EUROPEAN
COMMISSION

Brussels, 3.4.2023
SWD(2023) 75 final

COMMISSION STAFF WORKING DOCUMENT

Accompanying the document

Report from the Commission to the European Parliament and the Council

on the first review of the functioning of the adequacy decision for Japan

{COM(2023) 275 final}

1. INTRODUCTION

This document presents the findings of the Commission services regarding the first evaluation of the functioning of the Commission's implementing decision of 23 January 2019 pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information (the adequacy decision or the decision). The findings are based on information gathered in the review meeting on 26 October 2021, as well as its preparation and follow-up. Among others, it covers input from the Japanese authorities, relevant stakeholders and publicly available material.

2. THE ADEQUACY DECISION

In the adequacy decision, the Commission found that, for the purposes of Article 45 of Regulation (EU) 2016/679[1] ("GDPR"), Japan ensures an adequate level of protection for personal data transferred from the European Union (Union or EU) to so-called "businesses handling personal information"[2] in Japan[3]. Consequently, data transfers from the EU to Japan that fall within the scope of the decision are permitted under EU data protection law without additional requirements[4].

The adequacy decision covers the Act on the Protection of Personal Information (APPI), as complemented by the Supplementary Rules set out in Annex I of the decision, together with the representations and assurances contained in Annex II of the decision. The latter concern the limitations and safeguards as regards access by Japanese public authorities to the personal data transferred.

The APPI was enacted in 2003 and significantly reformed in 2017[5]. The 2017 reform strengthened existing safeguards but also introduced a number of new safeguards, thus bringing the Japanese data protection system closer to that in the EU. This comprised, for instance, the inclusion of a set of enforceable individual rights and the establishment of an independent supervisory authority – the Personal Information Protection Commission (PPC) – entrusted with the oversight and enforcement of the APPI[6].

To allow for the adoption of the adequacy decision, Japan put in place a limited number of additional safeguards. Based on Article 6 of the APPI and a Cabinet Decision, the PPC on 15 June 2018 adopted a set of Supplementary Rules with a view to further strengthen the

---

1 OJ L 119, 4.5.2016, p. 1.

2 In the version of the APPI that applied at the time of the adoption of the adequacy decision, this notion was referred to as "personal information handling business operator" (PIHBO). A business handling personal information is defined in Article 16(2) of the amended APPI as "a person that uses a personal information database or the equivalent for business", with the exclusion of the government and administrative agencies at both central and local level. The notion of "business" under the APPI is very broad in that it includes not only for-profit but also not-for-profit activities by all kinds of organisations and individuals. Moreover, "use for business" also covers personal information that is not used in the operator's (external) commercial relationships, but internally, for instance the processing of employee data. See recitals 32-34 of the decision.

3 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, OJ L 76, 19.3.2019, p. 1.

4 See Article 45 GDPR and recital 5 of the decision.

5 The amended APPI was promulgated on 9 September 2015 and came into force on 30 May 2017.

6 Recitals 9-11 of the decision.

protection of personal information transferred from the Union to Japan. The objective of these "Supplementary Rules" was to bridge certain relevant differences between the APPI and the GDPR, and thus to guarantee that EU individuals whose personal data is transferred from the Union enjoy a level of protection essentially equivalent to that of the GDPR. These additional safeguards strengthen, for example, the protection of sensitive data (by enlarging the categories of personal information considered sensitive data), the exercise of individual rights (by clarifying that individual rights may also be exercised for personal data held for a shorter period than six months, which at the time was not the case under the APPI)[7] and the conditions under which EU data can be further ("onward") transferred from Japan to another third country[8]. These Supplementary Rules are binding on Japanese operators importing data from the Union and can be enforced by the PPC or, directly by EU individuals, in the Japanese courts[9].

The Japanese government furthermore provided official representations, assurances and commitments to the Commission regarding limitations and safeguards as regards access to, and use of, personal data by Japanese public authorities for criminal law enforcement and national security purposes, clarifying that any such processing is limited to what is necessary and proportionate and subject to independent oversight and effective redress mechanisms[10]. These redress mechanisms include a specific dispute resolution procedure, administered and supervised by the PPC, that the Japanese government has created for EU individuals whose personal data is transferred based on the adequacy decision[11].

3. THE FIRST REVIEW – BACKGROUND, PREPARATION AND CONSULTATION OF STAKEHOLDERS

To regularly verify that the findings in the Commission's adequacy decision are still factually and legally justified, the decision provides for its periodic review based on all available information[12]. In this regard, it is important to note that, since the adoption of the adequacy decision, Japan has significantly amended the APPI on two occasions.

On 5 June 2020, the Japanese Parliament (Diet) adopted the *Amendment Act of the Act on the Protection of Personal Information of 2020* (2020 APPI amendment)[13]. The 2020 APPI amendment, which reflects the outcome of the first triennial review of the APPI (conducted by the PPC), strengthens the law in several areas. The amended APPI has fully entered into force on 1 April 2022 alongside an amended *Cabinet Order to Enforce the Act on the Protection of Personal Information* (Cabinet Order) and the amended *Enforcement Rules for the Act on the Protection of Personal Information* (Enforcement Rules)[14]. Both the amended Cabinet Order and Enforcement Rules were published on 24 March 2021. Furthermore, in August 2021 the

---

7 In the meantime, the 2020 APPI amendment has revised the definition of "personal data the business holds" so that it no longer excludes those personal data that are "set to be deleted" within a period of six months (Article 16(4) of the amended APPI). See hereafter section 4.1.1.1. In the version of the APPI that applied at the time of the adoption of the adequacy decision, this notion was referred to as "retained personal data".

8 Recitals 26, 31, 43, 49-51, 63, 68, 71, 76-79, 101 of the decision.

9 Recital 15 of the decision.

10 Recitals 113-170 of the decision.

11 Recitals 141-144, 149, 169 of the decision.

12 Recitals 180-183 and Article 3(4) of the decision.

13 An English translation is available at: https://www.ppc.go.jp/files/pdf/APPI_english.pdf

14 Order of the Personal Information Protection Commission No. 3, 2016.

PPC published updated versions of different PPC Guidelines, reflecting the changes made to the APPI by the 2020 APPI amendment.

On 12 May 2021, the *Act on the arrangement of related acts for the formation of a digital society* (hereafter "2021 APPI amendment") was adopted by the Diet[15]. The 2021 APPI amendment consolidates the APPI, the Act on the Protection of Personal Information Held by Administrative Organs (APPIHAO), and the Act on the Protection of Personal Information Held by incorporated Administrative Agencies, etc. (APPI-IAA) into one single data protection law that applies to both private entities and public authorities, while expanding the jurisdiction of the PPC accordingly. The amended APPI has fully entered into force on 1 April 2023, after parts of it already entered into force on 1 October 2021 and 1 April 2022. Unless stated otherwise, references to the amended APPI in this report refer to the version of the amended APPI that applies as of 1 April 2023[16].

Following the amendment of the APPI, Japan has had to revise the Supplementary Rules, to adapt them to the new text, for example because of changes in the numbering (see hereafter sections 4.1.1.1 and 4.1.1.3). These (technical) changes were introduced in close consultation with the Commission services. In addition, Japan has agreed to insert a new Supplementary Rule on pseudonymized personal information, to further clarify the application of the rules applying to this new data category (see hereafter section 4.1.1.4). The revised Supplementary Rules have been adopted on 15 March 2023 and entered into force on 1 April.

The Commission's review, which covers all aspects of the adequacy decision, has put particular emphasis on assessing the impact of these important legal developments.

To prepare the first review, the Commission services gathered information from the Japanese authorities on the functioning of the decision, in particular the implementation of the Supplementary Rules. Furthermore, the Commission services obtained additional information on the functioning of the decision and relevant developments in Japanese law and practice, both as regards the data protection rules applicable to private operators and with respect to government access, from public sources and local experts. The Commission services did not receive any information from the Member States pursuant to Article 2 and Article 3(2)-(3) of the adequacy decision.

After having analysed the input received and the additional information gathered, the Commission services met with the three representatives designated by the EDPB to take part in the review meeting[17] to further prepare the review and gather input on their experience with the functioning of the adequacy decision.

The review meeting took place on 26 October 2021. On the Japanese side, representatives of the PPC, the Ministry of Internal Affairs and Communications, the Ministry of Justice, the Ministry of Defence and the National Police Agency participated in the review. The EU

[15] See the press release, published by the Diet, available (in Japanese only) at: https://www.sangiin.go.jp/japanese/ugoki/r3/210512.html.

[16] An English translation is available at: https://www.japaneselawtranslation.go.jp/ja/laws/view/4241.

[17] The EDPB was represented at the review meeting by a representative from the *Österreichische Datenschutzbehörde* (Austrian data protection authority) and two representatives of the *Bayerisches Landesamt für Datenschutzaufsicht* (state protection authority for the German state of Bavaria), including its president.

delegation included the three representatives designated by the EDPB, alongside members of the European Commission services.

The review was organised by topics, each covering both the EU adequacy decision for Japan and the Japanese decision for the Union recognising the Union as providing an equivalent level of protection to the one guaranteed in Japan[18]. It covered the "commercial" aspects of the Japanese framework and issues relating to government access to personal data.

Further to the review meeting, the Commission and the PPC had several exchanges to follow-up on points that were discussed at said meeting and, in particular, to address the questions raised by the introduction in the APPI of rules on pseudonymized personal information.

Finally, the three EDPB representatives have been consulted on this document and provided feedback on the findings.

4. THE FIRST REVIEW – FINDINGS

4.1 COMMERCIAL ASPECTS

The following sections present the Commission services' findings with regard to the "commercial aspects" of the adequacy decision (i.e. the data protection rules applicable to businesses handling personal information). The Commission services' review of these aspects has in particular focussed on the impact of the 2020 and 2021 APPI amendments on the rights and obligations afforded to EU individuals (whose personal data is transferred from the Union) under Japanese law (section 4.1.1). In addition, the Commission services have evaluated whether the Supplementary Rules – which were enacted to offer enhanced protection to EU individuals when their personal data is transferred to Japan based on the adequacy decision – are functioning in the way that is envisaged in the decision (section 4.1.2). Finally, the Commission services have assessed relevant developments in the Japanese legal framework on oversight and enforcement since the adoption of the adequacy decision (section 4.1.3).

4.1.1 Relevant developments in the Japanese legal framework

In its adequacy decision, the Commission considered that the APPI, as complemented by the Supplementary Rules (and together with the representations and assurances contained in Annex II of the decision), ensures a level of protection for personal data transferred from the Union that is essentially equivalent to the one guaranteed by the GDPR[19]. As will be discussed in the following sections, the 2020 and 2021 APPI amendments have enhanced the level of protection guaranteed by the APPI in several important areas (data subject rights, principles of lawfulness and data security, restrictions on onward transfers, oversight and enforcement), and in this way also further increased the degree of convergence between the EU and Japanese data protection systems. At the same time, the 2020 APPI amendment has introduced a new

[18] In accordance with Article 28(1) APPI, the PPC may designate a foreign country as such when that country "has established a personal information protection system recognized to have equivalent standards to that in Japan regarding the protection of individual rights and interests". The effect of this designation is that a business operator in Japan may, without prejudice to the derogations set forth in Article 27(1) APPI, transfer personal data to said country without first having to obtain the data subject's consent to the transfer. See recital 77-78 of the decision.

[19] Recital 171 of the decision.

category of personal data – pseudonymized personal information– with a special data protection regime. As explained in more detail below, given the limited scope of application of this regime only with respect to processing for statistical purposes (which has been expressly clarified in the revised text of the Supplementary Rules), this does not put into question the adequacy finding.

4.1.1.1 Strengthening of data subject rights

The 2020 APPI amendment includes a number of important changes to the provisions governing the content and scope of the rights of data subjects, with the effect of strengthening these rights.

A first important change concerns the **scope of data subject rights** guaranteed by the APPI. Under the amended APPI, these rights now apply irrespective of the length of the period after which the personal data is scheduled to be deleted.

The scope of application of the data subject rights guaranteed by the APPI is closely connected, within the law's framework, to the notion of "personal data the business holds"[20]. Before the 2020 APPI amendment, this notion, as then defined in Article 2(7) of the APPI in conjunction with Article 5 of the Cabinet Order, excluded those personal data that are "set to be deleted" within a period of six months. While this exemption aimed at incentivising businesses handling personal information to retain and process data for the shortest period possible, it also directly affected the availability of data subject rights[21]. To ensure that EU data subjects would not be deprived of important rights for no other reason than the duration of the retention of their data by the concerned business handling personal information, Japan put in place a Supplementary Rule (Supplementary Rule (2)), requiring that personal data transferred from the Union shall be considered as "personal data the business holds" irrespective of the period within which it is set to be deleted[22].

The 2020 APPI amendment has revised the definition of "personal data the business holds" so that it no longer excludes those personal data that are "set to be deleted" within a period of six months[23]. The Japanese legislator has thus codified the former Supplementary Rule (2) (which has consequently been revoked). As a result of this change, every data subject (irrespective of nationality or residence) now benefits from the enhanced protection offered by the former Supplementary Rule (2). The Commission services welcome this change, which shows how the Japan adequacy decision has contributed to further convergence between the Union and the Japanese data protection framework.

Another important change brought by the 2020 APPI amendment concerns the strengthening of the **right of access** ('disclosure'), set out in Article 33 of the amended APPI (previously

[20] See Article 16(4) APPI. In the version of the APPI that applied at the time of the adoption of the adequacy decision, this notion was referred to as "retained personal data". Which rules of the APPI apply to the processing of personal data by a PIHBO depends on the category of "personal information" (Article 2(1) APPI) into which the data falls. In this regard, the APPI draws an important distinction between "personal data" in general and "personal data the business holds". Certain provisions of the APPI, notably Articles 32 to 35 relating to individual rights, apply only to this latter category. See recitals 23, 25-26 of the decision.

[21] Recital 25 of the decision.

[22] Recital 26 of the decision.

[23] Article 16(4) of the amended APPI.

Article 28). Under the amended APPI, the scope of the right of access is extended to so-called "records of provision to a third party". These are records that a business handling personal information is required to maintain of the personal data it has shared with and received from third parties[24]. Pursuant to Article 33(5) of the amended APPI, a data subject has the right to request from a business handling personal information the disclosure of such records[25]. This makes it easier for the individual to track the flow of his/her personal data, and to exercise his/her rights against the further recipients of such data.

The amended APPI furthermore gives the data subject more control over the methods of disclosure of his/her personal data. Previously, Article 28(2) of the APPI provided that, following a request for disclosure, a business handling personal information should disclose personal data the business holds to a data subject without delay "pursuant to a method prescribed by Cabinet Order". In turn, the Cabinet Order specified that such disclosure should be performed in writing, unless the business handling personal information and the data subject agree otherwise[26]. The new Article 33(2) APPI emphasises the data subject's freedom of choice by prescribing that disclosure shall take place "pursuant to a method the principal demands". The new provision is also more attuned to the modern digital society in that it guarantees the data subject's right to require disclosure by way of "electromagnetic record", which can in turn facilitate data portability[27]. Based on Article 33(2) of the amended APPI and the updated

[24] Based on Articles 30(1) and 30(3) the amended APPI and the updated Enforcement Rules, the record kept about data shared with a third party through the opt-out procedure pursuant to Article 27(2) of the APPI must contain the "date when the personal data was provided; the name and address of the third party and, in the case of a legal entity, the name and address of its representative; the name of the individual identified by the personal data and other matters sufficient to identify the individual" and the "items of personal data concerned". In case the data was shared based on the consent of the individual in accordance with Article 27(1) or 28(1) APPI, the record must contain the fact "that the consent of the person referred to in Article 27(1) or Article 28(1) of the Act has been obtained", "the name and address of the third party and, in the case of a legal entity, the name and address of its representative, the name of the individual identified by the personal data and other matters sufficient to identify the individual, and the items of personal data concerned". The record kept about data received from a third party must, where the data was provided through the opt-out procedure pursuant to Article 27(2) APPI, contain "the date on which the personal data was received; the name and address of the third party and, in the case of a legal entity, the name and address of its representative; the circumstances of the acquisition of the relevant personal data by the third party; the name of the individual identified by the personal data and other matters sufficient to identify the individual; the items of personal data concerned" and the fact that the PPC has been notified of the data sharing in accordance with that provision. In case of data that was provided on the basis of consent, the record about data received from a third party must contain the fact that "the consent of the person referred to in Article 27(1) or Article 28(1) of the Act has been obtained; the name and address of the third party and, in the case of a legal entity, the name and address of its representative; the circumstances of the acquisition of the relevant personal data by the third party; the name of the individual identified by the personal data and other matters sufficient to identify the individual; and the items of personal data concerned". See PPC Guidelines (Obligation to check and record at the time of provision to a third party), Chapter 4-2.

[25] This right is subject to certain exceptions prescribed by Cabinet Order. According to the PPC Guidelines, these exceptions apply in cases where (1) there is a risk of harm to life, body, property, or other rights and interests of the individual or a third party (e.g. when a record contains content indicating that the patient has an intractable disease, and disclosure of the record provided is likely to aggravate the patient's physical or mental condition), (2) there is a risk that the disclosure of the records will significantly impede the proper execution of the business of the PIHBO (e.g. when the same person repeatedly requests disclosure of the same information that requires a complex response, and there is a risk of significant business disruption, such as when the inquiry counter is effectively occupied and other inquiry response operations cannot be performed). See PPC Guidelines (General Rules), Chapter 3-8-3-3.

[26] See recital 83 of the decision.

[27] Article 33(1) and (2) of the amended APPI.

Enforcement Rules, the data subject thus has a right to choose between disclosure of his/her records by (1) electromagnetic records, (2) written documents, or (3) by a method other than (1) or (2) (e.g., audio data) as specified by the business handling personal information[28].

Finally, the 2020 APPI amendment has reinforced the **right to object** ('ceasing to use or deleting personal data'), now set out in Article 35 of the amended APPI (previously Article 30). Based on this provision a data subject has the right to request a business handling personal information that it ceases to "use or delete" the personal data the business holds on a number of grounds[29]. Under the amended APPI, this catalogue of grounds for which a data subject may object to the processing of his/her personal data has been significantly expanded. Previously, the right to object could only be invoked where the personal data was processed in violation of the old Article 16 APPI (regarding purpose limitation), Article 17 APPI (regarding acquisition by deceit, other improper means or, in case of sensitive data, without consent), or Articles 23(1), 24 APPI (regarding third party provision, including international transfers)[30]. The 2020 APPI amendment has introduced new grounds for the data subject to object to the processing of his/her personal data when "it has ceased to be necessary for the business to use that personal data" or when a data breach "likely" posing a risk to the rights and interests of data subjects has occurred[31]. Based on the amended PPC Guidelines, the use of information by a business handling personal information "has ceased to be necessary" when the purpose of use[32] has been achieved (namely, when there is no longer a rational reason to retain the information for such purpose, or when the business itself has been discontinued)[33].

Moreover, based on the new provision, the data subject, in addition, has the right to request from a business handling personal information that it ceases to use or delete the personal data that the business holds in case the processing of the personal data "is likely to harm the identifiable person's rights and interests"[34]. Following such a request, the business handling personal information must in principle cease the use of, or erase, the personal information unless in the specific circumstances of the case the rights and interests of the principal are outweighed by an overriding interest[35]. As an example of a situation where the processing of the data must be ceased, the updated PPC Guidelines mention the case where a business handling personal information is not taking sufficient security measures and there is thus the risk of a data breach. Another example, mentioned in the PPC Guidelines, is the case where an individual keeps receiving e-mails or calls from a business handling personal information for marketing purposes based on the use of his/her contact details, despite having requested to stop such e-mails or calls[36]. Thereby, the amended APPI, as interpreted in the updated PPC

---

[28] In certain cases, however, disclosure must be performed in writing, for instance if disclosure in electromagnetic form would require a costly expenditure or prove otherwise difficult. When the personal data does not exist or disclosure by a method of the data subject's choice is difficult, the PIHBO must inform the data subject immediately thereof. See Article 33(2) and (3) of the amended APPI.

[29] See recital 87 of the decision.

[30] See recital 87 of the decision.

[31] Article 35(5) of the amended APPI.

[32] In the version of the APPI that applied at the time of the adoption of the adequacy decision, this notion was referred to as "utilization purpose".

[33] PPC Guidelines (General Rules), Chapter 3-8-5-1.

[34] See Article 35(5) of the amended APPI.

[35] See PPC Guidelines (General Rules), Chapter 3-8-5-1.

[36] PPC Guidelines (General Rules), Chapter 3-8-5-1.

Guidelines, for the first time creates the possibility to oppose data processing for direct marketing purposes. In addition, according to explanations provided by the PPC, the use of personal data for profiling purposes will be regarded as an improper or harmful way of processing when it is discriminatory or interferes with an individual's rights or interests in an unlawful or otherwise unjustifiable manner.

The new grounds to request from a business handling personal information that it ceases to use or delete the personal data the business holds apply in addition to the already existing grounds for the exercise of this right. As was the case previously, when the request is founded, the business handling personal information must without delay discontinue the use of the data (including by deleting it), or the provision to a third party, to the extent necessary to remedy the violation[37]. If one of the exceptions applies (notably if the utilisation cease would cause particularly high costs), the business handling personal information must implement necessary alternative measures to protect the rights and interests of the individual concerned[38]. According to the interpretation developed in the updated PPC Guidelines, these alternative measures may vary depending on the circumstances, but in any case must address the threat of an infringement of the individual's rights and interests that has arisen, and contribute to the protection of those rights and interests (e.g., when the data subject requests the erasure of data that must be retained based on applicable laws and regulations, a solution might be for the business handling personal information to commit to the deletion of such data as soon as the mandatory retention period has expired)[39].

Finally, in drafting the 2020 APPI amendment, Japanese policymakers have sought to respond to concerns regarding (fully) automated processing of personal data, including profiling and where this involves the analysis of data for decision-making. Although the amended APPI (like the old APPI) does not contain a dedicated provision on automated individual decision-making, the PPC has explained that several of the changes made to the APPI aim to address these concerns. These include the new possibility for data subjects to object to the processing of their data when that processing "is likely to harm the identifiable person's rights and interests". They also include the new prohibition on processing personal data in an inappropriate way that may facilitate illegal or improper action (see below)[40]. In addition, with regard to the obligation for businesses handling personal information to specify the purpose of use of the personal information they have collected (Article 17(1) APPI), the updated PPC Guidelines clarify that "when analysing information such as behaviour and interests regarding the individual from information obtained from the individual, the business operator handling personal information must specify the purpose of use to the extent that the individual can predict or assume what type of handling is being performed"[41]. In any event, as regards personal data that has been collected in the Union, any decision based on automated processing will typically be taken by

[37] Article 35(6) of the amended APPI.

[38] Article 35(6) of the amended APPI. See footnote 55 of the decision for examples of requests requiring "a costly expenditure" or that would otherwise prove "difficult", and for examples of "necessary alternative measures".

[39] PPC Guidelines (General Rules), Chapter 3-8-5-3.

[40] According to explanations received from the PPC, an example of such inappropriate use would be "when the outcome of profiling is used for illegal discriminatory purposes against the individual, or used to illegally or unjustifiably infringe on one's rights and interests".

[41] PPC Guidelines (General Rules), Chapter 3-1-1.

the data controller in the Union (which has a direct relationship with the concerned data subject) and is thus subject to the GDPR[42].

4.1.1.2 Reinforcement of the obligations applying to businesses handling personal information

The 2020 APPI amendment includes new prohibitions and obligations for businesses handling personal information, reinforcing the principles of lawfulness and data security.

First, concerning the lawfulness principle, businesses handling personal information are now **prohibited from processing personal data in an inappropriate way that may facilitate illegal or improper action**. Previously, the old Article 17 APPI already provided that a business handling personal information shall not acquire personal information by deceit or other improper means. In addition, this provision stipulated that a such a business shall not acquire certain categories of data (such as sensitive data) without the consent of the data subject. The 2020 APPI amendment has enhanced these existing protections by adding a specific safeguard against the inappropriate (further) use of the collected personal data[43]. Based on the new Article 19 APPI, a business handling personal information is not allowed to utilize personal information in such a way "that there is a possibility of fomenting or inducing unlawful or unjust act". According to the interpretation developed in the updated PPC Guidelines, an "unlawful or unjust act" means an act that violates the APPI or other laws and regulations or that, although not strictly illegal, is considered contrary to public order or morals. Examples of such unlawful or unjust acts include, among others, the provision of personal information to an entity that is suspected of engaging in illegal activities, or the discriminatory use of personal information collected during recruitment and selection procedures (e.g. discrimination based solely on grounds of gender or nationality)[44].

Second, concerning the data security principle, businesses handling personal information are now subject to a newly introduced **duty to report data breaches.** Previously, there was no legal obligation under the APPI to report data breaches, although a number of businesses handling personal information – for instance those who are member of an "accredited personal information protection organisation" (Article 47 APPI) such as the JIPDEC[45] – participated in voluntary schemes to notify the PPC and affected data subject(s) of data breaches and to take necessary action[46]. In accordance with the new Article 26 APPI, businesses handling personal information are required to notify promptly both the PPC and concerned data subjects of any data breach (defined as "leaks, loss, or damage and other situations concerning the security of

[42] Recital 94 of the decision.

[43] Article 19 of the amended APPI.

[44] PPC Guidelines (General Rules), Chapter 3-2. According to explanations provided by the PPC, profiling can also be regarded as an improper or harmful way of using personal information within the meaning of the amended APPI, when it is used for illegal discriminatory purposes against an individual, or used to illegally or unjustifiably infringe an individual's rights or interests.

[45] As explained on the organisation's website, "JIPDEC" is the organisation's official English name, and not an acronym. When it was established in 1967, JIPDEC was an acronym for "Japan Information Processing and Development Center", however when it changed its Japanese name in 2011, "JIPDEC" became its official English name.

[46] See recital 73 of the decision.

personal data they handle") that is "likely to harm individual rights and interest"[47]. In that case, the data subject furthermore has the right to object to the further use of his/her data[48].

The types of data breaches that meet the "high" risk threshold, and thus trigger a notification obligation, are described in the amended Enforcement Rules as those which involve, or potentially involve: (i) sensitive personal data[49], (ii) financial injury caused by unauthorised usage of the data (e.g. leakage of credit card numbers from an e-commerce site), (iii) acts carried out for an "improper purpose" (e.g. personal data is encrypted by ransomware and cannot be recovered)[50], or (iv) a large number (more than a thousand) affected data subjects[51]. Furthermore, the amended Enforcement Rules stipulates the required content of a data breach notification[52]. For example, the report on a data breach to the PPC must inter alia contain information about the types of personal information and number of data subjects (possibly) affected by the breach, and the existence (or risk) and nature of "secondary" damage caused by the data breach (i.e. damage linked to the breach, such as financial consequences following from the leakage of credit card numbers)[53]. A notification to the data subject is not required when "it is difficult to inform a principal and when necessary alternative action is taken to protect a principal's rights and interests"[54]. According to the updated PPC Guidelines, this is for example the case when the personal data subject to the breach does not include the contact information of the affected data subject(s), and the only option is therefore to make the details of the breach known through public notice[55].

When a business handling personal information has outsourced the processing of personal data to an "entrusted person" or trustee (see Article 25 APPI), in principle both that business and the trustee must notify the PPC and the affected data subject(s), which they can do through a

---

47 In accordance with Article 6-3(1) and (2) of the updated Enforcement Rules, PIHBOs that are under a duty to report a data breach to the PPC must first notify the PPC of the breach by promptly filing a preliminary report, followed by a more detailed confirmation report that must be filed within 30 or 60 days from the date of discovery of the breach. According to the interpretation provided in the updated Guidelines for the Act on the Protection of Personal Information (General Rules), Chapter 3-5-3-3, the notion of "promptly" submitting the preliminary report depends on each individual case, but generally means within three to five days from the moment of discovery. Besides, the PIHBO must also "promptly" notify the concerned data subject. According to Chapter 3-5-4-2 of the updated Guidelines for the Act on the Protection of Personal Information (General Rules), this requires that notification be provided promptly, taking into consideration the details of the situation known at the time, the probability that the rights and interests of the individual will be protected by providing notification, and possible adverse effects on the individual of doing so.

48 Article 35(5) of the amended APPI. See Section 4.1.1.1. above.

49 In the version of the APPI that applied at the time of the adoption of the adequacy decision, this notion was referred to as "special care-required personal information".

50 According to explanations received from the PPC, this means a situation where an outsider has committed a data breach with a malicious intent (e.g. the data was stolen by a cybercriminal). In such a situation, the risk of the rights and interests of the data subject being infringed is considered to be higher than in cases where the data breach is caused by the negligence of the business operator.

51 PPC Guidelines (General Rules), Chapter 3-5-3-1.

52 PPC Guidelines (General Rules), see Chapter 3-5-3-4 as regards the information to be contained in the report to the PPC and Chapter 3-5-4-3 as regards the information to be provided in a notification to the data subject.

53 PPC Guidelines (General Rules), Chapter 3-5-3-3. In addition, the notification shall include: (1) a description (overview) of the breach, (2) information on the underlying causes, (3) status and nature of communications to affected data subjects, (4) whether and how the breach has been publicized, (5) measures implemented to prevent any recurrence, and (6) any additional measures that may serve as a useful reference.

54 Article 26(2) of the amended APPI.

55 PPC Guidelines (General Rules), Chapter 3-5-4-5.

joint report. However, the trustee may also choose to notify the outsourcing business handling personal information, in which case the trustee is exempted from the duty to report the data breach directly to the PPC and the affected data subject(s)[56].

4.1.1.3 Restrictions on onward transfers

The 2020 APPI amendment has strengthened the existing obligations of businesses handling personal information that transfer data from Japan to a third country, thereby enhancing the protections afforded in case of so-called 'onward transfers' (i.e. the further transfer of personal data 'imported' from the EU to recipients in a third country outside Japan). These changes, which are discussed in more detail below, bring the Japanese regime for international transfers closer to the transfer regime of Chapter V of the GDPR. This is especially the case with respect to transfers for which the Japanese data exporter has implemented measures that ensure the continuation of protection.

First, the 2020 APPI amendment has reinforced the requirements for (onward) transfers that are based on the prior consent of the data subject (the default requirement for transfers under the APPI).

Previously, the old Article 24 APPI did not specify which information data exporters are required to provide to the data subject in advance to obtain his/her consent for the transfer. To ensure that in case of onward transfers of data, originally received from the Union, such consent is particularly well informed, the EU and Japan had agreed as part of their adequacy talks to certain enhanced requirements for informed consent that were subsequently reflected in Supplementary Rule (4) (now Supplementary Rule (3)). More specifically, Supplementary Rule (4), as formulated at the time of the adoption of the decision, required that the concerned individual shall be "provided [with] information on the circumstances surrounding the transfer necessary for the principal to make a decision on his/her consent". On that basis, businesses handling personal information in Japan were required to inform the data subject of the fact that the data will be transferred abroad (outside the scope of application of the APPI) and of the specific country of destination. This was meant to allow the individual to assess any risks for privacy linked to the transfer[57].

The 2020 APPI amendment has essentially **codified the enhanced requirements for informed consent laid down in the old Supplementary Rule (4)**. Based on the new Article 28(2) APPI, together with the updated Enforcement Rules[58], the Japanese data exporter is now required to inform the data subject in advance about the name of the third country[59], the data protection framework of that country and the measures taken by the recipient in the third country to protect the data received. According to the interpretation developed in the updated PPC Guidelines, the information must be provided "in a manner that is easy to understand" and must enable the data subject to "reasonably recognize" the "essential differences" between that

[56] Article 26(1) of the amended APPI.
[57] Recital 76 of the decision.
[58] See Article 17(2) of the Enforcement Rules.
[59] If the PIHBO cannot identify the third country at the time of obtaining consent from the data subject for the transfer (e.g., a Japanese pharmaceutical company cannot identify the country responsible for the final approval of the medical research it is conducting when a doctor tries to obtain consent from a data subject), it must make this clear and provide explanations to the data subject, see Article 17(3) of the Enforcement Rules.

framework and the APPI, so that (s)he can better predict the risks associated with the transfer[60]. The guidelines notably specify that, to this end, the data subject must be informed of, *inter alia*, "the presence of third country legislation that, compared to the APPI, may have a significant impact on the rights and interests of the individual" (e.g. the existence of an obligation for businesses to cooperate extensively with government requests for personal data, or the existence of data retention rules that may prevent the data importer from fulfilling a request from a data subject to erase personal data)[61]. This to some extent mirrors requirements under EU data protection law as regards the assessment of possible risks stemming from (disproportionate) government access[62].

The codification of the enhanced requirements for consent that used to be part of Supplementary Rule (4) is a welcome development, as it reinforces the protections afforded to transfers based on consent (as the default requirement for data transfers under the APPI) and extends these enhanced protections to all data subjects, irrespective of whether personal data has been transferred from the EU or collected in Japan.

Second, the 2020 APPI amendment has strengthened the requirements for (onward) transfers that are not based on the consent of the data subject.

As explained in the adequacy decision, the consent of the data subject is not the only ground for (onward) transfers within the Japanese legal framework. Several exceptions to this default requirement exist[63]. To ensure continuity of protection in case of personal data transferred from the Union to Japan under the adequacy decision, Supplementary Rule (3) (previously Supplementary Rule (4)) enhances the level of protection for onward transfers of such data by the business handling personal information to a third country recipient. It does so by limiting and framing the bases for international transfers that can be used by the business as an alternative to consent. More specifically, personal data transferred under the decision may be subject to (onward) transfers without consent only in two cases: (i) where the data is sent to a third country which has been recognised by the PPC under Article 28 of the APPI (previously Article 24 APPI) as providing an equivalent level of protection to the one guaranteed in Japan; or (ii) where the business handling personal information and the third party recipient have together implemented measures providing a level of protection equivalent to the APPI, read together with the Supplementary Rules, by means of a contract, other forms of binding agreements or binding arrangements within a corporate group[64].

---

60 PPC Guidelines (Provision to a third party located in a foreign country), Chapter 5 and 5-2.

61 Other elements about which the data subject must be informed, depending on the circumstances of the transfer, include: (a) the presence or absence of a data protection framework in the third country; (b) the existence of objective indicators of the level of data protection in the third country (e.g. whether the county benefits from an EU adequacy decision); (c) the existence of obligations for the business operator (e.g. purpose limitation), and of data subject rights (e.g. right of access), corresponding to the eight principles set out in the OECD Privacy Guidelines (e.g. the "purpose specification", "use limitation", "security safeguards" and "individual participation" principle"). The OECD's Privacy Guidelines were first endorsed in 1980 and revised in 2013. They are available at: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188.

62 See Case C-311/18, *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems* ("Schrems II").

63 Recital 77 of the decision.

64 Recital 78 of the decision.

The 2020 APPI amendment has **strengthened the requirements that apply to data exporters relying on such 'equivalent measures'** to frame their (onward) transfers. Under the amended APPI, data exporters that, together with the third-party recipient, have implemented measures providing an equivalent level of protection, are required to take the "necessary measures" to ensure "continuous implementation" of the resulting obligations by the recipient, and, in response to a data subject's request, provide information about these measures[65]. In this regard, the updated Enforcement Rules specifies that the data exporter must periodically check the content of the measures taken by the third-party recipient, as well as their status of implementation[66], and assess (by an "appropriate and reasonable method") the existence of any foreign laws that might negatively affect compliance. In accordance with the interpretation developed in the updated PPC Guidelines, examples of such 'problematic' legislation include laws containing an obligation for businesses to cooperate extensively with foreign public authorities requesting access to personal data, or requirements for business operators to store personal data in the third country (i.e. data localisation), which could lead to a situation where the business operator is unable to respond to a request for deletion from a data subject. The updated PPC Guidelines furthermore clarify that the existence of such 'problematic' legislation may, for instance, be assessed by making inquiries to the foreign recipient or by periodically checking relevant information published by Japanese or foreign public authorities[67].

In case the implementation of the equivalent measures is no longer ensured, the updated Enforcement Rules prescribes that the data exporter must take "necessary and appropriate measures" to rectify the situation[68]. According to the interpretation developed in the updated PPC Guidelines, this is the case, for example, when the foreign recipient of the personal data processes that data in violation of its duties set out in the contract[69]. If it becomes "difficult" to ensure the continued implementation of the equivalent measures, the Enforcement Rules prescribes that provision of personal data to the recipient in the foreign country must be stopped[70]. Examples of such "difficult" situations, as mentioned in the updated PPC Guidelines, include cases where, after a serious data breach at the recipient's end, the latter fails to take the necessary and appropriate measure to prevent a similar data breach from occurring again. Another example that is mentioned in the Guidelines concerns the case where the recipient handles the transferred personal data in violation of the contract or binding agreement, and such violation is not remedied within a reasonable period, despite the Japanese data exporter requesting the recipient to do so[71].

Following a request from the data subject for information about the equivalent measures, the Enforcement Rules, as interpreted by the PPC Guidelines, specifies that the data exporter must

---

65 Article 28(3) of the amended APPI.

66 Article 18 of the Enforcement Rules. In accordance with the interpretation developed in the updated PPC Guidelines, "periodically" here means approximately once a year or more frequently than that. The method chosen by the data exporter to monitor the implementation of the measures taken by the recipient (e.g. audits) must be "appropriate and reasonable" in light of the content and scale of the personal data to be transferred. See PPC Guidelines (Provision to a third party located in a foreign country), Chapter 6-1.

67 See PPC Guidelines (Provision to a third party located in a foreign country), Chapter 6-1.

68 Article 18(1) of the Enforcement Rules.

69 PPC Guidelines (Provision to a third party located in a foreign country), Chapter 6-1.

70 Article 18(1) of the Enforcement Rules.

71 PPC Guidelines (Provision to a third party located in a foreign country), Chapter 6-1.

provide the data subject with information about these equivalent measures[72]. Such information shall concern in particular:

- the instrument setting out the measures ensuring a level of protection equivalent to the APPI (e.g. a data processing agreement).
- the measures to be implemented by the recipient under that instrument (for cases of entrustment, the PPC Guidelines mention as an example the provision of information to the effect that "personal data is handled within a range of specified utilization purposes, improper utilization is prohibited, necessary and proper safety control measures are taken, necessary and proper supervision of employees is executed, re-entrustment is prohibited, the recipient reports to the PPC and notifies the person in cases leakage or the like has occurred, provision of personal data to a third party is prohibited, and the like are defined in an agreement").
- the method and frequency (e.g. annual written reports) by which the data exporter periodically checks the implementation status of the corresponding measures taken by the data importer.
- the identification of the foreign country to which the data is transferred.
- whether any foreign laws (the content of which must be described) may negatively affect the implementation of the corresponding measures taken by the data importer.
- whether any obstacles exist on the side of the data importer that impede the implementation of the required measures, an overview of such obstacles, and the measures taken by the data exporter to address them.

A business handling personal information may only refrain from such (complete or partial) disclosure if provision of this information to the data subject is likely to "significantly hinder" its business operations. This cannot be assumed lightly, but may for instance occur, according to the updated PPC Guidelines, when "the same person repeatedly requests information on the same subject that requires a complicated response"[73].

The introduction of additional monitoring and information obligations for data exporters that have implemented 'equivalent measures' to ensure the continuation of protection in case of (onward) transfers is a positive development, bringing the Japanese regime for international transfers closer to the transfer regime of Chapter V of the GDPR. This is especially the case as regards the new duty of the data exporter to check periodically for the existence of any foreign laws that might negatively affect compliance with the equivalent measures. This obligation, as further developed in the updated Enforcement Rules and updated PPC Guidelines, at least to some extent mirrors requirements under EU data protection law to assess the impact of foreign laws on compliance with appropriate safeguards[74].

4.1.1.4 Introduction of new category of 'pseudonymized personal information'

[72] Article 18(3) of the Enforcement Rules and Chapter 6-2-2 of the PPC Guidelines (Provision to a third party located in a foreign country).

[73] PPC Guidelines (Provision to a third party located in a foreign country), Chapter 6-2-2.

[74] See Case C-311/18, *Data Protection Commissioner v Facebook Ireland Limited* ("Schrems II").

The 2020 APPI amendment has introduced new rules on the creation and use of a new type of personal data, namely "pseudonymized personal information"[75]. According to explanations received, these new rules aim to facilitate the (internal) use of personal information by businesses handling personal information essentially for statistical purposes (e.g. to identify trends and patterns with a view to benefit further activities such as research). To that end, the 2020 APPI amendment relaxes some of the requirements for the processing of pseudonymized personal information, subject to specific safeguards (see below).

Article 2(5) of the amended APPI defines "pseudonymized personal information" as "information relating to an individual that can be prepared in a way that makes it not possible to identify a specific individual unless collated with other information" by taking measures set out in the Act and specified in the Enforcement Rules (Article 41(1) APPI). Based on Article 31 of the Enforcement Rules, pseudonymisation requires the removal of any description that can identify a specific individual, unique personal identification code, and descriptions contained in personal information that are likely to cause damage due to improper use[76]. The immediate result of this process is the creation, by separation, of two types of information: pseudonymized personal information and the information that was removed to produce the pseudonymized personal information (removed information), where the latter is the 'key' that enables re-identification.

Requirements applicable to pseudonymized personal information, as defined in Article 2(5) of the amended APPI, are stipulated in Section 3 of Chapter IV of the Act ("Obligations of Businesses Handling Pseudonymized Personal Information"). Such information is governed by two different sets of rules, depending on whether the information constitutes personal information. In accordance with the interpretation developed in the updated PPC Guidelines, pseudonymized personal information is treated as personal information if it "can be easily cross-checked with other information, and thereby a specific individual can be identified", for instance if the business handling personal information is in simultaneous possession of the personal information from which the pseudonymized personal information was created, and the removed information[77]. In that case, the data is considered to be in a state "where it can be easily collated with other information and thereby identify a specific individual".

Businesses handling personal information that process pseudonymized personal information regarded as personal information are in principle subject to the 'standard' data protection rules (those specified in Section 2 (previously Section 1) of Chapter IV and in Article 148 (previously Article 42) of the amended APPI)[78]. However**,** in accordance with Article 41 APPI, several derogations from these rules apply. In particular, businesses handling personal

[75] Pseudonymized personal information is defined in the amended APPI as information relating to an individual that can be "prepared in a way that makes it not possible to identify a specific individual unless collated with other information" through measures set out in the Act and specified in the Enforcement Rules. See Article 2(5) and 41 of the amended APPI.

[76] See the PPC Guidelines (Pseudonymized personal information and Anonymously Processed Information), Chapter 2-2-2-1.

[77] See the PPC Guidelines (Pseudonymized personal information and Anonymously Processed Information), Chapter 2-2-1.

[78] The PPC Guidelines mention in particular the following provisions of the amended APPI: Article 19 (Prohibition of Inappropriate Utilization), 20 (Proper Acquisition), 23 (Security Control Action), 24 (Supervision over Employees) and 25 (Supervision over a Trustee). See the PPC Guidelines (Pseudonymized personal information and Anonymously Processed Information), Chapter 2-2-1.

information that process such information are allowed to change the purpose of the processing, without the consent of the individual, "beyond the extent that can be appreciably linked to what it was before the alteration"[79]. Such businesses are furthermore exempted from the duty to report a data breach concerning such information (Article 26)[80], the transparency obligation (Article 32) and the provisions regarding data subject rights (Articles 33-39)[81]. In addition, in the event a business handling personal information acquires pseudonymized personal data, or when it intends to change the purpose of processing, its notification obligation (Article 21) is limited to that of public notice[82]. Finally, the data accuracy principle (Article 22[83]) does not apply[84].

When pseudonymized personal information is not considered as personal information[85], only a limited subset of the 'standard' data protection rules applies. In accordance with Article 42 of the amended APPI, when processing 'non-personal' pseudonymized information, businesses handling personal information are (only) subject to the following provisions: Article 23 (data security)[86], Article 24 (supervision over employees), Article 25 (supervision over a trustee) and Article 40 (duty to handle complaints).

Both the use of pseudonymized personal information that is regarded as personal information and that which is not is subject to specific safeguards, in particular in terms of required

---

79 Article 41(9) APPI. The APPI relies on the principle that a business operator has to specify the purpose of use "as much as possible" (Article 17(1)) and is then bound by such use purpose when processing the data. In that respect, Article 17(2) of the APPI provides that the initial purpose must not be altered by the business handling personal information "beyond the extent that can be appreciably linked to what it was before the alteration", interpreted in the PPC Guidelines as corresponding to what can be objectively anticipated by the data subject based on "normal social conventions". See recitals 40-41 of the decision.

80 At the same time, Article 41(2) APPI requires the PIHBO to "take measures for the management of the security of deleted or other related information" and to do so "in accordance with standards prescribed by Order of the Personal Information Protection Commission as those necessary to prevent the leaking of deleted or other related information". Examples of measures that the business handling personal information should take according to these standards include "necessary and appropriate measures" to prevent "unauthorized access from outside" and "leakage of deleted information". See PPC Guidelines (Pseudonymized personal information and Anonymously Processed Information), Chapter 2-2-2-2.

81 Article 41(9) APPI, which states that "the provisions of Article 17, paragraph (2), Article 26 and Articles 32 through 39 do not apply regarding pseudonymized personal information, personal data that constitutes pseudonymized personal information, and personal data the business holds that constitutes pseudonymized personal information". Note that the provision does not list Article 40 APPI, which means that PIHBOs handling pseudonymized personal information are still subject to the duty to handle complaints (set out in that provision).

82 Article 41(4) APPI.

83 Whereas Article 41(5) APPI provides that the general data accuracy and data retention principles of Article 22 do not apply, it introduces the principle of limited data retention for pseudonymized personal information (i.e. it shall be deleted in case the information no longer needs to be used).

84 Article 41(5) APPI. According to explanations received, the 'standard' requirement of ensuring accuracy of the descriptions contained in the pseudonymized personal information continues to apply as long as this can be done without violating the prohibition on collating the pseudonymized personal information with other information to (re-) identify an individual.

85 Pseudonymized personal information that is not regarded as "personal information" within the meaning of the APPI must be distinguished from anonymously processed information. According to the explanations received, compared to the creation of anonymously processed information the creation of pseudonymized personal information requires a simpler procedure that does not require, for example, "deleting idiosyncratic descriptions etc." (Article 19 lit. 4 of the Enforcement Rules).

86 Limited to an obligation to take necessary measures to prevent the "leaking" of the pseudonymized personal information.

technical and organisational measures addressing possible risks of re-identification and limitations on data sharing. First, businesses handling personal information that process pseudonymized personal information are prohibited from collating said information with other information in order to (re-)identify a data subject[87]. Second, businesses handling personal information that are in simultaneous possession of pseudonymized personal information and removed information must take enhanced security measures, in accordance with standards prescribed by the Enforcement Rules, to prevent any leakage of the removed information[88]. Third, pseudonymized personal information may not be shared with a third party, subject to limited exceptions[89]. Fourth, businesses handling personal information are prohibited from using the pseudonymized personal information to contact data subjects[90].

At the review meeting and during subsequent exchanges the Commission services and the PPC have clarified the interpretation and application of the new APPI provisions on pseudonymized personal information.

According to explanations received from the PPC, the prohibition to share pseudonymized personal information with third parties (Article 41(6) of the amended APPI), together with the prohibition to collate such information with other information in to (re-)identify a data subject (Article 41(7) of the amended APPI), reflect the intention of the legislator to essentially limit the use of pseudonymized personal information to statistical purposes[91]. However, the amended APPI does not contain an *explicit* limitation to only process the information for statistical purposes[92]. With a view to reflect the intended application of the rules on pseudonymized personal information more clearly in Japanese law, and thus to ensure legal certainty and transparency, the PPC agreed to amend the Supplementary Rules. The new Supplementary Rule (4) stipulates that such information may only be used for statistical purposes – defined as processing for statistical surveys or the production of statistical results – to produce aggregate data, and that the result of the processing will not be used in support of measures or decisions

87 Articles 41(7) and 42(3) of the amended APPI.

88 Article 41(2) of the amended APPI. According to explanations received, pseudonymized personal information and the personal information from which the pseudonymized personal information was created should be managed separately to prevent violation of the obligation to prohibit identification set forth in Article 41(7) of the amended APPI.

89 Articles 41(6) and 42(1) of the amended APPI. Exceptions apply, first, in case of: (1) entrustment, (2) succession caused by merger or other reasons and (c) joint-processing. According to the explanations received, the rationale behind these three exceptions is that in case of entrustment, joint-use and business succession, the recipient of the pseudonymised data can be regarded as an integral part of the pseudonymized personal information handling business operator. Therefore, the recipient is not considered a third party. Furthermore, an exception applies in cases where disclosure is required based on laws and regulations. Examples of cases based on laws and regulations are mentioned on p. 54 of the PPC Guidelines (General Rules) and include, for instance, responding to an inquiry by the police on matters related to an investigation (Article 197 (2) of Code of Criminal Procedure (Act No. 131 of 1948) or responding to an investigation based on a warrant issued by a judge (Article 218 of the Code of Criminal Procedure).

90 Article 41(8) and 42(3) of the amended APPI.

91 See also the PPC Guidelines (Pseudonymized personal information and Anonymously Processed Information), Chapter 2-2-3-4, which lists "combining multiple pseudonym-processed information to create statistical information" as an example of "treatment not constituting acts of identification".

92 Unlike, for example, Article 89 GDPR and its related provisions (Article 5(1)(b) and (e), Article 9(2)(j), Article 14(5)(b), Article 17(3)(d) and Article 21(6) GDPR).

regarding any specific individual. This captures the common meaning and use of data used for "statistical purposes"[93].

Moreover, given that under EU data protection law pseudonymisation – unlike anonymisation – does not change the nature of the information as personal data, the new rule also makes clear that pseudonymized personal information originally received from the EU will always be treated in accordance with Article 41 of the amended APPI (i.e. the provision that governs the processing of pseudonymised data considered as "personal information")[94]. This also ensures that Supplementary Rule (5)[95], which seeks to ensure that the continuity of protection of data considered as personal data under the GDPR is not undermined when transferred on the basis of the adequacy decision.

The combination of the pseudonymisation of the data, the further specific safeguards set out in the APPI with respect to pseudonymized personal information – which address possible risks of re-identification and put limitations on data use and sharing – and the clarification in the Supplementary Rules as regards the specific statistical purpose of processing ensures that this new category of personal data is subject to protections essentially equivalent to those required for statistical processing under the GDPR[96]. Nevertheless, given its novelty, the Commission services will closely monitor the implementation of Article 41 APPI in practice and pay particular attention to its proper application as part of the next review.

4.1.1.5 Strengthening of the PPC's oversight and enforcement

As a result of the 2020 and 2021 APPI amendments, the PPC's oversight and enforcement has been strengthened. First, the 2020 APPI amendment has raised the maximum amount of the fines that can be imposed for violating a binding order[97]. Second, the 2021 APPI amendments has expanded the PPC's enforcement powers and has led to an increase of its resources.

---

93 See Recital 162 GDPR.

94 This excludes the application of Article 42 of the amended APPI which only preserves a limited number of safeguards for pseudonymized personal information not considered as personal information.

95 As is the case with pseudonymized personal information, "anonymized personal information", as defined by the APPI, includes data for which re-identification of the individual is still possible. This could mean that personal data transferred from the European Union might lose part of the available protections through a process that, under the GDPR, would be considered a form of "pseudonymization" rather than "anonymization" (thus not changing its nature as personal data). To address that situation, the Supplementary Rules provide for additional requirements applicable only to personal data transferred from the Union under this Decision. According to Supplementary Rule (5), such personal information shall only be considered "anonymized personal information" within the meaning of the APPI "if the personal information handling business operator takes measures that make the de-identification of the individual irreversible for anyone, including by deleting processing method etc. related information". See recitals 30-31 of the decision. In the version of the APPI that applied at the time of the adoption of the adequacy decision, the notion of "anonymized personal information" was referred to as "anonymously processed information".

96 In particular, Article 89 GDPR and its related provisions (Article 5(1)(b) and (e), Article 9(2)(j), Article 14(5)(b), Article 17(3)(d) and Article 21(6) GDPR). See also Article 11(2) GDPR, according to which Articles 15 to 20 GDPR do not apply if the controller is not in a position to identify the data subject. While this concerns cases pursuant to Article 11(1) GDPR, i.e. where the purpose for which the controller processes the personal data "do not or do no longer require" the identification of the data subject by the controller (with the consequence that the latter is not required to "maintain, acquire or process" identifying information), the situation of PIHBOs appears comparable in that the statistical purposes can (and in fact by law must) be achieved with pseudonymized personal information, under a legal prohibition to re-identify.

97 The maximum fines amount that can be imposed on a natural person has been raised from 300.000 yen to 1.000.000 yen (Article 178 of the amended APPI). In addition, a separate and increased maximum fine of one

As mentioned previously (see paragraph 3), the 2021 APPI amendment has harmonised the data protection rules previously laid down separately in the APPI, the APPIHAO and the APPI-IAA. In particular, the material scope of application of the APPI has been extended to include Administrative Organs and Incorporated Administrative Agencies. New chapters and (sub-) sections have been added to the APPI on the processing by these public authorities of personal information (Chapter V) and anonymized personal information (Chapter V, Section 5), and on the supervision of these authorities (Chapter VI, Subsection 3). Finally, the laws previously governing the processing of personal data by public authorities – the APPIHAO and APPI-IAA – have been revoked. Because of these changes, and as confirmed by the PPC, the oversight of compliance with the data protection rules has now exclusively been entrusted to the PPC.

Previously, the monitoring of compliance with the data protection rules applying to Administrative Organs and Incorporated Administrative Agencies was ensured by various authorities. For example, with respect to the correct application of the former APPIHAO, the competent minister or agency head (e.g. the Commissioner General of the NPA) had enforcement authority, subject to the supervision by the Ministry of Internal Affairs and Communications (MIC). Where it considered this necessary for ensuring compliance with the Act, MIC could request the submission of explanations and materials, and issue opinions, concerning the handling of personal information by the concerned Administrative Organ (Articles 50, 51 APPIHAO)[98].

Under the amended APPI, the PPC, in addition to overseeing the processing of personal data by businesses handling personal information falling under the APPI, is now responsible for overseeing the collection and further processing of personal data by Administrative Organs (including law enforcement authorities and public authorities collecting personal data for national security purposes) and Incorporated Administrative Agencies. Although the PPC has not been empowered to issue binding orders to, or impose fines on these public authorities, it may collect reports from them on the status of enforcement of the amended APPI (Article 165), request them to report or submit documents on processing operations and conduct on-site inspections (Article 156), provide guidance and advice (Article 157), issue recommendations (Article 158) and request reports on measures taken in response to such recommendations (Article 159).

The PPC has reported that, in reaction to the changes brought by the 2021 APPI amendment, its staff has been increased by around 50 persons, and currently comprises around 200 staff members at full capacity. The Commission services welcome this development, which will help to ensure that the PPC maintains an adequate oversight and enforcement capacity.

The Commission services furthermore note that the transformation of the APPI into a comprehensive data protection law covering both the private and public sector marks an important and positive development in the evolution of the Japanese data protection framework. Even though the amended APPI contains different provisions governing businesses handling personal information and Administrative Organs or Incorporated Administrative

hundred million yen (approximately 770.000 euros) has been introduced for corporations and other legal persons (Article 184(1) of the amended APPI).

98 See recital 136 of the decision.

Agencies, the 2021 APPI amendment, by incorporating those distinct rules into one law, has brought further convergence with the GDPR.

4.1.2 Application of the Supplementary Rules

This section presents the Commission services' findings as regards the application of the Supplementary Rules.

The Supplementary Rules were adopted on 15 June 2018. Following the entry into force of the 2020 APPI amendments, a number of technical changes to the rules have been introduced, reflecting the fact that some of the additional safeguards set out in the Supplementary Rules have in the meantime been incorporated into the APPI, thereby making them generally applicable to all personal data, irrespective of their origin or point of collection. These technical changes have been introduced by the PPC in close consultation with the Commission services.

Taking into account that the Supplementary Rules are a newly created instrument, enacted to offer enhanced protection to EU individuals when their personal data is transferred to Japan based on the adequacy decision, the Commission services have put particular emphasis on checking whether the Supplementary Rules – to the extent these have not been incorporated into the amended APPI and thus made generally applicable – are functioning as envisaged.

As part of the review, the PPC provided information on a number of awareness raising initiatives it has carried out. On the day the decision was adopted, the PPC published a press release on its website informing about the new framework for data transfers[99]. It also used its official website to provide the texts of both the APPI and the Supplementary Rules (the latter as part of the section on "Commission Rules"), together with an English translation in each case[100], as well as information on the overall legal framework for the protection of personal data (again also available in English)[101]. Lastly, it has published the updated PPC Guidelines on international data transfers and a document answering frequently asked questions (FAQs) about the APPI on its website (both in Japanese)[102]. The PPC has indicated that it is considering publishing an English translation of the FAQs, but for the moment it believes that translations into English should be focussed on more "high-priority items".

The PPC has also reported that it organised briefing seminars for business operators in Japan and Europe. However, the Commission services note that these seminars took place before the adoption of the adequacy decision and understand that they did not specifically address the Supplementary Rules. With a view to promote accountability, it would be useful for the PPC

---

99 Available (in English) at: https://www.ppc.go.jp/en/aboutus/roles/international/cooperation/20190123/

100 See at: https://www.ppc.go.jp/en/legal/. The PPC webpage on "Laws and Policies" distinguishes between different types of legal rules, according to a hierarchy of norms ("Act", "Cabinet Order", "Commission Rules" and "Notice, Guidelines, etc."). The Supplementary Rules are listed in the section on "Commission Rules", together with the "Enforcement Rules".

101 See https://www.ppc.go.jp/en/legal/ ('Materials').

102 See (in Japanese only):
https://www.ppc.go.jp/personalinfo/legal/guidelines_offshore/
https://www.ppc.go.jp/files/pdf/210101_guidlines02.pdf
FAQ (in Japanese only):
https://www.ppc.go.jp/personalinfo/faq/2009_APPI_QA/
https://www.ppc.go.jp/files/pdf/2106_APPI_QA.pdf

to publish guidelines or other guiding material explaining the specific requirements following from the Supplementary Rules, and to organise related briefing seminars.

Another important condition for the effective implementation of the Supplementary Rules is that businesses handling personal information use effective methods to be able to identify personal data received from the Union throughout their "life cycle". This is important because the Supplementary Rules supplement the APPI with stricter and/or more detailed rules[103].

The PPC has reported that it has not identified any problem in relation to the implementation of this requirement. To understand better how business operators in Japan ensure compliance with the APPI and the Supplementary Rules, the PPC has conducted interviews with business operators and their industry associations. According to the PPC, these interviews show that, depending on the nature and circumstances, business operators in Japan have been complying with the Supplementary Rules either by processing the personal data received from the Union separately, or by applying the stricter standards of the Supplementary Rules to all personal data they retain without distinguishing between data transferred from the Union and other data. In the former case, business operators have generally developed special internal rules for handling the personal data transferred from the Union that cover the additional protections. According to explanations offered by the PPC, in both cases personal data transferred from the Union based on the adequacy decision is subject to internal regulations and practices that meet the requirements of the APPI and the Supplementary Rules.

In its review of the application of the Supplementary Rules, the Commission services have furthermore paid special attention to the application of Supplementary Rule (3) (previously Supplementary Rule (4)) on onward transfers.

Article 28(1) of the amended APPI only allows the transfer of personal data to a third party outside the territory of Japan without prior consent in certain, limited cases[104]. To ensure continuity of protection in case of personal data transferred from the Union to Japan under the decision, Supplementary Rule (3) enhances the level of protection for onward transfers of such data by the business handling personal information to a third country recipient. It does so by limiting and framing the bases for international transfers that can be used by the business as an alternative to consent. More specifically, and without prejudice to the derogations set forth in Article 27(1) of the amended APPI, personal data transferred under the decision may be subject to (onward) transfers without consent only in two cases: (i) where the data is sent to a third country which has been recognised by the PPC under Article 28 of the APPI as providing an equivalent level of protection to the one guaranteed in Japan; or (ii) where the business handling personal information and the third party recipient have together implemented measures providing a level of protection equivalent to the APPI, read together with the Supplementary Rules, by means of a contract, other forms of binding agreements or binding arrangements within a corporate group[105].

As explained in the adequacy decision, the requirements set forth in Supplementary Rule (3) exclude the use of transfer instruments that do not create a binding relationship between the Japanese data exporter and the third country's data importer and that do not guarantee the

[103] Recital 15 of the decision.
[104] Recital 76 of the decision.
[105] Recital 78 of the decision.

required level of protection. This will be the case, for instance, of the APEC Cross Border Privacy Rules (CBPR) System, of which Japan is a participating economy, as in that system the protections do not result from an arrangement binding the exporter and the importer in the context of their bilateral relationship and are clearly of a lower level than the one guaranteed by the combination of the APPI and the Supplementary Rules[106].

With respect to the onward transfer of data originally received from the Union, according to information received from the PPC based on its interviews with several industry associations and business operators, such transfers "are most commonly framed by concluding a contract that binds the recipient to measures ensuring the continuity of protection". That being said, in the context of the review the PPC explained that it does not currently provide guidance on the recommended content (in terms of safeguards) of 'equivalent measures', be it in the form of guidelines or model data protection contracts ("model clauses").

Model clauses allow to bridge differences in data protection standards by creating a self-standing data protection regime at contractual level. They form a "ready-made" instrument (companies can simply rely on what has been pre-approved instead of having to negotiate model clauses in each individual case) that can offer clear benefits in terms of transparency, legal certainty and thus predictability. At the same time, model clauses represent a relatively low-cost solution, particularly for small- and medium-sized companies that cannot afford more costly and time-consuming alternatives (such as, for instance, certification). The Commission services note that model clauses currently support most of data transfers from the EU.

Based on the EU's positive experience with model clauses, the Commission services believe that the development of such clauses could further strengthen the safeguards for (onward) transfers in transfer scenarios where the business handling personal information in Japan and the third-party recipient intend to frame their transfer by together implementing measures providing a level of protection equivalent to the APPI, read together with the Supplementary Rules. For this reason, and given the growing importance of model clauses and their potential as a global tool for data transfers – as recognised for instance by ASEAN[107], the OECD[108], the G7[109] and the Ibero-American Network of data protection authorities[110] – the Commission services would be interested in future cooperation with Japan in the development of such clauses.

The Commission services furthermore note that, although the Supplementary Rules address the question of onward transfers from Japan of personal data received from the Union (by limiting

---

[106] See recital 79 of the decision. Similar considerations apply with respect to the APEC Privacy Recognition for Processors (PRP) System.

[107] See the ASEAN Model Contractual Clauses for Cross Border Data Flows (MCCs), available at: https://asean.org/wp-content/uploads/2021/08/ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows.pdf.

[108] See OECD Going Digital Toolkit, Interoperability of privacy and data protection frameworks, available at: https://goingdigital.oecd.org/data/notes/No21_ToolkitNote_PrivacyDataInteroperability.pdf, p. 18.

[109] See the Ministerial Declaration of the G7 Digital Ministers' meeting on 11 May 2022, Annex 1 (G7 Action Plan Promoting Data Free Flow with Trust) which, under the heading of "Building on commonalities in order to foster future interoperability" refers to the "increasingly common practices such as standard contractual clauses".

[110] See the Guide for the Implementation of Standard Contractual Clauses for the International Transfer of Personal Data published by the Ibero-American Network for the Protection of Personal Data (RIPD), available at: https://www.redipd.org/sites/default/files/2022-09/guia-clausulas-contractuales-modelo-para-tidp.pdf.

the possible grounds for transfers), the revised PPC Guidelines on international transfers do not refer to the Supplementary Rules. Neither do they mention the fact that, as explained above, onward transfers based on the APEC Cross Border Privacy Rules (CBPR) certification scheme are excluded. The Commission services recommend that these points are clarified by the PPC by updating the PPC Guidelines on international transfers. In this context, the Commission services take note of the establishment by APEC of a Global CBPR Forum which aims, inter alia, "to establish an international certification system based on the APEC Cross Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) Systems"[111]. While it appears that the details of the envisaged Global CBPR system are still being discussed, in case it would merely involve a territorial extension beyond the current APEC CBPR system, rather than a substantial strengthening of the applicable data protection safeguards, the exclusion of onward transfers would equally apply to the new scheme. The Commission services will continue to closely monitor future developments in this area.

Providing such guidance, including with respect to the content of 'equivalent measures', and further explanations on the application of the Supplementary Rules in the area of onward transfers could be particularly useful as it would concern aspects that are particularly relevant to companies operating in both jurisdictions.

As regards onward transfers based on an 'adequacy finding' by the PPC, the Commission services note that, to date, apart from the Union and the United Kingdom (UK)[112], the PPC has not adopted any decision recognising a third country as providing an equivalent level of data protection to the one guaranteed in Japan. The PPC has informed the Commission services that no recognition procedures are ongoing, and that for the moment it has no intention to start any such procedure. The Commission services will continue to closely monitor future developments in this area.

The PPC further reports that, since the adoption of the adequacy decision, Japan has entered the following new (trade) agreements comprising obligations on cross-border data flows:

1. Agreement between Japan and the United States of America concerning Digital Trade (signed on 7 October 2019 and entered into force on 1 January 2020);
2. Japan-UK Comprehensive Economic Partnership Agreement (signed on 23 October 2020 and entered into force on 1 January 2021);
3. Regional Comprehensive Economic Partnership (RCEP) Agreement (signed on 15 November 2020 and entered into force 1 January 2022).

Each of these agreements includes commitments on cross-border data flows, while allowing each party to adopt or maintain measures necessary to ensure data protection and privacy, listed as legitimate public policy objectives that can be invoked under certain conditions. According to the PPC, these conditions do not affect the requirements for cross-border data transfers set forth in Article 28 of the APPI and Supplementary Rule (3), including in situations where data transferred from the Union based on the adequacy decision is further transferred to the United States, the United Kingdom (to which personal data may be transferred on the basis of the

[111] See https://www.commerce.gov/global-cross-border-privacy-rules-declaration

[112] The PPC has explained that the UK was originally recognised as ensuring an 'adequate' level of protection being one of the EU Member States, and the designation remained valid even after the UK's withdrawal from the EU.

'adequacy finding' of the PPC) or parties to the RCEP. The Commission services take note of this explanation and will continue to closely monitor future developments in this area.

4.1.3 Oversight and enforcement by the PPC

To ensure an adequate level of data protection also in practice, the Japanese data protection regime provides for independent oversight by the PPC[113]. In addition, data subjects have access to a number of administrative and judicial redress avenues[114]. In the adequacy decision, the Commission considered that, taken as a whole, the oversight mechanisms and redress avenues in Japanese law enable infringements by businesses handling personal information (receiving personal data from the Union) to be identified and punished in practice. To evaluate whether this finding continues to be legally and factually justified, the Commission services have assessed how the PPC has monitored and enforced compliance with the APPI and the Supplementary Rules in the period following the adoption of the adequacy decision.

It is important to note at the outset that compliance with the APPI and the Supplementary Rules is ensured within the Japanese framework through a mix of 'hard' (coercive) and 'soft' (non-coercive) powers or instruments. On the one hand, the PPC has a set of 'classic' coercive powers to monitor and enforce compliance with the APPI and the Supplementary Rules. In particular, the PPC may request businesses handling personal information to report or submit documents on processing operations and may also carry out inspections, both on-site and of books or other documents[115]. In case a violation is detected it may, as a first step, issue a recommendation to the offender, which can subsequently be followed up by a binding order in case the recommendation is not followed[116]. Non-compliance with a binding order is considered a criminal offence and under the amended APPI a business handling personal information found guilty can be punished by imprisonment with labour for up to one year (previously up to six months) or a fine of up to 1,000,000 yen (previously 300,000 yen)[117]. In addition, a separate and increased maximum fine of one hundred million yen has been introduced for corporations and other legal persons (Article 184(1) of the amended APPI).

On the other hand, the APPI contains a dedicated provision tasking the PPC with providing guidance and advice as regards the handling of personal information[118]. Furthermore, the PPC has pointed out that, already before the adoption of the adequacy decision, it had set up a dedicated contact point for individuals who have concerns about the processing of their personal data by business operators in Japan. This contact point is referred to as the 'Inquiry Line for the Act on the Protection of Personal Information' (Inquiry Line)[119]. The PPC has explained that this facility is also available for EU individuals who have concerns about a Japanese business operators' handling of their personal data transferred from the Union under the adequacy decision, including compliance with the Supplementary Rules. To make the

[113] Recitals 95-102 of the decision.
[114] Recitals 103-112 of the decision.
[115] Article 146 APPI. Lack of cooperation with the PPC or obstruction to its investigation can be punished under the amended APPI with a fine of up to 500,000 yen (previously 300,000 yen), see Article 182(i) APPI.
[116] Article 148 APPI.
[117] Article 178 APPI.
[118] Article 147 APPI.
[119] The Inquiry Line was created on 30 May 2017 and thus predates the adoption of the adequacy decision, which was adopted on 23 January 2019.

Inquiry Line more accessible for these individuals, the PPC provides practical information about the use of this facility in English on its website[120].

As regards the actual use of the previously mentioned powers and instruments, the Commission services note that the PPC has made more use of its non-coercive powers than of its coercive powers in the period following the adoption of the adequacy decision. Regarding its oversight powers, the PPC has reported that in the period from 1 April 2019 to 30 September 2020, in 459 cases it requested a business handling personal information to report or submit documents on processing operations, while in six cases it conducted an (onsite) inspection. To date, no complaints concerning (non-)compliance with the Supplementary Rules have been received, and no investigations into such (non-) compliance have been conducted on the PPC's own initiative. As regards enforcement, the PPC has reported that it has issued five recommendations and two binding orders in the period from 1 April 2019 to 30 September 2020. In no case a business operator was sanctioned with a fine or imprisonment for violating a binding order.

These relatively low numbers for coercive measures contrast with the numbers concerning the PPC's use of its non-coercive powers or instruments. The PPC has reported that, in the period from 1 April 2019 to 30 September 2020, it offered guidance in 210 cases and mediated disputes following a complaint in 45 cases. Furthermore, according to the PPC from 30 May 2017 to 31 March 2021 it has received a total number of 66,802 inquiries through its Inquiry Line.

Although the PPC's non-coercive powers are of a non-binding nature, this does not mean that they do not have an impact on compliance. This is exemplified by the widely publicized Line-case[121]. On 23 April 2021, the PPC announced that it had issued guidance to Line Corporation, the company behind a widely used communication app in Japan (Line)[122]. In particular, it had advised to introduce a number of improvements to Line's system for data transfers to third countries. This guidance built on the preliminary results of an on-going investigation into Line Corporation's compliance with the APPI. The PPC had found, among other things, that Line Corporation had granted access to personal data (including chat messages) to its foreign processors, including a Chinese software company[123]. Although no specific violation of the APPI was found, since at that time the new transparency requirements for businesses handling personal information transferring personal data to third countries based on the consent of the data subject did not yet apply, the Line Corporation subsequently changed its privacy policy to better explain the purpose of its data transfers and to include the names of the countries of

[120] See https://www.ppc.go.jp/en/contactus/piinquiry/. Based on the information provided on this website, questions or complaints can be submitted by calling a specific telephone number. Calls will be answered from Monday to Friday between 9:30-17:30 (Japan time), except on national holidays and from 29 December to 3 January. The PPC has explained that complainants are advised to first contact the concerned PIHBO to see whether it can resolve the complaint itself before contacting the Inquiry Line. Therefore, the website states that "if you have any complaint on specific matters in relation to your personal information, please contact the company retaining your personal information, Accredited Personal Information Protection Organizations, local governments including local consumer centers or the National Consumer Affairs Center".

[121] See for example 'Line scandal alerts Japan on need to get serious about data protection', *Japan Times* 22 April 2021.

[122] See https://www.ppc.go.jp/files/pdf/210423_houdou.pdf (in Japanese only).

[123] The PPC has reported that it is "not aware of any cases of personal data from the EU acquired by the Line Corporation being transferred to a third country in violation of the APPI and/or the Supplementary Rules".

destination. It also made several other improvements to its system for international data transfers[124].

It is possible that the PPC's apparent preference for resorting to non-coercive powers or instruments instead of the use of its coercive powers to monitor and enforce compliance with the APPI and the Supplementary Rules reflects a general preference within the Japanese legal system for arbitration, mediation, or conciliation as an alternative to the judicial settlement of disputes, and for administrative guidance instead of binding decisions (injunctions)[125]. Even if that were to be the case, the Commission services would encourage the PPC to make more use of its (binding) enforcement powers. This appears especially important in relation to the PPC's oversight over the Supplementary Rules. According to explanations received from the PPC, it has not encountered any cases that raise concerns about compliance with the Supplementary Rules. While this is reassuring, full confidence in the proper implementation of the Supplementary Rules requires not only reactive, but also proactive supervision by the PPC. In response to remarks by the Commission services on this point at the review meeting, the PPC announced that it is considering conducting, on its own initiative, random checks to ensure compliance with the Supplementary Rules. This would be a welcome approach, and the Commission services are looking forward to any updates in this regard in the coming months. It is indeed important that the PPC proactively and randomly checks compliance with the Supplementary Rules and effectively addresses any violations it detects. As the 2020 and 2021 amendments of the APPI have strengthened the PPC's oversight powers, these random checks could be part of an overall effort to increase the use of such powers.

As regards the Inquiry Line, the Commission services note that, according to the PPC, assistance is in principle only available in Japanese. This is also what the website states ("Japanese only"). The PPC has explained that, when English language assistance is required, this is to the extent possible provided with the help of an English-speaking staff member. As the number of personnel who can respond in English is limited and service in English depends on the availability of the English-speaking staff member, the PPC is unable to guarantee that the service in English is always available. According to the PPC, this also explains the reference to a "Japanese only" service on its website.

The Commission services appreciate that the PPC provides information about this facility on its website in English and strives to offer English language assistance, as much as possible, to non-Japanese speakers. At the same time, it notes that the information on the Inquiry Line's webpage stating that it is available in "Japanese only" is likely to dissuade EU individuals from making use of this facility. In the context of the review, the PPC signalled its willingness to clarify on its website that English language assistance is available in principle. The Commission services encourage the PPC to do so. The Inquiry Line has the potential to become a very useful facility for EU individuals (and other foreigners) who have questions or concerns about the use of their personal data by Japanese operators. In addition, if more EU individuals

[124] See the PPC's press release about the case, available at: https://www.ppc.go.jp/files/pdf/210423_houdou.pdf (in Japanese only).

[125] Graham Greenleaf and Fumio Shimpo, 'The puzzle of Japanese data privacy enforcement', *International Data Privacy Law* 2014, p. 140-141: "The Japanese legal system is also characterized by a preference for arbitration, mediation, or conciliation as an alternative to the judicial settlement of disputes, and by various administrative practices which provide guidance falling short of formal law. Both practices are significant in Japan's data protection system".

would make use of this facility, it could also help the PPC to better monitor compliance of Japanese operators with the APPI and the Supplementary Rules when they are processing personal data transferred from the Union.

4.2 ASPECTS RELATING TO ACCESS AND USE OF PERSONAL DATA BY JAPANESE PUBLIC AUTHORITIES

In the adequacy decision, the Commission assessed the limitations and safeguards, including the oversight and individual redress mechanisms, available in Japanese law as regards the collection and subsequent use of personal data transferred from the Union by Japanese public authorities for public interest, in particular criminal law enforcement and national security purposes ("government access"). These redress mechanisms include a specific dispute resolution procedure, administered and supervised by the PPC, that the Japanese government has created for EU individuals whose personal data is transferred under the adequacy decision. Based on its analysis and on the specific representations, assurances and commitments received from the Japanese government that are contained in Annex II of the decision (which also covers this specific dispute resolution procedure), the Commission considered that any such government access will be limited to what is strictly necessary, and that effective legal protection against such interference exists[126].

This finding relies on both the Constitution of Japan, which contains a number of guarantees concerning the collection of personal data by public authorities in general, and specific statutory limitations and safeguards. The PPC has reported that no changes to these laws affecting the protection of personal data transferred from the Union based on the adequacy decision have occurred since that decision came into effect. However, other developments have taken place that are relevant for the functioning of the adequacy decision in this area. The next sections describe these developments.

4.2.1 Limitations and safeguards regarding the collection and use of personal data for law enforcement purposes

In the Japanese legal framework, the collection of electronic information for criminal law enforcement purposes may take place based on a warrant (compulsory collection) or a request for voluntary disclosure using a so-called "enquiry sheet". A relevant development with respect to the latter form of data collection is the adoption of a new circular ('Notification') by the National Police Agency to the Prefectural Police on the proper use of enquiry sheets[127].

The new Notification replaces the earlier Notification on "the proper use of written inquiries in investigative matters". This earlier Notification already clarified that the request must be made using a pre-established form ("Form No. 49" or so-called "enquiry sheet"), concern records "regarding a specific investigation" and that the requested information "must be necessary for [that] investigation". It also prescribed that, in each case, the chief investigator shall "fully examine the necessity, content, etc. of [the] individual enquiry" and must receive internal approval from a high-ranking official[128]. The new Notification builds on these

[126] Recital 173 of the decision.

[127] National Police Agency, Regarding Proper Use of Enquiry Form for Investigation related Matters, 27 March 2019, available at: https://www.npa.go.jp/laws/notification/keiji/keiki/310327-20.pdf (in Japanese only).

[128] See recital 127 of the decision.

safeguards and adds to them that requests for disclosure based on an enquiry-sheet should be kept to a minimum, considering the burden placed on the organisations that are asked to respond. In addition, the new Notification specifies that an enquiry sheet must receive internal approval from a police officer whose rank is higher than chief inspector.

As regards the practical reality of requests for voluntary disclosure, it has been noted that, due to the workload involved for the recipients of enquiry sheets and their privacy implications, against the background of growing public awareness of privacy rights, there is a marked tendency for businesses handling personal information to take a more cautious approach towards answering enquiry sheets. For example, in February 2019 the Nikkei newspaper reported the collection by law enforcement agencies of personal information from the largest loyalty program, Culture Convenience Club (CCC), which has approximately 68 million users, on a voluntary basis[129]. Following this report, CCC stopped cooperating with requests from law enforcement authorities for voluntary cooperation based on an enquiry sheet. It now only provides personal information to the police in case it is required to do so based on a warrant. CCC has also started publicizing transparency reports[130].

4.2.2 Oversight and redress

The redress mechanisms available in Japanese law include a specific dispute resolution procedure, administered and supervised by PPC, which the Japanese government has created for EU individuals whose personal data is transferred under the decision[131]. That mechanism builds on the cooperation obligation imposed on Japanese public authorities under Article 174 of the APPI and the special role of the PPC with respect to international data transfers under Article 6 of the APPI. The mechanism is not subject to any standing requirement and is open to any individual, independently of whether (s)he is suspected or accused of a criminal offence.

Under the mechanism, an individual who suspects that his/her data transferred from the Union has been collected or used by public authorities in Japan (including those responsible for criminal law enforcement) in violation of the applicable rules can submit a complaint to the PPC (individually or through the competent EU data protection authority within the meaning of Article 51 of the GDPR). The PPC shall handle the complaint and in a first step inform the competent public authorities, including the relevant oversight bodies, thereof. Those authorities are required to cooperate with the PPC, including by providing the necessary information and relevant material, so that the PPC can evaluate whether the collection or subsequent use of personal information has taken place in compliance with the applicable rules. If the evaluation shows that an infringement of the applicable rules has occurred, the concerned public authorities are required to remedy the violation, an obligation which is carried out under the supervision of the PPC. Once the evaluation is concluded, the PPC shall notify the individual within a reasonable time-period of the outcome of the evaluation, including any corrective

[129] 'Providing "Footprints" with Company Judgments', Nikkei Newspaper, 2 February 2019, available at: https://www.nikkei.com/article/DGXMZO40789930R00C19A2SHA000/ (in Japanese only)

[130] CCC, 'Regarding Transparency Report', available at: https://www.ccc.co.jp/customer_management/transparencyreport/. According to the CCC's transparency report, in the fiscal year 2020 (which in Japan runs from 1 April 2020 to 31 March 2021), CCC received 266 requests for the collection of electronic information from law enforcement authorities. Of those requests, 252 were based on a court warrant, while 14 were based on an enquiry sheet. CCC responded to 254 of those requests and refused to respond in nine cases.

[131] See recitals 141-144 of the decision.

action taken. At the same time, the PPC shall also inform the individual about the identity of the competent public authority and the possibility of seeking a confirmation of the outcome from that authority. The possibility to receive such a confirmation, including the reasons underpinning the decision of the competent authority, will help the individual in taking any further steps, including when seeking judicial redress.

The new enforcement powers of the PPC vis-à-vis public authorities, discussed previously (see section 4.1.1.5), will strengthen this mechanism. With its new powers, in particular the power to request Administrative Organs to report or submit documents on processing operations, to conduct on-site inspections, to issue recommendations and request reports on measures taken in response to such recommendations, the PPC is better placed to ensure the necessary cooperation of public authorities who are subject to the dispute resolution procedure.

As part of its implementation of the specific dispute resolution procedure as described above, the PPC has established a dedicated contact point to receive complaints from EU individuals who suspect that their data transferred from the Union has been collected or used by public authorities in Japan in violation of the applicable rules. Practical information about how to reach this contact point (referred to as the "Complaint Mediation Line for Japanese administrative authorities' handling of personal data transferred from the EU and the UK based on an adequacy decision etc.") is available in English on the PPC's website[132]. The website also provides some general information about the dispute resolution procedure, explaining, among other things, that "complainants may submit [their] complaint to the PPC through Data Protection Authorities (DPAs) in EU member states" and that "your information will be provided to the administrative authorities to which your complaint is addressed".

The PPC has reported that it has hired one full-time staff member to handle complaints submitted by EU individuals through this mediation line. In case this staff member is out of office, an English-speaking staff member is always available to replace him/her. The PPC has furthermore reported that, since the adequacy decision was adopted, no complaints were received from EU individuals who suspect that their data transferred from the Union has been collected or used by public authorities in Japan in violation of the applicable rules, be it through the contact point or via an EU data protection authority.

[132] https://www.ppc.go.jp/en/contactus/complaintmediationline/. According to this website, complaints can be submitted in English or Japanese by calling a specific telephone number. Calls will be answered from Monday to Friday during working hours between 10:00-12:00 AM and 01:00-6:00 PM (Japan time), except on national holidays and from 29 December to 3 January.