoming aware of this, where feasible, unless the breach is unlikely to result in a risk to individuals' rights and freedoms. If the breach is likely to have high impact on people, companies must also inform the affected individuals without undue delay.

To be able to meet their obligations, companies should have robust procedures in place to detect, investigate and remediate such breaches.

v. International data transfers

The cross-border element of the aviation industry makes data transfers an essential part of aviation operations. However, data transfers to non-EEA countries which are not deemed to provide an adequate level of protection are restricted under the GDPR. If your company is based in such a jurisdiction, transferring customer or employee data from the EEA to your headquarter must be based on a data transfer mechanism, such as Standard Contractual Clauses ("SCCs") or Binding Corporate Rules ("BCRs"). When there are no such appropriate safeguards in place, the data transfer might still be legitimised on the basis of derogation (such as explicit consent, contractual necessity, public interest, legal claims) or specific exemptions; however, these cases are limited to exceptional circumstances.

III. Brexit: how will it affect my GDPR compliance?

The UK left the EU on January 31, 2020. However, there is currently no change during the transition period which will last until the end of 2020 and during which the UK and the EU negotiate additional arrangements. The landscape is expected to change at the end of the transition period and organisations should closely follow developments to ensure their relevant UK data processing activities also comply with UK-based data protection legislation.

IV. Prevention is the best defence

As we examined above, failure to comply with the GDPR can have a significant impact on businesses. As it is said, there's only one way to eat an elephant: one bite at a time. GDPR compliance is not a sprint; it is a marathon and requires ongoing efforts and vigilance by everyone within the business.

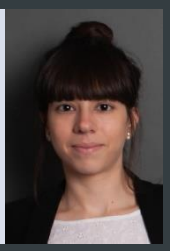
Bird & Bird has been active in the field of data protection for over 25 years. We are number 1 rated in the legal directories and we boast one of the largest practices in Europe and Asia Pacific who advise solely on data protection. If you are interested in our practices and would like to learn more about how we can assist with your GDPR compliance projects, please get in touch.

Did you know you can outsource your DPO/GDPR Representative responsibilities? Check out our Bird&Bird Privacy Solutions for further details.

Contacts

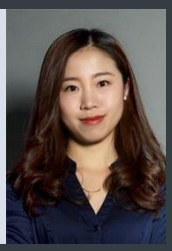
Gabriel Voisin
Partner, London

Tel: +44 (0)20 7415 6000
gabriel.voisin@twobirds.com



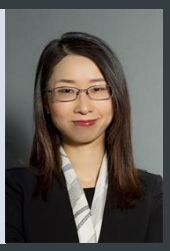
Katerina Tassi
Associate, London

Tel: +44 (0)20 7415 6000
katerina.tassi@twobirds.com



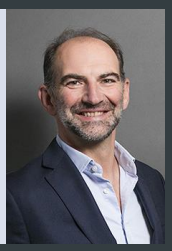
Tiantian Ke
Associate, Shanghai

Tel: +86 21 2312 1291
tiantian.ke@twobirds.com



Aubrey Tao
Managing Associate, Shanghai

Tel: + 86 21 2312 1202
aubrey.tao@twobirds.com



Leo Fattorini
Partner, Joint Head of International Aviation & Aerospace sector group

Tel: :+ 65 6428 9434
leo.fattorini@twobirds.com

Lucy England
Partner, London

Tel: +44 (0)20 7415 6000
lucy.england@twobirds.com

twobirds.com

Abu Dhabi & Amsterdam & Beijing & Bratislava & Brussels & Budapest & Copenhagen & Dubai & Dusseldorf & Frankfurt & The Hague & Hamburg & Helsinki & Hong Kong & London & Luxembourg & Lyon & Madrid & Milan & Munich & Paris & Prague & Rome & San Francisco & Shanghai & Singapore & Stockholm & Sydney & Warsaw