SPIRITED AWAY: THE EU'S ADEQUACY DECISION FOR JAPAN AS A ROADMAP FOR U.S. PRIVACY LAW AFTER *SCHREMS II*

INTRODUCTION

The European Union's General Data Protection Regulation ("GDPR") attempts to protect the rights of member states' citizens by enacting a regulatory scheme for processing personal data. The GDPR is notable both for the strength of the protection it offers and for the reach of said protection. The GDPR requires entities outside of the European Union ("EU") who process the personal data of EU citizens to have protections similar to those of the GDPR in place. Foreign persons, companies, and governments who process said data must be aware of, and abide by, the GDPR's provisions. The purpose of this paper is to analyze weaknesses in the U.S. system of privacy and data protection law by comparing the adequacy decision made for Japan to the *Schrems II* case recently decided in the EU. This note begins with a discussion of the history of data protection law in the EU and its importance to Europe before moving on to a description of the GDPR and its adequacy requirements. Then, this paper will parse the relevant considerations discussed in the Adequacy Decision for Japan and drawing comparisons to the U.S.' data protection measure under the EU-US Privacy Shield.

I. DATA PROTECTION LAW IN THE EUROPEAN UNION BEFORE THE GDPR.

The EU views data privacy[1] differently from the U.S.[2] As a result, the approaches the U.S. and EU take to data privacy regulation have diverged.[3] Beginning in the 1970s, the EU "deepened and expanded" the Fair

[1] "While U.S. lawyers may refer broadly to 'privacy' or to 'information privacy', European law discusses information privacy as 'data protection.' In Europe, data protection is increasingly seen as separate from the right to privacy. Data protection focuses on whether data is used fairly and with due process." Chris Jay Hoofnagle et al., *The European Union General Data Protection Regulation: What It Is and What It Means*, 28 INFO. & COMMC'NS TECH. L. 65, 70 (2019) (citations omitted).

[2] *E.g.*, *id.* at 79; MARTIN A. WEISS & KRISTIN ARCHICK, U.S.-EU DATA PRIVACY: FROM SAFE HARBOR TO PRIVACY SHIELD 1-7 (2016), https://fas.org/sgp/crs/misc/R44257.pdf. *See also* Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115, 117 (2017); Julia M. Fromholz, *The European Union Data Privacy Directive*, 15 BERK. TECH. L.J. 461 (2000).

[3] *See generally* Schwartz & Peifer, *supra* note 2.

Information Practices ("FIPs")[4] that were originally developed in the United States,[5] applying those privacy principles broadly to both public and private entities.[6] The EU lists data protection as a right in its Charter of Fundamental Rights,[7] elevating it to a status equal to that of freedom of religion, the right to own property, and freedom of expression.[8] This elevation of the right of data protection is "anchored in interests of dignity, personality, and self-determination."[9] The result is a system of data protection that is "strongly anchored at the constitutional level"[10] and that considers data privacy to be "part of its legal culture of fundamental rights."[11]

In 1995, the European Union adopted directive 95/46/EC ("the Data Protection Directive" or "the Directive") with the intention of lowering barriers to data transfer and providing more effective protection for EU

[4] FIPs, also known as Fair Information Practice Principles ("FIPPs"), are "a set of internationally recognized principles that inform information privacy policies both within government and the private sector." *The Fair Information Practice Principles (FIPPs) in the Information Sharing Environment (ISE)*, NAT'L PUB. SAFETY P'SHIP, https://www.nationalpublicsafetypartnership.org/Documents/The_Fair_Information_Practice_Principles_in_the_Information_Sharing_Environment.pdf (last visited Nov. 7, 2020). "The FIPs are a code of best practices for the handling of personal information by businesses and government." NEIL RICHARDS, INTELLECTUAL PRIVACY 76 (2017). FIPs include, *inter alia*, limitations on data collection and use, and openness and security requirements. *Fair Information Practice Principles*, INT'L ASS'N PRIV. PROS., https://iapp.org/resources/article/fair-information-practices/#:~:text=(1)%20The%20Collection%20Limitation%20Principle,2)%20The%20Data%20Quality%20Principle (last visited Nov. 7, 2020). For a discussion of the history of FIPs, see Robert Gellman, *Fair Information Practices: A Basic History* (Oct. 7, 2019), https://bobgellman.com/rg-docs/rg-FIPShistory.pdf.

[5] RICHARDS, *supra* note 4, at 73.

[6] Hoofnagle et al., *supra* note 1, at 70. "The key regulatory norms are centered around the enactment of Fair Information Practices (FIPs)." Schwartz & Peifer, *supra* note 2, at 128.

[7] Charter of Fundamental Rights of the European Union, art. 8, 2016, European Council [hereinafter EU Charter]. Article 8 reads in full:

> 1. Everyone has the right to the protection of personal data concerning him or her.
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
> 3. Compliance with these rules shall be subject to control by an independent authority.

Id.

[8] *See* EU Charter; *see also* Maja Brkan, *The Unstoppable Expansion of the EU Fundamental Right to Data Protection: Little Shop of Horrors?*, 23 MAASTRICHT J. EUR. & COMP. L. 812, 815 (2016); Schwartz & Peifer, *supra* note 2; Mira Burri & Rahel Schär, *The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy*, 6 J. INFO. POL'Y 479, 481 (2016) ("[T]he right to privacy is a key concept in EU law and has been given significant weight that reflects deep cultural values and understandings.").

[9] Schwartz & Peifer, *supra* note 2, at 123.

[10] *Id.* at 127.

[11] *Id.* at 126; *see also* Burri & Schär, *supra* note 8.

citizens by consolidating the privacy laws of member states.[12] The Data Protection Directive concerned protections afforded to the personal data[13] of EU citizens during its processing and communication to third parties.[14] Within the Directive's scope,[15] data processing[16] was allowed in only seven general circumstances.[17] However, the Directive included exceptions for data processed for the purpose of national security, criminal investigations, and "personal or household use" of data.[18] It also set out criteria that needed to be met to transfer EU citizens' data to parties in countries outside of the EU.[19] Also introduced in the Directive were "adequacy decisions," preventing the exportation of personal data to a third country unless that

[12] *See* 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 the Free Movement of Such Data, 1995 O.J. (L 281), ¶¶ 7-8 [hereinafter Data Protection Directive]; Hoofnagle et al., *supra* note 1, at 70-71; Fromholz, *supra* note 2, at 468.

[13] The Directive defines personal data as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." Data Protection Directive, *supra* note 12, at art. 2.

[14] *See* Data Protection Directive, *supra* note 12. For an in-depth discussion of the Data Protection Directive, see Ian Walden, *The Application of Directive 95/46/EC*, 3 EDI L. REV. 85 (1996).

[15] *See* Data Protection Directive, *supra* note 12, at art. 3 ("This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system."). "Filing system" is defined as "any structured set of personal data which are accessible according to specific criteria." *Id.* at art. 2.

[16] Data processing is defined as "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction." Data Protection Directive, *supra* note 12, at art. 2.

[17] The Directive provides that data may be processed if:

> (a) the data subject has unambiguously given his consent; or
>
> (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
>
> (c) processing is necessary for compliance with a legal obligation to which the controller is subject; or
>
> (d) processing is necessary in order to protect the vital interests of the data subject; or
>
> (e) 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 or in a third party to whom the data are disclosed; or
>
> (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

Data Protection Directive, *supra* note 12, at art. 7.

[18] *See id.* at art. 3.

[19] *Id.* at arts. 25-26.

country had been judged to have sufficient data protection measures in place.[20]

While the Directive laid out basic standards for data protection, it required individual member states to pass legislation at the national level to put those standards into effect.[21] The Data Protection Directive did make data protection law more uniform throughout the EU, but still allowed for variation between member states since each country enacted its own interpretation of the Directive's requirements.[22] Additionally, enforcement was often lacking because member states, regulated directly by their own laws and not the Data Protection Directive itself,[23] often only lightly enforced data protection laws, if at all, in an attempt to attract technology companies.[24] The Directive also provided for miniscule fines that failed to deter noncompliance.[25]

II. THE GENERAL DATA PROTECTION REGULATION.

A. Purpose, Application, and Important Definitions.

The GDPR was, in part, a response to concerns regarding the poor enforcement of the Data Protection Directive.[26] The GDPR is a regulatory scheme composed of "rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free

---

[20] *Id.* at art. 25.

[21] *See id.* at arts. 5-7; Hoofnagle et al., *supra* note 1, at 71; Fromholz, *supra* note 2, at 467-68; Schwartz & Peifer, *supra* note 2, at 128 (directives are not directly binding on member states, while regulations create "directly enforceable standards").

> [M]ember state[s] . . . adopt[ing] a national statute or law to implement [a directive] . . . is only necessary when the EU creates directives, [because they] are not directly enforceable by member states. . . . EU regulations are directly enforceable even if the text of the regulation is not present in the national law of a member state.

Elle Pyle et al., *Decoding GDPR: Familiar Terms Could Cause Major Confusion When GDPR Takes Effect*, 102 JUDICATURE 58, 65 n.1 (2018).

[22] *See* Data Protection Directive, *supra* note 12, at art. 5; Hoofnagle et al., *supra* note 1, at 71.

[23] *See* Schwartz & Peifer, *supra* note 2, at 128-29.

[24] Hoofnagle et al., *supra* note 1, at 71.

[25] *Id.* at 69.

[26] *See* Hoofnagle et al., *supra* note 1, at 69. For other weaknesses of the Data Protection Directive, see NEIL ROBINSON ET AL., REVIEW OF EU DATA PROTECTION DIRECTIVE: SUMMARY 8 (May 2009) https://ico.org.uk/media/about-the-ico/documents/1042347/review-of-eu-dp-directive-summary.pdf; *see also infra* text accompanying notes 28-29.

movement of personal data."[27] Adopted on April 14, 2016, the GDPR came into full effect on May 25, 2018,[28] repealing and replacing the Data Protection Directive.[29] While recognizing the Data Protection Regulation's "objectives and principles…remain[ed] sound," the GDPR acknowledged that the Directive had failed to establish a consistent data protection framework across the EU.[30] Changing technology further necessitated a "strong[er] and more coherent" protection scheme with more consistent enforcement.[31] The GDPR has two major objectives: "protect[ing] fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data"[32] and ensuring the "free movement of personal data within the [European] Union,"[33] but places greater emphasis on protecting individuals.[34]

The GDPR is widely considered "the most consequential regulatory development in information policy in a generation."[35] The passage and adoption of the GDPR spawned a myriad of papers discussing its implications and speculating as to its possible effects; even more articles were written to educate businesses, lawyers, and researchers about the GDPR and to apprise them of requirements for compliance.[36] Such a deluge

---

[27] Regulation (EU) 2016/679 of the European Parliament and of 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), art. 1 [hereinafter GDPR].

[28] W. Scott Blackmer, *GDPR: Getting Ready for the New EU General Data Protection Regulation*, INFOLAW GROUP: INSIGHTS (May 5, 2016), https://www.infolawgroup.com/insights/2016/05/articles/gdpr/gdpr-getting-ready-for-the-new-eu-general-data-protection-regulation?rq=GDPR; GDPR, *supra* note 27, at art. 99.

[29] GDPR, *supra* note 27, at art. 94.

[30] *Id.* at (9); *see also* Data Protection Directive, *supra* note 12, at art. 25.

[31] GDPR, *supra* note 27, at (7).

[32] *Id.* at art. 1.

[33] *Id.*

[34] *See* Hoofnagle et al., *supra* note 1, at 72.

[35] *Id.* at 66.

[36] *See, e.g.*, Jan Philipp Albrecht, *How the GDPR Will Change the World*, 2 EUR. DATA PROT. L. REV. 287 (2016); Note, Jacob M. Victor, *The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy*, 131 YALE L.J. 513 (2013); Jay F. Kramer & Sean B. Hoar, *GDPR, Part I: History of European Data Protection Law*, Lewis Brisbois, https://lewisbrisbois.com/assets/uploads/files/GDPR,_Part_I-_History_of_European_Data_Protection_Law.pdf (last visited Nov. 7, 2020); PAUL VOIGT & AXEL VON DEM BUSSCHE, THE EU GENERAL DATA PROTECTION REGULATION (GDPR): A PRACTICAL GUIDE (2017); Colin Tankard, *What the GDPR Means for Business*, NETWORK SECURITY (June 2016); IT GOVERNANCE, EU GENERAL DATA PROTECTION REGULATION (GDPR): AN IMPLEMENTATION AND COMPLIANCE GUIDE (2d ed. 2017); Miranda Mourby et al., *Are 'Pseudonymised' Data Always Personal Data? Implications of the GDPR for Administrative Data Research in the UK*, 34 COMPUT. L. & SEC. REV. 222 (2018); David Basin et al., *On Purpose and by Necessity: Compliance under the GDPR*, *in* FINANCIAL CRYPTOGRAPHY AND DATA SECURITY, FC 2018 20-37 (Sarah Meiklejohn & Kazue Sako,

of preparatory material might suggest that the GDPR marked a sea-change in data protection and privacy law, but the GDPR is closer to an "evolution" of the Data Protection Directive than a "revolution."[37]

Since the GDPR is an evolution of the Data Protection Directive, there are many similarities between the two regulations. Like the Directive before it, the GDPR is based on the FIPs.[38] However, the GDPR adds additional rights and provides further details about the rights of data subjects.[39] Similarly, the GDPR also regulates the processing of "personal data."[40] Personal data is defined in the GDPR as "any information relating to an identified or identifiable natural person,"[41] a nearly identical definition to that found in the Directive. This definition of personal data is broad, encompassing practically everything "that identifies a person or *could* identify a person."[42] Processing is defined as "any operation or set of operations which is performed on personal data or on sets of personal data."[43] With its key concepts defined so broadly, the GDPR applies nearly every time an entity "touches data that relate to an individual, whether the data are public or private, sensitive or non-sensitive, directly or indirectly

---

eds., 2018); Kimberly A. Houser & W. Gregory Voss, *GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy?*, 25 RICH. J.L. & TECH. 1 (2018); Kyle Petersen, *GDPR: What (and Why) You Need to Know About EU Data Protection Law*, UTAH BAR J., July-Aug. 2018, at 12; Inge Graef, *Algorithms and Fairness: What Role for Competition Law in Targeting Price Discrimination Towards End Consumers?*, 24 COLUM. J. EUR. L. 541 (2017); Alexis Salerno, *Protecting "Crown Jewel" Trade Secrets in the Cloud Through Voluntary Industry-Government Collaborations and Federal Legislation*, 21 U. PA. J. BUS. L. 442 (2018); Blackmer, *supra* note 28; Matt Wes, *Looking to Comply With GDPR? Here's a Primer on Anonymization and Pseudonymization*, INT'L ASS'N PRIV. PROS. (Apr. 25, 2017), https://iapp.org/news/a/looking-to-comply-with-gdpr-heres-a-primer-on-anonymization-and-pseudonymization/; Joshua Blume, *A Contextual Extraterritoriality Analysis of the DPIA and DPO Provisions in the GDPR*, 49 GEO. J. INT'L L. 1425 (2018); Kim Leonard Smouter-Umans, *GDPR and Research: Is the GDPR Eventually Going to Be Good or Bad for Research*, 2 INT'L J. DATA PROT. OFFICER, PRIV. OFFICER & PRIV. COUNS. 29 (2018); *Guide to the General Data Protection Regulation (GDPR)*, INFO. COMM'R OFF. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/ (last visited Nov. 8, 2020); Ruth Boardman et al., *Bird & Bird Guide to the General Data Protection Regulation*, BIRD & BIRD (May 2020) https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/bird--bird--guide-to-the-general-data-protection-regulation.pdf?la=en.

[37] Hoofnagle et al., *supra* note 1, at 69.

[38] *See id.* at 70. See *supra* note 4 and accompanying text for information about the Directive's roots in the FIPs.

[39] Hoofnagle et al., *supra* note 1, at 92.

[40] *See* Data Protection Directive, *supra* note 12; GDPR, *supra* note 27.

[41] GDPR, *supra* note 27, at art. 4. In full, the GDPR defines personal data as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." *Id.* "All privacy laws define covered data." Hoofnagle et al., *supra* note 1, at 72.

[42] Hoofnagle et al., *supra* note 1, at 72 (emphasis added); *see also* GDPR, *supra* note 27, at art. 2.

[43] GDPR, *supra* note 27, at art. 4. "[P]ractically everything that can be done with personal data will be considered to be 'processing.'" Hoofnagle et al., *supra* note 1, at 72.

identify a person, and whether identification is possible now or in the future."[44]

Several other terms used in the GDPR merit definition. First, a "controller" is an entity that governs how personal data is used.[45] In contrast, a "processor" is an entity that performs the actual processing of personal data.[46] The difference between a controller and a processor is subtle, yet very important for understanding the GDPR's regulatory scheme.[47] An entity "processes" data when, for example, it collects, stores, uses, or deletes data.[48] A "recipient" is an entity to whom personal data is disclosed.[49] Any entity other than the data subject or anyone authorized to process data by the controller or processor is a "third party."[50] A controller's "main establishment" is its administrative headquarters within the EU or wherever decisions over the use of data are made.[51] A processor's main establishment is its administrative headquarters within the EU or, if the administrative headquarters are not within the EU, the location where the data processing covered by EU law takes place.[52]

The GDPR applies whenever personal data is processed "wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to

---

[44] Hoofnagle et al., *supra* note 1, at 72-73.

[45] GDPR, *supra* note 27, at art. 4. A controller is "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." *Id.* "'Controllers' are those who determine the purposes and the means of processing of personal data." Hoofnagle et al., *supra* note 1, at 73.

[46] GDPR, *supra* note 27, at art. 4. "'Processors are entities that do something with personal data on behalf of controllers." Hoofnagle et al., *supra* note 1, at 73.

[47] The difference between a controller and a processor can be illustrated using the following example: "[I]f company Y gathers and analyzes survey data on the customers of company X, as instructed by company X, company X is the controller and company Y the data processor." Hoofnagle et al., *supra* note 1, at 73.

[48] GDPR, *supra* note 27, at art. 4. The list of activities that constitute "processing" enumerated in the GDPR is "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." *Id.*

[49] *Id.* at art. 4(9) ("a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.").

[50] *Id.* at art. 4(10).

[51] *See id.* at art. 4(16)(a) ("the place of [the controller's] 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.").

[52] *See id.* at art. 4(16)(b) ("the place of [the processor's central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation.").

form part of a filing system."[53] One of the most important features of the GDPR is its territorial scope. The regulation applies "in the context of the activities of an establishment of a controller or a processor in the [EU]," even if the processing does not happen within the EU.[54] The fact that processors are included within the scope of the regulation is a significant change from the Data Protection Directive.[55] If a controller or processor is located within the EU, the GDPR applies, even if the data processing takes place outside of the EU.[56] Under certain circumstances, the GDPR's provisions will apply to controllers and processors located outside of the EU when they process data related to the offering of goods or services from subjects within the EU[57] or monitor the behavior of data subjects within the EU.[58] The GDPR's requirements follow the data, even if the data is processed outside of the European Union.[59]

B. Provisions of the GDPR

Article Five of the GDPR lists principles[60] designed to achieve the GDPR's objectives.[61] Article Five's principles can be summarized as "lawfulness, fairness and transparency;" "purpose limitation;" "data minimization;" "accuracy;" "storage limitation;" "integrity and confidentiality;" and "accountability."[62] It is the duty of a controller to

---

[53] GDPR, *supra* note 27, at art. 2(1). There are exceptions, notably for "a natural person in the course of a purely personal or household activity" and during criminal investigations or to protect public safety. *Id.* at art. 2(18); *see also* Hoofnagle et al., *supra* note 1, at 75-76. "'[F]iling system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis." GDPR, *supra* note 27, at art. 4.

[54] GDPR, *supra* note 27, at art. 3(1).

[55] *See* Burri & Schär, *supra* note 8, at 492-93, 495.

[56] *See id.* at 495-96; GDPR, *supra* note 27, at art. 3; Hoofnagle et al., *supra* note 1, at 68; Voss, *supra* note 36, at 222-34.

[57] This applies irrespective of whether any payment occurred. *See* GDPR, *supra* note 27, at art. 3(2).

[58] *Id.*; *see* Hoofnagle et al., *supra* note 1, at 74 ("[I]f an American company places tracking cookies on the computers of people in the EU, the GDPR will apply.").

[59] *See* GDPR, *supra* note 27, at art. 3; Voss, *supra* note 36, at 222-23; Burri & Schär, *supra* note 8, at 496; Hoofnagle et al., *supra* note 1, at 68, 74.

[60] GDPR, *supra* note 27, at art. 5

[61] *See* Burri & Schär, *supra* note 8, at 489. For the objectives of the GDPR, see *supra* text accompanying notes 32-34.

[62] *See* GDPR, *supra* note 27, at art. 5. According to Article Five, personal data must be

> (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
>
> (b) collected for specified, explicit and legitimate purposes…further processing for…purposes in the public interest, scientific or historical research purposes or statistical purposes shall…not be considered to be incompatible with the initial purposes ('purpose limitation');

ensure that its data practices fall within the coverage of the GDPR and comply with these principles.[63]

Article Six lays out the circumstances in which it is legal to process data.[64] The GDPR is a permissive regulation, meaning that, within the regulation's scope, the processing of personal data is banned except in those specific circumstances the statute allows.[65]

The first such circumstance is when the data subject has consented to the processing of their data.[66] The GDPR requires consent to be a "freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."[67] Unlike in the U.S.,[68] consent is not valid if the performance of a contract or fulfillment of a service is conditioned on obtaining consent for data processing unnecessary to the transaction or service.[69] If a data subject does consent to the processing of their personal data, a controller must still abide

---

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate[] [with] regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes…subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) 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 ('integrity and confidentiality').

Id. "Parts of the GDPR could be characterized as 'principles-based regulation.'" Hoofnagle et al., *supra* note 1, at 67.

[63] *See* GDPR, *supra* note 27, at art. 5(2); Peter H. Chase, Senior Fellow, German Marshall Fund of the U.S., Perspectives on the General Data Protection Regulation of the European Union, Remarks Before the Committee on Banking, Housing and Urban Affairs of the United States Senate, 5 (May 7, 2019).

[64] GDPR, *supra* note 27, at art. 6(1).

[65] *See id.* at art. 6(1)(a) ("Processing shall be lawful *only if* and to the extent that at least one of the [listed circumstances] applies.") (emphasis added).

[66] *Id.*

[67] *Id.* at art. 4(11).

[68] In the United States, consumers often must consent to a service provider's privacy policy or be denied service. Hoofnagle et al., *supra* note 1, at 79.

[69] GDPR, *supra* note 27, at art. 7(4). "The GDPR is "skeptical of U.S. lawyers' favorite tool: consent, particularly of the low-quality or 'take it or leave it' variety." Hoofnagle et al., *supra* note 1, at 68.

by the requirements of Article Five.[70] The second permissive circumstance is data processing necessary in the course of performing a contract involving the data subject.[71] Third, personal data processing is allowed when a controller must process personal data so as to comply with legal regulations.[72] Fourth, data processing may occur when necessary to "protect the vital interests of the data subject or of another natural person."[73] Fifth, data processing is allowed when required by public interest or within a controller's official authority.[74] Sixth, processing of personal data is allowed when it is for a legitimate interest of the controller.[75] While the GDPR is a regulation (and therefore binding on member states),[76] it empowers member states to adapt the requirements for certain provisions in Article 6.[77] Article Nine prohibits the processing of so-called "special categories of personal data," including race or ethnic origin; political affiliations, religious beliefs, or philosophical ideologies; union membership; genetic and biometric data; data related to health; and data regarding a person's sexual orientation.[78]

Chapter III of the GDPR enumerates the rights held by data subjects.[79] Article 12 requires a controller to share information in a transparent, clear, and intelligible manner when necessary, and to "facilitate the exercise of data subject rights under" other articles.[80] Articles 13 and 14 require the controller to share information when data is or is not collected.[81]

---

[70] *See* Hoofnagle et al., *supra* note 1, at 80.

[71] GDPR, *supra* note 27, at art. 6(1)(b). "The processing must be genuinely necessary to perform the contract for this basis to apply. To illustrate: if somebody orders a pizza, the pizzeria can give the customer's address (a piece of personal data) to the delivery person, because [it] is 'necessary' to deliver the pizza, and . . . perform the contract." Hoofnagle et al., *supra* note 1, at 80.

[72] GDPR, *supra* note 27, at art. 6(1)(c).

[73] *Id.* at art. 6(1)(d). This provision provides for the processing of personal data when said processing is necessary to protect a person's life. *Vital Interests*, INFO. COMM'R OFF., https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/vital-interests/ (last visited Nov. 8, 2020).

[74] GDPR, *supra* note 27, at art. 6(1)(e). For additional information, see *Public Task*, INFO. COMM'R OFF., https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/vital-interests/ (last visited Nov. 8, 2020).

[75] GDPR, *supra* note 27, at art. 6(1)(f). The provision states in full that processing is lawful when"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."

Id.

[76] Pyle et al., *supra* note 21, at 59.

[77] GDPR, *supra* note 27, at art. 6(2).

[78] *Id.* at art. 9(1). Article Nine has several exceptions, several of which mirror those found in Article Six. *See id.* at arts. 6(1), 9(2).

[79] *See id.* at Ch. III.

[80] *Id.* at art. 12.

[81] *Id.* at arts. 13-14.

Articles 15 through 21 describe the right of access,[82] the right of rectification,[83] the "right to be forgotten,"[84] the right to restrict processing,[85] the right to notification of data erasure,[86] the right to data portability,[87] and the right of a data subject to object to the processing of his or her data.[88]

Chapter IV details the obligations of controllers and processors.[89] First, a controller has the responsibility to ensure that its data processing is in compliance with the GDPR.[90] A controller also has the duty to ensure that it is adhering to the principles outlined in the GDPR[91] and enacting appropriate policies and measures to achieve those principles.[92] Additionally, a controller must ensure that only the necessary data from any particular user is processed when appropriate.[93] A controller may only use a process that will comply with the GDPR's provisions.[94] Processors cannot subcontract with other processors unless the controller consents.[95] Article 28 also provides for contractual governance of controller-processor relationships and specifies provisions to be included in those governing contracts, as well as other requirements.[96] Processors or third parties with access to personal data cannot process said data unless authorized to do so by the controller, unless the processing in question is required by law.[97] Article 32 requires controllers and processors to maintain appropriate security measures over data.[98] Such measures include pseudonymization and encryption, the ability to maintain data integrity, the ability to restore data after a "physical or technical incident," and processes for analyzing the adequacy of security measures already in place.[99] In the event of a data

[82] *Id.* at art. 15.
[83] *Id.* at art. 16.
[84] *Id.* at art. 17.
[85] *Id.* at art. 18.
[86] *Id.* at art. 19.
[87] *Id.* at art. 20.
[88] *Id.* at art. 21.
[89] *See id.* at Ch. IV.
[90] *Id.* at art. 24.
[91] *See id.* at art. 5.
[92] *See id.* at art. 25.
[93] *See id.*; *see also supra* text accompanying notes 63-66.
[94] *Id.* at art. 28(1).
[95] *Id.* at art. 28(2); *see also* Hoofnagle et al., *supra* note 1, at 73.
[96] *See* GDPR, *supra* note 27, at art. 28(3).
[97] GDPR, *supra* note 27, at art. 29.
[98] *Id.* at art. 32.
[99] *Id.* at art. 32(1). This list is non-exhaustive. *See id.*

breach,[100] a controller must notify supervisory authorities[101] and the affected data subjects.[102]

III. ADEQUACY DECISIONS AND DATA SHARING AGREEMENTS

Chapter V of the GDPR regulates the transfer of personal data to countries and entities outside of the European Union.[103] A transfer of data for processing is allowed only if the transfer complies with the GDPR's regulations.[104] The European Commission must determine that a third country or extra-EU organization has adequate protections in place to allow the transfer of personal data to occur;[105] these determinations are called adequacy decisions.[106] Adequacy decisions are made based on how comparable data protection measures offered by the receiving country are to those found in the EU (i.e., those found in the GDPR).[107]

The European Commission takes a variety of factors into account when making an adequacy decision, including any privacy and data protection

---

[100] "[A] breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed." *Id.* at art. 4(12).

[101] *Id.* at art. 33.

[102] *Id.* at art. 34.

[103] *See id.* at Ch. V.

[104] *Id.* at art. 44.

[105] *See id.* at art. 45; John Bowman, *Clock Ticks on Brexit Adequacy Decision*, INT'L ASS'N PRIV. PROS. (Oct. 27, 2020), https://iapp.org/news/a/clock-ticks-on-brexit-adequacy-decision/. The European Commission is the European Union's "executive arm." *European Commission*, EUROPEAN UNION, https://europa.eu/european-union/about-eu/institutions-bodies/european-commission_en (May 7, 2020). The Commission also has legislative functions such as proposing and drafting new laws, and judicial functions, notably resolving trade disputes between EU member-states. Clifford A. Jones, *European Commission*, ENCYCLOPEDIA BRITANNICA (June 5, 2017), https://www.britannica.com/topic/European-Commission. The Commission is composed of "Commissioners" nominated by each EU member-states, but charged with representing the interests of the European Union as a whole rather than the interests of member-states individually. *Id.*

[106] "An adequacy decision is a formal decision made by the EU which recognises that another country, territory, sector or international organisation provides an equivalent level of protection for personal data as the EU does." *Adequacy*, INFO. COMM'R OFF. https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-and-the-eu-in-detail/adequacy/ (last visited Feb. 4, 2022).

[107] *See, e.g.*, European Council Press Release, European Council (Art. 50) Guidelines on the Framework for the Future EU-UK Relationship (Mar. 23, 2018), https://www.consilium.europa.eu/media/33458/23-euco-art50-guidelines.pdf ("As regards personal data, protection should be governed by Union rules on adequacy with a view to ensuring a level of protection essentially equivalent to that of the Union."); Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information, 2019 O.J. (C/2019/304/) ¶3, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.076.01.0001.01.ENG&toc=OJ:L:2019:076:TOC; GDPR, *supra* note 27, at ¶104 [hereinafter Japan Adequacy Decision].

legislation in place, the existence of supervisory authorities, and whether the third country has entered any international agreements concerning data protection.[108] If, after considering the elements listed in Article 45, the Commission decides the third country, or a subdivision of that country, has adequate protections in place, it may adopt an "implementing act" to that effect.[109] Decisions that found adequate protections existed are relatively rare—only twelve localities have been deemed to have adequate data protections, including Canada, Japan, Israel, Switzerland, and New Zealand.[110]

If no implementing act has been adopted deciding that a third country has adequate protections in place, the only way a controller or processor can transfer data to that country is if they provide the appropriate safeguards themselves.[111] Notably, these safeguards include the use of contractual clauses,[112] wherein the controller and the entity within the third country

---

[108] *Id.* at art. 45(2). In full, article 45(2) lists the following elements the European Commission considers:

> (a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;
>
> (b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and
>
> (c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.
>
> *Id.*

[109] *Id.* at art. 45(3).

[110] Twelve localities have received adequacy decisions: Andorra, Argentina, Canada, the Faroe Islands, Guernsey, Israel, the Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay. *Adequacy Decisions: How the EU Determines if a non-EU Country Has an Adequate Level of Data Protection*, EUROPEAN UNION, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (last visited Jan. 14, 2021).

[111] *See id.* at art. 46.

[112] *See id.* at art. 46(3).

contract for the use of adequate security measures.[113] Other means by which a controller and third country entity can ensure adequate protections include corporate rules, approved certifications, and rules adopted by supervisory authorities in the receiving country.[114]

The GDPR gives a list of factors for consideration in Article 45(2)(a)-(c).[115] In simple terms, the European Commission analyzes the country in question's applicable data protection laws, enforcement mechanisms, and international obligations.[116] Subsection (a) focuses on the existence of "relevant legislation" and other laws or rules dealing with data protection, but also requires the existence of "the rule of law, [and] respect for human

---

[113] *See id.* at art. 46(3).

> [W]hen the data are transferred to an organization that is based in a non-EU country for which there is no adequacy decision, this will only be deemed legitimate when the organization in question contractually guarantees that it will uphold, within its organization, a level of data protection that is similar to the GDPR, including all of the material and procedural safeguards. Consequently, the data transferred to an organization in a non-EU country will still be under a similar level of protection as when they would have stayed on EU territory [sic].

Hoofnagle et al., *supra* note 1, at 84.

[114] *See* GDPR, *supra* note 27, at art. 46(2).

[115] *Id.* Article 45(2) reads in full as follows:

> 2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:
>
> (a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;
>
> (b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and
>
> (c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

Id.

[116] *See id.*

rights and fundamental freedoms."[117] Subsection (b) emphasizes "the existence of…independent supervisory authorities" that ensure compliance with data protection regulations.[118] These supervisory authorities should also have enforcement powers strong enough to allow data subjects to exercise their rights and to enable that agency to cooperate with the data protection agencies of EU member-states.[119] Subsection (c) instructs the Commission to examine the "international commitments" to which the third country is a party, especially any agreements that concern data protection and use.[120] If a country is found to meet the requisite criteria, the European Commission will issue an implementing act to establish that the country in question has adequate protections in place.[121] Without an adequacy decision in place, a third party can only receive personal data from the EU if the transfer of data has "appropriate safeguards."[122]

IV. THE JAPAN ADEQUACY DECISION

The European Commission's latest adequacy decision concerned Japan.[123] Released in 2019, it delineates an ideal example of the Commission's process. The Commission began by reviewing the applicable data protection legal framework in Japan.[124] First, the Commission reviewed the root of data protection and privacy laws in Japan, beginning with the

[117] *Id.* at art. 45(2)(a). Examples of laws besides those strictly concerning data protection that should be considered include those concerning national security and defense, criminal law, and case law. *Id.*

[118] *Id.* at art. 45(2)(b).

[119] *Id.*

[120] *Id.* at art. 45(2)(c).

[121] *Id.* at art. 45(3). However, that is not the end of the process. Any country that receives an adequacy decision (i.e. has been deemed to have adequate protection) must be reviewed again on an ongoing basis, with a maximum period of four years between reviews. *See id.* The purpose of these subsequent reviews is to examine and account for any relevant developments in the third country or elsewhere that "could affect the functioning of decisions adopted pursuant to paragraph 3 of [Article 45]." *Id.* at art. 45(4). If significant enough changes have occurred such that the country in question "no longer ensures an adequate level of protection within the meaning of paragraph 2 of [Article 45]," the Commission can revoke or change its previous adequacy decision. *Id.* at art. 45(5). The Commission is empowered to use an implementing act to "repeal, amend or suspend" the prior adequacy decision. *Id.* If this occurs, the Commission can work with the country to rectify any issues that caused the Commission to revoke the previous adequacy decision. *Id.* at art. 45(6).

[122] *Id.* at art. 46(1).

[123] Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information, 2019 O.J. (L 76), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.076.01.0001.01.ENG&toc=OJ:L:2019:076:TOC [hereinafter Japan Decision].

[124] Japan Decision, *supra* note 123, at § 2.1.

Constitution of Japan[125] and cases from the Supreme Court of Japan that held people have a right to avoid unnecessary disclosure of their private information to third parties.[126] The Commission next reviewed newer data laws passed in Japan, focusing especially on the Act on the Protection of Personal Information ("APPI") and subsequent amendments.[127]

In its decision, the European Commission transitioned from discussing the applicable regulatory scheme of Japan to reviewing its supervisory authorities.[128] The Personal Information Protection Commission ("PPC") is Japan's regulatory body charged with the supervision and regulation of the use of personal data.[129] The PPC has the power to review the records of entities it oversees, provide guidance and recommendations, and issue orders to enforce data protection regulations.[130] The Commission looked favorably on the establishment of the PPC, as well as other aspects of amendments to the APPI which "[brought] the Japanese data protection system closer to the European one."[131] The PPC fulfills the role of the "independent supervisory authority" described in the GDPR.[132] The Commission supported the Japanese Government's amendments to the APPI which gave the PPC enough regulatory power to sufficiently enforce the APPI and meet the supervisory authority standard,[133] including the PPC's power to protect individual rights.[134]

The European Commission also reviewed Japanese law to determine whether the Japanese regulatory scheme would apply to the relevant personal data of EU residents.[135] While the Japanese regulatory system differs from the GDPR, these differences did not dissuade the Commission from deeming the Japanese regulatory scheme an adequate protection, either because the differences were functionally irrelevant[136] or because distinctions made in Japanese law would not apply to data imported from

---

[125] *Id.* at ¶¶ 6-8.

[126] *Id.* at ¶ 7.

[127] Japan Decision, *supra* note 123, at ¶¶ 9-14.

[128] *Id.* at ¶¶ 15-16, § 2.4.

[129] *See, e.g.*, *id.* at ¶ 96; *Supervision*, PERS. INFO. PROT. COMM'N, https://www.ppc.go.jp/en/aboutus/roles/supervision/ (last visited Jan. 15, 2021); *Mission*, PERS. INFO. PROT. COMM'N, https://www.ppc.go.jp/en/aboutus/roles/ (last visited Jan. 15, 2021).

[130] Japan Decision, *supra* note 123, at ¶¶ 97-98.

[131] *Id.* at ¶ 11.

[132] GDPR, *supra* note 27, at art. 45(2)(b). The PPC operates independently, as described in the GDPR. *See* Japan Decision, *supra* note 123, at ¶ 97.

[133] *See* Japan Decision, *supra* note 123, at ¶¶ 13-16, 101-02.

[134] *See id.* at ¶100.

[135] *See, e.g.*, *id.* at §§ 2.2.1-2.2.7.

[136] *See, e.g.*, *id.* at ¶ 17. Japanese laws use the term "handling" rather than processing (as in the GDPR), but the definition of handling is broad enough to encompass similar activities, resulting in a functional equivalence. *See id.*

the European Union.[137] Additionally, "Supplementary Rules" adopted by the PPC were specifically designed to "enhance the protection of personal information transferred from the European Union to Japan."[138] Finally, the Commission tied its adequacy decision to the APPI, meaning transfers are approved if the transferred data would be covered by the APPI since it provides an adequate level of protection for personal data.[139]

The Commission then discussed several points that were drawn directly from the GDPR; specifically, Article Five was discussed in depth. The GDPR requires that data is collected and analyzed for "specified, explicit and legitimate purposes."[140] The APPI requires data processors to specify the purpose for which they are collecting data, and then forbids them from using the data for other purposes.[141] The APPI further prohibits a processor from inappropriately altering the purpose for which they collected the personal data and performing analysis unrelated to the purpose for which it was initially collected.[142] The Supplementary Rules also limit the purposes for which personal data originating in the European Union may be processed.[143]

Purpose limitation principles relate to other requirements of the GDPR, namely the lawfulness and fairness of processing.[144] In the EU, data will necessarily be collected in compliance with the GDPR,[145] including the purpose limitations found in Articles Five and Six.[146] As Japanese law requires processors to affirm the purpose for which they are processing personal data, the Japanese processor will have to confirm it is processing the data for the purpose for which it was collected within the EU, and will therefore have to abide by that purpose to lawfully process the data.[147]

---

[137] *See id.* at § 2.2.2. For example, data sent from the European Union would automatically qualify as the type regulated by the APPI by virtue of being sent electronically. *See id.* at ¶ 22.

[138] *Id.* at ¶ 15; *see also id.* at ¶¶ 30-31. For example, the Supplementary Rules provide for the PPC treating violations concerning data originating in the European Union as serious violations. *Id.* at ¶ 101.

[139] *See id.* at ¶ 38.

[140] GDPR, *supra* note 27, at art. 5(1)(b); *see also supra* note 65 and accompanying text.

[141] Japan Decision, *supra* note 123, at ¶¶ 39-40.

[142] *Id.* at ¶¶ 41-42.

[143] *Id.* at ¶ 43.

[144] *Id.* at ¶ 44. The requirements in both the GDPR and the APPI that a personal data processor or controller get consent from the data subject before, for example, processing data for a different purpose than it was originally collected for, also heavily factor in this discussion. For consent requirements in the GDPR, see, e.g., GDPR, *supra* note 27, at art. 6(1)(a); Japan Decision, *supra* note 123 at ¶ 40.

[145] *See* Japan Decision, *supra* note 123, at ¶ 48 ("[Regarding] transfers from the European Union, personal data will necessarily have been first collected and processed in the EU in compliance with [the GDPR].").

[146] *See id.*; GDPR, *supra* note 27, at art. 5-6.

[147] *See* Japan Decision, *supra* note 123, at ¶¶ 48-51.

The APPI also satisfies the data minimization requirement of the GDPR.[148] The APPI prohibits Japanese processors from collecting and using data beyond the scope of their intended processing, and further requires processors keep their personal data up to date in a manner reasonable for the data's intended use.[149] Both of these measures reflect those found the GDPR.[150] The storage limitations present in the APPI require personal data be deleted as soon as it is no longer necessary, satisfying the storage limitation requirement in the GDPR.[151] Japanese law also provides for the security of personal data in a way the European Commission deemed satisfactory under the GDPR.[152] Article Nine of the GDPR prohibits the processing of "special categories" of data, including race, religion, and sexual orientation data except in specified cases.[153] These categories are adequately reflected in the APPI, even if the terminology used is not identical.[154] The APPI satisfactorily holds Japanese processors accountable,[155] meeting the accountability principle.[156]

The European Commission next examined the individual rights available to data subjects under Japanese law.[157] The GDPR is greatly concerned with data protection as a personal right, explicitly stating that "[t]he protection of natural persons in relation to the processing of personal data is a fundamental right."[158] Under the GDPR, individuals have certain rights they may exercise regarding the collection and processing of their personal data.[159] The Commission found that the APPI and Japanese law granted enforceable individual rights to data subjects.[160] Significantly, some of the

---

[148] *See id.* at § 2.3.3. For a definition of data minimization, see *supra* note 62.

[149] *See* Japan Decision, *supra* note 133, at ¶¶ 53-54.

[150] The data minimization principle is found in Article 5(1)(c) of the GDPR. The accuracy requirement can be found in Article 5(1)(d) of the GDPR.

[151] *See* Japan Decision, *supra* note 133, at § 2.3.4; GDPR, *supra* note 27, at art. 5(1)(e).

[152] *See* Japan Decision, *supra* note 133, at § 2.3.5.

[153] GDPR, *supra* note 27, at art. 9(1)-(2). See *supra* note 81 and accompanying text for more on Article Nine special categories of personal data.

[154] *See* Japan Decision, *supra* note 133, at ¶¶ 66-68.

[155] *See id.* at § 2.3.8.

[156] GDPR, *supra* note 27, at art. 5(2) ("The controller shall be responsible for, and be able to demonstrate compliance with" the GDPR's requirements).

[157] *See* Japan Decision, *supra* note 123, at § 2.3.10.

[158] GDPR, *supra* note 27, at ¶ 1; *see also supra* text accompanying notes 7-11.

[159] *E.g.*, GDPR, *supra* note 27, at art. 15 (Right of access to information about the processing of a data subject's personal data); *id.* at art. 16 (Right to rectification of inaccurate personal data); *id.* at art. 17 (Right to erasure, also known as the right to be forgotten); *id.* at art. 18 (Right to restriction of processing under certain circumstances); *id.* at art. 20 (Right to data transportability, or the right to receive and send a data subject's own personal data); *id.* at art. 21 (Right to object to lawful processing).

[160] Japan Decision, *supra* note 133, at ¶ 81. Rights outlined in the adequacy decision itself include a "right to correction" of inaccurate data, a right to request the personal data held by a processor, a "right

enforceable individual rights granted under Japanese law are very similar, if not identical, to those contained in the GDPR.[161] While the rights granted under Japanese law are subject to some restrictions,[162] the Commission found those restrictions compatible with, and comparable to, European law.[163]

The Commission dealt with another difference between the APPI and the GDPR, the lack of ways to oppose "processing for direct marketing purposes,"[164] in the same way it dealt with purpose restrictions; while Japanese law might not meet the standards of the GDPR in this specific area, the fact that the data would be collected in the EU (combined with the APPI's purpose restrictions)[165] would give individuals sufficient means of redress.[166] Since the GDPR's regulations follow the data,[167] sufficient protections are in place even in areas where the APPI is inadequate. The Commission went on to examine the means of judicial redress and enforcement of these individual rights later in its decision.[168] "In order to ensure adequate protection and in particular the enforcement of individual rights, the data subject should be provided with effective administrative and judicial redress, including compensation for damages."[169] Under the APPI, individuals can submit their grievances directly to the controller.[170] The PPC can also provide mediation when a complaint is filed, as can local government services.[171] Data subjects can also lodge complaints with Japan's National Consumer Affairs Center.[172] If a processor or controller violates the APPI a data subject can seek an injunction or monetary damages

to utilisation cease," and the right to object to distribution of personal data to a third party. *See id.* at ¶¶ 82, 92.

[161] For example, the GDPR's right of access found in Article 15 is very similar to the APPI's right to request disclosure of identifying information as described in paragraph 82 of the Japan Decision. The GDPR's right to rectification (of inaccurate data) is like the APPI's "right to correction." *See* Japan Decision, *supra* note 133, at ¶¶ 81-82, 86.

[162] *Id.* at ¶ 84.

[163] *See id.* The three restrictions under Japanese law relate to individual or third party interests, "serious interference" in a processor's business, and violation of other laws. *Id.* The Commission drew parallels between these restrictions and those restriction on the exercise of individual rights enumerated in Article 23 of the GDPR, including restrictions based on national security, criminal investigations, judicial proceedings, and individual rights of other parties. GDPR, *supra* note 27, at art. 23(1).

[164] Japan Decision, *supra* note 133, at ¶ 89.

[165] *See supra* notes 150-57 and accompanying text.

[166] *See* Japan Decision, *supra* note 133, at ¶ 89.

[167] *See* GDPR, *supra* note 27, at art. 3; *supra* note 62.

[168] *See* Japan Decision, *supra* note 133, at § 2.4.2.

[169] *Id.* at ¶ 103.

[170] *Id.* at ¶ 104.

[171] *Id.*

[172] *Id.*

in civil actions based on tort law or the APPI itself.[173] Data subjects can also initiate criminal proceedings against a controller or processor for violations of the APPI.[174] Data subjects can also pursue several different remedies against the PPC itself.[175]

An important consideration for the Commission in making the adequacy decision about Japan was the amount of access the Japanese government would have to personal data originating in the European Union.[176] Japan has limits on the data collection done by its government, based on the Constitution of Japan and its national jurisprudence.[177] As previously discussed, Japan ensures that its citizens have a right to not have their data passed on to a third party without their consent.[178] The Japanese Constitution also contains provisions ensuring the security of persons in their papers and effects, requiring a court order based on "adequate cause" to conduct searches and seizures.[179] "Consequently, Japanese authorities have no legal authority to collect personal information by compulsory means in situations where no violation of the law has yet occurred."[180] The Japanese Constitution provides for the general secrecy of communications, and data collection as part of an investigation must be authorized by law.[181] The APPI also regulates and limits the Japanese government's collection and use of personal data.[182]

---

[173] *Id.* at ¶ 105-06. Civil actions include injunctions to disclose retained personal data, correct inaccurate personal data, or "to cease unlawful processing or [distribution to a] third party." *Id.* at ¶ 105.

[174] *Id.* at ¶ 108 ("[A] data subject may file a complaint with a public prosecutor or judicial police official with respect to APPI violations that can lead to criminal sanctions.").

[175] *Id.* at ¶¶ 109-12. Individuals can file administrative appeals, file lawsuits, or seek compensation by the state. *Id.* at ¶¶ 110-12.

[176] *Id.* at § 3, ¶ 113.

[177] *Id.* at ¶ 114.

[178] *Id.*

[179] *See id.* This provision is highly reminiscent of the Fourth Amendment to the United States Constitution. *See* U.S. CONST. amend. IV.

[180] Japan Decision, *supra* note 133, at ¶ 114.

[181] *Id.* at ¶ 115-16.

[182] *Id.* at ¶ 118. Under the APPI, the government

> (i) may only retain personal information to the extent this is necessary for carrying out their duties;
>
> (ii) shall not use such information for an "unjust" purpose or disclose it to a third person without justification;
>
> (iii) shall specify the purpose and not change that purpose beyond what can reasonably be considered as relevant for the original purpose [];

V. *SCHREMS II* AND THE U.S. PRIVACY SHIELD MEASURES

The Schrems cases arose when an Austrian law student, Max Schrems, began drawing attention to the amount of data U.S.-based social media website Facebook was collecting on its users.[183] After Edward Snowden leaked information about U.S. surveillance programs in 2013,[184] including the existence of the PRISM program run by the NSA,[185] Schrems lodged complaints with the Irish Data Protection Commission regarding the transfer of European Facebook users' data to Facebook servers located in the U.S.[186] and challenged the Safe Harbor Agreement, which allowed

> (iv) shall…not use or provide a third person with the retained personal information for other purposes and, if they consider this necessary, impose restrictions on the purpose or method of use by third parties;
>
> (v) shall endeavour to ensure the correctness of the information (data quality);
>
> (vi) shall take the necessary measures for the proper management of the information and to prevent leakage, loss or damage []; and
>
> (vii) shall endeavour to properly and expeditiously process any complaints regarding the processing of the information.

Id.

[183] *See* Kashmir Hill, *Max Schrems: The Austrian Thorn in Facebook's Side*, FORBES (Feb. 7, 2012, 10:03 AM), https://www.forbes.com/sites/kashmirhill/2012/02/07/the-austrian-thorn-in-facebooks-side/?sh=262ef9297b0b. While studying in the United States, Austrian law student Max Schrems attended a talk given by a privacy lawyer working for Facebook. *Id.* Appalled at the speaker's grasp of European data privacy law, Schrems requested his records from Facebook and received over 1200 pages of stored information, ranging from friend requests to chat records to accounts that had logged into Facebook from the same computer. *Id.* For more on the types of information kept by Facebook, see Kashmir Hill, *Facebook Keeps A History Of Everyone Who Has Ever Poked You, Along With A Lot Of Other Data*, FORBES (Sept. 27, 2011, 4:36 PM), https://www.forbes.com/sites/kashmirhill/2011/09/27/facebook-keeps-a-history-of-everyone-who-has-ever-poked-you-along-with-a-lot-of-other-data/?sh=15e7764eff6b.

[184] *See generally* Paul Szoldra, *This is Everything Edward Snowden Revealed in One Year of Unprecedented Top-Secret Leaks*, BUS. INSIDER (Sept. 16, 2016, 7:00 AM), https://www.businessinsider.com/snowden-leaks-timeline-2016-9; Lorenzo Franceschi-Bicchierai, *The 10 Biggest Revelations From Edward Snowden's Leaks*, MASHABLE (June 05, 2014), https://mashable.com/2014/06/05/edward-snowden-revelations/; Bryan Burrough, Sarah Ellison & Suzanna Andrews, *The Snowden Saga: a Shadowland of Secrets And Light*, VANITY FAIR (Apr. 23, 2014), https://www.vanityfair.com/news/politics/2014/05/edward-snowden-politics-interview.

[185] *See generally* Franceschi-Bicchierai, *supra* note 184; Timothy B. Lee, *Here's Everything We Know About PRISM to Date*, Wash. Post (June 12, 2013, 2:43 PM), https://www.washingtonpost.com/news/wonk/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/; Benjamin Dreyfus & Emily Dreyfus, *What is the NSA's PRISM Program? (FAQ)*, CNET (June 7, 2013, 11:44 AM), https://www.cnet.com/news/what-is-the-nsas-prism-program-faq/; Michael B Kelley, *The Best Explanation Yet of How the NSA's PRISM Surveillance Program Works*, BUS. INSIDER (June 15, 2013, 1:22 PM), https://www.businessinsider.com/how-prism-surveillance-works-2013-6.

[186] Letter from Maximilian Schrems to the Irish Data Protection Commissioner (June 25, 2013) (available at http://europe-v-facebook.org/EN/Complaints/complaints.html).

private data transfers to the U.S. under the Data Protection Directive, in court.[187]

The Safe Harbor Agreement was invalidated in *Schrems I* as the Court of Justice of the European Union (CJEU)[188] found the U.S. did not provide an adequate level of data protection under the terms of that agreement.[189] The U.S. and EU entered into the EU-US Privacy Shield in 2016 to replace the invalidated Safe Harbor Agreement.[190] In *Schrems II*, the CJEU was tasked with determining whether the Privacy Shield in fact provided adequate protections for European data subjects under the terms of the GDPR.[191] A main consideration in this determination revolved around the ability of the U.S. government to access the data of Europeans through intelligence and surveillance programs like PRISM.[192]

The decision in *Schrems II* was narrower in scope than the Japan Adequacy Decision. The CJEU focused its analysis of the protection offered by the U.S. around two major themes: the effectiveness of the U.S.'s oversight mechanisms and the judicial redressability of violations of EU subjects' rights.[193] The CJEU found that the U.S. did not have oversight mechanisms in place that were sufficient to ensure adequate protection,[194] nor did the U.S. ensure that individuals had the necessary means of redress for violations of their rights.[195] Because of these failures, the Privacy Shield did not meet the "essentially equivalent protection" requirement and was thus ruled invalid.[196]

The GDPR includes the existence of an independent body that supervises data protection laws as something to consider in making an adequacy

---

[187] *See* WEISS & ARCHICK, *supra* note 2, at 8-9; Case C-362/14, Maximilian Schrems v. Data Protection Commissioner, ECLI:EU:C:2015:650, (Oct. 6, 2015) [hereinafter *Schrems I*] (invalidating the Safe Harbor Agreement between the EU and the US).

[188] "The Court of Justice of the European Union (CJEU) interprets EU law to make sure it is applied in the same way in all EU countries, and settles legal disputes between national governments and EU institutions." *Court of Justice of the European Union (CJEU)*, EUROPEAN UNION, https://europa.eu/european-union/about-eu/institutions-bodies/court-justice_en (last visited Mar. 21, 2021).

[189] *See generally Schrems I*, *supra* note 187.

[190] *See* European Commission Press Release IP/16/2461, European Commission launches EU-U.S. Privacy Shield: Stronger Protection for Transatlantic Data Flows (July 12, 2016). For more on the adoption of the Privacy Shield, see WEISS & ARCHICK, *supra* note 2, at 8-11.

[191] *See* Case C-311/18, Data Protection Comm'r v Facebook Ireland Ltd. and Maximillian Schrems, ECLI:EU:C:2020:559, ¶ 1 (July 16, 2020) [hereinafter *Schrems II*]. Although the *Schrems* cases originally arose under the Data Protection Directive, the CJEU found that the questions before it could be analyzed using the GDPR. *Id.* at ¶¶ 77-79, 161.

[192] *See id.* at ¶¶ 165-68, 178; *see also supra* note 185 and accompanying text.

[193] These themes are drawn from GDPR art. 45. *See supra* note 115 and accompanying text.

[194] *See Schrems II*, *supra* note 191, at ¶ 197.

[195] *See id.* at ¶¶ 190-92.

[196] *Id.* at ¶ 201.

decision.[197] In an attempt to satisfy this condition under the Privacy Shield, the U.S. created an "Ombudsperson Mechanism" both as a means of oversight and to respond to privacy complaints.[198] The Ombudsperson was ostensibly politically independent and independent of the intelligence community in the U.S.; however, the CJEU had doubts as to how free from political influence the position would actually be due to its ties to the Executive branch.[199] The CJEU also doubted that the Ombudsperson Mechanism would have the necessary enforcement powers.[200] "There is nothing in that decision to indicate that that ombudsperson has the power to adopt decisions that are binding on those intelligence services and does not mention any legal safeguards that would accompany that political commitment on which data subjects could rely."[201] The Ombudsperson was insufficient as a supervisory body because it could not "ensur[e] and enforc[e] compliance" with the terms of the Privacy Shield.[202]

By comparison, the PPC fares better when examining both its independence and enforcement powers. The PPC *does* have the ability to compel compliance with the Japanese regulatory scheme, including in individual cases.[203] Additionally, the PPC has regulations helping it maintain independence, such as a ban on members engaging in political activities.[204] Another difference that may have weighed on the CJEU's view of the PPC's independence is that the PPC is composed of eight members, who are appointed by the Prime Minister and confirmed by the Diet.[205] Given the multiple members, and especially the involvement of the legislature in the selection process, one could reasonably conclude that Japan's enforcement body is less influenced by the executive branch than the single Ombudsperson working within the U.S. State Department. The CJEU also thought that the yearly reauthorization of surveillance programs was insufficient to satisfy the oversight requirement.[206] Finally, the PPC can create legally binding interpretations of law, while neither the

[197] GDPR, *supra* note 27, at art. 45(2)(b).
[198] *See* 2016 O.J. (L 207), at (116)-(118), annex III.
[199] *Schrems II*, *supra* note 191, at ¶¶ 194-97 (noting that the Ombudsperson would be appointed by the Secretary of State and a member of the U.S. State Department).
[200] The GDPR indicates that supervisory authorities should have "adequate enforcement powers." GDPR, *supra* note 27, at art. 45(2)(b).
[201] *Schrems II*, *supra* note 191, at ¶ 196.
[202] GDPR, *supra* note 27, at art. 45(2)(b).
[203] Japan Decision, *supra* note 23, at ¶¶ 14-16, 50, 97-100.
[204] *See id.* at ¶¶ 96-97.
[205] *Id.* at ¶ 96.
[206] *See Schrems II*, *supra* note 191, at ¶¶ 179-81.

Ombudsperson nor the other executive-branch-based protections had any binding effects on the U.S. government.[207]

The second major consideration of the CJEU in *Schrems II* was the availability of individual means of redress.[208] The Fourth Amendment to the U.S. Constitution[209] does not apply to Europeans, depriving them of one of the main avenues of challenging surveillance under U.S. law.[210] Furthermore, constitutional standing requirements[211] would present a substantial obstacle to efforts by Europeans to challenge surveillance measures.[212] The CJEU notes that the surveillance of data from European residents is subject to various limitations imposed by the executive.[213] However, those limitations did not give Europeans a means of enforcing their data protection rights.[214] Additionally, aspects of the U.S. surveillance program are not subject to judicial oversight.[215] The lack of judicial oversight is one reason the U.S. data protection measures are not essentially equivalent to EU protections.[216] While EU citizens could send complaints to the Ombudsperson, the lack of effective enforcement capabilities rendered such actions virtually pointless.[217] The lack of effective remedies for EU residents under the Privacy Shield is in stark contrast to the opportunities presented in the Japan Adequacy Decision. Unlike the U.S. Constitution, the APPI applies equally to EU citizens.[218] Also unlike in the U.S., violations of the APPI can lead to criminal actions as well as civil.[219] In Japan, Europeans can also bring actions under tort law to get injunctive relief.[220] Another major difference is that Europeans can bring actions against the PPC, while they would be unlikely to successfully sue the U.S.

---

[207] *See* Japan Decision, *supra* note 123, at ¶¶ 15-16, 98; *Schrems II*, *supra* note 191, at ¶¶ 180-92.

[208] *See* GDPR, *supra* note 27, at art. 45(2)(a) ("The Commission shall…take account of… effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred."); *Schrems II*, *supra* note 191, at ¶ 188.

[209] U.S. Const. amend. IV.

[210] *Schrems II*, *supra* note 191, at ¶ 65.

[211] *See generally* Lujan v. Defenders of Wildlife, 504 U.S. 555 (1992).

[212] *See Schrems II*, *supra* note 191, at ¶ 65.

[213] Particularly relevant are Exec. Order No. 12,333, 3 C.F.R. 200 (1981) and Presidential Policy Directive 28 (Jan. 17, 2014), https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

[214] *See Schrems II*, *supra* note 191, at ¶¶ 65, 180-197; *see generally* United States v. Verdugo-Urquidez, 494 U.S. 259 (1990).

[215] *See Schrems II*, *supra* note 191, at ¶ 65.

[216] *See id.* at ¶¶ 183-185.

[217] *See* Annex III, *supra* note 198; *Schrems II*, *supra* note 191, at ¶¶ 45, 195-97.

[218] *See* Japan Decision, *supra* note 123, at ¶ 34 ("As regards the beneficiaries of the protections set forth in the APPI, the Act makes no distinction based on an individual's nationality, residence or location. The same applies to the possibilities for individuals to seek redress, be it from the PPC or from courts.").

[219] *Id.* at ¶ 105; *see also supra* note 173 and accompanying text.

[220] *See id.* at ¶¶ 106-07.

government or a subdivision of it because of the doctrine of sovereign immunity.[221]

CONCLUSION

As demonstrated in this note, similar threads appear in both the Japan Adequacy Decision and in *Schrems II*. The Japan Decision was much broader in scope, which is appropriate for a "comprehensive analysis of the third country's legal order."[222] Yet it is still valuable to draw comparisons to the recent *Schrems II* decision as a means of analyzing shortfalls in the U.S. data protection regulatory scheme. As demonstrated, the U.S. is specifically and severely lacking means of redress for the violation of individual rights of non-U.S. citizens and lacks an effective overseer of data protection laws. Many solutions have been suggested, from life-tenured federal judge review boards to multi-national privacy treaties.[223] Whatever the solution, the U.S. needs to make changes to its data protection laws to avoid these serious conflicts with the European Union moving forward.

Nick Blue[*]

[221] *See id.* at ¶ 109-12; *Schrems II* (Opinion) at 446.

[222] Japan Decision, *supra* note 123, at ¶ 3.

[223] *See* Jennifer Bryant, Joseph Duball, & Ryan Chiavetta, *Industry Gauges Guture of Privacy Shield Replacement*, INT'L ASS'N PRIVACY PROS. (Mar. 11, 2021), https://iapp.org/news/a/industry-gauges-future-of-privacy-shield-replacement/; Ira Rubenstein & Peter Margulies, *Risk and Rights in Transatlantic Data Transfers: EU Privacy Law, U.S. Surveillance, and the Search for Common Ground*, (Feb. 18, 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3786415.

[*] Nick Blue is an Associate Staff Editor for the Washington University Global Studies Law Review and a J.D. Candidate at the Washington University School of Law (2022).