AIRLINE COMMERCIAL USE OF EU PERSONAL DATA IN THE CONTEXT OF THE GDPR, *BRITISH AIRWAYS* AND *SCHREMS II*

W. GREGORY VOSS*

In July 2019, shortly after the end of the first year of application of the EU General Data Protection Regulation (GDPR), the UK's data protection regulator announced its intention to fine British Airways £183 million under the GDPR in connection with a data breach. That proposed penalty, which would have been the highest administrative fine to-date under the GDPR if finally issued in the amount announced, highlighted the relevance of the GDPR to airlines. As a result of the territorial scope of the GDPR, the regulation interests European and non-European airlines alike. This study, which focuses on requirements for the commercial use of EU personal data by U.S. airlines (but which should interest non-U.S. airlines, as well), uses actual cases to help analyze the application of the GDPR to the airline industry, including the British Airways GDPR penalty case. It is one of the first studies to do so, and as such contributes to the literature.

When the GDPR applies to them, airlines should become fully aware of its key relevant provisions, starting with those related to the GDPR's scope and its underlying data protection principles, discussed in this study. In addition, airlines must have a legal basis to process EU personal data under the GDPR and, as this study shows, must have adequately prepared for data subject requests to exercise rights and for potential data breaches. Several examples of the first GDPR sanctions in the airline industry are detailed, and lessons drawn from them. In this context, this study determines that data security is a key element. Finally, the 2020 Schrems II decision invalidating the EU-U.S. Privacy Shield is examined, and its potential impact on the transfer of EU personal data from the European Union to the United States by airlines is studied,

* Associate Professor of Business Law, TBS Business School, Toulouse, France. The author would like to thank the editors of the Colorado Technology Law Journal for their editing work and helpful comments. The author may be reached at g.voss@tbs-education.fr.

following an analysis of U.S. airline privacy policies available on the Internet in the European Union. In this context, the use of standard contractual clauses (SCCs) in order to allow for data export from the European Union is considered.

INTRODUCTION

One thing that is certain: airlines are collecting large amounts of customer personal data, notably for use in customer service, customer insight and big data purposes,[1] as well as for marketing and advertising.[2] That data must be protected. This study focuses on data protection rules for the commercial use of EU personal data under the European Union's General Data Protection Regulation[3] (GDPR) as they impact airlines—specifically U.S. airlines—and lessons from the GDPR's enforcement in the sector. However, the analysis contained herein will prove helpful for other airlines (including other non-EU ones) and businesses from other sectors making use of EU personal data, as well.

Shortly following the end of the GDPR's first year of application, in July 2019, the United Kingdom's supervisory authority—the Information Commissioner's Office (ICO)—acknowledged its intention to fine British Airways £183 million (roughly $230 million using historical exchange rates[4]) under the

1. Justin Bachman, *Airlines Have Your Personal Data, And They're Using It*, BLOOMBERG (Nov. 16, 2017 1:00 AM), https://www.bloomberg.com/news/articles/2017-11-16/airlines-have-your-personal-data-and-they-re-using-it [https://perma.cc/P2RS-DZL9].

2. For example, Delta uses "Information related to a flight booking or purchase of our products or services," "Information related to your membership in our Delta Sky Club, the SkyMiles Program or other account, or activities within our SkyMiles Partners and Promotional Partners," and "Information related to your preferences and personal and professional interests, and your opinions of our services" to "send you marketing communications, offers, and invitations to events," which may be based on "segmentation and modelling of your personal information." *Privacy Policy*, DELTA AIR LINES, INC., https://www.delta.com/fr/en/legal/privacy-and-security [https://perma.cc/HBX4-96V5] [hereinafter Delta Privacy Policy].

3. *See generally* Regulation (EU) 2016/679, of the European Parliament and the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter GDPR]. As used in this study, the term "EU personal data" refers to the personal data of individuals (data subjects) who are in the European Union.

4. Actually, $229.61 million, converted at the £ (GBP)/ $ (USD) exchange rate for July 8, 2019. *See Currency Converter*, OANDA, https://www1.oanda.com/currency/converter/ [https://perma.cc/2BXQ-2TMS].

GDPR for a data breach.[5] Pursuant to the UK Data Protection Act 2018,[6] which implements the GDPR in the United Kingdom,[7] the ICO must give such a notice prior to issuing a penalty notice. When the intention to fine was announced, it involved an amount that would have made it the largest GDPR fine to date, if the amount had been confirmed.[8] At the same time, cybersecurity has become a hot topic, with other personal data breaches announced.[9] Recognizing the importance of cybersecurity to the aviation sector, in 2018 the European Network and Information Security Agency (ENISA)—now either known by its acronym or by its role as the European Union Agency for Cybersecurity—held an EU civil

5. *See Intention to fine British Airways £183.39m under GDPR for data breach*, INFO. COMMISSIONER'S OFF. (July 8, 2019), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/ [https://perma.cc/3NY9-F898].

6. *See generally* Data Protection Act 2018, c. 12, §155, sch. 16, para. 2(1) (UK), https://www.legislation.gov.uk/ukpga/2018/12/schedule/16/enacted [https://perma.cc/7SCF-VQ2D] ("Before giving a person a penalty notice, the Commissioner must, by written notice (a 'notice of intent') inform the person that the Commissioner intends to give a penalty notice.").

7. *See National Laws: Current and Historic: United Kingdom: Third Generation Legislation*, U. OF CAMBRIDGE ("third generation period under the General Data Protection Regulation (2016–present)"), https://www.cipil.law.cam.ac.uk/resources/european-data-protection-national-laws-current-and-historic [https://perma.cc/54JF-4HG8].

8. The procedure in the UK is that, once the ICO issues notice of intention to fine, the company subject to the notice may make representations to try to reduce the fine, prior to the ICO issuing a penalty notice, which may still be appealed. *See* Kelly McMullon, *ICO Issues First Intentions to Fine Under the GDPR*, PROSKAUER: PRIVACY L. BLOG (July 25, 2019), https://privacylaw.proskauer.com/2019/07/articles/data-privacy-laws/ico-issues-first-intentions-to-fine-under-the-gdpr/ [https://perma.cc/GWC3-D5JX]. The penalty notice must be issued within six months of the notice of intent, but through an agreement between the ICO and the person subject to the notice of intent, this period may be extended. *See* Data Protection Act 2018, c. 12, §155, sch. 16 paras. 2(2)–(3) (UK).

9. Two examples are Marriott International, Inc.'s Starwood guest reservation database breach, disclosed in 2018, and the Yahoo! Inc. breach in 2013 and 2014. *See, e.g.*, Rebecca Rabinowitz, *From Securities to Cybersecurity: The SEC Zeroes in on Cybersecurity*, 61 B.C. L. REV. 1535, 1535–37 (2020); *see also* Lawrence J. Trautman & Peter C. Ormerod, *Corporate Directors' and Officers' Cybersecurity Standard of Care: The Yahoo Data Breach*, 66 AM. UNIV. L. REV. 1231 (2017). The Marriott breach also resulted in an ICO fine. *See ICO fines Marriott International Inc £18.4million for failing to keep customers' personal data secure*, INFO. COMMISSIONER'S OFF. (Oct. 30, 2020), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-marriott-international-inc-184million-for-failing-to-keep-customers-personal-data-secure/ [https://perma.cc/CX9Q-4LDG]; *see also* Joanna Partridge, *Marriott International faces class action suit over mass data breach*, THE GUARDIAN (Aug. 19, 2020 1:21 PM), https://www.theguardian.com/business/2020/aug/19/marriott-international-faces-class-action-suit-over-mass-data-breach [https://perma.cc/T36D-C649] (also referring to a 2016 ICO fine on TalkTalk for "security failings which led to a cyber attack" prior to application of the GDPR).

cybersecurity exercise depicting cyberattacks at EU airports.[10] These issues and others provide challenges for compliance in the aviation industry concerning personal data protection, which in the European Union includes requirements for providing security for the data[11] and notification for certain data breaches.[12]

In May 2018, the GDPR came into force.[13] The GDPR covers the collection and processing of personal data,[14] both by entities established within the European Union and, in certain circumstances, by entities not having an EU establishment.[15] The entity that "determines the purposes and the means of processing" is referred to as the "controller,"[16] and there may be one or more processors[17] that process the personal data on the controller's behalf, as well.[18] A contract must be established between the

10. *See Cyber Europe 2018 – Get prepared for the next cyber crisis*, EUR. UNION AGENCY FOR CYBERSECURITY (June 7, 2018), https://www.enisa.europa.eu/news/enisa-news/cyber-europe-2018-get-prepared-for-the-next-cyber-crisis [https://perma.cc/S2JC-F9K6]. For more background on ENISA, *see* W. Gregory Voss, *The Concept of Accountability in the Context of the Evolving Role of ENISA in Data Protection, ePrivacy, and Cybersecurity* (Ch. 11), *in* TECHNOCRACY AND THE LAW: ACCOUNTABILITY, GOVERNANCE AND EXPERTISE 247 (Alessandra Arcuri & Florin Coman-Kund, eds., 2021).

11. GDPR, *supra* note 3, art. 32.

12. *Id.* art. 33 (setting out requirements of notification of certain personal data breaches to the competent supervisory authority). In addition, certain breaches must be communicated to the relevant data subjects. *Id*. art. 34.

13. *Id.* art. 99(2).

14. "Personal data," are defined as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." *Id.* art. 4(1). For a discussion of the broad extent of coverage of this term, *see generally* W. Gregory Voss & Kimberly A. Houser, *Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies*, 56 AM. BUS. L.J. 287, 313–24 (2019). For an earlier comparison of this term with the U.S. term "personally identifiable information" or "PII," prior to the finalization of the GDPR, *see generally* Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 CALIF. L. REV. 877 (2014).

15. GDPR, *supra* note 3, art. 3.

16. *Id.* art. 4(7) ("'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.").

17. A processor is defined as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller." *Id.* art. 4(8).

18. Determining whether an entity is a controller or a processor in complicated processing operations may be difficult. The EDPB has issued guidance, which may be a good place to start for those who seek to make such a determination. *See* EUROPEAN DATA PROTECTION BOARD, GUIDELINES 07/2020 ON THE CONCEPTS OF CONTROLLER AND PROCESSOR IN THE GDPR, Version 1.0 (Nov. 12, 2019), https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf [https://perma.cc/5533-ADC6]. Note that these Guidelines may be

controller and a processor setting out "the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller,"[19] if a processor is used.

The GDPR is a complex instrument: it contains one-hundred seventy-three recitals[20] in the introductory part of the text and ninety-nine articles[21] in the body of the regulation.[22] Under EU procedure, recitals set out in a concise manner "the reasons for the main provisions of the enacting terms of the act."[23] The ECJ frequently looks to the recitals of a legal act to determine the purposes of its provisions.[24] The GDPR takes the form of a regulation, which is "binding in its entirety and directly applicable in all Member States."[25] In this way it differs from a directive, which is "binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods."[26] Thus, a directive—

subject to modification following a public consultation. *See* EUROPEAN DATA PROTECTION BOARD, GUIDELINES 7/2020 ON THE CONCEPTS OF CONTROLLER AND PROCESSOR IN THE GDPR, https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en [https://perma.cc/UG4P-9WDA]. *See also* W. GREGORY VOSS & KATHERINE WOODCOCK, NAVIGATING EU PRIVACY AND DATA PROTECTION LAWS 36–39 (2015) (providing practical tips to help decide whether an entity is a controller or a processor).

19. GDPR, *supra* note 3, art. 28(3) (paragraphs (a)–(h) of this section stipulate required provisions of such contract, insofar as the processor is concerned).

20. Recitals are included in the introductory part of EU legislation, referred to as the preamble. *See* EUR. UNION, JOINT PRACTICAL GUIDE OF THE EUROPEAN PARLIAMENT, THE COUNCIL AND THE COMMISSION, FOR PERSONS INVOLVED IN THE DRAFTING OF EUR. UNION LEGISLATION 24 (2015), https://eur-lex.europa.eu/content/techleg/KB0213228ENN.pdf [https://perma.cc/J65E-27BK] ("'Preamble' means everything between the title and the enacting terms of the act, namely the citations, the recitals and the solemn forms which precede and follow them."). They resemble whereas clauses. [hereinafter Joint Practical Guide].

21. The body of the legislative text is referred to as the "enacting terms," or "legislative part" of the legislative text, and it includes the articles. *Id.* ("The 'enacting terms' are the legislative part of the act. They are composed of articles, . . .").

22. *See generally* GDPR, *supra* note 3.

23. JOINT PRACTICAL GUIDE, *supra* note 20, at 32. For further discussion on the role of recitals, *see*, *e.g.*, Margot Kaminski, *The Right to Explanation, Explained*, 34 BERKELEY TECH. L.J. 189, 193–94 (2019) ("[T]hey are not binding law, but they are often cited as authoritative interpretations where the GDPR is vague.").

24. *See* MARIA MOUSMOUTI, DESIGNING EFFECTIVE LEGISLATION 27 (2019) (citations omitted).

25. Consolidated Version of the Treaty on the Functioning of the European Union art. 288, June 7, 2016, 2016 O.J. (C 202) 47, https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0006.01/DOC_3&format=PDF [https://perma.cc/2ECD-D52Z].

26. *Id.*

such as the 1995 EU Data Protection Directive (1995 Directive)[27] that the GDPR repealed and replaced[28]—may be implemented (or in EU legal language "transposed"[29]) differently in one Member State from the manner in another, often by adoption of a national act of a Member State parliament, while a regulation such as the GDPR constitutes uniform law with respect to its contents.

Failure to comply with the GDPR may potentially have significant consequences. EU Member State data protection regulators (such as the ICO[30]), known in the GDPR as "supervisory authorities," but referred to more colloquially as "data protection authorities" or "DPAs,"[31] have extensive powers such as the ability

27. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 [hereinafter 1995 Directive].

28. GDPR, *supra* note 3, art. 94.

29. In the sense of this study, transposition may be defined as incorporation of EU legal requirements contained in a directive into Member State national legislation. *See*, *e.g.*, Asya Zhelyazkova, *Complying with EU Directives' Requirements: The Link Between EU Decision-Making and the Correct Transposition of EU Provisions*, 20 J. EUR. PUB. POL'Y 702 (2013), https://www.researchgate.net/profile/Asya_Zhelyazkova/publication/263193802_Complying_with_EU_directives'_requirements_the_link_between_EU_decision-making_and_the_correct_transposition_of_EU_provisions/links/5bc846d792851cae21adb872/Complying-with-EU-directives-requirements-the-link-between-EU-decision-making-and-the-correct-transposition-of-EU-provisions.pdf [https://perma.cc/2FDG-NJ56].

30. After Brexit occurred on January 31, 2020, and until the end of a transition period at the end 2020, the GDPR continued to apply in the United Kingdom, for which the ICO is the supervisory authority, despite the United Kingdom no longer being an EU Member State. After that the GDPR will be kept in the United Kingdom's domestic law, although the United Kingdom "will have the independence to keep the framework under review." William RM Long & Francesca Blythe, *The Privacy, Data Protection and Cybersecurity Law Review: United Kingdom*, L. REVS. (Oct. 21, 2020), https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/united-kingdom [https://perma.cc/8W9C-HZSY]. The UK-EU Trade and Cooperation Agreement, concluded on December 24, 2020, which provisionally applied beginning on January 1, 2021, provided that the GDPR would apply for an additional period of up to six months following the end of the transition period. *See ICO statement in response to UK Government's announcement on the extended period for personal data flows, that will allow time to complete the adequacy process*, INFO. COMMISSIONER'S OFF. (Dec. 28, 2020), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/12/ico-statement-in-response-to-uk-governments-announcement-on-the-extended-period-for-personal-data-flows-that-will-allow-time-to-complete-the-adequacy-process/ [https://perma.cc/3H2D-M974].

31. The GDPR defines a "supervisory authority" as "an independent public authority which is established by a Member State pursuant to Article 51." GDPR, *supra* note 3, art. 4(21). In Article 51, the GDPR provides that "Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority')." Thus, a supervisory authority, which is also sometimes referred to as a data protection authority or agency (DPA), may

to order the cessation of processing[32] or to impose major administrative fines (in the case of a company this may go up to the greater of €20,000,000 or 4% of revenue in certain cases[33]), in the event of data protection violations. This gives companies such as airlines incentives for compliance,[34] as, for example, DPAs may lower the fines if a controller or a processor has implemented appropriate technical or organizational measures,[35] or taken other measures to ensure compliance.[36] Furthermore, the GDPR enforcement toolkit includes other potential actions, in addition to lodging a complaint with a supervisory authority:[37] actions against a supervisory authority,[38] actions by non-profit organizations mandated by individuals,[39] individual actions in the courts,[40] and Member States may provide for criminal penalties[41] as well.

The GDPR also established the European Data Protection Board (EDPB), which is referred to as "the Board," in the GDPR,[42] but "EDPB" in this study. The heads of EU Member State DPAs and the European Data Protection Supervisor (EDPS)[43] or their representatives constitute the membership of the EDPB.[44] The EDPB sees to the GDPR's consistent application and provides various guidelines, recommendations and good practices as part of

be thought of as the data protection regulator of one of the EU Member States. *Id*. art. 51.

32. GDPR, *supra* note 3, art. 58(2)(f).

33. *Id*. art. 83(5).

34. *See generally*, W. Gregory Voss, *Internal Compliance Mechanisms for Firms in the EU General Data Protection Regulation,* 50 REVUE JURIDIQUE THÉMIS 783, 817–818 (2018).

35. Roberto Cassar, *Distributed Ledger Technology in the Airline Industry: Potential Applications and Potential Implications*, 83 J. AIR L. & COM. 455, 469 (2018).

36. *See generally Internal Compliance Mechanisms for Firms, supra* note 34, at 818–819.

37. GDPR, *supra* note 3, art. 77. These and the other actions available under the GDPR are detailed in W. Gregory Voss & Hugues Bouthinon-Dumas, *EU General Data Protection Regulation Sanctions in Theory and in Practice*, 37 SANTA CLARA HIGH TECH. L.J. 1 (2021).

38. GDPR, *supra* note 3, art. 78.

39. *Id*. art. 80.

40. *Id*. art. 79.

41. *Id*. art. 84. *See also id.* recital (149).

42. *Id*. art. 68.

43. The European Data Protection Supervisor (EDPS) provides the secretariat of the EDPB. *See id*. art. 75(1). The EDPS is the European Union's independent data protection authority, in particular responsible for monitoring and ensuring data protection of personal data processed by EU institutions and bodies. *About*, EUR. DATA PROTECTION SUPERVISOR, https://edps.europa.eu/about-edps_en [https://perma.cc/4WR9-6M6K].

44. GDPR, *supra* note 3, art. 68(3).

this task.[45] As part of a consistency mechanism,[46] the EDPB may adopt opinions,[47] and binding decisions for dispute resolution in individual cases,[48] such as when there are "conflicting views on which of the supervisory authorities concerned is competent for the main establishment"[49] of a controller or a processor under the GDPR's one-stop-shop mechanism,[50] which allows the DPA of the main establishment to act as the lead supervisory authority for cross-border processing by such controller or processor.[51]

This study will specifically investigate data protection issues involved in the commercial use of EU personal data by airlines—what one commentator refers to as "*first order uses*" of passenger data[52]—following the application of the GDPR, and with the benefit of experience since such date. Thus, it specifically excludes from its scope transfers of Passenger Name Record (PNR) data for law enforcement purposes and for the fight against crime and terrorism,[53] which have been described as "*second order uses*."[54] In Part I, this study details important provisions of the GDPR, which will help the reader to understand GDPR sanctions and requirements in the airline sector, as well as transborder data flows, discussed in the following parts.

This study is structured as follows: after a presentation of some of the main provisions of the GDPR relevant to the aviation sector

45. *Id*. art. 70(1). On the role of guidelines of the EDPB (and of its predecessor under the 1995 Directive—the Article 29 Data Protection Working Party)—*see* Kaminski, *supra* note 23, at 194–95 ("Article 29 Working Party guidelines, again, do not have the direct force of law. They are, nonetheless, strongly indicative of how enforcers will interpret the law. Now that the GDPR is in effect, these guidelines have additional, though indirect, teeth," due to the relationship between the EDPB and national DPAs).

46. GDPR, *supra* note 3, art. 63.

47. *Id*. art. 64.

48. *Id*. art. 65.

49. *Id*. art. 65(1)(b). Taking the case of a "controller with establishments in more than one Member State," the "main establishment" is defined as "the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment." *Id*. art. 4(16).

50. *Id*. art. 56. *See id*. art. 60 (on cooperation between the supervisory authorities in connection with the one-stop-shop mechanism. *See also* Voss & Bouthinon-Dumas, *supra* note 37 (discussing the one-stop-shop mechanism).

51. GDPR, *supra* note 3, art. 56(1).

52. *See* Brendan Lord, *The Protection of Personal Data in International Civil Aviation: The Transatlantic Clash of Opinions*, 44 AIR & SPACE L. 261 (2019) (the author comments that "[t]hese operational, *first order uses* of passenger data serve a functional, commercial purpose for the air carriers and have been largely uncontroversial." (emphasis in original)(citations omitted)).

53. Migration and Home Affairs, *Passenger Name Record (PNR)*, EUR. COMMISSION, https://ec.europa.eu/home-affairs/what-we-do/policies/police-cooperation/information-exchange/pnr_en [https://perma.cc/SC9M-5L7A].

54. *See* Lord, *supra* note 52, at 262.

(Part I), this study will detail GDPR sanctions in the airline industry up to present, drawing lessons from these cases (Part II). Then, the issue of transborder data flows in the aviation sector will be detailed, focusing on the *Schrems II* decision[55] of the Court of Justice of the European Union (ECJ)—the European Union's highest court[56]—and its impact on the transborder transfer basis of U.S. airlines (Part III). Finally, concluding remarks will be made.

I. GDPR PROVISIONS

The GDPR is an omnibus data protection legislation—applicable regardless of the industry—unlike the U.S. sectoral privacy legislation.[57] It is an evolution of the 1995 Directive,[58] with which it shares this omnibus nature. This study sets out some essential elements of the GDPR relevant to the commercial use of personal data in the aviation sector: (A) when the GDPR applies, (B) its basic data protection principles, (C) the required legal basis for data processing, data subject rights, accountability, and (D) requirements for data transfers.

A. Application

Simply put, the GDPR applies when there is (1) processing of the personal data of individuals (or "natural persons") in the

55. Case C-211/18 Data Prot. Comm'r v. Facebook Ir. Ltd. & Maximilian Schrems (July 16, 2020), [hereinafter *Schrems II*].

56. *See* WILLIAM MCGEVERAN, PRIVACY AND DATA PROTECTION LAW 281–82 (2016) (describing the Court of Justice as the European Union's highest court, with its interpretations of EU law binding EU Member States).

57. *See* Emmanuel Pernot-Leplay, *EU Influence on Data Privacy Laws: Is the US Approach Converging with the EU Model?*, 18 COLO. TECH. L.J. 101 (2019); *see also* Tyler J. Smith, *Haystack in a Hurricane; Mandated Disclosure and the Sectoral Approach to the Right to Privacy,* YALE J. ON REG. BULL. (Feb. 12, 2020), https://www.yalejreg.com/bulletin/haystack-in-a-hurricane-mandated-disclosure-and-the-sectoral-approach-to-the-right-to-privacy/ [https://perma.cc/W4QW-V6H4].

58. *See*, *e.g.*, ORLA LYNSKEY, THE FOUNDATIONS OF EU DATA PROTECTION LAW 5 (2015) (describing the GDPR, as then proposed but not yet adopted, as being "predicated on a similar blueprint" to that of the 1995 Directive, and citing the former European Data Protection Supervisor regarding the continuity of the legislation, with similar basic concepts and principles underlying the two).

European Union,[59] referred to as "data subjects,"[60] and (2) the material and territorial scope requirements of the GDPR are met.

1. Processing of Personal Data

The concept of processing of personal data is a very broad one. The term is defined as:

> [A]ny operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.[61]

Almost anything done with personal data—from their original collection to their retrieval for eventual use following storage and organization—will be covered by this term.[62] This is also the case with airline use of personal data: for example, an airline may collect data about an individual's travel for a frequent flyer program or about an individual's favorite activities or hobbies, which will involve their collection and storage and probably their structuring, terms contained within the definition of "processing." This may be done in order to tailor travel offers to the individual, which could involve retrieval, consultation and use of the data, likewise falling within the ambit of processing. In addition, the airline could collect more basic personal data such as name, address, telephone number, and so on. To the extent an airline flies to the European Union, it will hold and process the personal data of EU individuals. This is

59. GDPR, *supra* note 3, recital 14 (explaining that the GDPR does not apply to the data of legal persons such as corporations in that "the protections…apply to natural persons."). The GDPR does not apply to the data of legal persons such as corporations. *Id.* ("The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data. This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person.").

60. *Id.* art. 4(1) (data subject is defined in relation to the relevant personal data: he or she is the "identified or identifiable natural person" to whom the information relates).

61. *Id.* art. 4(2). *See supra* text accompanying note 14 (providing a definition of "personal data").

62. EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, HANDBOOK ON EUROPEAN DATA PROTECTION LAW 97–98 (2018) (stating that data processing concerns any operations performed on personal data)**Error! Hyperlink reference not valid.**.

noted in one study related to a Middle Eastern airline.[63] Once it is determined that there is processing of personal data, a determination should be carried out of whether that processing fits within the scope of the GDPR.[64]

2. Material Scope

The GDPR applies with respect to the processing of personal data "wholly or partly by automated means and to the processing other than automated means of personal data which form part of a filing system or are intended to form part of a filing system."[65] A "filing system" is defined as "any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis."[66] Any commercial airline company will likely be storing customer personal data in a computer data base for automated processing, or externalizing them for processing by a processor.

There are, however, several exceptions to the GDPR's material scope. First, if the activity falls outside of European Union law, it is not within the GDPR's material scope.[67] This might be the case in the area of national security, which is the purview of EU Member State law.[68] Next, activities of EU Member States related to the common foreign and security policy fall out of the GDPR's scope.[69] Furthermore, activities of competent authorities in the areas of crime prevention, investigation, and prosecution also fall outside of the GDPR's scope.[70] None of these activities are covered by this study. Moreover, purely personal or household activities by a natural person are excluded.[71] As this study covers commercial activities by corporate entities (legal persons), such exclusion is not of a concern here. Distinct EU legislation applies to personal data

63. *See* Adib Charif, Ali Kassir & Ahmad Ashaal, *General Data Protection Regulation (GDPR) in the Airlines Industry: Privacy in the Eyes of the Lebanese Consumers*, 1 EUR. J. INTERDISC. RES. 60, 61 (Sept. 2020) ("Although Lebanon is not a European country, the Lebanese National Carrier, Middle East Airlines – Air Liban S.A.L., has a traffic right to different European destinations (such as London, France, Italy, etc.) and thus holds and process data about European customers.").

64. This analysis has been illustrated by a chart in Voss & Houser, *supra* note 14, 293, fig.1.

65. GDPR, *supra* note 3, art. 2(1).

66. *Id*. art. 4(6).

67. *Id*. art. 2(2)(a).

68. *See* Herke Kranenborg, *Article 2 Material Scope*, *in* THE EU GENERAL DATA PROTECTION REGULATION (GDPR): A COMMENTARY 60, 69 (Christopher Kuner, Lee A. Bygrave & Christopher Docksey, eds., 2020).

69. GDPR, *supra* note 3, art. 2(2)(b).

70. *Id*. art. 2(2)(d).

71. *Id*. art. 2(2)(c).

processing by EU institutions and bodies[72] and to intermediary service provider liability issues.[73]

In addition to a determination whether processing falls within the material scope of the GDPR, an analysis must be made of its territorial scope, the subject of this study's next section.

3. Territorial Scope

The GDPR applies to personal data processing "in connection with the activities of an establishment of a controller or processor in the [European] Union, regardless of whether the processing takes place in the [European] Union or not."[74] The concept of establishment refers to the exercise of activities through stable arrangements, such as a branch or a subsidiary.[75] In *Google Spain,* a case predating the GDPR and involving Google's Spanish subsidiary Google Spain SL (referred to in this excerpt as an establishment), and Google Inc., a company in California that operates a search engine, the ECJ found that:

> [I]t must be held that the processing of personal data for the purposes of the service of a search engine such as Google Search, which is operated by an undertaking that has its seat in a third State but has an establishment in a Member State, is carried out 'in the context of the activities' of that establishment if the latter is intended to promote and sell, in that Member State, advertising space offered by the search engine which serves to make the service offered by that engine profitable.[76]

This indicates the broad way in which the ECJ interprets whether or not processing is carried out in connection with an EU establishment's activities. This will be of interest to airlines and other commercial companies, which might have establishments in the European Union, which is likely the case for those airlines flying to Europe.

72. *Id*. art. 2(3).

73. *Id*. art. 2(4).

74. *Id*. art. 3(1).

75. *Id.* recital 22; VOSS & WOODCOCK, *supra* note 18, at 224 (defining an "establishment" as "a place where a controller conducts the "effective and real exercise of activities," where the controller has "human and technical resources necessary" in order to achieve certain services through "stable arrangements.""); *see also* W. Gregory Voss, *Cross-Border Data Flows, the GDPR, and Data Governance*, 29 WASH. INT'L L.J. 485, 495 (2020).

76. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, 2014 E.C.R., ¶ 55.

However, an airline need not have an establishment in the European Union in order for the GDPR to apply—merely offering goods or services to those in the European Union will suffice. Article 3(2) of the GDPR provides as follows:

> This Regulation applies to the processing of personal data of data subjects who are in the [European] Union by a controller or processor not established in the [European] Union, where the processing activities are related to:
> (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the [European] Union; or
> (b) the monitoring of their behaviour as far as their behaviour takes place within the [European] Union.[77]

In applying paragraph (a) of this provision of the GDPR, the EDPB adopts a "targeting criterion," whereby "the provision is aimed at activities that intentionally, rather than inadvertently or incidentally, target individuals in the EU."[78] Factors that might indicate that individuals in the EU are not targeted may include requiring a local non-EU telephone number, or requiring payment in a currency other than the Euro in order to obtain goods or services.[79] Another element of the application of the targeting criterion is assessing "whether the conduct on the part of the controller, which determines the means and purposes of processing, demonstrates its intention to offer goods or a services to a data subject located in the Union."[80]

Recital (23) of the GDPR provides further guidance, citing the following factors that indicate targeting: "the use of a language or a currency generally used in one or more [EU] Member States, with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the [European] Union."[81] Yet, it cautions that the mere accessibility of a website in the European Union alone is not enough to determine there is targeting.[82] The EDPB also offers additional factors which would indicate that individuals in the European Union are

77. GDPR, *supra* note 3, art. 3(2).

78. EUROPEAN DATA PROTECTION BOARD, GUIDELINES 3/2018 ON THE TERRITORIAL SCOPE OF THE GDPR, Version 2.1, 15 (Nov. 12, 2019), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf [https://perma.cc/UJY2-Y6XE] [hereinafter Guidelines 3/2018].

79. *Id.* at 15–16.

80. *Id.* at 17.

81. GDPR, *supra* note 3, recital 23.

82. *Id.*

targeted, such as marketing and advertising in the European Union, having an activity with an international nature, such as "certain tourist activities," use of EU domain names, and so on, although the factors may not be enough individually to indicate targeting and should be reviewed together.[83] When an airline does not have an EU establishment, an analysis of the airline's website accessibility from the European Union and documentation should be conducted to see if relevant factors indicating an offer of goods or services to individual data subjects in the European Union are present and sufficient to find that the GDPR applies. If the desire is not to target EU persons, then airlines should verify and then modify their websites and documentation, if necessary, in order to ensure that it is clear that EU persons are not targeted.

Article 3(2)(b) discusses the behavior monitoring of EU data subjects that might result in application of the GDPR, so long as the relevant behavior takes place in the European Union.[84] According to recital (24):

> [I]t should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning him or her or for analysing or predicting her or his personal preferences, behaviours and attitudes.[85]

The EDPB also considers that tracking through networks other than the internet or through other technologies such as wearable and smart devices may be behavioral monitoring.[86] Monitoring activities could include behavioral advertising, geo-localization for marketing, use of cookies or fingerprinting for tracking, monitoring health status, studies of behavior based on individual profiles, including for marketing, and so on.[87]

When the GDPR applies by virtue of the territorial scope provisions of Article 3(2), the relevant controller or processor not established in the European Union must designate in writing a representative in the European Union,[88] unless the processing concerned:

> [I]s occasional, does not include, on a large scale, processing of special categories of data … or processing of personal data

83. Guidelines 3/2018, *supra* note 78, at 17–18.
84. GDPR, *supra* note 3, art. 3(2)(b).
85. *Id*. recital 24.
86. Guidelines 3/2018, *supra* note 78, at 19.
87. *Id*. at 20.
88. GDPR, *supra* note 3, art. 27(1).

> relating to criminal convictions and offences …, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing.[89]

Finally, the territorial scope requirement of the GDPR will also be met where the controller is established "in a place where Member State law applies by virtue of public international law."[90] Now this study turns to requirements when the GDPR does apply, starting with data protection principles.

B. Data Protection Principles

The data protection principles of the GDPR have their roots in the U.S. fair information practice principles (FIPPs), early EU Member State data protection law, and the Organization for Economic Co-operation and Development (OECD) Guiding Principles.[91] Airlines, which utilize EU personal data for commercial uses should become familiar with these principles and incorporate them into their processes, procedures, and products and services. As embodied in the GDPR, these may be summarized as: data quality, purpose limitation, integrity and confidentiality, transparency, rights of the data subject, accountability, and lawfulness and fairness of processing.[92] This study handles each of these in order below.

1. Data Quality

The data quality principle includes accuracy, data minimization, and storage limitation. Accuracy refers to the requirement that personal data should be "accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified

89. *Id*. art. 27(2)(a). The requirement of a representative also does not apply to a public authority or body. *Id*. art. 27(2)(b).

90. *Id*. art. 3(3).

91. W. Gregory Voss, *Obstacles to Transatlantic Harmonization of Data Privacy Law in Context*, 2019 U. ILL. J.L. TECH. & POL'Y 405, 412 (2019).

92. *Id*. annex at 463 (Of these, the data quality principle is roughly equivalent to the data quality principle of the FIPPs; the purpose limitation principle is roughly similar to the purpose specification and use limitation FIPPs; the integrity and confidentiality principle is roughly similar to the security safeguards principle of the FIPPs; and the transparency and rights of the data subject principles are roughly equivalent to the FIPPs of the same name, although data subject rights are more developed under the GDPR (e.g., with the "right to be forgotten" and the right to data portability)).

without delay … ."[93] This is relatively straightforward and gives rise to a data subject right to erasure discussed in Section 5 below. Data minimization means that the personal data should be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed … ."[94] This part of the data quality principle makes sense, too: processing too much data leads to risk of infringing data subjects' right to personal data protection and also increases risks of harm in the event of a data breach. Storage limitation is a temporal counterpart to data minimization in a way. This part of the data quality principle provides that personal data shall be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed … ."[95]

2. Purpose Limitation

The purpose limitation data protection principle provides that personal data shall be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes … ."[96] In doing so, this principle subsumes two sub-principles: purpose specification and use limitation.[97] In the notification provisions of the GDPR, the controller is required to inform the data subject of "the purposes of the processing for which the personal data are intended," in both the case where the data are collected directly from him or her,[98] or when collected indirectly.[99] This may be considered purpose specification.

Where processing is anticipated for a purpose which is not the same as that for which the data have been collected, where the data processing is not based on consent or on a Union or Member State law constituting certain measures relating to national security, defense, public security, or law enforcement listed in GDPR Article 23, the controller must take into account several factors in order to determine whether that purpose is compatible with the original purpose:

93. GDPR, *supra* note 3, art. 5(1)(d).

94. *Id*. art. 5(1)(c).

95. *Id*. art. 5(1)(e).

96. *Id*. art. 5(1)(b).

97. *Obstacles to Transatlantic Harmonization of Data Privacy Law in Context*, *supra* note 91, at 463.

98. GDPR, *supra* note 3, art. 13(1)(c).

99. *Id*. art. 14(1)(c).

> (a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
> (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
> (c) the nature of the personal data, in particular whether special categories of personal data are processed, … or whether personal data related to criminal convictions and offences are process, …;
> (d) the possible consequences of the intended further processing for data subjects;
> (e) the existence of appropriate safeguards, which may include encryption or pseudonymization.[100]

This is related to use limitation, which in the GDPR is subsumed into the data protection principle of purpose limitation and provides that personal data should not be further processed for purpose which is "incompatible" with the purpose for their processing that was originally specified.[101]

3. Integrity and Confidentiality

The integrity and confidentiality data protection principle, which refers to security, provides that personal data shall be "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."[102] Article 32 of the GDPR requires that data controllers and processors "implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk," with respect to personal data and their processing, taking into consideration the state of the art, costs of implementation, and risks to data subjects.[103]

This principle is fleshed out more in GDPR Article 32. That article provides in part that, "[t]aking into account the state of the art, the costs of implementation and the nature, scope, context and

100. *Id*. art. 6(4).

101. *Id*. art. 5(1)(b) (requiring personal data to be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes," and providing an exception for further processing "for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.").

102. *Id*. art. 5(1)(f).

103. *Id*. art. 32(1).

purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk …"[104] The provision then continues to cite potential examples of such measures, such as pseudonymization and encryption,[105] resiliency,[106] and so on. The term that it uses, appropriate technical and organizational measures, is not defined in the GDPR, however this may add flexibility to allow requirements to evolve with technical developments and risks over time. While the GDPR does not prescribe any particular security standard or technology,[107] EU Member State law might do so,[108] and referring to data security recommendations, such as those of ENISA on pseudonymization,[109] might be helpful for airlines here. Indeed, in order to establish that British Airways failed to implement appropriate technical and organizational measures to ensure adequate security under the GDPR, the ICO in its Penalty Notice referred to guidelines or recommendations available publicly: good practices from the UK government's Centre for the Protection of National Infrastructure; guidance from the UK government's National Cyber Security Centre; and guidance from the U.S. Department of Commerce's National Institute for Standards and Technology (NIST); in addition to security guidance from the DPA, itself.[110] Furthermore, the EU Network and Information Security (NIS) Directive establishes minimum information security requirements for operators of essential services, such as air carriers,[111] although these are not, strictly speaking, related to personal data protection.

New requirements for data breach notifications complement the integrity and confidentiality principle. GDPR Article 33 requires that "[i]n the case of a personal data breach, the controller

104. *Id*.

105. *Id*. art. 32(1)(a).

106. *Id*. art. 32(1)(b).

107. Cédric Burton, *Article 32. Security of Processing*, *in* THE EU GENERAL DATA PROTECTION REGULATION (GDPR): A COMMENTARY, *supra* note 68, at 630, 636 .

108. *E.g.*, *id*. at 633, (explaining that German law "contains a detailed list of requirements to ensure the security of data processing.") (citation omitted).

109. *See generally* EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA), PSEUDONYMISATION TECHS. AND BEST PRACTICES (2019), https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices [https://perma.cc/YNL8-QBMW].

110. INFO. COMM'R'S OFFICE, *Penalty Notice, Case ref. COM0783542, British Airways plc*, 30–32 (Oct. 16, 2020), https://ico.org.uk/media/action-weve-taken/mpns/2618421/ba-penalty-20201016.pdf [https://perma.cc/5NQV-YW9V].

111. *The European Union Cybersecurity agency, ENISA, in Interview*, EASA (Dec. 18, 2017), https://www.easa.europa.eu/newsroom-and-events/news/european-union-cybersecurity-agency-enisa-interview [https://perma.cc/5XXR-8AZ3].

shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach" to the competent DPA.[112] This obligation shall not apply if the breach is "unlikely to result in a risk to the rights and freedoms of natural persons."[113] Furthermore, if the notification is made more than 72 hours after becoming aware of the breach, reasons for the delay must be provided, as well.[114] An additional provision requires that, "[w]hen the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay."[115] The case of Air Europa, in Part II.E., provides one example of the failure to notify a data breach to the competent DPA in a timely manner.

Finally, it should be noted that the integrity and confidentiality principle has proven to be important in the GDPR sanction cases to-date in the aviation sector, as this study concludes in Part II.G. This is all the more reason for airlines to focus on data security, adopt appropriate technical measures such as encryption, anonymization and pseudonymization,[116] and establish internal procedures allowing them to comply with breach notification requirements, if a breach occurs.

4. Transparency

Transparency refers to the requirement that personal data should be processed "in a transparent manner in relation to the data subject."[117] This provision should be read together with the various notification requirements of the GDPR. For example, Article 12 requires that the controller shall provide certain information to data subjects "in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child."[118] Furthermore, the "information shall be provided in writing, or by other means, including, where appropriate, by electronic means."[119] The GDPR provides for specific types of information to be provided to the data subject, where personal data are collected

112. GDPR, *supra* note 3 art. 33(1).
113. *Id*.
114. *Id*.
115. *Id*. art. 34(1).
116. *See* Joshua Meltzer, *Why Schrems II Requires US-EU Agreement on Surveillance and Privacy*, BROOKINGS INST. (Dec. 8, 2020), https://www.brookings.edu/techstream/why-schrems-ii-requires-us-eu-agreement-on-surveillance-and-privacy/ [https://perma.cc/LTL3-UPMQ].
117. GDPR, *supra* note 3, art. 5(1)(a).
118. *Id*. art. 12(1).
119. *Id*.

directly from the data subject,[120] or where the personal data have been obtained indirectly, and not obtained from the data subject.[121] However, three sets of conditions are set out and when one set is met, such communication need not be made to the data subject:

(a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption;
(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialize;
(c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure, whereby the data subjects are informed in an equally effective manner.[122]

As part of an airline's accountability efforts, each of these elements should be documented.

5. Rights of the Data Subject

The GDPR accords data subjects certain rights, with which airlines subject to the GDPR should become familiar. In accordance with the transparency principle, airlines will have to inform customers whose personal data they hold of these rights.[123] Furthermore, the use of metadata, or "data that provides information about other data,"[124] and their use in querying data, may be helpful in complying with data subject requests under data subject rights, by allowing controllers and processors to find the data they hold on the data subject making the request to exercise their rights.[125] Those rights are: a right of access, a right to rectification, a right to erasure ("right to be forgotten"), a right to restriction of processing, a right to data portability, a right to object, and a right not to be subject to a decision based solely on automated

120. *Id*. art. 13.
121. *Id*. art. 14.
122. *Id*. art. 34(3).
123. *See*, *e.g.*, *id*. art. 13(2)(b) (setting out the requirement for the controller to provide the following information to the data subject when the personal data are obtained: information on "the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing, as well as the right to data portability.").
124. *Metadata*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/metadata [https://perma.cc/858B-8S28].
125. Voss, *supra* note 75, at 523.

processing including profiling, where such decision has legal effects on him or her. This study will take each of those rights in order below.

a. Right of Access

The GDPR provides that the data subject "shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and where that is the case, access to the personal data" and certain additional information.[126] This right has led to "subject access requests" or "SARs." One example of a failure to comply with such a request is included in the discussion on Iberia in Part II.D. In many ways, this right allows data subjects to be able to exercise the other rights, specifically the right to erasure and the right to rectification.

b. Right to Rectification

This provides the data subject the right "to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplemental statement."[127]

c. Right to Erasure ("Right to Be Forgotten")

Far from being an all-extensive right, this right actually applies to limited circumstances, and is similar to the corresponding right in the 1995 Directive.[128] The GDPR provides that "[t]he data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay" where one of the specified grounds applies.[129]

These grounds include: where the data are "no longer necessary in relation to the purposes for which they were collected or otherwise processed,"[130] where consent to processing is

126. GDPR, *supra* note 3, art. 15(1).

127. *Id*. art. 16.

128. W. Gregory Voss & Céline Castets-Renard, *Proposal for an International Taxonomy on the Various Forms of the "Right to Be Forgotten": A Study on the Convergence of Norms*, 14 COLO. TECH. L.J. 281, 306 (2016). On this right under the 1995 Directive, *see also* Herke Kranenborg, *Article 17. Right to Erasure ('Right to be Forgotten')*, *in* THE EU GENERAL DATA PROTECTION REGULATION (GDPR): A COMMENTARY, *supra* note 68, at 475, 477.

129. GDPR, *supra* note 3, art. 17(1).

130. *Id*. art. 17(1)(a).

withdrawn, and that is the legal basis for the processing,[131] where the data subject objects to the processing, absent "overriding legitimate grounds for the processing," or where he or she objects and the processing is for "direct marketing purposes,"[132] where the data have been unlawfully processed,[133] where the data need to be erased to comply with a legal obligation imposed on the controller,[134] or where "the personal data have been collected in relation to the offer of information society services referred to in Article 8(1)."[135] There are limitations to this right, where processing is necessary for freedom of expression or information,[136] for a legal obligation or a task carried out in the public interest or in the exercise of official authority,[137] for public health,[138] for archiving in the public interest or for certain research,[139] and for the establishment, exercise, or defense of legal claims.[140] One new provision warrants reproduction in full:

> Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those data.[141]

This latter obligation was weakened from the original right to be forgotten proposed by the Commission.[142]

One failure to comply with a request to exercise this right to erasure is referred to in the discussion on Iberia, in Part II.D.

d. Right to Restriction of Processing

If one of the listed cases applies, "The data subject shall have the right to obtain from the controller restriction of processing."[143] These cases include restriction while the controller checks the

131. *Id*. art. 17(1)(b).
132. *Id*. arts. 17(1)(c); 21(1), (2).
133. *Id*. art. 17(1)(d).
134. *Id*. art. 17(1)(e).
135. *Id*. art. 17(1)(f).
136. *Id*. art. 17(3)(a).
137. *Id*. art. 17(3)(b).
138. *Id*. art. 17(3)(c).
139. *Id*. art. 17(3)(d).
140. *Id*. art. 17(3)(e).
141. *Id*. art. 17(2).
142. *See* Kranenborg, *supra* note 128, at 483.
143. GDPR, *supra* note 3, art. 18(1).

accuracy of personal data challenged by the data subject,[144] where "the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead,"[145] where data are no longer needed by the controller for the processing but the data subject needs them for legal claims,[146] or where the data subject objects to processing exercising its right to object, during verification "whether the legitimate grounds of the controller override those of the data subject."[147]

e. Right to Data Portability

The right to data portability is a new right under the GDPR; it did not exist under the 1995 Directive, which was adopted prior to the creation and explosion in use of social networks. It provides in part:

> The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:
> (a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and
> (b) the processing is carried out by automated means.[148]

The data subject may request that the data be transmitted from one controller to the other, where feasible.[149]

f. Right to Object

Data subjects have the right to object to the processing of their personal data, in which case "the controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims."[150] The legitimate grounds balancing test is difficult for the controller to meet, because the

144. *Id*. art. 18(1)(a).
145. *Id*. art. 18(1)(b).
146. *Id*. art. 18(1)(c).
147. *Id*. art. 18(1)(d).
148. *Id*. art. 20(1).
149. *Id*. art. 20(2).
150. *Id*. art. 21(1).

grounds must be "overwhelming."[151] When the data subject objects to processing for direct marketing purposes, including profiling for those purposes, this may be done at any time.[152] In the case of processing "for scientific or historical research purposes or statistical purposes… the data subject…shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest."[153]

g. Right Not to Be Subject to a Decision Based Solely on Automated Processing, Including Profiling

A "data subject [has] the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."[154] This last right is not an absolute one, as exceptions to its application are provided. These include where the decision is necessary to enter into or perform a contract;[155] where it is authorized by EU or Member State law, subject to the requirement that the law lay down suitable measures for the protection of the data subjects rights, freedoms, and legitimate interests;[156] or where the data subject has given his or her explicit consent.[157] In the case of a contract or explicit consent, the controller must "implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision."[158] Note that some restrictions on the use of special categories of data for such decisions apply,[159] in which case fewer exceptions are allowed.[160]

151. *See* Gabriela Zanfir-Fortuna, *Article 21 Right to Object*, *in* THE EU GENERAL DATA PROTECTION REGULATION (GDPR): A COMMENTARY, *supra* note 68, at 508, 517.

152. GDPR, *supra* note 3, art. 21(2).

153. *Id*. art. 21(6).

154. *Id*. art. 22(1).

155. *Id*. art. 22(2)(a).

156. *Id*. art. 22(2)(b).

157. *Id*. art. 22(2)(c).

158. *Id*. art. 22(3).

159. *See id*. art. 22(4).

160. *See* Kaminski, *supra* note 23, at 198.

6. Accountability

The concept of accountability means "being able to demonstrate compliance with the data protection rules,"[161] and this at any time. This entails, *inter alia*, record-keeping regarding the processing of personal data, to prove compliance with the GDPR.[162] Most responsibilities under the GDPR are for the controller,[163] although there are certain obligations of the processor, as well.[164]

As part of ensuring accountability, various mechanisms may be mandatory, depending on the case: data protection impact assessments,[165] prior consultation and prior authorization,[166] and data protection officers.[167] These may all be considered compliance mechanisms.[168] Furthermore, many controllers are required to maintain records of processing activities,[169] although this requirement does not apply to certain SMEs,[170] however, this exception is not likely relevant to U.S. airlines.[171]

161. Giovanni Buttarelli, Keynote Speech to the Privacy and Security Conference: Privacy in an age of hyperconnectivity 4 (Nov. 7, 2016) (transcript available on the website of the European Data Protection Supervisor).

162. *See*, *e.g.*, Voss, *supra* note 34, at 802.

163. *See*, *e.g.*, GDPR, *supra* note 3, art. 24(1) ("Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation.").

164. *See*, *e.g.*, *id.* art. 32(1) ("[T]he controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk…").

165. Voss, *supra* note 34, at 802.

166. *Id.*

167. *Id.*

168. *See id.,* at 802–06.

169. GDPR, *supra* note 3, art. 30(1).

170. *Id.* art. 30(5) ("The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data …").

171. As an example, the last of the airlines on Annex A, Hawaiian Airlines, had 7,492 active employees as of June 30, 2020, well above the 250-person ceiling for SMEs indicated in GDPR art. 30(5). *See Quarterly Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934*, HAWAIIAN HOLDINGS INC. (May 7, 2020) 28, https://app.quotemedia.com/data/downloadFiling?webmasterId=102175&ref=114993012&type=HTML&symbol=HA&companyName=Hawaiian+Holdings+Inc.&formType=10Q&formDescription=General+form+for+quarterly+reports+under+Section+13+or+15%28d%29&dateFiled=2020-05-07&CK=1172222 [https://perma.cc/6M35-U8EC].

7. Lawfulness and Fairness of Processing

In the text of the GDPR, the lawfulness and fairness of processing is linked to transparency,[172] but this study has chosen to separate the terms, especially with respect to lawfulness. The requirement here is that there be a legal basis for the processing. The potential bases for processing are the following six: consent of the data subject;[173] processing is necessary for a contract with the data subject;[174] processing is necessary for the controller's compliance with a legal obligation imposed on it;[175] processing is necessary to protect the vital interests of the data subject or another individual;[176] processing is necessary for the "performance of a task carried out in the public interest or in the exercise of official authority vested in the controller";[177] and processing is necessary "for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."[178] While the consent basis is perhaps the one most commonly thought of,[179] it is subject to several conditions,[180] and the contract basis may be useful in a commercial context.[181] The last basis—legitimate interests—may be the most restrictive one as it is subject to a balancing test,[182] especially in the case of a child's data.

172. GDPR, *supra* note 3, art. 5(1)(a) ("[P]ersonal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency').")

173. *Id.* art. 6(1)(a).

174. *Id.* art. 6(1)(b).

175. *Id.* art. 6(1)(c).

176. *Id.* art. 6(1)(d).

177. *Id.* art. 6(1)(e).

178. *Id.* art. 6(1)(f).

179. *See, e.g.*, WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 63 (2018) (referring to consent as the GDPR's "linchpin").

180. *See* GDPR, *supra* note 3, art. 7.

181. *E.g.*, Waltraut Kotschy, *Article 6. Lawfulness of Processing*, *in* THE EU GENERAL DATA PROTECTION REGULATION (GDPR): A COMMENTARY, *supra* note 68, at 321, 331 ("Contrary to the case where consent is the legal basis for processing, the data subject as a contractual partner cannot freely terminate processing of his/her data based on a contract. Only by terminating the contract will the legal basis for processing (at least partly) be removed."). However, this basis may be inappropriate in certain employment situations where the imbalance of power between the employer and the employee may not allow the employee to effectively refuse certain contractual terms. *See id.* at 330.

182. One commentator has remarked that "[t]he reference to 'interests *or* fundamental rights' along with the fact that the interests are not qualified by 'legitimate', means that the position of the data subject is protected extensively." *Id.* at 338.

C. Requirements for Data Transfers

The GDPR requires that in order for personal data of persons in the European Union to be exported for processing outside of that EU single market, the conditions set forth in Chapter V of the GDPR must be met by the controller or the processor, including with respect to onward transfers. [183] This covers the cases where the data are being processed or are meant to be processed after transfer to a country outside of the European Union ("a third country") or to an international organization.[184] Importantly, those conditions include the general provision that transfers may take place where the European Commission (Commission) has issued an adequacy decision for the relevant third country, which acknowledges that such country ensures an "adequate level of protection" for EU personal data.[185] Thus, an adequacy decision is a determination by the Commission of the adequacy of the third country's data protection laws which allows cross-border transfers of EU personal data to that third country under Chapter V of the GDPR.[186] At present, few countries benefit from an adequacy decision.[187]

Several criteria are set out in the GDPR for the adequacy determination, such as the rule of law, relevant legislation,[188] the existence and effective functioning of an independent supervisory authority in the third country or to which an international

183. GDPR, *supra* note 3, art. 44 (Chapter V includes arts. 44-50 of the GDPR). *See* Voss, *supra* note 75, at 506. (Onward transfers may be explained as "further transfers to another country outside of the European Union (or European Economic Area), or to another international organization.").

184. GDPR, *supra* note 3, art. 4(26) (defining "international organization" as an organization "and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries."). *See* Lee A Bygrave & Luca Tosoni, *Article 4(26). International Organisations*, *in* THE EU GENERAL DATA PROTECTION REGULATION (GDPR): A COMMENTARY, *supra* note 68, at 303, 306–07 (giving examples of international organizations including the United Nations, the International Telecommunications Union, the International Committee of the Red Cross, and Interpol. However, noting that typically non-governmental organizations (NGOs), "which are established on private initiative and governed by the domestic law of the State where they are incorporated or have their headquarters," would not fit within the term (citation omitted).)

185. GDPR, *supra* note 3, art. 45(1).

186. *See* VOSS & WOODCOCK, *supra* note 18, at 221 (referring to an "adequacy determination").

187. These include Andorra, Argentina, Canada (for commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay, with discussions ongoing with South Korea. EUROPEAN COMMISSION, *Adequacy decisions*, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en [https://perma.cc/VR8L-WJ6F].

188. GDPR, *supra* note 3, art. 45(2)(a).

organization is subject,[189] and international commitments of the third country or international organization.[190] The standard to meet, however, is not the third country's laws mirroring the GDPR, but providing the "core requirements" of that legislation.[191] In the event that no adequacy decision has been made with respect to the relevant third country or international organization, the data exporter, whether it be a controller or a processor, must provide appropriate safeguards,[192] which may take the form of a "legally binding and enforceable instrument between public authorities or bodies,"[193] binding corporate rules (BCRs),[194] standard data protection (or contractual) clauses (or SCCs) pursuant to a Commission SCC decision[195] or as adopted by a supervisory authority and approved by the Commission,[196] among other instruments. Furthermore, derogations for specific situations, in the absence of an adequacy decision or appropriate safeguards, are available.[197]

These requirements for data transfers, including implications for airlines, will be further discussed in the context of the *Schrems II* decision in Part III of this study.

II. GDPR SANCTIONS IN THE AVIATION INDUSTRY TO-DATE

This Section analyzes GDPR sanctions in the aviation field from May 25, 2018, through March 18, 2021. Although all of the carriers involved are European ones, given the extraterritorial effect of the GDPR, these cases should provide insights for non-European carriers subject to the GDPR as well, including those established in the United States. The prior EU law—the 1995 Directive for example—led to the sanction of non-EU carrier Cathay

189. *Id*. art. 45(2)(b).

190. *Id*. art. 45(2)(c).

191. ART. 29 DATA PROTECTION WORKING PARTY, ADEQUACY REFERENTIAL, 18/EN WP254rev.01(Feb. 6, 2018), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108 [https://perma.cc/349D-RH5M]; *see also* Voss, *supra* note 91, at 459–60 (discussing, inter alia, the "essentially equivalent" standard of the ECJ's *Schrems I* jurisprudence).

192. GDPR, *supra* note 3, art. 46(1) (this is conditional on "enforceable data subject rights and effective legal remedies for data subjects" being available).

193. *Id*. art. 46(2)(a).

194. *Id*. art. 46(2)(b). "Binding corporate rules" are defined as "personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings or group of enterprises engaged in joint economic activity." *Id*. art. 4(20).

195. *Id*. art. 46(2)(c). *See* Comm'n Decision of 5 Feb. 2010, 2010 O.J. (L 39/5) (announcing relevant decision in the case of a transfer from an EU controller to a non-EU processor).

196. *Id*. art. 46(2)(d).

197. *Id*. art. 49(1).

Pacific for inadequate security in a data breach context, for a period ending just before application of the GDPR.[198]

A. British Airways

British Airways (BA) received the first notice of intention to fine under the GDPR by the UK supervisory authority (the Information Commissioner's Office, or ICO), on July 8, 2019.[199] The ICO announced its intention to fine BA £183.39 million related to a cyber incident involving the diversion of user traffic from the BA website to a fraudulent site, notified to the ICO by the airline itself.[200] The proposed fine was reported to represent 1.5% of BA's annual revenue.[201] The incident resulted in the compromising of personal data (logins, credit card numbers, names, addresses, and travel reservation information) of approximately half a million customers, due to poor security at BA, in violation of GDPR Article 32.[202] One privacy professional described the hack of BA as being more sophisticated than prior attacks by the organization behind the hack, and they used digital skimming techniques.[203] Another author comments that the hackers compromised "the BA site's data integrity" and that, contrary to payment card industry standards, CVV codes were left unencrypted by BA.[204]

In early 2020, it was reported that the ICO had extended the period prior to fining BA, in agreement with the company, until

198. *International airline fined £500,000 for failing to secure its customers' personal data*, INFO. COMMISSIONER'S OFF. (Mar. 4, 2020), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/03/international-airline-fined-500-000-for-failing-to-secure-its-customers-personal-data/ [https://perma.cc/7YUR-LVCE] (the case was brought under the Data Protection Act 1998, the United Kingdom's implementation of the 1995 Directive). *See also* Monetary Penalty Notice, INFO. COMMISSIONER'S OFF., (Feb. 10, 2020) (finding jurisdiction as Cathay Pacific "maintains a branch in the United Kingdom …. As such it is "established in the UK.").

199. *See* GDPR ENFORCEMENT TRACKER, enforcementtracker.com [https://perma.cc/F2BZ-HFGK], (this listing of GDPR fines is compiled by global law firm CMS, through its German member CMS Hasche Sigle Partnerschaft von Rechtsanwälten und Steuerberatern mbB).

200. INFO. COMMISSIONER'S OFF., *supra* note 5; Mark Rogan, *GDPR's Big Moment Has Just Arrived – With a $228 Million Data Breach Fine*, CPO MAGAZINE (Sept. 12, 2019), https://www.cpomagazine.com/data-protection/gdprs-big-moment-has-just-arrived-with-a-228-million-data-breach-fine/ [https://perma.cc/F498-TU4K].

201. Mark Sweney, *BA faces £183m fine over passenger data breach*, THE GUARDIAN (Jul. 8, 2019, 5:29 PM), https://www.theguardian.com/business/2019/jul/08/ba-fine-customer-data-breach-british-airways [https://perma.cc/U5JB-9WMA].

202. *Id.*

203. Tash Whitaker, *The BA Data Breach*, 2 INT'L J. DATA PROTECTION OFFICER, PRIVACY OFFICER & PRIVACY COUNS. 15 (2018) (Speaking of the Magecart organization hackers, the author comments that, "[i]n essence, they camouflaged themselves to avoid detection, rather than just doing a hit and run.").

204. Roland L. Trope, *To Secure, or Not Secure, Data Integrity—That Is the Question: Cybersecurity Developments*, 75 BUS. LAW. 1655, 1663–64 (2019).

March 31, 2020.[205] In April 2020, this time period was extended.[206] On July 31, 2020, BA's parent company, International Consolidated Airlines Group (IAG), announced that an:

> [E]xceptional charge of €22 million represents management's best estimate of the amount of any penalty issued by the Information Commissioner's Office (ICO) in the United Kingdom, relating to the theft of customer data at British Airways in 2018. The process is ongoing, and no final penalty notice has been issued. The exceptional charge has been recorded within Property, IT and other costs in the Income statement, with a corresponding amount recorded in Provisions.[207]

Such amount represents a reduction by 89% of the ICO penalty, in the context of a year of the shutdown of air travel due to the COVID-19 pandemic,[208] but still one of the highest fines issued by a DPA under the GDPR to-date.[209] The final fine notice confirmed the reduction to £20,000,000[210] (€22,046,000[211]). The case is note-worthy, not just because of the amount of the fine, but also for the ICO's explicit consideration of the COVID-19

205. Gareth Corfield, *UK data watchdog kicks £280 British Airways and Marriott GDPR fines into legal long grass*, THE REGISTER (Jan. 13, 2020, 9:06 AM), https://www.theregister.com/2020/01/13/ico_british_airways_marriott_fines_delayed/ [https://perma.cc/5M84-6QRM].

206. Neil Hodge, *British Airways banking on drastic reduction of record GDPR fine*, COMPLIANCE WEEK (Aug. 3, 2020, 3:04 PM), https://www.complianceweek.com/data-privacy/british-airways-banking-on-drastic-reduction-of-record-gdpr-fine/29272.article [https://perma.cc/5QBL-2258].

207. *IAG 2nd Quarter 2020 Results,* INT'L AIRLINES GROUP (July 31, 2020), https://otp.tools.investis.com/clients/uk/international_airlines_group/rns/regulatory-story.aspx?cid=2457&newsid=1405286 [https://perma.cc/NA7L-MXGG]. This new figure would represent approximately $26 million. *See* Hodge, *supra* note 206.

208. Gareth Corfield, *UK data watchdog having a hard time making GDPR fines stick: Marriott scores another extension, BA prepares to pay 11% of £183m penalty threat*, THE REGISTER (Aug. 5, 2020, 11:25 AM), https://www.theregister.com/2020/08/05/marriott_starwood_gdpr_fine_british_airways/ [https://perma.cc/8XER-DN22].

209. Edward Machin, *EUR 22 million set aside for British Airways 2018 data breach*, ROPES & GRAY (July 31, 2020), https://ropesgrayinsights.passle.net/post/102gcqp/eur-22-million-set-aside-for-british-airways-2018-data-breach [https://perma.cc/LX8Y-RRTV] ("[I]t would also be the second highest GDPR fine of any EU regulator to date."). However, note that the CNIL's €50 million fine imposed on Google, the Hamburg DPA's €35,258,708 fine on H&M Hennes & Mauritz Online Shop and the Garante's €27.8 million fine on TIM are higher. *See* GDPR ENFORCEMENT TRACKER, *supra* note 199. Thus, this penalty would be the fourth highest GDPR fine to-date, if effectively imposed on BA.

210. British Airways, *Penalty Notice*, INFO. COMMISSIONER'S OFF. (Oct. 16, 2020), https://ico.org.uk/action-weve-taken/enforcement/british-airways/ [https://perma.cc/9ZCM-YQVL].

211. GDPR ENFORCEMENT TRACKER, *supra* note 199.

pandemic's impact on the British Airway's business in assessing the amount of the fine.[212] The case also provides an example of the use of the GDPR's one-stop-shop mechanism, as the ICO brought the case to a conclusion acting as lead supervisory authority in cooperation with other EU DPAs.[213]

Furthermore, this case illustrates expectations of DPAs concerning data security measures necessary in order for airlines to comply with GDPR Articles 5(1)(f) and 32. The ICO cited publicly available guidance to show that British Airways did not take the necessary technical and organizational measures to prevent or mitigate a "supply-chain attack."[214] Specifically, the ICO noted that British Airways could have prevented, or at least mitigated the attack taking the following action: "limiting access to applications, data and tools to only that which are required to fulfil a user's role;" "undertaking rigorous testing, in the form of simulating a cyber-attack, on the business' systems;" and "protecting employee and third party accounts with multi-factor authentication."[215]

B. Vueling

Vueling Airlines received the first actual administrative fine under the GDPR covered by this study in the amount of €30,000, on October 1, 2019, issued by the Spanish supervisory authority Agencia Española de Protección de Datos (AEPD).[216] In reality, the case involved an infringement of the LSSI (the Spanish Law on Information Society Services and Electronic Commerce), Article 22.2, which states that "Service providers may use of data storage and retrieval devices on recipients' terminal equipment, provided that they have given their consent after they have been provided with clear and complete information on their use, in particular, on the purposes of the data processing."[217] Those storage and retrieval

212. *ICO fines British Airways £20m for data breach affecting more than 400,000 customers*, INFO. COMMISSIONER'S OFF. (Oct. 16, 2020), 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/ [https://perma.cc/NLX7-MFUR] ("As part of the regulatory process the ICO considered both representations from BA and the economic impact of COVID-19 on their business before setting a final penalty.") (hereinafter *ICO fines British Airways £20m).*

213. *Id.* ("Because the BA breach happened in June 2018, before the UK left the EU, the ICO investigated on behalf of all EU authorities as lead supervisory authority under the GDPR. The penalty and action have been approved by the other EU DPAs through the GDPR's cooperation process.").

214. *See Penalty Notice*, *supra* note 110, at 28–32, 55–56.

215. *ICO fines British Airways £20m*, *supra* note 212.

216. GDPR ENFORCEMENT TRACKER, *supra* note 199.

217. *The Spanish Data Protection Authority fined the company Vueling for the cookie policy used on its website with 30,000 euros*, EUR. DATA PROTECTION BOARD, (Oct. 17,

devices may be "cookies."Although references to a violation of the LSSI were mentioned, this case involves the use of powers bestowed upon the AEPD and other DPAs by Article 58(2) of the GDPR,[218] as well as their powers of investigation under Article 57(1) of the GDPR.[219]

The LSSI[220] is the Spanish implementation in domestic law of the EU ePrivacy Directive,[221] as amended by EU Directive 2009/136/EC,[222] especially with regard to cookies. In this sense, cookies may be defined as "small files downloaded to a computer or terminal device such as a smartphone or tablet when the user accesses certain websites. These are used for recognizing a returning user's device or computer, as they are sent back to the originating website on each subsequent visit."[223] The ePrivacy Directive complements the general 1995 Directive—and now the GDPR—with respect to privacy in the specific sector of electronic

2019), https://edpb.europa.eu/news/national-news/2019/spanish-data-protection-authority-fined-company-vueling-cookie-policy-used_en [https://perma.cc/T32T-YH4T] [hereinafter Vueling Fine].

218. Agencia Española de Protección de Datos (AEPD), Procedimiento Sanctionador Nº: PS/00300/2019, Resolución R/00499/2019 de Terminación del Procedimiento por Pago Voluntario at 6 (Oct. 10, 2019), https://www.aepd.es/es/documento/ps-00300-2019.pdf [https://perma.cc/SSX4-U555] [hereinafter Fundamentos de Derecho].

219. *Id*. at 1 (Hechos: Segundo).

220. Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI) [Law No. 34/2002 of July 11 on Information Society Services and Electronic Commerce] (B.O.E. 2002, 13758) (Spain), https://www.boe.es/boe/dias/2002/07/12/pdfs/A25388-25403.pdf [https://perma.cc/HN4A-AFVW], as amended by Real Decreto-ley 13/2012, de 30 de marzo por el que se transponen directivas en materia de mercados interiores de electricidad y gas y en materia de comunicaciones electrónicas, y por el que se adoptan medidas para la corrección de las desviaciones por desajustes entre los costes e ingresos de los sectores eléctrico y gasista [Royal Decree-Law 13/2012, of March 30, transposing directives on internal electricity and gas markets and electronic communications, and adopting measures to correct deviations from mismatches between the costs and revenues of the electricity and gas sectors] (B.O.E. 2012, 4442) [hereinafter LSSI].

221. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002, Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications), 2002 O. J. (L 201) 37, (July 31, 2002).

222. Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 Amending Directive 2002/22/ EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services; Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector and Regulation (EC) No 2006/2004 on Cooperation between National Authorities Responsible for the Enforcement of Consumer Protection Laws, 2009 O.J. (L 337) 11 (Dec. 18, 2009) (Sometimes this Amending Directive is referred to as the "Cookie Directive," because of that part of its focus).

223. VOSS & WOODCOCK, *supra* note 18, at 222. *See also Cookie*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/cookie (defining a cookie as "a small file or part of a file stored on a World Wide Web user's computer, created and subsequently read by a website server, and containing personal information (such as a user identification code, customized preferences, or a record of pages visited).").

communications,[224] although to better interface with the GDPR, an ePrivacy Regulation has been proposed,[225] but not yet adopted.[226]

Article 19.2 specifies that, in particular, with respect to the collection of personal data, information to be furnished to data subjects, and the creation and maintenance of personal data files, "Organic Law 15/1999, of December 13, on Protection of Personal Data and its implementing regulation shall apply,"[227] which refers to the Spanish transposition of the 1995 Directive.[228] As the 1995 Directive was repealed on the date of entry into application of the GDPR on May 25, 2018,[229] references to the 1995 Directive are to be construed as references to the GDPR.[230]

Vueling's customers were unable to configure cookies downloaded onto their computers through the airline's website.[231] According to the press release reproduced by the EDPB, "What the company does not provide is a management system or cookie configuration panel that allows the user to delete them in a granular way," as to fit personal preferences,[232] however, the airline told the AEPD that they were implementing a mechanism to allow users to select the types of cookies that they wanted to have installed on their terminal equipment.[233] The AEPD reduced the amount of the sanction to €18,000 as a result of the airline's voluntary payment of that sum.[234]

224. W. Gregory Voss, *First the GDPR, Now the Proposed ePrivacy Regulation*, 21 J. INTERNET L. 3 (2017).

225. *Id*. at 4.

226. *See* Samuel Stolton, *German Presidency charts new COVID19 'metadata' rules in leaked ePrivacy text*, EURACTIV (Nov. 5, 2020), https://www.euractiv.com/section/digital/news/german-presidency-charts-new-covid19-metadata-rules-in-leaked-eprivacy-text/ [https://perma.cc/JV8M-R2GZ] (commenting that "In the Council, however, progress on the ePrivacy regulation has been dogged by disagreements over issues ranging from the inclusion of provisions in the regulation to allow for the detection of child pornography, to consent requirements and rules for the tracking of online activity through the use of cookies.").

227. LSSI, *supra* note 220, art. 19.2, author's translation ("En todo caso, será de applicación la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y su normativa de desarollo, en especial, en lo que se refiere a la obtención de datos personales, la información a los interesados y la creación y maintenimiento de ficheros de datos personales.").

228. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (B.O.E. 1999, 23750) (Spain), https://boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf [https://perma.cc/P254-DCRN].

229. GDPR, *supra* note 3, art. 94(1).

230. *Id*. art. 94(2).

231. Vueling Fine, *supra* note 217.

232. *Id*.

233. Fundamentos de Derecho, *supra* note 218, at 2 (Facts (*Hechos*), para. 3(2) (Tercero, 2°)).

234. *Id*. at 5.

C. *TAROM*

Romanian air carrier TAROM received two sanctions during the period studied. The first sanction was issued on December 4, 2019, and later, another sanction on July 30, 2020, both by the Romanian National Supervisory Authority for Personal Data Processing (ANSPDCP).[235] The ANSPDCP is the Romanian supervisory authority for purposes of the GDPR, and a member of the EDPB.[236] In the first case, ANSPDCP fined TAROM the equivalent of €20,000 for failing to secure data, leading to an employee's unauthorized access to the booking application and the photographing of a list containing personal data of twenty-two customers of the airline, and disclosure of such list online.[237] Similarly, in the second case, ANSPDCP found that there was a violation of the data security provision (Article 32) of the GDPR as TAROM "did not implement adequate technical and organisational measures" so as to ensure that any natural person acting under its authority and with access to personal data only process them at TAROM's request.[238] This failure led to unauthorized access to, and disclosure of, personal data of five TAROM passengers, which was sanctioned by a fine equivalent to €5,000.[239]

D. *Iberia*

Spanish flag carrier, Iberia Líneas Aéreas de España, S.A. Operadora Unipersonal (Iberia), was issued administrative sanctions twice by the AEPD on February 3, 2020, and on July 20, 2020.[240] In the first case, which involved a data subject's request to leave Iberia's frequent flyer program (Iberia Plus) and to have his or her data erased, however the data subject continued to receive emails, showing that the airline had not complied with his or her requests, and Iberia was fined €20,000.[241] There was a lack of legal

235. GDPR ENFORCEMENT TRACKER, *supra* note 199.

236. *Members*, EUR. DATA PROTECTION BOARD, https://edpb.europa.eu/about-edpb/board/members_en [https://perma.cc/PU6T-ACQX].

237. *Fine for the infringement of the GDPR (SC CNTAR TAROM SA),* THE NATIONAL SUPERVISORY AUTHORITY FOR PERSONAL DATA PROCESSING (ANSPDCP), https://www.dataprotection.ro/index.jsp?page=Sanctiune_CN_TAROM&lang=en [https://perma.cc/7JZZ-MYLD].

238. *Sanction for the infringement of GDPR* (*SC CNTAR TAROM SA*), THE NATIONAL SUPERVISORY AUTHORITY FOR PERSONAL DATA PROCESSING (ANSPDCP), https://www.dataprotection.ro/index.jsp?page=Sanctiune%20pentru%20incalcare%20RGPD%2027_07_20&lang=en [https://perma.cc/KV8T-RVBM].

239. *Id*.

240. GDPR ENFORCEMENT TRACKER, *supra* note 199.

241. AEPD (Agencia Española de Protección de Datos), Procedimiento Sanctionador N°: PS/00402/2019, Resolución de Procedimento Sancionador (Iberia Líneas Aéreas de España, S.A. Operadora Unipersonal) (Feb. 3, 2020),

basis for the processing of the data subject's personal data under GDPR Article 6(1), as the data subject had not given consent, as defined in GDPR Article 4(11),[242] to receive the emails. In the second case, the data subject exercised his or her right to access to personal data, consisting of recordings of four telephone conversations, however Iberia neither provided such recordings, nor notified the AEPD of action taken.[243]

E. Air Europa

On March 18, 2021, the AEPD issued a total administrative fine of €600,000 to Spanish carrier Air Europa Líneas Aéreas S.A.,[244] an airline that IAG—Iberia's parent—has agreed to acquire, subject to European Commission approval.[245] The fine follows the late notification to the Spanish DPA—with a delay of forty-one days, without justification—of a security breach involving unauthorized access to contact details and bank accounts affecting close to a half-million individuals, which constituted a violation of Article 33 of the GDPR, and failure to have implemented appropriate technical and organizational measures to ensure data security, which constitutes a violation of Article 32(1) of the GDPR.[246] Indeed, a report of a security company engaged by the airline in connection with the breach indicated that the intrusion probably originated from unsafe systems available on the internet, certain devices had not installed software updates regularly, and there had been no specific measures taken to protect the data accessed by the hackers, such as the use of encryption or tokenization.[247]

https://www.aepd.es/es/documento/ps-00402-2019.pdf [https://perma.cc/L9CX-UWH4], at 1 (Antecedentes).

242. *Id*. at 3–4 (Fundamentos de Derecho, para. II).

243. AEPD (Agencia Española de Protección de Datos), Procedimiento Sanctionador N°: PS/00060/2020, Resolución R/00304/2020 de Terminación del Procedimento por Pago Voluntario (Iberia Líneas Aéreas de España, S.A. Operadora Unipersonal) (July 20, 2020), https://www.aepd.es/es/documento/ps-00060-2020.pdf [https://perma.cc/37A4-24WA], at 2 (Hechos: Segundo).

244. AEPD (Agencia Española de Protección de Datos), Procedimiento Sanctionador N°: PS/00179/2020 (Air Europa Líneas Aéreas S.A.) (Mar. 18, 2021), https://www.aepd.es/es/documento/ps-00179-2020.pdf [https://perma.cc/EJD8-JCTJ].

245. *British Airways-owner IAG buys Air Europa in cut-price 500 million euro deal*, REUTERS (Jan. 20, 2021 9:52 AM), https://www.reuters.com/article/uk-aireuropa-m-a-iag-idUSKBN29P0W3 [https://perma.cc/5NGY-B54P].

246. Spain: AEPD fines Air Europa €600,000 for GDPR security and notification failures, Data Guidance (Mar. 18, 2021), https://www.dataguidance.com/news/spain-aepd-fines-air-europa-€600000-gdpr-security-and [https://perma.cc/U8TC-YXGT].

247. AEPD (Agencia Española de Protección de Datos), Procedimiento Sanctionador N°: PS/00179/2020, *supra* note 244, at 31.

The breach included unauthorized access to credit card information—numbers, expiration dates and CVV codes—and in certain cases, information about the identity of the cardholders, all obtained through hacking and malware.[248] The AEPD referred to the fact that it initially learned of the breach from credit card companies and Banco Popular,[249] whereas it would have been better if the airline had communicated first to the Spanish DPA, in a timely fashion, as one of the factors in a DPA's decision to impose a fine, or not, and its amount, is "the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement."[250]

F. Others—Airline Sales Agent and Travel Agency

Although not directly related to airlines, unlike the preceding cases, this study also briefly considers a handful of cases in the ancillary to the aviation industry—cases regarding an airline sales agent and a travel agency.

1. Louis Aviation Ltd.

An airline sales agent in Cyprus, Louis Aviation Ltd.,[251] is one of the members of a group of companies (also including LGS Handling Ltd. and Louis Travel Ltd.), that was issued three fines on October 25, 2019, by the Cypriot supervisory authority, in the amounts of €70,000, €10,000, and €2,000, respectively.[252] In each of these cases, a human resources automated tool—an absenteeism formula referred to as the "Bradford factor"—was used for the purpose of scoring sick leave and profiling employees based on the results. The reasoning behind the use of this tool, "was that short, frequent, and unplanned absences lead to a higher disorganizing of the company rather than longer absences."[253] This practice was considered unlawful personal data processing in violation of GDPR provisions on legitimate basis for processing (Article 6) and processing of special categories of data (Article 9).[254]

248. *Id*. at 1–2.

249. *Id*. at 33.

250. GDPR, *supra* note 3, art. 83(2)(h).

251. *Louis Aviation*, LOUIS GROUP, https://www.louisgroup.com/companies/louis-aviation [https://perma.cc/6PKL-P4BK].

252. GDPR ENFORCEMENT TRACKER, *supra* note 199.

253. *The Cypriot Supervisory Authority banned the processing of an automated tool, used for scoring sick leaves of employees, known as the "Bradford Factor" and subsequently fined the controller*, EUR. DATA PROTECTION BOARD (Jan. 27, 2020), https://edpb.europa.eu/news/national-news/2020/cypriot-supervisory-authority-banned-processing-automated-tool-used-scoring_en [https://perma.cc/MG6B-VRPJ].

254. *Id.*

2. Global Business Travel Spain SLU

In this case, travel agency Global Business Travel Spain SLU was found to have violated GDPR Articles 32(2) and 32(4) regarding security of personal data, as an employee was able to access the health data of a data subject, showing the travel agency's failure to prevent the unauthorized disclosure. [255] These violations resulted in a fine of €3,000, paid on June 6, 2020.[256]

G. Conclusion on GDPR Sanctions in the Aviation Industry

The foregoing cases highlight examples of the application of the GDPR in the aviation industry setting, focusing mainly on airlines. All of the cases involve EU airlines: three of these being IAG brands—BA, Iberia, and Vueling,[257] a company subject to an agreement for its acquisition by IAG—Air Europa, and TAROM. Even though this is the case, as the Cathay Pacific example showed us, these cases may be helpful with respect to U.S. or other non-EU airlines, as Cathay Pacific (a non-EU carrier) was sanctioned by the ICO under the predecessor legislation to the GDPR—the 1995 Directive.

One major violation that jumps out at the reader from the above cases is a failure to ensure adequate security for personal data in violation of GDPR Article 32. Other violations involve a lack of a legitimate basis for data processing and failure to notify a data breach in a timely manner, among other provisions of the GDPR. The fines issued by EU Member State DPAs have all been relatively minor, with none above €600,000, save the notable exception of BA. Even the BA fine seems to have been lowered following representations made by the airline after the ICO's notice of intention to fine. Also, cooperation with the DPAs is important (voluntarily paying fines in Spain allowed the lowering of one fine and failure to provide information to a DPA in another case was a violation). Airlines also must comply with data subject requests to exercise rights.

This study now looks at transborder data flows of personal data collected for commercial purposes, intentionally excluding PNR data flows for law enforcement purposes and for the fight against crime and terrorism.

255. *AEPD – PS/00247/2019*, GDPRHUB, https://gdprhub.eu/index.php?title=AEPD_-_PS/00247/2019 [https://perma.cc/42S4-RQ6R].

256. *Id.*

257. *Our brands*, INT'L AIRLINES GROUP, https://www.iairgroup.com/en/our-brands [https://perma.cc/X4YJ-8965].

III. TRANSBORDER DATA FLOWS AND THE *SCHREMS II* DECISION

This study will first survey the safeguards used by U.S. airlines for transborder data flows, prior to discussing the *Schrems II* court decision and detailing its potential impact on those safeguards. As a reminder, such safeguards are necessary in order for data flows from the European Union to a third country to be legal under the GDPR, where that third country has not received a Commission adequacy decision, and they may include SCCs or BCRs, among other possible appropriate safeguards.[258] However, an adequacy decision adopted by the Commission under the 1995 Directive concerning the EU-U.S. Privacy Shield framework (Privacy Shield)[259] was the perhaps unexpected subject matter of *Schrems II*, discussed in Section B.

A. Safeguards for Transborder Data Flows in Aviation

In order to assess the safeguards used by U.S. airlines for transborder data flows, this study first analyzed information available from the websites of the nine airlines in the Fortune 500 ranking,[260] as those sites are seen from the European Union (France). These are detailed in Annex A. More specifically, the results of this study's analysis of U.S. airlines' privacy policies show that, when a basis for transborder data transfers is indicated, it is in the majority of cases the use of standard contractual clauses.[261] Only one airline (United) refers to the Privacy Shield (discussed briefly in Section B) as a basis, in the alternative, together with standard contractual clauses (SCCs).[262] It appears that one airline

258. GDPR, *supra* note 3, art. 46.

259. Commission Implementing Decision (EU) 2016/1250, 2016 O.J. (L 207) 1, 3, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016D1250&from=EN [https://perma.cc/K627-QAPW].

260. *Fortune 500: 2020: Airlines*, FORTUNE, https://fortune.com/fortune500/2020/search/?f500_industry=Airlines [https://perma.cc/C3K8-DEK3] (the total ranking actually listed one thousand companies).

261. This is the case for Delta, American, United (in the alternative, together with Privacy Shield), JetBlue and Hawaiian (although Hawaiian just refers to contractual or other safeguards, without specifying that these are the EU standard contractual clauses). *See generally* Nigel Cory, Ellysse Dick & Daniel Castro, *The Role and Value of Standard Contractual Clauses in EU-U.S. Digital Trade*, INFO. TECH. & INNOVATION FOUND. (Dec. 17, 2020), https://itif.org/publications/2020/12/17/role-and-value-standard-contractual-clauses-eu-us-digital-trade [https://perma.cc/X6CC-339Y].

262. *Customer Data Privacy Policy*, UNITED, https://www.united.com/ual/en/us/fly/privacy.html [https://perma.cc/3FS2-KGA7].

(Southwest) relies upon consent as a basis.[263] It,[264] and the other airlines that have neither standard contractual clauses nor Privacy Shield as a transborder transfer basis (Alaska[265] and Spirit[266]), do not fly to Europe, with the possible exception of SkyWest. That company acts through partnerships with major airlines, three of which do fly to Europe: Delta,[267] American[268] and United.[269] Although this does not preclude the application of the GDPR, it may mean that Southwest, Alaska, and Spirit have fewer EU data subjects as customers and are not as aware of the relevant transborder data transfer requirements as those carriers that fly to Europe. Alternatively, they may not be targeting customers from the European Union or monitoring their behavior, so as not to meet the territorial scope provisions of the GDPR discussed in Part I.A.3, although a thorough analysis would need to be conducted in order to determine whether or not the GDPR applies to them.

The bases for transborder personal data transfers used by the carriers that do fly to Europe—standard contractual clauses (SCCs) and the EU-U.S. Privacy Shield (Privacy Shield)—were the subjects of a recent ECJ court case—*Schrems II*—that this study now analyzes.

B. Schrems II *Decision*

The European Union Court of Justice (ECJ) Grand Chamber issued its decision in the *Schrems II* case on July 16, 2020.[270] The decision responded to a request for a preliminary ruling by the High Court of Ireland.[271] The case was brought by Maximilian Schrems,

263. *Privacy Policy (UPDATED)*, SOUTHWEST (effective Jan. 1, 2020), https://www.southwest.com/html/about-southwest/terms-and-conditions/privacy-policy-pol.html [https://perma.cc/R5HH-2HYH].

264. *Route Search Tool*, SOUTHWEST, https://www.southwest.com/flight/routemap_dyn.html?clk=GSUBNAV-AIR-ROUTEMAP [https://perma.cc/C8RP-W7ZX].

265. *Explore our destination network*, ALASKA AIRLINES, https://www.alaskaair.com/en/?INT=sitemap-prodID:Destinations [https://perma.cc/Z8RG-NE8L].

266. *Where We Fly*, SPIRIT, https://www.spirit.com/route-maps [https://perma.cc/Z29G-SPY2].

267. *Flights to Europe*, DELTA, https://www.delta.com/us/en/flight-deals/europe-flights [https://perma.cc/KQ2Q-ZKFE].

268. *Where we fly*, AM. AIRLINES, http://aa.fltmaps.com/en [https://perma.cc/H8UE-W67R].

269. *Route maps*, UNITED, https://www.united.com/web/en-us/content/travel/route-maps.aspx?POS=FR [https://perma.cc/5S38-SPNV].

270. *Schrems II*, *supra* note 55, at 1.

271. *Id.* para. 2 (The request related to proceedings between the Data Protection Commission (Ireland) and Facebook Ireland Ltd. and Maximilian Schrems, on a complaint brought by the latter regarding Facebook's transfer of his personal data to the United States.). For a short explanation of preliminary rulings, *see generally* Voss & Houser, *supra* note 14.

an Austrian national, who had previously brought a similar case—referred to as *Schrems I*.[272] *Schrems I* involved the Safe Harbor, a framework negotiated between the U.S. Department of Commerce and the Commission that allowed companies to self-certify that they provided EU data subjects with the rights under the framework, intended to be similar to the rights they had under the 1995 Directive. [273] It thus allowed data transfers from the European Union to self-certifying companies in the United States under the resulting Commission adequacy decision.[274] Schrems claimed that under the Safe Harbor, Facebook would transfer his data to the United States, where it would be accessible by U.S. authorities, as there was not adequate protection there against the mass surveillance that had been exposed in the Edward Snowden disclosures.[275] As a consequence, the ECJ invalidated the Safe Harbor on October 6, 2015, which was replaced by a somewhat improved framework—the Privacy Shield—on July 12, 2016, following intense negotiations and allowing a Commission adequacy decision.[276]

In *Schrems II*, Schrems used similar arguments against Facebook's use of SCCs to transfer personal data to the United States,[277] under the Commission's SCC Decision.[278] The ECJ upheld the validity of the SCC Decision, generally, as "examination of the SCC Decision in the light of Articles 7, 8 and 47 of the Charter has disclosed nothing to affect the validity of that decision."[279] However, transfers subject to appropriate safeguards may be made "on condition that enforceable data subject rights and effective legal remedies for data subjects are available."[280] Realistically, there must be a case-by-case assessment of the adequacy of the appropriate safeguards to ascertain the level of protection ensured.

272. Case C-362/14, Schrems v. Data Prot. Comm'r (*Schrems I*), ECLI:EU:C:2015:650 (Oct. 6, 2015).

273. *See* W. Gregory Voss, *The Future of Transatlantic Data Flows: Privacy Shield or Bust?*, 19 J. INTERNET L. 8, 9 (2016).

274. *Id*. at 12.

275. *See* Voss, *Cross-Border Data Flows, the GDPR, and Data Governance*, *supra* note 75, at 513.

276. *Id*. at 513–14.

277. Kimberly A. Houser & W. Gregory Voss, *The European Commission on the Privacy Shield: All Bark and No Bite?*, UNIV. ILL. J.L. TECH. & POL'Y: TIMELY TECH 1, 2 (2018), http://illinoisjltp.com/timelytech/the-european-commission-on-the-privacy-shield-all-bark-and-no-bite/ [https://perma.cc/3MA5-BFP2].

278. For detail on the Commission's SCC decision, *see id*.

279. *Schrems II*, *supra* note 55, para. 149. Here and elsewhere in this study, "the Charter" refers to Charter for Fundamental Rights of the European Union. CHARTER OF THE FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION, 2012 O.J. (C 326) at 391 [hereinafter *Charter*] (Art. 7 is the right to "Respect for private and family life"; Art. 8 is the right to "Protection of personal data"; and Art. 47 is the "Right to an effective remedy and to a fair trial.").

280. GDPR, *supra* note 3, art. 46(1). *See also Schrems II*, *supra* note 55 para. 103.

Both the contractual clauses and, "as regards any access by the public authorities of that third country to the personal data transferred, the relevant aspects of the legal system of that third country, in particular those set out, in a non-exhaustive manner, in Article 45(2)" of the GDPR, must be considered.[281] The ECJ indicated that "it may prove necessary to supplement the guarantees contained in those data protection clauses" so that the GDPR's level of protection of individuals in not undermined,[282] depending on the circumstances. The controller or processor exporting the data is responsible for verifying "on a case-by-case basis, and where appropriate, in collaboration with the recipient of the data, whether the law of the third country of destination ensures adequate protection, under EU law, of personal data transferred pursuant to standard data protection clauses, by providing, where necessary, additional safeguards."[283] Failing that, the DPA should suspend or end the transferring of personal data.[284]

Certain obligations under the SCCs should be highlighted here. A data recipient must "inform the controller . . . promptly of any inability to comply with its obligations" under the contract, and certifies that "it has no reason to believe that the legislation applicable to it prevents it from fulfilling its obligations under the contract" and must also promptly notify any changes in applicable national legislation which may have a substantial adverse effect on the SCC warranties and obligations.[285] In cases where the recipient is unable to comply with the SCC clauses, the controller is to suspend the data transfer and/or terminate the contract.[286] This may result in the requirement that transferred data be returned or destroyed and may give rise to a right to compensation.[287] A competent DPA is required to suspend or prohibit a data transfer "if, in its view and in the light of all the circumstances to the transfer" the SCCs "are not or cannot be complied with in that third country and the protection of the data transferred that is required by the EU law cannot be ensured by other means, where the controller or a processor has not itself suspended or put an end to the transfer."[288]

281. *Schrems II*, *supra* note 55, para. 105.

282. *Id*. para. 132.

283. *Id*. para. 134.

284. *Id*. para. 135 (the ECJ mentions that this is the case where the third country's law "imposes on the recipient of personal data from the European Union obligations which are contrary to those clauses and are, therefore, capable of impinging on the contractual guarantee of an adequate level of protection against access by the public authorities of that third country to that data.").

285. *Id*. para. 139.

286. *Id*. para. 140.

287. *Id*. para. 143.

288. *Id*. para. 146.

While the ECJ did not invalidate SCCs generally, as a result of U.S. surveillance the ECJ found the Privacy Shield Decision invalid.[289] In effect, where Section 702 of the Foreign Intelligence Surveillance Act (FISA), as amended,[290] and Executive Order (E.O.) 12333[291] served as the bases for surveillance programs but were "not covered by requirements ensuring, subject to the principle of proportionality, a level of protection essentially equivalent to that guaranteed by the second sentence of Article 52(1) of the Charter,"[292] the ECJ determined that "Section 702 of the FISA does not indicate any limitations on the power it concerns to implement surveillance programmes for the purposes of foreign intelligence or the existence of guarantees for non-US persons potentially targeted by those programmes."[293] Furthermore, under Presidential Policy Directive 28 (PPD-28), which was issued as part of the documents furnished in connection with the Privacy Shield and "extended certain privacy protections to non-U.S. citizens when subject to foreign intelligence surveillance,"[294] although EU citizens are granted certain rights binding on U.S. intelligence authorities, they did not obtain actionable rights in U.S. courts against the U.S. authorities, and thus Privacy Shield "cannot ensure a level of protection essentially equivalent to that arising from the Charter."[295] A similar lack of actionable rights exists with respect to E.O. 12333.[296] The ECJ concluded that,

> In those circumstances, the limitations on the protection of personal data arising from the domestic law of the United States on the access and use by US public authorities of such data transferred from the European Union to the United States, which the Commission assessed in the Privacy Shield Decision, are not circumscribed in a way that satisfies requirements that are essentially equivalent to those

289. *Id*. para. 201.

290. Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1881 (2018).

291. Exec. Order No. 12,333, 46 Fed. Reg. 59,941 (Dec. 4, 1981).

292. *Schrems II*, *supra* note 55, paras. 174, 178 (Under the second sentence of Article 52(1) of the Charter, subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.)

293. *Id*. para. 180.

294. Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115, 172 (2017) (stating the PPD-28 enshrines certain principles, such as data minimization, but also highlighting the tenuous nature of such an executive directive).

295. *Schrems II*, *supra* note 55, para. 181.

296. *Id*. para. 182.

> required, under EU law, by the second sentence of Article 52(1) of the Charter.[297]

Moreover, the ECJ rejected arguments that the Privacy Shield Ombudsperson, established under the Privacy Shield, allowed for data subjects to be able to obtain judicial redress, when necessary, as there was no proof that the Ombudsperson could bind U.S. intelligence services by his or her decisions.[298] As a result, the ECJ considered that the mechanism "does not provide any cause of action before a body which offers the persons whose data is transferred to the United States guarantees essentially equivalent to those required under Article 47 of the Charter."[299]

C. Potential Impact of Schrems II Decision on Safeguards Used in Aviation

As a practical matter, the *Schrems II* decision eliminated one way that personal data could be transferred from the European Union to the United States—the Privacy Shield.[300] However, looking at Annex A, only one of the airlines indicated uses the Privacy Shield to allow for transborder data flows. That airline is United, which must now depend on its other safeguard, SCCs, for its data transfers to the United States, as the Privacy Shield has been invalidated. Delta, American, United, and JetBlue, then, all explicitly use SCCs, which were not invalidated by the ECJ, even if conditions for their use were set forth.

With respect to data transfers based on SCCs,[301] the question arises, do the surveillance measures based on Section 702 FISA and E.O. 12333 impact a U.S. airline so that it is unable to receive such data legally under the SCCs say when its subsidiary in the European Union seeks to transfer data to the United States, taking into account the considerations set out in *Schrems II*? In the case of

297. *Id*. para. 185.

298. *Id*. para. 196.

299. *Id*. para. 197.

300. *See* Anupam Chander, *Is Data Localization a Solution for* Schrems II*?*, 23 J. INT'L ECON. L. 771, 773 (2020).

301. Although none of the airlines listed in Annex A disclosed using BCRs for the transfer of personal data from the European Union to the United States, the EDPB has confirmed that this assessment would need to be performed for the use of BCRs as well. *Frequently Asked Questions on the Judgment of the Court of Justice of the European Union in Case C-311/18*, EUR. DATA PROTECTION BOARD, 2 (July 23, 2020), https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf [https://perma.cc/NFS8-BNJM] ("The threshold set by the Court also applies to all appropriate safeguards under Article 46 GDPR used to transfer data from the EEA to any third country.") [hereinafter Frequently Asked Questions].

Section 702 FISA, the EDPB reminds us that instrument applies to an "electronic communications service provider,"[302] defined as:

> (A) a telecommunications carrier, as that term is defined in section 153 of Title 47;
> (B) a provider of electronic communication service, as that term is defined in section 2510 of title 18;
> (C) a provider of a remote computing service, as that term is defined in section 2711 of title 18;
> (D) any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored; or
> (E) an officer, employee, or agent of an entity described in subparagraph (A), (B), (C), or (D).[303]

Although it is for the airline to make this determination, at first blush it would appear that airlines are not the target, then, of this provision. For example, one commentator gives examples of companies that fit within the above categories: (A) AT&T, T- Mobile and Verizon; (B) and (C) Facebook, Google and AWS.[304] However, according to Department of Justice guidance that he cites, (D) is broad enough to capture companies just on the basis of their providing their employees email service.[305] Yet, another commentator specifically indicates that SCCs could still work for

302. *Id*.

303. 50 U.S.C. § 1881(b)(4) (2018).

304. Richard Lawne, *US surveillance: s702 FISA, EO 12333, PRISM and UPSTREAM*, FIELD FISHER (Aug. 13, 2020), https://www.fieldfisher.com/en/insights/us-surveillance-s702-fisa-eo-12333-prism-and-ups [https://perma.cc/UA36-EKL7].

305. *Id*. ("According to guidance issued by the Department of Justice, the definition is broad enough that it could potentially capture any company that provides its employees with corporate email or a similar ability to send and receive electronic communications, regardless of the company's primary business or function.") (citation omitted).

airlines, for example.[306] A similar determination must be made with respect to E.O. 12333.[307]

Nonetheless, if the airline is transferring the data to the United States, say to use AWS (or another company subject to surveillance under Section 702 FISA) to store those data in the cloud, presumably SCCs for such transfer would fail the *Schrems II* assessment. Furthermore, one German DPA (Baden-Württemberg) issued guidance following S*chrems II* and considered encryption, anonymization and pseudonymization should be used as additional safeguards for transfers to the United States.[308] In any event, if the

306. David Meyer, *What U.S. companies should consider following the bombshell EU Privacy Shield ruling*, FORTUNE (July 16, 2020, 5:37 PM), https://fortune.com/2020/07/16/privacy-shield-eu-us-companies-business/ [https://perma.cc/NMY8-EXVN] ("Of course, not every American company serving Europeans is a Facebook or Google. If you don't have U.S. agencies scrutinizing your data under Section 702 of FISA—if, for example, you're an airline or a retailer—then SCCs could still work for you. The big difference now is that you'll first have to convince EU privacy regulators that European customers' data isn't subject to surveillance in the U.S.").

307. Frequently Asked Questions, *supra* note 301, at 3 (This is as, "[w]hether or not you can transfer personal data on the basis of SCCs will depend on the result of your assessment, taking into account the circumstances of the transfers, and supplementary measures you could put in place. The supplementary measures along with the SCCs, … would have to ensure that U.S. law does not impinge on the adequate level of protection they guarantee."); *Id.* note 2 at 2 (The EDPB notes that E.O. 12333 "organises electronic surveillance," defined as the "acquisition of a non-public communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a non electronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio direction-finding equipment solely to determine the location of a transmitter."); Lawne, *supra* note 304 (A commentator notes, with respect to E.O. 12333, "Unlike FISA, surveillance under EO 12333 does not rely on the compelled assistance of electronic communications service providers. The technical details remain classified and obscure, but the NSA has confirmed it involves exploiting vulnerabilities in telecommunications infrastructure.").

308. *German DPA Issues Guidance on Data Transfers Following Schrems II*, HUNTON ANDREWS KURTH PRIVACY & INFO. SEC. L. BLOG (Sept. 2, 2020), https://www.huntonprivacyblog.com/2020/09/02/german-dpa-issues-guidance-on-data-transfers-following-schrems-ii/ [https://perma.cc/D2HV-XUJY] ("For data transfers to the U.S., data controllers should seek to provide additional safeguards to mitigate risks, in particular (1) encryption for which 'only the data exporter has the key' and which 'cannot be broken by U.S. [intelligence] services,' (2) anonymization or (3) pseudonymization, where 'only the data exporter can re-identify the data.'"). Note that the EDPB has provided recommendations including a full list of supplementary measures that might be taken by companies if their "Article 46 GDPR transfer tool is not effective," as a result of the legal framework in the destination country. *See Recommendations 01/2020 on Measures That Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data*, EUR. DATA PROTECTION BOARD, (Nov. 10, 2020), 15, https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf [https://perma.cc/A686-QSNY]. (Such examples of supplementary measures are included in Annex 2 to such Recommendations, at 21-37 and include technical and organizational measures, and

airline is a controller transferring personal data to the United States, it will have to make the assessment required by the *Schrems II* decision;[309] if it is the recipient of personal data, it will have to make a similar assessment and inform the data exporter of any inability to comply with its obligations under the contract, including as a result of U.S. legislation or regulation.[310]

Finally, one company in Annex A may be using consent as a basis for transfers, although it is unclear whether this use is meant for the personal data of EU data subjects. If that is the case, under the GDPR this would be considered a derogatory measure and would need to meet certain conditions set out in the law: "the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards."[311] The Baden-Württemberg DPA indicated that derogations should be interpreted restrictively,[312] and the EDPB has confirmed that "[i]t is still possible to transfer data from the EEA to the U.S. on the basis of derogations foreseen in Article 49 GDPR provided the conditions are set forth in this Article apply."[313] In the case of consent, it must be explicit, "specific for the particular data transfer or set of transfers," and informed concerning the risks of the transfer.[314]

While this Section has centered on U.S. air carriers, other non-EU carriers and companies operating internationally in other sectors should pay attention to the *Schrems II* decision, as well. While countries other than the United States have not benefitted from a "Privacy Shield," SCCs may be used to export personal data from the European Union to them. Following *Schrems II* it is clear that the data controllers using these safeguards must assess, "prior to any transfer, whether the level of protection required by EU law is respected in the third country concerned."[315] This will require an expertise in the law of the destination country, and transfers to certain countries may be problematic for reasons related to the rule

additional contractual measures. However, a discussion of all of these elements is beyond the scope of this study.).

309. Christopher Kuner, *The Schrems II Judgement of the Court of Justice and the Future of Data Transfer Regulation*, EUR. L. BLOG (July 17, 2020), https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/ [https://perma.cc/B49P-LU73].

310. *German DPA Issues Guidance on Data Transfers Following Schrems II*, *supra* note 308.

311. GDPR, *supra* note 3, art. 49(1)(a).

312. *German DPA Issues Guidance on Data Transfers Following Schrems II*, *supra* note 308.

313. Frequently Asked Questions, *supra* note 301, at 4.

314. *Id*.

315. *Schrems II*, *supra* note 55, para. 142.

of law.[316] In addition, the controllers' investigation may be hindered by the unavailability or lack of legislation on law enforcement or security access to transferred personal data.[317] Ultimately, the *Schrems II* decision reinforces the notion of a necessity for controllers to investigate the legal environment of the data ecosystem and to control activities down the data flow supply chain,[318] and practically anticipates one solution put forth by a German regulator: "companies could store their data in Europe."[319]

CONCLUSION

This study, which focuses on requirements for the commercial use of EU personal data by U.S. airlines, and specifically excludes the transfer of PNR data, begins by highlighting the *British Airways* GDPR penalty case, which had a certain resonance when the ICO's notice of intention to issue the highest administrative fine to date under the GDPR was publicized. However, the amount was eventually reduced, showing in part the discretion of DPAs to adjust penalties for factors such as—in this case—the economic impact of the COVID-19 pandemic on the controller involved. Then several important provisions of the GDPR for the aviation sector are detailed. While most airlines that fly to the European Union will have an establishment there that will be subject to the GDPR, airlines that do not fly to the European Union may still be subject to the GDPR, if it is found that they are targeting sales of services to EU persons, or are monitoring their behavior in the European Union. Several elements that may indicate that individuals in the European Union are targeted are discussed, and airline websites and documentation should be reviewed to see if these are present and are sufficient for the GDPR to apply. Alternatively, the website and documentation could be modified to make clear that such persons are not targeted.

316. Kuner, *supra* note 309 ("This will require data controllers to become experts in third-country law in a way that is probably beyond the capabilities of many of them, and raises questions in particular about data transfers to third countries that are non-democratic or where the rule of law does not apply.").

317. *See id*. (commenting that, "[t]he obligations that the Court puts on data controllers to investigate the level of protection will be even more difficult for transfers to countries such as China, where legislation dealing with law enforcement and the security services may be difficult to obtain or non-existent.").

318. *See* Voss, *Cross-Border Data Flows, the GDPR, and Data Governance, supra* note 75, at 528–29.

319. Vincent Manancourt, *The Demise of Privacy Shield May Be the End of US-Europe Data Transfers*, POLITICO (Aug. 3, 2020, 6:00 AM), https://www.politico.eu/article/privacy-shield-is-dead-long-live-data-localization/ [https://perma.cc/V9X3-GHWV] (the German regulator cited is the Baden-Württemberg privacy regulator Stefan Brink).

When the GDPR applies to them, airlines should become fully aware of key provisions of the GDPR, and its underlying data protection principles. It is important that airlines have appropriate technical and organizational measures in place in order to ensure security of personal data and to be able to respond to data subject requests to exercise rights and requirements to notify data breaches, within time limits established by the GDPR. Airlines must have a legal basis to process personal data under the GDPR, and certain conditions apply if this basis is the consent of the data subject.

Several examples of the first GDPR sanctions in the airline industry have been detailed, and lessons from them drawn. In this context, security of data and response to data subject requests to exercise rights appear to be key elements. With respect to security requirements, guidance from ENISA, NIST, and national cybersecurity bodies may be helpful. Finally, the 2020 *Schrems II* decision invalidating the EU-U.S. Privacy Shield Decision was examined, and its potential impact on the transfer of personal data from the European Union to the United States by airlines was studied.

ANNEX A

Fortune 500 (2020) Ranking[320]	**Airline Company**	**Basis for Transborder Transfers**
68	Delta Air Lines, Inc.	Model Clauses approved by the European Commission; "in some limited circumstances" by derogation under GDPR Article 49 (for performance of a contract or where necessary for legal proceedings) [321]
70	American Airlines Group	Standard data protection contractual clauses[322]
76	United Airlines Holdings, Inc.	Standard Contractual Clauses, or certification schemes such as the EU - US Privacy Shield[323]
141	Southwest Airlines Co.	Consent- "You agree to such transfer, storing and/or processing outside the country in which you are located."[324]
360	Alaska Air Group (Alaska Airlines, Inc.)	None indicated[325] (although various bases for processing data are listed (e.g., consent, legitimate interests,

320. *Fortune 500*, *supra* note 260.

321. Delta Privacy Policy, *supra* note 2.

322. *Privacy Policy*, AMERICAN AIRLINES (Sept. 30, 2020), https://www.aa.com/i18n/customer-service/support/privacy-policy.jsp [https://perma.cc/N2TM-ST5J].

323. *Customer Data Privacy Policy*, UNITED, https://www.united.com/ual/en/FR/fly/privacy-eu-full.html#tcm:76-9543 [https://perma.cc/FWS8-YU6J].

324. *Privacy Policy (UPDATED): Transfer of Information*, SOUTHWEST (Jan. 1, 2020), https://www.southwest.com/html/about-southwest/terms-and-conditions/privacy-policy-pol.html#Advertising_Analytics_Services_Online_Tracking [https://perma.cc/BJ39-HENX] (note that this website does not have a version specifically tailored to France).

325. *Alaska Airlines Privacy Notice: International Transfers of Personal Data*, ALASKA AIRLINES (Dec. 18, 2019), https://www.alaskaair.com/content/legal/privacy-policy?lid=footer:privacyPolicy#privacy-notice [https://perma.cc/7MFA-EDKT] (the language in this section refers to a transfer of data from the United States to another country, rather than from the European Union to a third country).

		etc.)[326]
394	JetBlue Airways	Standard international data transfer contractual terms approved by the European Commission[327]
658	Spirit Airlines	None indicated[328]
788	SkyWest, Inc. (SkyWest Airlines)	None indicated[329]
819	Hawaiian Holdings (Hawaiian Airlines)	Contractual or other safeguards to the extent legally required[330]

326. *Id.*

327. *JetBlue Airways Privacy Policy: Additional Disclosures for EU Data Subjects: D. Cross Border Transfers of Your Personal Information*, JETBLUE (Jan. 1, 2020), https://www.jetblue.com/legal/privacy [https://perma.cc/PB6Y-J99J].

328. *Privacy Policy*, SPIRIT (July 1, 2020), https://content.spirit.com/Shared/en-us/Documents/Privacy_Policy.pdf [https://perma.cc/CJA7-X6YC].

329. *About: About SkyWest Airlines*, SKYWEST AIRLINES, https://www.skywest.com/about-skywest-airlines [https://perma.cc/KJS2-HUKE] ("SkyWest Airlines operates through partnerships with United Airlines, Delta Air Lines, American Airlines and Alaska Airlines," so potentially the privacy policies of those partner airlines would apply, as relevant, as no privacy policy is shown on SkyWest's website).

330. *Privacy Policy: Cross-Border Transfers*, HAWAIIAN AIRLINES (Aug. 19, 2020), https://www.hawaiianairlines.com/legal/privacy-policy [https://perma.cc/J2G8-EWBP].