The Use of Personal Data in the Commercial Aviation Industry

RadcliffesLeBrasseur UK LLP

Alan D. Meneghetti

Introduction

The opportunities created by data, and in particular personal data, can be immensely valuable for all manner of businesses, for both market insight and financial reasons. The commercial aviation sector is of course no different in this respect, especially given the sheer volume and variety of data generated by the aviation industry – from engineering and scientific data, to flight data and weather data, through to consumer data, passenger data, security data, personal and in some cases (what we in the EU refer to as) special categories of personal data (that is, data regarding an individual's race and ethnic origins, medical information, religious beliefs and so on).[1]

The generation of data gives rise to many questions, including:

- where that data is collected;
- how that data is treated by the recipient or holder of that data;
- where that data is stored;
- whether that data is transferred from the initial recipient of it to others and, if so, to whom, where and on what basis;
- whether or not that data needs to be stored securely and, if so, whether it is indeed stored securely;
- if that data needs to be stored securely, the standards of security to which that data storage needs to comply;
- the use of that data; and
- if that data relates to an individual (a "data subject"), whether the data subject supplied their consent knowingly, willingly and whilst being fully informed of: (i) the uses to which their data will be put; (ii) where their data will be stored and processed; and (iii) the security arrangements that are in place with respect to their data (and – a corollary of sorts – whether they can withdraw their consent and "take their data back").

The answers to, and indeed the relevance of, these questions depend on the type of data which is involved – flight, weather, technical and engineering data (for example) will be treated differently and viewed by different recipients than, say, a passenger's personal data which might be collected by duty-free shops, the airport (either directly or through its website), the ground handlers and security companies, and/or the airline operators. It is also worth keeping in mind that not all types of data are protected by law – whilst certain types of data (most notably, personal data) will be legislatively protected in many jurisdictions, other types of data may be protected simply by the parties dealing with that data on the basis that it is confidential or business-sensitive (e.g. the average spend at the various duty-free shops).

In this short chapter, some instances where, and the touchpoints at which, personal data is collected in the commercial aviation industry are explored. It should be noted that this is a vast topic in and of itself, and one can write dedicated chapters and even books on the issues raised by, and the answers to, the questions set out above. This chapter merely aims to provide a starting point for the key questions raised. This chapter does not explore the added ramifications presented by the use of artificial intelligence (or simply "AI", as it is most commonly referred to), and the ethics around this which are being worked out, it seems, almost on a weekly basis.

Collection Points

Personal data will be collected throughout the entire "passenger experience" from the beginning, starting with the booking of an airline ticket, to the potential purchasing of duty-free products on board, as demonstrated in the example set out below.

Case Study

A passenger wishing to travel from London Gatwick will log on to the Gatwick Airport website to find out the best way to travel to the airport. While browsing, cookies will be collected which track the passenger's movements through the website. In certain situations, the passenger may volunteer their email address and other personal information in order to be contacted by the airport in the event of delays (due to, for example, bad weather) or to receive regular updates and news from the airport.

Before leaving their house, or whilst on their mobile, the passenger may check in online, select their seat on the aircraft, advance-purchase any duty-free items for collection on board and input their meal choice and any other dietary requirements they may have (at which point, more cookies are collected, as well as personal data – this time by the airline on which the passenger is travelling). Potentially, special categories of personal data can also be collected; for example, pointers to the passenger's physical health and religion may (although, admittedly, not necessarily) be indicated by meal choices and special requirements (for example, the need for a wheelchair, extra oxygen on board or special assistance).

Once at the airport, the passenger will self-tag and drop their bag at the airline's bag-drop counter (again, delivering personal data regarding their name, passport details, address, flight details and so on), pass through customs and immigration (at which point, more personal data is submitted to the customs and immigration authorities) and proceed to security, where they may be scanned using a full body scanner (which collects personal data regarding the passenger, at least to the extent the scanners are able to identify any physical health issues such as implants, not to mention generating images of the passenger's body which raise a number of privacy concerns for adults, let alone minors).[2]

The passenger may then purchase further duty-free goods on their debit or credit card, showing their boarding card and possibly also an airport rewards card (both of which are scanned – again, more personal data is collected, this time regarding the passenger's whereabouts and purchasing preferences), and boards the aircraft where, if they are travelling internationally, they may have to complete an immigration form requesting further personal data. The passenger may also purchase more goods on board (on their debit or credit card) and submit their frequent-flyer details.

All scenarios and related collection points are not included in the above case study, but the scenario does illustrate the point that, whilst not quite limitless, the opportunities for various organisations and companies to collect personal data, each and every time a passenger travels, are multifarious.

Treatment of the Data Collected by the Data Controller

Generally, the manner in which personal data is collected and treated by the collecting entity is driven by the intended purpose for which that data is collected.

Security and Crime Prevention

The first question that should be asked is whether the personal data collected was for the purposes of security and/or crime prevention, or rather in order to bolster the collecting entity's business intelligence and business requirements (for example, passenger habits, passenger dietary requirements and so on). By way of example, in 2019 South Wales Police were found to be justified in their use of automated facial recognition (AFR) in a commercial setting to search for individuals found on a watch list. Despite arguments that the data being collected was of a highly personal nature, the High Court found that the use of the technology was permissible because South Wales Police had complied with all the relevant equality legislation, were processing personal data in manner consistent with all other relevant legislation, and had implemented sufficient safeguards to prevent appropriate and non-arbitrary use of AFR.

In the case of the former, strict controls exist around exactly:

- what personal data may be harvested (usually the minimum which is necessary and which is usually specified);
- how long that personal data may be kept (this varies from jurisdiction to jurisdiction, but the usual rule of thumb is as long as may be required, unless otherwise legislatively specified). In the UK, the guidance issued by the Information Commissioner's Office (ICO) on the use of CCTV[3] stipulates that the personal data should be kept for the '*minimum amount of time necessary to fulfil its original purpose*';
- the original purpose for which that data was collected; and
- whether that personal data may be transferred out of the jurisdiction or to other crime prevention agencies (generally this will be acceptable if the purpose of the transfer is to prevent the occurrence of crimes).

Furthermore, in the case of personal data collected for security purposes, the issue of whether the data subjects concerned have consented to the collection of their personal data and its subsequent use does not usually arise, as this data may be collected without the consent of the data subject, provided it is required for the purposes of the prevention of crime and is collected and held in accordance with the relevant legislation.

In virtually every jurisdiction, personal data collected for the purposes of crime prevention may be collected without the consent of the data subject, provided that all relevant legislative controls in relation to the collection and use of that personal data are adhered to and that the personal data is only used for the express purposes for which it is collected. In the UK, for instance, these provisions may be located in Schedule 2 of the Data Protection Act 2018.

On 14 April 2016, the European Parliament approved the terms of the EU Passenger Name Record ("PNR") Directive, obliging airlines flying into the EU to hand the EU destination country their passengers' personal data in order to help the authorities fight terrorism and serious crime. Member States had until 25 May 2018 to implement the Directive into their national laws. The Directive requires Member States to set up "Passenger Information Units" ("PIUs") to manage the personal data collected by airlines. The information has to be retained for a period of five years, but after an initial six-month period, certain data is to be removed (such as the name, address and contact details of the passenger). While this Directive only applies to flights originating outside the EU, Member States may decide to extend this requirement to internal flights within the EU, as well as require tour operators and travel agencies to hand over the personal data they have collected to PIUs. In turn, the PIUs are ultimately responsible for transferring the personal data (if required) to the relevant national authorities as well as liaising with other PIUs to improve European co-operation in tackling terrorism and trafficking.[4]

Commercial Purposes

Contrast a security/crime prevention scenario with a situation in which the personal data of the passenger is collected for commercial reasons; for example, when the passenger purchases an item at a duty-free shop and swipes their debit or credit card or loyalty card, when they submit their information (perhaps by dropping their business card into a box) for the chance to win a prize, or when they check in for a flight. In the EU there is a general prohibition of data transfers to non-EU countries that are not officially recognised as having an adequate level of data protection (only a relatively small number of countries have been officially deemed as such by the EU; something which, by all accounts, is not a quick process).[5] The sharing of personal data within the EU is now also subject to stricter laws on data processing and sharing. The EU General Data Protection Regulation 2016/679 ("GDPR") was transposed into the national laws of Member States on 25 May 2018.

Despite speculation on whether the UK Government would introduce new national laws to mirror the GDPR, following the result of the referendum to leave the EU on 23 June 2016, Her Majesty's Government further enhanced the data protection regime in the UK with the enactment of the Data Protection Act 2018 ("DPA 2018"), which expressly incorporated the provisions of the GDPR into domestic UK legislation.

The GDPR strengthens the rights of the data subject in many different areas of data protection, including, but not limited to, the following:

- whenever a company is required to obtain the consent of the data subject, this consent will have to be given by means of an unambiguous and clear affirmative action (such as ticking a box on the company's website) in circumstances where that data subject acts freely and is fully informed as to the purposes for which their personal data will be processed;
- the data subject has, in certain circumstances, a right to object to the processing of their personal data under Article 21 of the GDPR, such as when the company collecting that personal data intends to use it for marketing purposes;

- the data subject also has a 'right to be forgotten' under Article 17 of the GDPR, where a request can be made to the company collecting that personal data to stop processing the data subject's personal data if it is unable to provide a legitimate reason for retaining that personal data; and
- when a data breach occurs (for example, personal data has been unlawfully accessed by a third party), the company collecting that personal data (which will usually be the data controller) is under a legal duty to inform the data subject 'without undue delay' and immediately notify the relevant data protection supervisory authority of that breach.[6]

The GDPR applies to any entity that controls or processes personal data of any individual in the EU (regardless of whether that processing takes place in or outside the EU or whether that individual is an EU resident or not). Taking the example scenario above, this would apply to a wide range of businesses, from loyalty card providers to airlines. The legislation does not, however, apply to authorities which process personal data for the purposes of public security, such as customs authorities (this type of processing is subject to other legislative requirements).[7]

The example of the prize draw is a more challenging one – section 352 of the Gambling Act 2005 (the "Gambling Act") (which is the main legal statute in the UK that governs prize draws) states that any disclosure of personal data must comply with the DPA 2018. Similarly, the GDPR applies equally to activities that fall under the Gambling Act. Currently a major challenge for those operating prize draws, raffles and the like is that, if a form is completed to enter into a prize draw, it may have terms and conditions regulating the collection of personal data but, in the author's view, if the form only refers to terms which cannot be read at the time of completion of the form, it may be difficult to enforce these terms against a consumer. Similarly, when a business card is dropped into a box for a prize draw, it is rare for terms and conditions describing the processing of the personal data collected to be shown, with the subsequent challenge for the data collector (usually the data controller, but in cases where the collector is only collecting the data on behalf of another and is not determining the use to which that personal data may be put, the collector may only be the data processor) of demonstrating that it has the requisite consents in place to use that data (for example, to contact the data subject regarding future promotions and so on).

It is, of course and at least in the EU, incumbent upon the data controller to establish, in the event of a challenge,[8] that the data controller has the required consents in place; even more so with the new data protection laws applicable under the GDPR. In particular, the new requirement under the GDPR for the data subject to give their consent by a clear affirmative action (the so-called "tick box" requirement) may require operators of prize draws to clearly display the terms and conditions, and obtain the data subject's express consent evidenced by a clear affirmative action, as a condition for the data subject to be eligible to participate in the prize draw.

In the case of passengers travelling by air from the EU to the USA, personal passenger data (ranging from the passenger's name through to their frequent-flyer information, billing information and all available contact information) may be transferred from the EU to the USA under the terms of a PNR agreement between the USA and the EU.[9] An attempt was made to put in place similar arrangements between the EU and Canada and between the EU and Australia; however, in July 2017, the Court of Justice of the European Union found that the PNR agreement between the EU and Canada could not be concluded in the form it was in at that time, because several of the provisions set out in the PNR agreement were incompatible with the fundamental rights recognised by the EU. Negotiations to broker a deal on a new PNR agreement were commenced between the EU and Canada in June 2018 and, at the time of writing, are ongoing.

With respect to business-to-business transfers, an agreement was reached in 2016 between the EU and USA which allows US companies to store, share and use the personal data of EU citizens, provided the company can meet a number of criteria. Referred to as the EU-US Privacy Shield, the aim of the legislation (which came into force on 1 August 2016) was to re-establish a transatlantic data framework after its predecessor (known as the "Safe Harbor" mechanism) was struck down by the European Court of Justice in 2015 for failing to adequately protect the personal data of EU data subjects. The EU-US Privacy Shield was reviewed and re-affirmed in October 2019, but struck down in 2020 by the Court of Justice in the Schrems II case (*Case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems*).

At the time of writing, no new framework arrangement had been agreed between the USA and the EU, and so the bases on which transfers of personal data from the EU to the USA can take place are somewhat more curtailed than they were at the start of 2020.

Personal data may also be transferred from the EU to outside of the European Economic Area where the parties, between which the personal data is being transferred, have entered into an agreement incorporating the Standard Contractual Clauses ("SCCs") adopted by the European Commission.[10] Personal data may also be transferred between companies operating within the same corporate group structure, through approved Binding Corporate Rules ("BCRs") applied across the relevant corporate group. Whilst the Court of Justice in Schrems II stated that the SCCs were a valid means of transferring personal data from the EU to a country which did not have a finding of adequacy, it did blast out a rather large note of caution by stating that they would not be an effective means of transferring personal data if there were not effective mechanisms in that non-EU country that made it possible, in practice, to ensure compliance with the level of protection required by EU law and if it were impossible to adhere to the SCCs. In the case of the USA, the CJEU was of the view that the federal security agencies and the "*requirements of US national security, public interest and law enforcement have primacy, thus condoning interference with the fundamental rights of persons whose data are transferred…The limitations on the protection of personal data arising from the domestic law of the United States... are not circumscribed in a way that satisfies requirements.*" Contractual terms agreed between the parties cannot circumscribe the powers of the US authorities which led to the invalidation of the Privacy Shield.

It is worth noting that the Court also determined that supervisory authorities are required to suspend or prohibit transfers to a third country in reliance on the SCCs where the clauses cannot be complied with and the appropriate level of protection cannot be assured by other means.[11]

The SCCs are currently under revision, and new SCCs are expected to be released during 2021.[12]

It is presently unclear what mechanism should be used in the event of onward transfers of data once that data has been transferred outside of the EEA for parties not bound by BCRs in the same corporate group or not otherwise bound by contractual obligations that incorporate the SCCs. At best, there is a lack of uncertainty and uniformity in the way this question is being addressed by travel agents and airlines.

Breaches

Breaches of the relevant legislation invariably lead to administrative fines and penalties in the jurisdiction concerned. This

is especially the case under the GDPR, where a penalty for non-compliance can see a company being fined up to €20m, or 4% of annual global turnover – whichever is higher.[13] The severity of getting it wrong in respect of personal data was made unequivocally clear in July 2019, when the ICO announced a record fine of £183m (subsequently reduced to £20m) in respect of British Airways, following an unprecedented passenger data breach in which the personal data of around half a million customers was stolen.[14]

In addition, pursuant to the GDPR, 'appropriate measures' may be taken by the supervisory authority to deal with data breaches: for minor infringements (dependent on the nature, gravity and duration of the incident), this may be in the form of a reprimand; while more serious infringements could carry criminal penalties under the laws of each Member State.[15] In non-EU jurisdictions where data protection legislation is still relatively new,[16] it is often a challenge to know what approach the relevant regulator will take to breaches, and what types of fine they are prepared to mete out.

Other Concerns

Other concerns arise in relation to the: (i) collection; (ii) retention; (iii) use; and (iv) storage of personal data, especially around the location of that storage. Further concerns arise out of the transfer of personal data; in particular, to whom that personal data may be transferred (whether as a result of the sale of a marketing list, an intra-group data-sharing arrangement or otherwise). The ability of a company to store and transfer a data subject's personal information has been further limited by provisions in the GDPR, most notably through the requirement for the company not to store personal data for a period which is longer than required for the purpose for which that personal data was originally collected.[17] In addition, the data controller must establish, pursuant to Article 25 of the GDPR, appropriate internal technical and organisational measures which are designed to implement the data protection principles and protect the rights of the data subjects.

Unfortunately, length constraints do not permit this chapter to look into these issues in any depth; however, it is worth noting that data controllers need to be constantly mindful of the consents which they have obtained from their data subjects, as well as what the data controllers are permitted to do in the absence of those consents.[18]

Conclusion

The next challenge, from a privacy perspective, for the aviation industry will be the implementation of the draft EU ePrivacy Regulation ("ePrivacy Regulation") which was published in January 2017 by the European Commission.[19] Although it is still uncertain when this legislation will be agreed, yet alone enacted in the Member States, it is intended that it will replace the current Directive 2002/58/EC on Privacy and Electronic Communications.

The scope of the ePrivacy Regulation is that it will supplement the GDPR in addressing, in detail, electronic communications and the tracking of internet users more broadly. The aim is to enhance the security and confidentiality of all electronic communications and technologies that process personal and non-personal data. Like the GDPR, the ePrivacy Regulation will not just affect airlines physically in the EU, but also any airline that deals with data originating in the EU.

As the aviation industry typically carries out large amounts of online marketing and digital services, the effects of the ePrivacy Regulation are likely to be felt throughout the industry.

From the data protection laws that have been implemented at EU level, it seems that data protection is moving in many different directions. Firstly, the introduction of the PNR Directive shows that counter-terrorism and serious crime prevention are at the top of EU and national governments' priorities, to such an extent that the protection of personal data is willing to be sacrificed in the interests of national and global security.

In any event, it is fair to say that operators in the aviation sector have their work cut out for the future as they continue the process of implementing the new regulatory changes into the industry. Whilst the benefits of collecting and retaining personal data will continue to grow, the regime in which operators work is becoming stricter and is requiring more attention, not only to the manner in which personal data is collected and the consents which are required to be obtained, but also to the way in which that personal data is stored, processed, managed and safeguarded.

Endnotes

1. A list of what constitute special categories of personal data in the European Union, and specifically the United Kingdom, and the requirements around the processing of that data, can be found in Article 9 of the GDPR and sections 10 and 11 of the UK Data Protection Act 2018.
2. This is a concern which many privacy advocates argue is disproportionate to any gains in security which body scanners may offer.
3. https://ico.org.uk/your-data-matters/cctv/ (as at the time of writing, the guidance had not been updated to take account of the GDPR or the UK DPA 2018).
4. The Passenger Name Record Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016.
5. The jurisdictions which, at the time of writing, have been deemed adequate by the European Commission are Andorra, Argentina, Canada (only commercial organisations), the Faroe Islands, Guernsey, the Isle of Man, Israel, Japan, Jersey, New Zealand, Switzerland, Uruguay and the United States of America (if the recipient belongs to the Privacy Shield framework). Adequacy talks are ongoing with South Korea.
6. The General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.
7. Such as the PNR Directive (Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016).
8. Whether by a data subject challenging the legitimacy of the data controller's right to contact them, or the relevant data protection supervisory authority (usually investigating complaints from data subjects, around those data subjects being contacted by the data controller without their consent).
9. Agreement between the USA and the EU on the use and transfer of Passenger Name Records to the United States Department of Homeland Security (Interinstitutional File 2011/0382 (NLE)).
10. The validity of SCCs is currently being considered by the CJEU in C-311/18 concerning the dispute between Facebook and Max Schrems.
11. It is also worth noting the guidance issued by the European Data Protection Board during November 2020 (and available at: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf and https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf).

12. The draft SCCs are available for download at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries.
13. See Article 83 GDPR.
14. ICO: 'Intention to fine British Airways £183.39m under GDPR for data breach', dated 8 July 2019; https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/.
15. See Article 83 GDPR.
16. For example, South Africa obtained its first data protection-specific legislation, the Protection of Personal Information Act, in 2013 (the Act was passed into law on 26 November 2013), and came into force on 1 July 2020. Responsible parties (that is, data controllers) have one year from this date to ensure that all their processing confirms to POPIA.
17. See Article 5 GDPR and, in particular, Article 5(1)(e).
18. For example, without the consent of the data subject, data may be transferred out of the EU to organisations in countries which have been endorsed by the EU as offering 'an adequate level of protection'.
19. https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX%3A52017PC0010.

Alan D. Meneghetti is a partner in the Corporate department at RadcliffesLeBrasseur. He undertakes a full range of privacy, commercial and regulatory work in the general commercial, aviation and manufacturing sectors. His practice ranges from handling regulatory issues to the procurement of suppliers and responses to tenders, to data protection and privacy, information technology, intellectual property, and the drafting and negotiating of various commercial agreements, such as outsourcing, supply, service, and research and development. He has worked extensively on matters in Africa, the Americas, Europe and the United Kingdom.
Alan is a regular contributor to publications and speaker at conferences in these sectors, and his articles and book reviews have been widely published.

RadcliffesLeBrasseur UK LLP
85 Fleet Street
London EC4Y 1AE
United Kingdom

Tel: +44 20 7227 6704
Email: alan.meneghetti@rlb-law.com
URL: www.rlb-law.com

RadcliffesLeBrasseur is a leading UK-based law firm providing business, regulatory, not-for-profit and private legal advice.
RadcliffesLeBrasseur is listed as a leading firm in the *Legal 500* and *Chambers and Partners* directories, and named in *The Times Best Law Firms 2020*. The firm provides legal services nationally from offices in London, Leeds and Cardiff.
The services offered by the firm in the aviation sector include:

- Financing of new and used aircraft, engines and equipment.
- Aviation business structuring.
- Acting before the Federal Aviation Administration and the Department of Transportation.
- Commercial litigation and international disputes.
- Environmental regulatory and legislative matters.
- An interdisciplinary approach, including commercial, corporate, employment, immigration, property, dispute resolution and regulatory advice.

RadcliffesLeBrasseur's clients in the aviation industry include lessors, manufacturers, financial institutions, repair facilities, parts distributors and insurers.

www.rlb-law.com

RadcliffesLeBrasseur LLP