Europe and Japan towards the Future – the first post GDPR adequacy decision of the European Commission

Natascha Gerlach and Jan-Frederik Keustermans[1]

1. INTRODUCTION

On January 23 the European Commission announced the adoption of an adequacy decision regarding Japan,[2] the first adequacy decision since the entry into force on May 25, 2018 of 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" or "GDPR"). The process towards adequacy commenced long before the GDPR came into force, but was completed under GDPR and will be directional for future adequacy assessments not only for being the first decision under GDPR, but also the first in the continued wake of the Schrems ruling of the Court of Justice of the European Union on Safe Harbor, which recalibrated much of the European Commission's adequacy assessment process.[3]

At the same time of the European Commission's finding of adequacy regarding Japan, Japan recognized the adequacy of the European data protection regime creating, according to the Commission, the world's largest area of safe personal data flows.[4] These first reciprocal decisions about adequacy for personal data transfers are seen as complementing the EU-Japan Economic Partnership Agreement adding the free flow of data to the removal of duties, ease of regulatory burdens and sustainable development partnership,[5] creating a new dynamic for future economic relations between Japan and the European Union ("EU").

This paper will provide an overview of the adequacy mechanism and a brief outline of the EU-Japan Adequacy Decision itself.

---

1 Natascha Gerlach is a Senior Attorney at Cleary Gottlieb in their Brussels office and currently serves as Vice Chair The Sedona Conference Working Group 6 Steering Committee. Jan-Frederik Keustermans is an associate in the Brussels office of Cleary Gottlieb.

2 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 (hereinafter, the "EU-Japan Adequacy Decision"), available online at 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.

3 CJEU, Judgment of the Court (Grand Chamber) of October 6, 2015, *Maximillian Schrems v Data Protection Commissioner*, C-362/14.

4 European Commission, Press Release, "European Commission adopts adequacy decision on Japan, creating the world's largest area of safe data flows", January 23, 2019, available online at http://europa.eu/rapid/press-release_IP-19-421_en.htm.

5 European Commission, Press Release, "EU-Japan trade agreement on track to enter into force in February 2019", December 12, 2018, available online at http://europa.eu/rapid/press-release_IP-18-6749_en.htm.

2. CONTEXT: GDPR AND CROSS-BORDER DATA FLOWS

2.1 Restrictions on transferring personal data from within Europe

Under EU data protection law, a transfer of personal data[6] from within the European Economic Area ("EEA")[7] to a third country outside the EEA is prohibited, unless where the European Commission has issued an adequacy decision, appropriate safeguards are put in place by the transferor and recipient of the data, [8] or one of the derogations defined in Article 49 of GDPR applies.[9] Due to the significant administrative and compliance burden associated with putting in place appropriate safeguards and binding corporate rules and the narrow scope of the derogations in Article 49 of GDPR, [10] an adequacy decision represents an obvious and significant advantage for the ease of safe cross-border data flows.

2.2 Focus: European Commission adequacy decisions

2.2.1 Legal nature of adequacy decisions

An "adequacy decision" is an implementing act[11] taken by the European Commission in accordance with the procedure prescribed in Article 45(3) of GDPR pursuant to which a third country (*i.e.*, not a member state of the EEA), a territory or one or more specified sectors within a third country, or an international organization, is recognized as ensuring an adequate level of protection of fundamental rights, including the fundamental right to data protection as enshrined in the EU legal order.[12]

---

6 As defined in Article 4(1) of GDPR 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*."

7 The EEA is comprised of all EU members states, plus Norway, Liechtenstein and Iceland. The EEA Joint Committee, which is responsible for incorporating EU legislation into the EEA Agreement, did so for the GDPR in July of 2018.

8 Article 46 GDPR, including pursuant to so-called "standard contractual clauses", an approved code of conduct or certification mechanism, or where the transfer is a group-internal transfer subject to binding corporate rules adopted in accordance with Article 47 GDPR.

9 Subject to Article 48 of GDPR, in case the transfer is proposed to be done pursuant to a judgment of a court or tribunal and any decision of an administrative authority of a third country.

10 Article 49 GDPR is titled "Derogations for *specific situations*" with a high threshold to compliance.

11 In accordance with 291(2) TFEU and Regulation (EU) No 182/2011. During the legislative process leading up to GDPR, the European Parliament had suggested a delegated act would be more appropriate. The implementing act strengthens the European Commission's position in that later withdrawal of competencies are not possible, except by the Commission itself.

12 Adequacy was regulated by Article 25 of Directive 95/46/EC before. A major difference to the previous regime is the explicit catalogue listed in Article 45(2) of GDPR and the fact that territories, sectors and international organization are now specifically included. Adequacy decisions under the Directive covered the United States (Safe Harbor) (2000), Switzerland (2000), Canada (commercial organizations only) (2002), Guernsey (2003), Argentina (2003), the Isle of Man (2004), Jersey (2008), Andorra (2010), the Faroe Islands (2010), Israel (2011), Uruguay (2012) New Zealand (2013) and the United States (Privacy Shield) (2016). Note that although the Directive did not expressly provide for "partial" adequacy

An adequacy decision is binding on all EU member states and data protection authorities,[13] and transfers of personal data from an EU (and EEA) member state to a third country, territory, sector or organization covered by an adequacy decision do not require any additional data-transfer safeguards or authorizations under EU law, but must still comply with all requirements of GDPR that would also apply to intra-EU processing of personal data.[14]

2.2.2 Process of adequacy decisions

Before approval, the initial proposal for an adequacy decision, which would originate with the European Commission Directorate-General for Justice and Consumers (DG JUSTICE), has to undergo a multistep formal comitology procedure in line with Art. 45(3) and Art. 93(2) GDPR.[15] Before that, Recital 166 requires the Commission to involve expert level consultation when developing draft decisions. It also requires the Commission to send the relevant documents to the European Parliament and the Council.[16] Both the Parliament and the Council have a right to scrutiny under Article 11 of Regulation (EU) 182/2011, in accordance with which they can inform the Commission that a draft decision exceeds the implementing powers.[17]

In accordance with the comitology procedure, the Commission provides the draft decision to a committee consisting of competent representatives of the EU member states, who can approve the draft with a qualified majority, at which point the Commission can adopt the decision.[18]

The European Data Protection Board ("EDPB") representing the data protection authorities of each of the EU member states will also deliver an opinion on the draft decision in accordance with Article 70(1)(s) of GDPR.

---

decisions (*i.e.*, covering a subsection of a third country's jurisdiction), the adequacy decisions on Canada and the United States were in fact limited in scope, in the sense that the Canada adequacy decision applies only to private entities falling under the scope of the Canadian Personal Information Protection and Electronic Documents Act and the Privacy Shield framework applies only to companies committing to abide by the Privacy Shield principles. Pre-GDPR adequacy decisions remain in force until amended, replaced or repealed by the Commission in accordance with Article 45, sections (3) or (5) of GDPR.

13 Recital 103 GDPR.

14 In particular the key data protection principles set forth in Article 5 of GDPR, including the requirement to identify a legal basis for the processing (including transfer) of personal data (Article 6 of GDPR), transparency requirements and (where applicable) the obligation to enter into Article 26 GDPR joint controller arrangements or Article 28 GDPR controller-processor agreements.

15 In accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers.

16 The EU Parliament's Committee on Civil Liberties, Justice and Home Affairs ("LIBE") delivered a resolution on the draft decision before it was adopted, available online at www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+MOTION+B8-2018-0561+0+DOC+PDF+V0//EN&language=EN.

17 See also Pötters Handbuch DS-GVO, Art. 93 RN 7 (in German).

18 Paal/Pauly/Pauly DS-GVO Art. 93 RN 8 (in German); see Article 3 of Regulation (EU) No 182/2011 for the full procedure.

The formal process is in practice preceded by informal preliminary talks between representatives of the European Commission and the government of the third country in question. During those informal talks, parties discuss and negotiate in detail about the scope and provisions of the draft adequacy decision.

The European Commission must assess whether the jurisdiction under review provides "adequate" protection of fundamental rights, which is the relevant threshold the jurisdiction must meet in order to be eligible for an adequacy decision.[19] The CJEU defined in *Schrems* that the adequacy standard under EU data protection law requires the third country to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights "essentially equivalent" to that guaranteed in the EU legal order.[20] This standard was confirmed in Recital 104 of GDPR. The quest for "essential equivalence" does not mean that the data protection laws in the third country under review or the level of protection must be identical to those applicable and provided in the EU.[21] As the former Article 29 Working Party stated in its 2017 "Adequacy Referential" working document, "*the objective is not to mirror point by point the European legislation, but to establish the essential core requirements of that legislation*." [22] This obviously leaves margin for a practical assessment.[23]

The Commission will review and assess how a particular third country respects the rule of law, access to justice and international human rights norms and standards.[24] The Commission will also review the country's generally applicable and, where relevant, sectoral laws, as well as specific legislation

---

19 Article 45(1) and (2) of GDPR.

20 CJEU, Judgment of the Court (Grand Chamber) of October 6, 2015, *Maximillian Schrems v Data Protection Commissioner*, C-362/14, §§ 71,73, 74 and 96.

21 CJEU, *Schrems* (C-362/14), §73.

22 Article 29 Working Party, Working Document on Adequacy Referential (updated), WP254, adopted on November 28, 2017, available online at https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=57550, p. 3. The Adequacy Referential document, just like other key pre-GDPR Working Party opinions, was formally endorsed by the EDPB during its first plenary meeting on May 25, 2018, see https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_en.

23 For instance, although the Japanese data protection law's use of the word that translates to "handling" instead of "processing" (as used in GDPR) for example, the Commission stated that the concepts and scope of application of the Japanese law and GDPR are substantially identical (see Recital 17 of the EU-Japan Adequacy Decision). The fact that Japanese law does not distinguish between "controllers" and "processors", a key distinction under GDPR, was also not seen as disqualifying (see Recital 35 of the EU-Japan Adequacy Decision). Likewise, definitional discrepancies between "personal data" under GDPR and "personal information", "retained personal data" and "anonymously processed personal information" under the Japanese law was acceptable to the Commission, provided that the resulting scope of application of the Japanese law would in practice not be narrower than that of GDPR (see Recitals 18-31 of the EU-Japan Adequacy Decision), including through the adoption of certain supplementary rules to protection EU personal data as discussed in further detail below.

24 In particular whether or not the third country is a party to the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data and its Additional Protocol ("Convention 108"); see Recital 105 of GDPR.

concerning public security, defense, national security and public order and criminal law.[25]

Specific non-exclusive assessment criteria are set forth in Article 45(2) of GDPR and further guidance was provided by the Article 29 Working Party.[26] According to the Working Party, the two basic elements to be assessed by the Commission should be "*the content of the rules applicable and the means for ensuring their effective application*."[27] This two-pronged approach is fleshed-out by the Working Party through the enumeration of minimum "content principles" and "procedural and enforcement mechanisms" that the legal framework under investigation by the Commission must guarantee.[28] The Commission cannot rely on the review of written law,[29] but it must also take into account empiric evidence about the actual enforcement of, and compliance with, those laws in the jurisdiction being considered for adequacy. In line with the strengthening of independent data protection authorities in the EU under GDPR, the Commission will pay careful attention to the powers, governance and legal and operational independence of the competent data protection authority in the relevant jurisdiction, as well as to the possibilities for individuals to have access to effective judicial remedies directly (*i.e.*, without having to go through the data protection authority).

Finally, the Commission's assessment will also include a review of how the relevant jurisdiction's law enforcement and security agencies may collect and access personal data originating from the EU.[30]

2.2.3 Review and challenges of adequacy decisions

Pursuant to Article 45(5) of GDPR, the Commission must repeal, amend or suspend an adequacy decision if available information reveals that the relevant third country, territory, sector or international organization no longer ensure an adequate level of protection. This information can arise in the context of the mandatory periodic review of an adequacy decision in accordance with Article 45(3) of GDPR or because information is brought to the attention of the Commission through other channels by another EU institution (including the EDPB), a national data protection authority or individuals. If a lack of adequate protection is revealed, the Commission enters into consultations with the relevant third country or organization in order to try and remediate the

25 Recital 104 of GDPR.

26 *Ibid* footnote 22.

27 *Id.*, p. 3.

28 *Id.*, pp. 5-8. Additional content requirements apply to the processing of special categories of data (sensitive data), direct marketing activities and automated decision making and profiling.

29 Including more than just data protection legislation, but casting a wide net and assessing other areas of the law as well as norms not necessarily reaching the level of formal law, see Paal/Pauly/Pauly DS_GVO Art. 45, 4a (in German).

30 This third area of assessment has been increasingly relevant since the Snowden revelations and the CJEU's Schrems ruling.

situation.[31] In principle, if the Commission decides to repeal, amend or suspend an adequacy decision, it should provide for a phase-out period or other form of transition period in order not to disrupt ongoing data flows. In case of urgency, however, based on "duly justified imperative grounds", the Commission's decision to repeal, amend or suspend can be given immediate effect.[32] Because the Commission has never taken the formal step of repealing, amending or suspending an adequacy decision, it remains to be seen how these procedures would be applied in practice.

In addition to the Commission-driven procedure outlined above, Article 56(5) of GDPR requires that the competent data protection authorities of EU member states must be able to engage in effective legal proceedings under national law if they find a claim by a person against an adequacy decision well founded.[33] The most obvious context in which this can arise, as we have seen in *Schrems*, is where a data subject challenges a transfer of personal data implemented pursuant to an adequacy decision based on the argument that the adequacy decision itself is incompatible with GDPR or overarching principles of data protection and other fundamental human rights enshrined in the EU legal order.

3. THE EU-JAPAN ADEQUACY DECISION

3.1 Process and timeline

At the time GDPR was adopted in 2016, Japan and the EU had been in earnest trade talks since at least April 2010 with a view to entering into a comprehensive EU-Japan Economic Partnership Agreement (or EPA).[34]

Japan amended its domestic data protection laws in 2015 and the new laws entered into force on May 30, 2017, in the form of the updated Act on the Protection of Personal Information (Act No. 57, 2003 or "APPI"). On January 1, 2016, Japan established its own independent data protection authority, the Personal Information Protection Commission ("PPC"). These were major steps towards obtaining the EU adequacy decision.[35]

In parallel to the intensified negotiations with Japan, negotiations also started between the EU and South Korea with respect to a possible adequacy decision.[36]

---

31 Article 45(6) GDPR.

32 Article 45(5), second paragraph GDPR.

33 See also CJEU, *Schrems* (C-362/14), §65 ("*It is incumbent upon the national legislature to provide for legal remedies enabling the national supervisory authority concerned to put forward the objections which it considers well founded before the national courts in order for them, if they share its doubts as to the validity of the Commission decision, to make a reference for a preliminary ruling for the purpose of examination of the decision's validity*").

34 See, for example, Council of the European Union, Joint Press Statement for the 19th EU-Japan Summit, Tokyo, April 28, 2010, available online at https://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/en/er/114063.pdf.

35 Recitals 11-16 of the EU-Japan Adequacy Decision.

36 European Commission, Communication from the Commission to the European Parliament and the Council, "Exchanging and Protecting Personal Data in a Globalised World", January 10, 2017,

In December 2017, the European Parliament adopted a resolution urging the Commission to speed up the adoption of adequacy decisions with important trading partners of the EU such as Japan and South Korea.[37]

Then on May 25, 2018, the GDPR entered into force and became directly applicable across all EU member states.[38]

On June 15, 2018, as part of the pre-decision process, the PPC adopted certain "Supplementary Rules" under the APPI governing the processing of personal data transferred from the EU based on a European Commission adequacy decision.[39] The Japanese government also provided additional representations, assurances and commitments to the Commission about access to personal data by law enforcement and national security agencies in Japan.[40]

Pre-decision talks were essentially completed in July 2018 when the EU-Japan Economic Partnership Agreement was signed in Tokyo.[41] On September 5, 2018, the European Commission announced that the formal procedure to adopt the EU-Japan adequacy decision was launched in accordance with Article 45 of GDPR.[42] Upon completion, the European Commission formally adopted the EU-Japan adequacy decision on January 23, 2019 with immediate effect.

3.2 Content of the decision: Scope, justification and substantive provisions

It has to be noted, that the EU-Japan Adequacy Decisions does not cover any and all transfers of personal data between the EU and Japan. Although the scope of application is significantly broader in comparison to the EU-US Privacy Shield, similar to the EU-Canada Adequacy Decision, the processing of personal data by public sector entities (not falling within the scope of the APPI) is for instance not covered.[43] Additionally, personal data transferred to recipients falling within certain specifically enumerated categories (such as members of the press, professional writers, education

---

COM(2017) 7 final, available online at https://ec.europa.eu/newsroom/document.cfm?doc_id=41157, p. 8.

37 European Parliament resolution of December 12, 2017 on "Towards a digital trade strategy", available online at http://www.europarl.europa.eu/doceo/document/TA-8-2017-0488_EN.html?redirect (also expressly referring to the ongoing trade talks on the EU-Japan Economic Partnership Agreement).

38 Article 288 TFEU.

39 The Supplementary Rules are reproduced in Annex 1 to the EU-Japan Adequacy Decision.

40 These are included in Annex 2 to the EU-Japan Adequacy Decision.

41 European Commission, Press Release, "The European Union and Japan agreed to create the world's largest area of safe data flows", July 17, 2018, available online at http://europa.eu/rapid/press-release_IP-18-4501_en.htm; see also European Commission, Press Release, "EU and Japan sign Economic Partnership Agreement", July 17, 2018, available online at http://europa.eu/rapid/press-release_IP-18-4526_en.htm.

42 European Commission, Press Release, "International data flows: Commission launches the adoption of its adequacy decision on Japan", September 5, 2018, available online at http://europa.eu/rapid/press-release_IP-18-5433_en.htm.

43 Article 1(1) and Recital 10 of the EU-Japan Adequacy Decision.

institutions, religious and political bodies), are also not in scope.[44] The principal effect of the European Commission's adequacy decision for Japan is that the transfer of personal data from within the EU to "personal information handling business operators" (or "PIHBOs") in Japan that are subject to the APPI can take place subject to the legal requirements of the GDPR outside of Chapter V of GDPR.[45]

With respect to substantive protections, the Commission outlined its assessment of the adequacy of the Japanese framework in recitals 6 through 175 of the adequacy decision following along the guiding data protection principles of the GDPR and including the recent reforms to the APPI to move it closer to the European level of protection, including the establishment of an independent supervisory authority (the PPC), centralizing oversight.[46]

The Commission's primary areas of focus were to ensure that Japan would implement additional data protection safeguards by: (i) creating a set of rules providing individuals in the EU whose personal data are transferred to Japan with additional safeguards that will bridge several differences between the two data protection systems, binding on Japanese companies importing data from the EU and enforceable by the PCC and Japanese courts (*i.e.*, the Supplementary Rules), (ii) restricting access to EU personal data by Japanese public authorities for criminal law enforcement and national security purposes, ensuring that any such use of personal data would be limited to what is necessary and proportionate and subject to independent oversight and effective redress mechanisms, and (iii) creating a complaint-handling mechanism to investigate and resolve complaints from EU individuals.[47]

As highlighted by the European Commission, the APPI grants data subjects with a number of rights similar to those provided in GDPR, including a "disclosure" right (similar to access rights under GDPR) and rights to rectification, erasure and object to certain data processing activities.[48] Data subjects can submit a complaint to the equivalent of a controller (the relevant PIHBO) in the first instance or with so-called consumer centers established pursuant to the Japanese Consumer Safety Act, which are competent also for violation of the APPI.[49] This would trigger a mediation mechanism the Commission found to be effective.[50]

---

44 Article 1 (2) of the EU-Japan Adequacy Decision; These exceptions apply to the extent all or part of the purposes of processing of the relevant personal data corresponds to one of the purposes listed in Article 2 (*i.e.*, to the extent the relevant processing is done for the core activities of the relevant organizations) and not solely for another purpose (*e.g.*, a broadcasting institution processing personal data unrelated to its press purposes).

45 Article 1 of the EU-Japan Adequacy Decision.

46 Recital 11 of the EU Japanese Adequacy Decision.

47 European Commission, Press Release, "International data flows: Commission launches the adoption of its adequacy decision on Japan", September 5, 2018, available online at http://europa.eu/rapid/press-release_IP-18-5433_en.htm.

48 Recital 81 and following of the EU-Japan Adequacy Decision.

49 Recital 104 of the EU-Japan Adequacy Decision; it is not evident though, that they would be able to handle a complaint that is made in English or any other of the European languages.

50 Recital 104 of the EU-Japan Adequacy Decision.

Civil actions including damages and injunctive relief are also available under Japanese law for violation of the individual's rights[51] or the violation of general data protection principles or other obligations the PIHBO is subject to.[52] Violations of the APPI can lead to criminal sanctions and complaints with a public prosecutor can be filed by a data subject.[53]Finally, redress against decisions or inaction of the PPC is available where needed.[54]

Implementing rules can be issued based on the APPI, which include Enforcement Rules adopted by the PPC such as the "Supplementary Rules under the Act on the Protection of Personal Information for the Handling of Personal Data Transferred from the EU based on an Adequacy Decision" which form Annex I of the adequacy decision.[55] As a consequence, Japanese businesses receiving or otherwise processing personal data from the EEA will need to tag or keep separate such personal data from a technical and organizational perspective to be able to continue to identify the data throughout its "life cycle" and to ensure compliance with the Supplementary Rules.[56] This places an increased organizational compliance burden on undertakings processing data under the Supplementary Rules and it remains to be seen how this will be implemented practically by different types of businesses.[57]

The Supplementary Rules also further align Japanese law with GDPR rules on the key areas of (i) the processing of special categories of data ("sensitive data"), [58] (ii) data subject access rights, (iii) the principle of purpose limitation, (iv) restrictions on onwards transfers of EEA data from Japan to another third country jurisdiction not covered by an adequacy decision[59] and (v) the threshold for anonymization of data (*i.e.*, application of the high standard developed under EU law for personal data to be considered fully anonymized). These rules apply to personal data transferred from the EEA to Japan and are legally binding on Japanese businesses that are subject to the APPI, enforceable by the PPC and in Japanese courts.

---

51 Without the need for the individual to prove harm; see Recital 105 of the EU-Japan Adequacy Decision.

52 Recital 106 of the EU-Japan Adequacy Decision.

53 Recital 10 of the EU-Japan Adequacy Decision 8.

54 Recital 109 and following of the EU-Japan Adequacy Decision.

55 Recital 12 and Annex I of the EU-Japan Adequacy Decision.

56 Recital 15 of the EU-Japan Adequacy Decision.

57 For example, personal data transferred to a Japanese organization based on the EU-Japan Adequacy Decision shall continue to be governed by the processing purposes identified in the EU in accordance with GDPR and a change of that purposes under Japanese law at any stage of the further processing will require the Japanese organization to obtain the relevant EU data subject's consent (Supplementary Rule no. 3; see also Recital 43 of the EU-Japan Adequacy Decision).

58 Recital 68 of the EU-Japan Adequacy Decision.

59 However, onward transfers of personal data from Japan to a jurisdiction the PPC considers as offering adequate protection would be allowed even in the absence of an EU adequacy decision covering that onward-transfer jurisdiction. So far, the PPC has only recognized the EU itself as such a jurisdiction offering adequate protection and the European Commission has indicated that it will closely monitor any future adequacy decisions by the PPC and, if necessary, use its review and repeal powers under Article 45 GDPR, in accordance with Article 3(1) of the EU-Japan Adequacy Decision (see also, Recitals 79, 176, 177 and 184 of the EU-Japan Adequacy Decision).

Finally, the Commission particularly reviewed in great detail the access of data transferred from the EU to Japan by law enforcement and for national security purposes.[60] The Commission obtained the representation by the Japanese government forming Annex 2 to the EU-Japan Adequacy Decision regarding redress options,[61] including the assurance that a new redress mechanism would be created for handling and resolving complaints lodged by EU individuals in situations where personal data exported from the EU would be accessed by Japanese public authorities, to be executed and supervised by the PPC.[62]

3.3 The EDPB Review

As indicated earlier, the European Data Protection Board ("EDPB") provides an opinion to the European Commission on proposed adequacy decisions as part of the process foreseen by the GDPR.[63] The EDPB will identify possible insufficiencies in the proposed adequacy framework and, where applicable, propose changes to the draft adequacy decision to address these insufficiencies.[64]

Prior to the formal adoption of an opinion by the EDPB for the EU-Japan Adequacy Decision, the draft decision was already amended twice to address EDPB concerns. The amendments included in particular broadening the scope of categories of personal data that would be treated as sensitive data under the Supplementary Rules and clarifying that the Supplementary Rules themselves apply to all personal data transferred from the EU to Japan, irrespective of their retention period,which is the basis for a key distinction under the APPI as it applies to Japanese personal data.[65]

Another specific area of concern for the EDPB in their final opinion was the possibility for the PPC to authorize onwards transfers to third countries not covered by an EU adequacy decision.[66] This concern was partially addressed by the Commission in the final text of the EU-Japan Adequacy Decision by specifically referring to this possibility when describing its monitoring activities and the situations in which the Commission could consider repealing or suspending the EU-Japan Adequacy Decision.[67]

The EDPB noted that the effectiveness of judicial redress for EU citizens in Japan could be in question, including because the existing mechanisms were mostly available in

---

60 Recital 113 and following of the EU-Japan Adequacy Decision.

61 Annex II (II. C.) of the EU-Japan Adequacy Decision.

62 Annex II (5) of the EU Japan Adequacy Decision.

63 Article 70(1)(s) of GDPR.

64 Article 29 Working Party, Working Document on Adequacy Referential (updated), WP254, adopted on November 28, 2017, p. 4.

65 See European Data Protection Board (EDPB), Opinion 28/2018 regarding the European Commission Draft Implementing Decision on the adequate protection of personal data in Japan, adopted on December 5, 2018, available online at https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-282018-regarding-european-commission-draft_en, p. 5.

66 *Id.*, pp. 6 and 18-21.

67 Recital 181 of the Adequacy Decision

Japanese only.[68] Only the practical application will show how effective the options Annex II of the decision now affords will be, including the PPC led complaint handling.

The EDPB voiced other substantial concerns, including the challenges in effectively monitoring the practical implementation of the Supplementary Rules in Japan as well as the precise legal value of the Supplementary Rules in the Japanese legal system as interpreted by Japanese courts,[69] that may not have been fully addressed by the final adequacy decision.

Another important concern potentially remaining regards the APPI not containing generally applicable provisions on the right to object to automated processing and decision making.[70] The Commission stated in the recitals to the adequacy decision that these are addressed in sectoral rules, [71] but it is unclear how the protection offered under APPI is essentially equivalent to GDPR in this respect if not all organizations that are subject to APPI are subject to these sectoral restrictions on automated processing. The Commission argues, that as regards personal data collected in the EU, any decision based on automated processing will typically be taken by a data controller in the EU (so subject to GDPR) and not in Japan. [72] It remains to be seen whether this will be the case and whether this consideration can be a sufficient standard for essential equivalence.

Finally, the EDPB emphasized the importance of this first adequacy decision under the GDPR and the fact that the decision was not just based on Japanese data protection law but further supplementary rules, the practicability of which has to be assessed going forward.[73]

In light of these substantial concerns, Article 3(4) of the adequacy decision sets the first review of the decision at the two-year mark, a suggestion adopted from the EDPB[74] to gain clarity on the progress of practical and operational implementation of the only recently adopted new privacy rules in Japan, with the possible consequences set out in Article 3(5) of the decision.

4. NEXT STEPS

As indicated above, the EU-Japan Adequacy Decision will undergo its first periodic Commission review after two years, [75] at which point the Commission shall decide

68 EDPB Opinion 28/2018, p. 6.

69 *Id.*, pp. 5-6 and 10-12.

70 EDPB Opinion 28/2018, §§116-120.

71 Recital 93 of the EU Japan Adequacy Decision.

72 Recital 94 of the EU Japan Adequacy Decision.

73 EDPB Opinion 28/2018, §§ 41-44.

74 EDPB Opinion 28/2018, §§ 30, 56.

75 Article 3(4) EU-Japan Adequacy Decision; The review shall involve representatives of the EDPB, in consultation with the PPC, and its result shall be made public in a report to be submitted by the Commission to the European Parliament and the European Council (see Recitals 180-183 of the EU-Japan Adequacy Decision).

whether a two-year-cycle for periodic review should be maintained or whether a review at least every four years should suffice.[76]

The Commission has indicated that it will in any event continuously monitor any changes to the Japanese legal framework and compliance by the Japanese authorities with the representations, assurances and commitments provided in Annex 2 to the EU-Japan Adequacy Decision.[77]

The reciprocity of the EU-Japan Adequacy decision leads to interesting questions with respect to the influence of future adequacy decision either side may make with respect to onward transfers.[78]

Looking to the future, a possible South Korea adequacy decision remains dependent on amendments to South Korean data protection laws the Commission will likely require before initiating the formal adequacy decision procedure.[79] The expectation is that, following those reforms, South Korean law will have become essentially equivalent to EU law in its entirety, irrespective of the source of personal data or the identity or sector of the undertakings processing the data, meaning that there may not be a need for "supplementary rules" attached to a South Korea adequacy decision that create a two-track data protection framework like the one created by the EU-Japan Adequacy Decision. [80]

The Japan adequacy decision as well as the ongoing negotiations with South Korea also show the importance of the region for the EU (and vice versa) and the increasing role the protection of personal data and the fundamental rights of data subjects continue to play in the context also of economic relations.[81]

---

76 This decision shall be made in accordance with the same comitology procedure that applies to the adoption of the adequacy decision itself; see Article 45(3) GDPR; Article 3(4) and Recital 181 EU-Japan Adequacy Decision.

77 Article 3(1) and Recital 177 of the EU-Japan Adequacy Decision.

78 With access to the data by national security agencies playing a determining role. This may, for instance, influence adequacy considerations for the UK after the ECoHR Big Brother Decision, *Case of Big Brother Watch and Others v. The United Kingdom* (Applications nos. 58170/13, 62322/14 and 24960/15).

79 Amendments to South Korea's four main data protection laws have already been introduced in November 2018, see Greenleaf, Graham, *Japan and Korea: Different Paths to EU Adequacy* (December 10, 2018), (2018) 156 Privacy Laws & Business International Report, p. 10. One point of discussion appears to be the independence of the South Korean government agency charged with enforcing applicable data protection laws.

80 Note that South Korea had previously applied for a more narrow adequacy decision on a parallel track, covering only the digital communications industry, which, if granted by the European Commission, would have become the first sector-specific adequacy decision under EU data protection law. For that purpose, South Korea amended its Act on the Promotion of IT Network Use and Information Protection (Network Act) in December 2018; See also Greenleaf, Graham, *Japan and Korea: Different Paths to EU Adequacy* (December 10, 2018), (2018) 156 Privacy Laws & Business International Report, p. 10.

81 The Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CP-TPP) signed in March 2018 also recognized the importance of the unhindered flow of (electronic) data for electronic commerce and with it the confidence of the consumer in e-commerce (Article 14.2).