EUROPEAN
COMMISSION

Brussels, 23.1.2019
C(2019) 304 final

COMMISSION IMPLEMENTING DECISION

of 23.1.2019

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

(Text with EEA relevance)

COMMISSION IMPLEMENTING DECISION

of 23.1.2019

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

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)[1], and in particular Article 45(3) thereof,

After consulting the European Data Protection Supervisor,

1. Introduction

(1) Regulation (EU) 2016/679 sets out the rules for the transfer of personal data from controllers or processors in the European Union to third countries and international organisations to the extent that such transfers fall within its scope. The rules on international transfers of personal data are laid down in Chapter V of that Regulation, more specifically in Articles 44 to 50. The flow of personal data to and from countries outside the European Union is necessary for the expansion of international cooperation and international trade, while guaranteeing that the level of protection afforded to personal data in the European Union is not undermined.

(2) Pursuant to Article 45(3) of Regulation (EU) 2016/679, the Commission may decide, by means of an implementing act, that a third country, a territory or one or more specified sectors within a third country or an international organisation ensure an adequate level of protection. Under this condition, transfers of personal data to that third country, territory, sector or international organisation can take place without the need to obtain any further authorisation, as provided for in Article 45(1) and recital 103 of the Regulation.

(3) As specified in Article 45(2) of Regulation (EU) 2016/679, the adoption of an adequacy decision has to be based on a comprehensive analysis of the third country's legal order, with respect to both the rules applicable to the data importers and the limitations and safeguards as regards access to personal data by public authorities. The assessment has to determine whether the third country in question guarantees a level of protection "essentially equivalent" to that ensured within the European Union (recital 104 of Regulation (EU) 2016/679). As clarified by the Court of Justice of the European Union, this does not require an identical level of protection.[2] In particular,

[1] OJ L 119, 4.5.2016, p. 1. ("GDPR").

[2] Case C-362/14, *Maximillian Schrems* v. *Data Protection Commissioner* ("*Schrems*"), EU:C:2015:650, paragraph 73.

the means to which the third country in question has recourse may differ from the ones employed in the European Union, as long as they prove, in practice, effective for ensuring an adequate level of protection.[3] The adequacy standard therefore does not require a point-to-point replication of Union rules. Rather, the test lies in whether, through the substance of privacy rights and their effective implementation, supervision and enforcement, the foreign system as a whole delivers the required level of protection.[4]

(4) The Commission has carefully analysed Japanese law and practice. Based on the findings developed in recitals (6) to (175), the Commission concludes that Japan ensures an adequate level of protection for personal data transferred to organisations falling within the scope of application of the Act on the Protection of Personal Information[5] and subject to the additional conditions referred to in this Decision. These conditions are laid down in the Supplementary Rules (Annex I) adopted by the Personal Information Protection Commission (PPC)[6] and the official representations, assurances and commitments by the Japanese government to the European Commission (Annex II).

(5) This Decision has the effect that transfers from a controller or processor in the European Economic Area (EEA)[7] to such organisations in Japan may take place without the need to obtain any further authorisation. This Decision does not affect the direct application of Regulation (EU) 2016/679 to such organisations when the conditions of its Article 3 are fulfilled.

2. The rules applying to the processing of data by business operators

2.1. The Japanese data protection framework

(6) The legal system governing privacy and data protection in Japan has its roots in the Constitution promulgated in 1946.

(7) Article 13 of the Constitution states:

> "All of the people shall be respected as individuals. Their right to life, liberty, and the pursuit of happiness shall, to the extent that it does not interfere with the public welfare, be the supreme consideration in legislation and in other governmental affairs."

(8) Based on that Article, the Japanese Supreme Court has clarified the rights of individuals as regards the protection of personal information. In a decision of 1969, it recognised the right to privacy and data protection as a constitutional right.[8] Notably, the Court held that "every individual has the liberty of protecting his/her own personal information from being disclosed to a third party or made public without good reason."

---

3 *Schrems*, paragraph 74.

4 See Communication from the Commission to the European Parliament and the Council, Exchanging and Protecting Personal Data in a Globalised World, COM(2017)7 of 10.01.2017, section 3.1., pp. 6-7.

5 Act on the Protection of Personal Information (Act No. 57, 2003).

6 More information on PPC is available at the following link: https://www.ppc.go.jp/en/ (including contact details for queries and complaints: https://www.ppc.go.jp/en/contactus/access/).

7 This Decision has EEA relevance. The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Joint Committee Decision (JCD) incorporating Regulation (EU) 2016/679 into Annex XI of the EEA Agreement was adopted by the EEA Joint Committee on 6 July 2018 and entered into force on 20 July 2018. The Regulation is thus covered by that agreement.

8 Supreme Court, Judgment of the Grand Bench of 24 December 1969, Keishu Vol. 23, N° 12, p. 1625.

Moreover, in a decision of 6 March 2008 ("Juki-Net")[9], the Supreme Court held that "citizens' liberty in private life shall be protected against the exercise of public authority, and it can be construed that, as one of an individual's liberties in private life, every individual has the liberty of protecting his/her own personal information from being disclosed to a third party or being made public without good reason."[10]

(9) On 30 May 2003, Japan enacted a series of laws in the area of data protection:

- The Act on the Protection of Personal Information (APPI);
- The Act on the Protection of Personal Information Held by Administrative Organs (APPIHAO);
- The Act on the Protection of Personal Information Held by Incorporated Administrative Agencies (APPI-IAA).

(10) The two latter acts (amended in 2016) contain provisions applicable to the protection of personal information by public sector entities. Data processing falling within the scope of application of those acts is not the object of the adequacy finding contained in this Decision, which is limited to the protection of personal information by "Personal Information Handling Business Operators" (PIHBOs) within the meaning of the APPI.

(11) The APPI has been reformed in recent years. The amended APPI was promulgated on 9 September 2015 and came into force on 30 May 2017. The amendment introduced a number of new safeguards, and also strengthened existing safeguards, thus bringing the Japanese data protection system closer to the European one. This includes, for instance, a set of enforceable individual rights or the establishment of an independent supervisory authority (PPC) entrusted with the oversight and enforcement of the APPI.

(12) In addition to the APPI, processing of personal information falling within the scope of this Decision is subject to implementing rules issued on the basis of the APPI. This includes an Amendment to the Cabinet Order to Enforce the Act on the Protection of Personal Information of 5 October 2016, and so-called Enforcement Rules for the Act on the Protection of Personal Information adopted by the PPC[11]. Both sets of rules are legally binding and enforceable and entered into force at the same time as the amended APPI.

(13) Moreover, on 28 October 2016 the Cabinet of Japan (consisting of the Prime Minister and the Ministers forming his government) issued a "Basic Policy" to "comprehensively and integrally promote measures concerning the protection of personal information". Pursuant to Article 7 of the APPI, the "Basic Policy" is issued in the form of a Cabinet Decision and includes policy orientations concerning the enforcement of the APPI, directed to both the central government and local governments.

(14) Recently, by a Cabinet Decision adopted on 12 June 2018, the Japanese government amended the "Basic Policy". With a view to facilitating international data transfers, that Cabinet Decision delegates to the PPC, as the authority competent for administering and implementing the APPI, "the power to take the necessary action to bridge differences of the systems and operations between Japan and the concerned foreign country based on Article 6 of the Act in view of ensuring appropriate handling of personal information received from such country". The Cabinet Decision stipulates

[9] Supreme Court, Judgment of 6 March 2008, Minshu Vol. 62 No. 3, p. 665.
[10] Supreme Court, Judgment of 6 March 2008, Minshu Vol. 62 No. 3, p. 665.
[11] Available at: https://www.ppc.go.jp/files/pdf/PPC_rules.pdf.

that this includes the power to establish enhanced protections through the adoption by the PPC of stricter rules supplementing and going beyond those laid down in the APPI and the Cabinet Order. Pursuant to that Decision, these stricter rules shall be binding and enforceable on Japanese business operators.

(15) On the basis of Article 6 of the APPI and that Cabinet Decision, the PPC on 15 June 2018 adopted "Supplementary Rules under the Act on the Protection of Personal Information for the Handling of Personal Data Transferred from the EU based on an Adequacy Decision" (the "Supplementary Rules") with a view to enhance the protection of personal information transferred from the European Union to Japan based on the present adequacy decision. Those Supplementary Rules are legally binding on Japanese business operators and enforceable, both by the PPC and by courts, in the same way as the provisions of the APPI that the Rules supplement with stricter and/or more detailed rules.[12] As Japanese business operators receiving and/or further processing personal data from the European Union will be under a legal obligation to comply with the Supplementary Rules, they will need to ensure (e.g. by technical ("tagging") or organisational means (storing in a dedicated database)) that they can identify such personal data throughout their "life cycle".[13] In the following sections, the content of each Supplementary Rule is analysed as part of the assessment of the articles of the APPI it complements.

(16) Unlike before the 2015 amendment when this fell into the competence of various Japanese Ministries in specific sectors, the APPI empowers the PPC to adopt "Guidelines" "to ensure the proper and effective implementation of action to be taken by a business operator" under the data protection rules. Through its Guidelines, PPC provides an authoritative interpretation of those rules, in particular the APPI. According to the information received from the PPC, those Guidelines form an integral part of the legal framework, to be read together with the text of the APPI, the Cabinet Order, the PPC Rules and a set of Q&A[14] prepared by PPC. They are therefore "binding on business operators". Where the Guidelines state that a business operator "must" or "should not" act in a specified way, the PPC will consider that non-compliance with the relevant provisions amounts to a violation of the law.[15]

---

12 See Supplementary Rules, (introductory section).

13 This is not put into question by the general requirement to maintain records (only) for a certain period of time. Even though the origin of the data is among the information that the acquiring PIHBO has to confirm according to Article 26(1) of the APPI, the requirement pursuant to Article 26(4) of the APPI in conjunction with Article 18 of the PPC Rules only concerns a particular form of record (see Article 16 of the PPC Rules) and does not prevent a PIHBO from ensuring identification of the data for longer periods. This has been confirmed by the PPC which has stated that "[t]he information on the origin of the EU data must be kept by the PIHBO for as long as it is necessary in order to be able to comply with the Supplementary Rules".

14 PPC, Questions & Answers, 16 February 2017 (amended on 30 May 2017), available at the following link: https://www.ppc.go.jp/files/pdf/kojouhouQA.pdf. The Q&A discuss a number of issues addressed in the Guidelines by providing practical examples such as what constitutes sensitive personal data, the interpretation of individual consent, third-party transfers in the context of cloud computing, or the record-keeping obligation applied to cross-border transfers. The Q&A are only available in Japanese.

15 Following a specific question, the PPC has informed the EDPB that "the Japanese courts base the[ir] interpretation on the Guidelines when applying the APPI/PPC Rules in individual cases brought before them and have thus directly referred to the text of the PPC Guidelines in their judgments. Therefore, also from this perspective the PPC Guidelines are binding on business operators. PPC is not aware that the Court has ever diverged from the Guidelines." In this respect, PPC has referred the Commission to a judgment in the area of data protection where the court explicitly based itself on guidelines for its findings (see Osaka District Court, decision of 19 May 2006, Hanrei Jiho, Vol. 1948, p. 122, where the court ruled that the business operator had an obligation to take a security control action based on such guidelines).

2.2. Material and personal scope

(17) The scope of application of the APPI is determined by the defined concepts of Personal Information, Personal Data and Personal Information Handling Business Operator. At the same time, the APPI provides for some important exemptions from its scope, most importantly for Anonymously Processed Personal Data and for specific types of processing by certain operators. While the APPI does not use the term "processing", it relies on the equivalent concept of "handling" which, according to the information received from the PPC, covers "any act on personal data" including the acquisition, input, accumulation, organisation, storage, editing/processing, renewal, erasure, output, utilization, or provision of personal information.

2.2.1. Definition of personal information

(18) First of all, as regards its material scope, the APPI distinguishes personal information from personal data, with only certain of the provisions of the Act being applicable to the former category. According to Article 2(1) of the APPI, the concept of "personal information" includes any information relating to a living individual which enables the identification of that individual. The definition distinguishes two categories of personal information: (i) individual identification codes and (ii) other personal information whereby a specific individual can be identified. The latter category also includes information which by itself does not enable identification but, when "readily collated" with other information, allows the identification of a specific individual. According to the PPC Guidelines[16], whether information can be considered as "readily collated" shall be judged on a case by case basis, taking into consideration the actual situation ("condition") of the business operator. This will be assumed if such collation is (or can be) performed by an average ("normal") business operator using the means available to that operator. For instance, information is not "readily collated" with other information if a business operator needs to make unusual efforts or commit illegal acts to obtain the information to be collated from one or more other business operators.

2.2.2. Definition of personal data

(19) Only certain forms of personal information fall within the notion of "personal data" under the APPI. In fact, "personal data" is defined as "personal information constituting a personal information database", i.e. a "collective body of information" comprising personal information "systematically organized so as to be able to search for particular personal information using a computer"[17] or "prescribed by cabinet order as having been systematically organized so as to be able to easily search for particular personal information" but "excluding those prescribed by cabinet order as having little possibility of harming an individual's rights and interests considering their utilization method".[18]

(20) This exception is further specified in Article 3(1) of the Cabinet Order, according to which the three following cumulative conditions must be fulfilled: (i) the collective body of information must have been "issued for the purpose of being sold to a large number of unspecified persons and the issuance of which has not been conducted in violation of the provisions of a law or order based thereon"; (ii) must be capable of being "purchased at any time by a large number of unspecified persons" and (iii) the personal data contained therein must be "provided for their original purpose without adding other

[16] PPC Guidelines (General Rule Edition), p. 6.

[17] This covers any electronic filing system. The PPC Guidelines (General Edition, p. 17) provide specific examples in this respect, for example an email address list stored in the email client software.

[18] Article 2(4) and (6) of the APPI.

information relating to a living individual". According to the explanations received from the PPC, this narrow exception was introduced with the aim of excluding telephone books or similar types of directories.

(21) For data collected in Japan, this distinction between "personal information" and "personal data" is relevant because such information may not always be part of a "personal information database" (for example, a single data set collected and processed manually) and therefore those provisions of the APPI that only relate to personal data will not apply.[19]

(22) By contrast, this distinction will not be relevant for personal data imported from the European Union to Japan on the basis of an adequacy decision. As such data will typically be transferred by electronic means (given that in the digital era this is the usual way of exchanging data, especially over a large distance as between the EU and Japan), and hence become part of the data importer's electronic filing system, such EU data will fall into the category of "personal data" under the APPI. In the exceptional case that personal data would be transferred from the EU by other means (e.g. in paper form), it will still be covered by the APPI if following the transfer it becomes part of a "collective body of information" systematically organised so as to allow easy search for specific information (Article 2(4)(ii) APPI). According to Article 3(2) of the Cabinet Order, this will be the case where the information is arranged "according to a certain rule" and the database includes tools such as for instance a table of contents or index to facilitate the search. This corresponds to the definition of a "filing system" within the meaning of Article 2(1) of the GDPR.

2.2.3. Definition of retained personal data

(23) Certain provisions of the APPI, notably Articles 27 to 30 relating to individual rights, apply only to a specific category of personal data, namely "retained personal data". Those are defined under Article 2(7) of the APPI as personal data other than those which are either (i) "prescribed by cabinet order as likely to harm the public or other interests if their presence or absence is made known" or (ii) "set to be deleted within a period of no longer than one year that is prescribed by cabinet order".

(24) As regards the first of those two categories, it is explained in Article 4 of the Cabinet Order and covers four types of exemptions.[20] These exemptions pursue similar objectives as those listed in Article 23(1) of Regulation (EU) 2016/679, notably protection of the data subject ("principal" in the terminology of the APPI) and the freedom of others, national security, public security, criminal law enforcement or other important objectives of general public interest. In addition, it results from the wording

[19] For example, Article 23 of the APPI on the conditions for sharing personal data with third parties.

[20] Namely, personal data (i) "in relation to which there is a possibility that if the presence or absence of the said personal data is made known, it would harm a principal or third party's life, body or fortune"; (ii) data "in relation to which there is a possibility that if the presence or absence of the said personal data is made known, it would encourage or induce an illegal or unjust act"; (iii) data "in relation to which there is a possibility that if the presence or absence of the said personal data is made known, it would undermine national security, destroy a trust relationship with a foreign country or international organisation, or suffer disadvantage in negotiations with a foreign country or international organisation"; and (iv) those "in relation to which there is a possibility that if the presence or absence of the said personal data is made known, it would hinder the maintenance of public safety and order such as the prevention, suppression or investigation of a crime".

of Article 4(1)(i)-(iv) of the Cabinet Order that their application always presupposes a specific risk for one of the protected important interests.[21]

(25) The second category has been further specified in Article 5 of the Cabinet Order. Read in conjunction with Article 2(7) of the APPI, it exempts from the scope of the notion of retained personal data, and thus from the individual rights under the APPI, those personal data that are "set to be deleted" within a period of six months. The PPC has explained that this exemption aims at incentivising business operators to retain and process data for the shortest period possible. However, this would mean that EU data subjects would not be able to benefit from important rights for no other reason than the duration of the retention of their data by the concerned business operator.

(26) In order to address this situation, Supplementary Rule (2) requires that personal data transferred from the European Union "be handled as retained personal data within the meaning of Article 2, paragraph (7) of the Act, irrespective of the period within which it is set to be deleted". Hence, the retention period will have no bearing on the rights afforded to EU data subjects.

2.2.4. Definition of anonymously processed personal information

(27) Requirements applicable to anonymously processed personal information, as defined in Article 2(9) of the APPI, are stipulated in Section 2 of Chapter 4 of the Act ("Duties of an Anonymously Processed Information Handling Business Operator"). Conversely, such information is not governed by the provisions of Section 1 of Chapter IV of the APPI which includes the articles stipulating the data protection safeguards and rights applying to the processing of personal data under that Act. Consequently, while "anonymously processed personal information" is not subject to the "standard" data protection rules (those specified in Section 1 of Chapter IV and in Article 42 of the APPI), they do fall within the scope of application of the APPI, notably Articles 36 to 39.

(28) According to Article 2(9) of the APPI, "anonymously processed personal information" is information relating to an individual that has been "produced from processing personal information" through measures prescribed in the APPI (Article 36(1)) and specified in the PPC rules (Article 19), with the result that it has become impossible to identify a specific individual or restore the personal information.

(29) It results from those provisions, as also confirmed by the PPC, that the process of rendering personal information "anonymous" does not need to be technically irreversible. Pursuant to Article 36(2) of the APPI, business operators handling "anonymously processed personal information" are merely required to prevent re-identification by taking measures to ensure the security of "the descriptions etc. and individual identification codes deleted from personal information used to produce the anonymously processed information, and information relating to a processing method carried out".

(30) Given that "anonymously processed 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 Regulation (EU) 2016/679, would

[21] Under these conditions, no notification of the individual is required. This is in line with Article 23(2)(h) of the GDPR, which provides that data subjects do not have to be informed about the restriction if this "may be prejudicial to the purpose of the restriction".

be considered a form of "pseudonymisation" rather than "anonymisation" (thus not changing its nature as personal data).

(31) To address that situation, the Supplementary Rules provide for additional requirements applicable only to personal data transferred from the European Union under this Decision. According to Rule (5) of the Supplementary Rules, such personal information shall only be considered "anonymously processed 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". The latter has been specified in the Supplementary Rules as information relating to descriptions and individual identification codes which were deleted from personal information used to produce "anonymously processed personal information", as well as information relating to a processing method applied while deleting these descriptions and individual identification codes. In other terms, the Supplementary Rules require the business operator producing "anonymously processed personal information" to destroy the "key" permitting re-identification of the data. This means that personal data originating from the European Union will fall under the APPI provisions regarding "anonymously processed personal information" only in cases where they would likewise be considered anonymous information under Regulation (EU) 2016/679.[22]

2.2.5. Definition of Personal Information Handling Business Operator (PIHBO)

(32) Concerning its personal scope, the APPI applies only to PIHBOs. A PIHBO is defined in Article 2(5) of the APPI as "a person providing a personal information database etc. for use in business", with the exclusion of the government and administrative agencies at both central and local level.

(33) According to the PPC Guidelines, "business" means any "conduct aimed at exercising, for a certain goal, regardless of whether or not for profit, repeatedly and continuously, a socially recognised enterprise". Organisations without legal personality (such as de facto associations) or individuals are considered as a PIHBO if they provide (use) a personal information database etc. for their business.[23]. Therefore, 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 in 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.

(34) As regards the beneficiaries of the protections set forth in the APPI, the Act makes no distinction based on an individual's nationality, residence or location. The same applies to the possibilities for individuals to seek redress, be it from the PPC or from courts.

2.2.6. Concepts of controller and processor

(35) Under the APPI, no specific distinction is drawn between the obligations imposed on controllers and processors. The absence of this distinction does not affect the level of protection because all PIHBOs are subject to all provisions of the Act. A PIHBO that entrusts the handling of personal data to a trustee (the equivalent of a processor under the GDPR) remains subject to the obligations under the APPI and Supplementary

[22] See Regulation (EU) 2016/679, recital 26.
[23] PPC Guidelines (General Rule Edition), p. 18.

Rules with regard to the data it has entrusted. Additionally, under Article 22 of the APPI, it is bound to "exercise necessary and appropriate supervision" over the trustee. In turn, as the PPC has confirmed, the trustee is itself bound by all the obligations in the APPI and the Supplementary Rules.

2.2.7. Sectoral exclusions

(36) Article 76 of the APPI excludes certain types of data processing from the application of Chapter IV of the Act, which contains the central data protection provisions (basic principles, obligations of business operators, individual rights, supervision by the PPC). Processing covered by the sectoral exclusion in Article 76 is also exempted from the enforcement powers of the PPC, pursuant to Article 43(2) of the APPI.[24]

(37) The relevant categories for the sectoral exclusion in Article 76 of the APPI are defined by using a double criterion based on the type of PIHBO processing the personal information and the purpose of processing. More specifically, the exclusion applies to: (i) broadcasting institutions, newspaper publishers, communication agencies or other press organisations (including any individuals carrying out press activities as their business) to the extent they process personal information for press purposes; (ii) persons engaged in professional writing, to the extent this involves personal information; (iii) universities and any other organisations or groups aimed at academic studies, or any person belonging to such an organisation, to the extent they process personal information for the purpose of academic studies; (iv) religious bodies to the extent they process personal information for purposes of religious activity (including all related activities); and (v) political bodies to the extent they process personal information for the purposes of their political activity (including all related activities). Processing of personal information for one of the purposes listed in Article 76 by other types of PIHBOs as well as processing of personal information by one of the listed PIHBOs for other purposes, for instance in the employment context, remain covered by the provisions of Chapter IV.

(38) In order to ensure an adequate level of protection of personal data transferred from the European Union to business operators in Japan, only processing of personal information falling within the scope of Chapter IV of the APPI – i.e. by a PIHBO to the extent the processing situation does not correspond to one of the sectoral exclusions – should be covered by this Decision. Its scope should therefore be aligned to that of the APPI. According to the information received from the PPC, where a PIHBO covered by this Decision subsequently modifies the utilisation purpose (to the extent this is permissible) and would then be covered by one of the sectoral exclusions in Article 76 of the APPI, this would be considered as an international transfer (given that, in such cases, the processing of the personal information would no longer be covered by Chapter IV of the APPI and thus fall outside its scope of application). The same would apply in case a PIHBO provides personal information to an entity covered by Article 76 of the APPI for use for one of the processing purposes indicated in that provision. As regards personal data transferred from the European Union, this would therefore constitute an onward transfer subject to the relevant safeguards (notably those specified in Article 24 of the APPI and Supplementary Rule (4)). Where the PIHBO relies on the data subject's consent[25], it would have to provide him/her with all

[24] Regarding other operators, the PPC shall, when exercising its powers of investigation and enforcement, not preclude them from exercising their right to freedom of expression, freedom of academia, freedom of religion, and freedom of political activity (Article 43(1) of the APPI).

[25] As explained by the PPC, consent is interpreted in the PPC Guidelines as an "expression of a principal's intention to the effect that he/she accepts that his/her personal information may be handled with a method

the necessary information, including that the personal information would no longer be protected by the APPI.

2.3. Safeguards, rights and obligations

2.3.1. Purpose limitation

(39) Personal data should be processed for a specific purpose and subsequently used only insofar as this is not incompatible with the purpose of processing. This data protection principle is guaranteed under Articles 15 and 16 of the APPI.

(40) The APPI relies on the principle that a business operator has to specify the utilisation purpose "as explicitly as possible" (Article 15(1)) and is then bound by such purpose when processing the data.

(41) In that respect, Article 15(2) of the APPI provides that the initial purpose must not be altered by the PIHBO "beyond the scope recognized reasonably relevant to the pre-altered utilization purpose", interpreted in the PPC Guidelines as corresponding to what can be objectively anticipated by the data subject based on "normal social conventions".[26]

(42) Moreover, under Article 16(1) of the APPI, PIHBOs are prohibited from handling personal information beyond the "necessary scope to achieve a utilization purpose" specified under Article 15 without obtaining in advance a data subject's consent, unless one of the derogations in Article 16(3) applies.[27]

(43) When it comes to personal information acquired from another business operator, the PIHBO is, in principle, free to set a new utilisation purpose.[28] In order to ensure that, in case of a transfer from the European Union, such a recipient is bound by the purpose for which the data was transferred, Supplementary Rule (3) requires that, in cases "where a [PIHBO] receives personal data from the EU based on an adequacy decision" or such an operator "receives from another [PIHBO] personal data previously transferred from the EU based on an adequacy decision" (onward sharing), the recipient has to "specify the purpose of utilising the said personal data within the scope of the utilisation purpose for which the data was originally or subsequently

---

indicated by a personal information handling business". The PPC Guidelines (General Rule Edition, p.24) list the ways of consenting that are considered "usual business practices in Japan", i.e. oral agreement, returning forms or other documents, agreement via e-mail, ticking a box on a web page, clicking on a home page, using a consent button, tapping a touch panel, etc. All these methods constitute an express form of consent.

[26] The Q&A issued by PPC contain a number of examples to illustrate this notion. Examples of situations where the alteration remains within a reasonably relevant scope notably include the use of personal information acquired from buyers of goods or services in the context of a commercial transaction, for the purpose of informing those buyers about other relevant goods or services available (e.g. a fitness club operator who registers the e-mail addresses of members to inform them about courses and programs). At the same time, the Q&A also include an example of a situation where the alteration of the utilisation purpose is not allowed, namely if a company sends information on the company's goods and services to e-mail addresses that it has collected for the purpose of warning about fraud or theft of a membership card.

[27] These exemptions may result from other laws and regulations, or concern situations where the handling of personal information is necessary (i) for the "protection of human life, body or property"; (ii) to "enhance public hygiene or promote the growth of healthy children"; or (iii) "to cooperate with government agencies or bodies or with their representatives" in the performance of their statutory tasks. Moreover, categories (i) and (ii) only apply if it is difficult to obtain a data subject's consent, and category (iii) only if there is a risk that obtaining a data subject's consent would interfere with the performance of such tasks.

[28] This being said, based on Article 23(1) of the APPI, consent of the individual is in principle required for the disclosure of data to a third party. In this way, the individual is able to exercise some control on the use of his/her data by another business operator.

received". In other words, the rule ensures that in a transfer context the purpose specified pursuant to Regulation (EU) 2016/679 continues to determine the processing, and that a change of that purpose at any stage of the processing chain in Japan would require the consent of the EU data subject. While obtaining this consent requires the PIHBO to contact the data subject, where this is not possible the consequence is simply that the original purpose has to be maintained.

2.3.2. Lawfulness and fairness of processing

(44) The additional protection referred to in recital (43) is all the more relevant as it is through the purpose limitation principle that the Japanese system also ensures that personal data is processed lawfully and fairly.

(45) Under the APPI, when a PIHBO collects personal information, it is required to specify the purpose of utilising the personal information in a detailed manner[29] and promptly inform the data subject of (or disclose to the public) this utilisation purpose.[30] In addition, Article 17 of the APPI provides that a PIHBO shall not acquire personal information by deceit or other improper means. As regards certain categories of data such as special-care required personal information, their acquisition requires the consent of the data subject (Article 17(2) of the APPI).

(46) Subsequently, as explained in recitals (41) and (42), the PIHBO is prohibited from processing the personal information for other purposes, except where the data subject consents to such processing or where one of the derogations pursuant to Article 16(3) of the APPI applies.

(47) Finally, when it comes to the further provision of personal information to a third party[31], Article 23(1) of the APPI limits such disclosure to specific cases, with the prior consent by the data subject as the general rule.[32] Article 23(2), (3) and (4) of the APPI provide for exceptions to the requirement to obtain consent. However, these exceptions do only apply to non-sensitive data and require that the business operator in advance informs the individuals concerned of the intention to disclose their personal information to a third party and the possibility to object to any further disclosure.[33]

(48) As regards transfers from the European Union, personal data will necessarily have been first collected and processed in the EU in compliance with Regulation (EU) 2016/679. This will always involve, on the one hand, collection and processing, including for the transfer from the European Union to Japan, on the basis of one of the legal grounds listed in Article 6(1) of the Regulation and, on the other hand, collection for a specific, explicit and legitimate purpose as well as the prohibition of further

[29] According to Article 15(1) of the APPI, such specification has to be "as explicitly as possible".

[30] Article 18(1) of the APPI.

[31] While trustees are excluded from the notion of "third party" for the purposes of the application of Article 23 (see paragraph 5), this exclusion applies only insofar as the trustee handles personal data within the limits of the entrustment ("within the necessary scope to achieve a utilization purpose"), i.e. acts as a processor.

[32] The other (exceptional) grounds are: (i) the provision of personal information "based on laws and regulations"; (ii) cases "in which there is a need to protect a human life, body or fortune, and when it is difficult to obtain a principal's consent"; (iii) cases "in which there is a special need to enhance public hygiene or promote fostering healthy children, and when it is difficult to obtain a principal's consent"; and (iv) cases "in which there is a need to cooperate in regard to a central government organisation or a local government, or a person entrusted by them performing affairs prescribed by laws and regulations, and when there is a possibility that obtaining a principal's consent would interfere with the performance of the said affairs".

[33] The information to be provided includes, notably, the categories of personal data to be shared with a third party and the method of transmission. Moreover, the PIHBO must inform the data subject of the possibility to oppose the transmission and how to make such a request.

processing, including by way of a transfer, in a manner that is incompatible with such purpose as laid down in Articles 5(1)(b) and 6(4) of the Regulation.

(49) Following the transfer, according to Supplementary Rule (3), the PIHBO that will receive the data will have to "confirm" the specific purpose(s) underlying the transfer (i.e. the purpose specified pursuant to Regulation (EU) 2016/679) and further process that data in line with such purpose(s).[34] This means not only that the initial acquirer of such personal data in Japan but also any future recipient of the data (including a trustee) is bound by the purpose(s) specified under the Regulation.

(50) Furthermore, in case the PIHBO would like to change the purpose as previously specified under Regulation (EU) 2016/679, pursuant to Article 16(1) of the APPI it would have to obtain, in principle, the consent of the data subject. Without that consent, any data processing going beyond the scope necessary for achieving that utilisation purpose would constitute a violation of Article 16(1) that would be enforceable by the PPC and the courts.

(51) Hence, given that under Regulation (EU) 2016/679 a transfer requires a valid legal basis and specific purpose, which are reflected in the utilization purpose "confirmed" under the APPI, the combination of the relevant provisions of the APPI and of Supplementary Rule (3) ensures the continued lawfulness of the processing of EU data in Japan.

2.3.3. Data accuracy and minimisation

(52) Data should be accurate and, where necessary, kept up to date. It should also be adequate, relevant and not excessive in relation to the purposes for which it is processed.

(53) These principles are ensured in Japanese law by Article 16(1) of the APPI, which prohibits the handling of personal information beyond "the necessary scope to achieve a utilisation purpose". As explained by the PPC, this not only excludes the use of data that is not adequate and the excessive use of data (beyond what is necessary for achieving the utilisation purpose), but also entails the prohibition to handle data not relevant for the achievement of the utilisation purpose.

(54) As concerns the obligation to keep data accurate and up to date, Article 19 of the APPI requires the PIHBO to "strive to keep personal data accurate and up-to-date within the scope necessary to achieve a utilisation purpose". That provision should be read together with Article 16(1) of the APPI: according to the explanations received from the PPC, if a PIHBO fails to meet the prescribed standards of accuracy, the processing of the personal information will not be considered as achieving the utilisation purpose and hence, its handling will become unlawful under Article 16(1).

2.3.4. Storage limitation

(55) Data should in principle be kept for no longer than is necessary for the purposes for which the personal data is processed.

(56) According to Article 19 of the APPI, PIHBOs are required to "strive […] to delete the personal data without delay when such utilisation has become unnecessary". That provision needs to be read in conjunction with Article 16(1) of the APPI prohibiting

[34] According to Article 26(1)(ii) of the APPI, a PIHBO is required, when receiving personal data from a third party, to "confirm" (verify) the "details of the acquisition of the personal data by the third party", including the purpose of that acquisition. Although Article 26 does not expressly specify that the PIHBO then has to follow that purpose, this is explicitly required by Supplementary Rule (3).

the handling of personal information beyond "the necessary scope to achieve a utilisation purpose". Once the utilisation purpose has been achieved, processing of personal information cannot be considered necessary anymore and, hence, cannot continue (unless the PIHBO obtains the data subject's consent to do so).

2.3.5. Data security

(57) Personal data should be processed in a manner that ensures their security, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage. To that end, business operators should take appropriate technical or organisational measures to protect personal data from possible threats. These measures should be assessed taking into consideration the state of the art and related costs.

(58) This principle is implemented in Japanese law by Article 20 of the APPI, providing that a PIHBO "shall take necessary and appropriate action for the security control of personal data including preventing the leakage, loss or damage of its handled personal data." The PPC Guidelines explain the measures to be taken, including the methods for the establishment of basic policies, data handling rules and various "control actions" (regarding organisational safety as well as human, physical and technological security).[35] In addition, the PPC Guidelines and a dedicated Notice (Appendix 8 on "Contents of the safety management measures that have to be taken") published by the PPC provide more details on measures concerning security incidents involving, for example, the leakage of personal information, as part of the security management measures to be taken by PIHBOs.[36]

(59) Furthermore, whenever personal information is handled by employees or sub-contractors, "necessary and appropriate supervision" must be ensured under Articles 20 and 21 of the APPI for security control purposes. Finally, pursuant to Article 83 of the APPI, intentional leakage or theft of personal information is punishable by a sanction of up to one year of imprisonment.

2.3.6. Transparency

(60) Data subjects should be informed of the main features of the processing of their personal data.

(61) Article 18(1) of the APPI requires the PIHBO to make information about the utilisation purpose of the personal information acquired available to the data subject, except for "cases where a utilisation purpose has been disclosed in advance to the public". The same obligation applies in case of a permissible change of purpose (Article 18(3)). This also ensures that the data subject is informed of the fact that his/her data has been collected. Although the APPI does not generally require the PIHBO to inform the data subject about the expected recipients of personal information at the stage of collection, such information is a necessary condition for any subsequent disclosure of information to a third party (recipient) based on Article 23(2), hence where this is done without prior consent of the data subject.

(62) As regards "retained personal data", Article 27 APPI provides that the PIHBO shall inform the data subject about its identity (contact details), the utilisation purpose and

[35] PPC Guidelines (General Rule Edition), p. 41 and pp. 86 to 98.

[36] According to section 3-3-2 of the PPC Guidelines, in case such leakage, damage or loss occurs, the PIHBO is required to carry out the necessary investigations and in particular assess the magnitude of the infringment to the individual's rights and interests as well as the nature and the amount of personal information concerned.

the procedures for responding to a request concerning the data subject's individual rights under Articles 28, 29 and 30 of the APPI.

(63) As under the Supplementary Rules personal data transferred from the European Union will be considered "retained personal data" irrespective of their retention period (unless covered by exemptions), they will always be subject to the transparency requirements under both of the aforementioned provisions.

(64) Both the requirements of Article 18 and the obligation to inform about the utilisation purpose under Article 27 of the APPI are subject to the same set of exceptions, mostly based on public interest considerations and the protection of rights and interests of the data subject, third parties and the controller.[37] According to the interpretation developed in the PPC Guidelines, those exceptions apply in very specific situations, such as where information on the utilisation purpose would risk undermining legitimate measures taken by the business operator to protect certain interests (e.g. fight against fraud, industrial espionage, sabotage).

2.3.7. Special categories of data

(65) Specific safeguards should exist where "special categories" of data are being processed.

(66) "Special care-required personal information" is defined in Article 2(3) of the APPI. That provision refers to "personal information comprising a principal's race, creed, social status, medical history, criminal record, fact of having suffered damage by a crime, or other descriptions etc. prescribed by Cabinet Order as those of which the handling requires special care so as not to cause unfair discrimination, prejudice or other disadvantages to the principal." These categories correspond for a large part to the list of sensitive data under Articles 9 and 10 of Regulation (EU) 2016/679. In particular, "medical history" corresponds to health data, while "criminal record and the fact of having suffered damage by a crime" are substantially the same as the categories referred to in Article 10 of Regulation (EU) 2016/679. The categories referred to in Article 2(3) of the APPI are subject to further interpretation in the Cabinet Order and PPC Guidelines. According to section 2.3 point (8) of the PPC Guidelines, the sub-categories of "medical history" detailed in Article 2(ii) and (iii) of the Cabinet Order are interpreted as covering genetic and biometric data. Also, while the list does not expressly include the terms "ethnic origin" and "political opinion", it does include references to "race" and "creed". As explained in section 2.3 points (1) and (2) of the PPC Guidelines, reference to "race" covers "ethnic ties or ties to a certain part of the world", while "creed" is understood as including both religious and political views.

(67) As is clear from the wording of the provision, this is not a closed list as further categories of data can be added to the extent that their processing creates a risk of "unfair discrimination, prejudice or other disadvantages to the principal".

(68) While the concept of "sensitive" data is inherently a social construct in that it is grounded in cultural and legal traditions, moral considerations, policy choices etc. of a given society, given the importance of ensuring adequate safeguards to sensitive data

[37] These are (i) cases in which there is a possibility that informing the data subject of the utilisation purpose, or making it public, would "harm a principal or third party's life, body, fortune or other rights and interests" or "the rights or legitimate interests of the […] PIHBO"; (ii) cases in which "there is a need to cooperate in regard to a central government organisation or a local government" in the performance of their statutory tasks and if such information or disclosure would interfere with such "affairs"; (iii) cases in which the utilisation purpose is clear based on the situation in which the data has been acquired.

when transferred to business operators in Japan the Commission has obtained that the special protections afforded to "special care-required personal information" under Japanese law are extended to all categories recognised as "sensitive data" in Regulation (EU) 2016/679. To this end, Supplementary Rule (1) provides that data transferred from the European Union concerning an individual's sex life, sexual orientation or trade-union membership shall be processed by PIHBOs "in the same manner as special care-required personal information within the meaning of Article 2, paragraph (3) of the [APPI]".

(69) Concerning the additional substantive safeguards applying to special care-required personal information, according to Article 17(2) of the APPI, PIHBOs are not allowed to acquire such type of data without prior consent of the individual concerned, subject only to limited exceptions.[38] Furthermore, this category of personal information is excluded from the possibility of third party disclosure based on the procedure provided for under Article 23(2) of the APPI (allowing transmission of data to third parties without the prior consent of the individual concerned).

2.3.8. Accountability

(70) Under the accountability principle, entities processing data are required to put in place appropriate technical and organisational measures to effectively comply with their data protection obligations and be able to demonstrate such compliance, in particular to the competent supervisory authority.

(71) As mentioned in footnote 34 (recital (49)), PIHBOs are required, under Article 26(1) of the APPI, to verify the identity of a third party providing personal data to them and the "circumstances" under which such data was acquired by the third party (in case of personal data covered by this Decision, according to the APPI and Supplementary Rule (3) those circumstances shall include the fact that the data originates from the European Union as well as the purpose of the original data transfer). Among others, that measure aims at ensuring the lawfulness of data processing throughout the chain of PIHBOs handling the personal data. Furthermore, under Article 26(3) of the APPI, PIHBOs are required to keep a record of the date of receipt and the (mandatory) information received from the third party pursuant to paragraph 1, as well as the name of the individual concerned (data subject), the categories of data processed and, to the extent relevant, the fact that the data subject has given consent for sharing his/her personal data. As specified in Article 18 of the PPC Rules, those records must be

[38] The exemptions are the following: (i) "cases based on laws and regulations"; (ii) "cases in which there is a need to protect a human life, body or fortune, and when it is difficult to obtain a principal's consent"; (iii) "cases in which there is a special need to enhance public hygiene or promote fostering healthy children, and when it is difficult to obtain a principal's consent"; (iv) "cases in which there is a need to cooperate with regard to a central government organisation or a local government, or a person entrusted by them performing affairs prescribed by laws and regulations, and when there is a possibility that obtaining a principal's consent would interfere with the performance of the said affairs"; and (v) cases in which the said special care-required personal information is disclosed to the public by a data subject, a government organisation, a local government, a person falling within one of the categories of Article 76(1) or other persons prescribed by rules of the PPC. A further category concerns "other cases prescribed by Cabinet Order as equivalent to those cases set forth in each preceding item" and under the current Cabinet Order notably covers conspicuous features of a person (e.g. a visible health condition) if the sensitive data has been acquired (unintentionally) by visual observation, filming or photographing of the data subject, e.g. by CCTV cameras.

preserved for a period of at least one to three years, depending on the circumstances. In the exercise of its tasks, the PPC can require the submission of such records.[39]

(72) PIHBOs have to promptly and appropriately deal with complaints from concerned individuals about the processing of their personal information. To facilitate the handling of complaints, they shall establish a "system necessary for achieving [this] purpose", which implies that they should put in place appropriate procedures within their organisation (for instance assign responsibilities or provide a contact point).

(73) Finally, the APPI creates a framework for the participation of sectoral industry organisations in ensuring a high level of compliance (see Chapter IV, Section 4). The role of such accredited personal information protection organisations[40] is to promote the protection of personal information by supporting businesses through their expertise, but also to contribute to the implementation of safeguards, notably by handling individual complaints and helping to solve related conflicts. To that end, they may request participating PIHBOs, if appropriate, to adopt necessary measures.[41] Moreover, in case of data breaches or other security incidents PHIBOs shall in principle inform the PPC as well as the data subject (or the public) and take necessary action, including measures to minimise any damage and to prevent any recurrence of similar incidents.[42] While those are voluntary schemes, on 10 August 2017 the PPC had listed 44 organisations, with the largest one, Japan Information Processing and Development Center (JIPDEC), alone counting 15,436 participating business operators.[43] Accredited schemes include sector associations such as for instance the Japan Securities Dealers Association, the Japan Association of Car Driving Schools or the Association of Marriage Brokers.[44]

(74) Accredited personal information protection organisations submit annual reports on their operations. According to the "Overview of the Implementation Status [of] the APPI in FY 2015" published by the PPC, accredited personal information protection organisations received a total of 442 complaints, required 123 explanations from business operators under their jurisdiction, requested documents from these operators in 41 cases, gave 181 instructions and made two recommendations.[45]

2.3.9. Restrictions on onward transfers

(75) The level of protection afforded to personal data transferred from the European Union to business operators in Japan must not be undermined by the further transfer of such data to recipients in a third country outside Japan. Such "onward transfers", which from the perspective of the Japanese business operator constitute international transfers from Japan, should be permitted only where the further recipient outside Japan is itself subject to rules ensuring a similar level of protection as guaranteed within the Japanese legal order.

---

39 According to Article 40(1) of the APPI, the PPC may, to the extent necessary to implement the relevant provisions of the APPI, require a PIHBO to submit necessary information or material relating to the handling of personal information.

40 The APPI provides i.a. for rules on the accreditation of such organisations; see Articles 47-50 of the APPI.

41 Article 52 of the APPI.

42 PPC Notification No. 1/2017 "Concerning the actions to be taken in such instances as the cases where a personal data breach or other incident has occurred".

43 According to the figures published on JIPDEC's PrivacyMark website, dated 2 October 2017.

44 PPC, List of accredited personal information protection organisations, available on the internet at: https://www.ppc.go.jp/personal/nintei/list/ or https://www.ppc.go.jp/files/pdf/nintei_list.pdf.

45 PPC, Overview of Implementation Status of the APPI in FY 2015 (October 2016), available (only in Japanese) on the internet at: https://www.ppc.go.jp/files/pdf/personal_sekougaiyou_27ppc.pdf.

(76) A first protection is enshrined in Article 24 of the APPI which generally prohibits the transfer of personal data to a third party outside the territory of Japan without the prior consent of the individual concerned. Supplementary Rule (4) ensures that in the case of data transfers from the European Union such consent will be particularly well informed as it requires that the individual concerned shall be "provided information on the circumstances surrounding the transfer necessary for the principal to make a decision on his/her consent". On that basis, the data subject shall be informed 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 will allow him/her to assess the risk for privacy involved with the transfer. Also, as can be inferred from Article 23 of the APPI (see recital 47), the information provided to the principal should cover the compulsory items under its paragraph 2, namely the categories of personal data provided to a third party and the method of disclosure.

(77) Article 24 of the APPI, applied together with Article 11-2 of the PPC Rules, provides several exceptions to this consent-based rule. Furthermore, pursuant to Article 24, the same derogations as those applicable under Article 23(1) of the APPI apply also to international data transfers.[46]

(78) To ensure continuity of protection in case of personal data transferred from the European Union to Japan under this Decision, Supplementary Rule (4) enhances the level of protection for onward transfers of such data by the PIHBO to a third country recipient. It does so by limiting and framing the bases for international transfers that can be used by the PIHBO as an alternative to consent. More specifically, and without prejudice to the derogations set forth in Article 23(1) of the APPI, personal data transferred under this 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 24 of the APPI as providing an equivalent level of protection to the one guaranteed in Japan[47]; or (ii) where the PIHBO 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. The second category corresponds to the instruments used under Regulation (EU) 2016/679 to ensure appropriate safeguards (in particular, contractual clauses and binding corporate rules). In addition, as confirmed by the PPC, even in those cases, the transfer remains subject to the general rules applicable to any provision of personal data to a third party under the APPI (i.e. the requirement to obtain consent under Article 23(1) or, alternatively, the information requirement with a possibility to opt out under Article 23(2) of the APPI). In case the data subject cannot be reached with a request for consent or in order to provide the required advance information under Article 23(2) of the APPI, the transfer may not take place.

(79) Therefore, outside the cases where the PPC has found that the third country in question ensures a level of protection equivalent to the one guaranteed by the APPI[48],

---

[46] See footnote 32.

[47] According to Article 11 of the PPC Rules, this not only requires substantive standards equivalent to the APPI effectively supervised by an independent enforcement authority, but also that the implementation of the relevant rules in the third country is ensured.

[48] So far, the PPC has not yet adopted any decision under Article 24 of the APPI recognising a third country as providing an equivalent level of protection to the one guaranteed in Japan. The only decision it currently considers adopting concerns the EEA. As regards possible other decisions in the future, the Commission will closely monitor the situation and, if necessary, take appropriate measures to address possible adverse effects for the continuity of protection (see below recitals 176, 177, 184 and Article 3(1)).

the requirements set forth in Supplementary Rule (4) exclude the use of transfer instruments that do no create a binding relationship between the Japanese data exporter and the third country's data importer of the data and that do not guarantee the 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[49], 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.[50]

(80) Finally, a further safeguard in case of (onward) transfers follows from Articles 20 and 22 of the APPI. According to these provisions, where a third country operator (data importer) acts on behalf of the PIHBO (data exporter), that is as a (sub-) processor, the latter has to ensure supervision over the former as regards security of data processing.

2.3.10. Individual rights

(81) Like EU data protection law, the APPI grants individuals a number of enforceable rights. This includes the right to access ('disclosure'), rectification and erasure as well as the right to object ('utilisation cease').

(82) First, pursuant to Article 28(1) and (2) of the APPI, a data subject has a right to request from a PIHBO to "disclos[e] retained personal data that can identify him- or herself" and, upon receipt of such a request, the PIHBO "shall […] disclose retained personal data" to the data subject. Article 29 (right to correction) and 30 (right to utilisation cease) have the same structure as Article 28.

(83) Article 9 of the Cabinet Order specifies that disclosure of personal information as referred to in Article 28(2) of the APPI shall be performed in writing, unless the PIHBO and the data subject have agreed otherwise.

(84) These rights are subject to three types of restrictions, relating to the individual's own or third parties' rights and interests[51], serious interference with the PIHBO's business operations[52] as well as cases in which disclosure would violate other laws or regulations.[53] The situations in which these restrictions would apply are similar to

---

[49] Although only two Japanese companies have certified under the APEC CBPR System (see https://english.jipdec.or.jp/sp/protection_org/cbpr/list.html). Outside Japan, the only other business operators that have certified under this System are a small number (23) of U.S. companies (see https://www.trustarc.com/consumer-resources/trusted-directory/#apec-list).

[50] For example, no definition and specific protections for sensitive data, no obligation of limited data retention. See also Article 29 Working Party, Opinion 02/2014 on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross-Border Privacy Rules submitted to APEC CBPR Accountability Agents, 6 March 2014.

[51] According to the PPC, only such interests may justify a restriction that are "worth protecting legally". This assessment has to be carried out on a case-by-case basis "taking into account the interference with the fundamental right to privacy including data protection as recognised by the Constitution and judicial precedents." Protected interests may include, for instance, trade or other commercial secrets.

[52] The concept of "interfering seriously with the proper implementation of the operator's business" is illustrated in the PPC Guidelines through different examples, for instance repeated and identical complex requests made by the same individual where such requests involve a significant burden for a business operator that would compromise its ability to answer other requests (PPC Guidelines (General Rule Edition), p. 62). More generally, the PPC has confirmed that this category is limited to exceptional cases going beyond mere inconvenience. In particular, a PIHBO cannot refuse disclosure merely because a large amount of data has been sought.

[53] As confirmed by the PPC, such laws have to respect the right to privacy as ensured in the Constitution and thus "reflect a necessary and reasonsable restriction."

some of the exceptions applicable under Article 23(1) of Regulation (EU) 2016/679, which allows for restrictions of the rights of individuals for reasons related to the "protection of the data subject or the rights and freedoms of others" or "other important objectives of general public interest". Although the category of cases in which disclosure would violate "other laws or regulations" may appear broad, laws and regulations providing for limitations in this regard must respect the constitutional right to privacy and may impose restrictions only to the extent that the exercise of this right would "interfere with the public welfare"[54]. This requires a balancing of the interests at stake.

(85) According to Article 28(3) of the APPI, if the requested data does not exist, or where the PIHBO concerned decides not to grant access to the retained data, it is required to inform the individual without delay.

(86) Second, pursuant to Article 29(1) and (2) of the APPI, a data subject has a right to request the correction, addition or deletion of his/her retained personal data in the case where the data is inaccurate. Upon receipt of such a request, the PIHBO "shall […] conduct a necessary investigation" and, based on the results of such an investigation, "make a correction etc. of the contents of the retained data".

(87) Third, pursuant to Article 30(1) and (2) of the APPI a data subject has a right to request from a PIHBO to discontinue using personal information, or to delete such information, when it is handled in violation of Article 16 (regarding purpose limitation) or has been improperly acquired in violation of Article 17 of the APPI (regarding acquisition by deceit, other improper means or, in case of sensitive data, without consent). Likewise, under Article 30(3) and (4) of the APPI, the individual has a right to request from the PIHBO to cease the provision of the information to a third party where this would violate the provisions of Article 23(1) or Article 24 of the APPI (regarding third party provision, including international transfers).

(88) When the request is founded, the PIHBO shall without delay discontinue the use of the data, or the provision to a third party, to the extent necessary to remedy the violation or, if a case is covered by an exception (notably if the utilisation cease would cause particularly high costs)[55], implement necessary alternative measures to protect the rights and interests of the individual concerned.

---

[54] Article 13 of the Constitution has been interpreted by the Supreme Court as providing for a right to privacy (see supra at recitals (7) and (8)). Although this right can be restricted in cases where it "interferes with public welfare", in its judgment of 6 March 2008 (see recital (8)) the Supreme Court made clear that any restriction (permitting, in this case, a public authority to collect and process personal data) needs to be balanced against the right to privacy, taking into account factors such as the nature of the data at stake, the risks that processing of this data creates for individuals, the applicable safeguards and the public interest benefits resulting from the processing. This is very similar to the type of balancing required under EU law, on the basis of the principles of necessity and proportionality, for authorising any restriction to data protection rights and safeguards.

[55] For further explanations on these exceptions see Professor Katsuya Uga, Article by Article Commentary of the revised Act on the Protection of Personal Information, 2015, p. 217. For instance, an example for a request causing "large amount of expenses" is the case where only some names on a long list (e.g. in a directory) are processed in violation of the purpose limitation principle and the directory is already on sale, with the effect that calling back these copies and replacing them with new ones would be very costly. In the same example, where copies of the directory have already been sold to many people and it is impossible to collect all of them, it would also be "difficult to fulfil a utilization cease". In these scenarios, "necessary alternative action" could include, for example, publishing or distributing a correction notice. Such action does not exclude other forms of (judicial) redress, be it for the invasion of privacy rights, reputational damage (defamation) caused by the publication or the violation of other interests.

(89) Differently from EU law, the APPI and relevant sub-statutory rules do not contain legal provisions specifically addressing the possibility to oppose processing for direct marketing purposes. However, such processing will, under this Decision, take place in the context of a transfer of personal data that was previously collected in the European Union. Under Article 21(2) of Regulation (EU) 2016/679, the data subject shall always have the possibility to oppose a transfer of data for the purpose of processing for direct marketing. Moreover, as explained in recital (43), under Supplementary Rule (3), a PIHBO is required to process the data received under the Decision for the same purpose for which the data have been transferred from the European Union, unless the data subject consents to change the utilisation purpose.Hence, if the transfer has been made for any purpose other than direct marketing, a PIHBO in Japan will be barred from processing the data for the purpose of direct marketing without consent of the EU data subject.

(90) In all cases referred to in Articles 28 and 29 of the APPI, the PIHBO is required to notify the individual about the outcome of his/her request without delay, and moreover has to explain any (partial) refusal based on the statutory exceptions provided for in Articles 27 to 30 (Article 31 of the APPI).

(91) As regards the conditions for making a request, Article 32 of the APPI (together with the Cabinet Order) allows the PIHBO to determine reasonable procedures, including in terms of the information needed to identify the retained personal data. However, according to paragraph (4) of this Article, PIHBOs must not impose an "excessive burden on a principal". In certain cases the PIHBOs may also impose fees as long as their amount stays "within the scope considered reasonable in consideration of actual costs" (Article 33 of the APPI).

(92) Finally, the individual may object to the provision of his/her personal information to a third party under Article 23(2) of the APPI, or refuse consent under Article 23(1) (thus preventing disclosure in case no other legal basis would be available). Likewise, the individual can stop the processing of data for a different purpose by refusing to provide consent pursuant to Article 16(1) of the APPI.

(93) Differently from EU law, the APPI and relevant sub-statutory rules do not contain general provisions addressing the issue of decisions affecting the data subject and based solely on the automated processing of personal data. However, the issue is addressed in certain sectoral rules applicable in Japan that are particularly relevant for this type of processing. This includes sectors in which companies most likely resort to the automated processing of personal data to take decisions affecting individuals (e.g. the financial sector). For example, the "Comprehensive Guidelines for Supervision over Major Banks", as revised in June 2017, require that the concerned individual be provided with specific explanations on the reasons for the rejection of a request to conclude a loan agreement. Those rules thus offer protections in the likely rather limited number of cases where automated decisions would be taken by the "importing" Japanese business operator itself (rather than the "exporting" EU data controller).

(94) In any event, as regards personal data that has been collected in the European Union, any decision based on automated processing will typically be taken by the data controller in the Union (which has a direct relationship with the concerned data subject) and is thus subject to Regulation (EU) 2016/679.[56] This includes transfer

[56] Conversely, in the exceptional case where the Japanese operator has a direct relationship with the EU data subject, this will typically be a consequence of it having targeted the individual in the European Union by offering him/her goods or services or monitoring his/her behaviour. In this scenario, the Japanese operator

scenarios where the processing is carried out by a foreign (e.g. Japanese) business operator acting as an agent (processor) on behalf of the EU controller (or as a sub-processor acting on behalf of the EU processor having received the data from an EU controller that collected it) which on this basis then takes the decision. Therefore, the absence of specific rules on automated decision making in the APPI is unlikely to affect the level of protection of the personal data transferred under this Decision.

2.4. Oversight and enforcement

2.4.1. Independent oversight

(95) In order to ensure that an adequate level of data protection is guaranteed also in practice, an independent supervisory authority tasked with powers to monitor and enforce compliance with the data protection rules should be in place. This authority should act with complete independence and impartiality in performing its duties and exercising its powers.

(96) In Japan, the authority in charge of monitoring and enforcing the APPI is the PPC. It is composed of a Chairperson and eight Commissioners appointed by the Prime Minister with the consent of both Houses of the Diet. The term of office for the Chairperson and each of the Commissioners is five years, with the possibility for reappointment (Article 64 of the APPI). Commissioners may only be dismissed for good cause in a limited set of exceptional circumstances[57] and must not be actively engaged in political activities. Moreover, under the APPI, full-time Commissioners must abstain from any other remunerated activities, or business activities. All Commissioners are also subject to internal rules preventing them from participation in deliberations in case of a possible conflict of interests. The PPC is assisted by a Secretariat, led by a Secretary-General, that has been established for the purpose of carrying out the tasks assigned to the PPC (Article 70 of the APPI). Both the Commissioners and all officials in the Secretariat are bound by strict rules of secrecy (Articles 72, 82 of the APPI).

(97) The powers of the PPC, which it exercises in full independence[58], are mainly provided for in Articles 40, 41 and 42 of the APPI. Under Article 40, the PPC may request PIHBOs to report or submit documents on processing operations and may also carry out inspections, both on-site and of books or other documents. To the extent necessary to enforce the APPI, the PPC may also provide PIHBOs with guidance or advice as regards the handling of personal information. The PPC has already made use of this power under Article 41 APPI by addressing guidance to Facebook, following the Facebook/Cambridge Analytica revelations.

(98) Most importantly, the PPC has the power – acting on a complaint or its own initiative – to issue recommendations and orders in order to enforce the APPI and other binding rules (including the Supplementary Rules) in individual cases. Those powers are laid down in Article 42 of the APPI. While its paragraphs 1 and 2 provide for a two-step mechanism whereby the PPC may issue an order (only) following a prior

---

will itself fall within the scope of application of Regulation (EU) 2016/679 (Article 3(2)) and thus has to directly comply with EU data protection law.

[57] According to Article 65 of the APPI, dismissal against the will of the respective Commissioner is only possible on one of the following grounds: (i) opening of bankruptcy proceedings; (ii) conviction for violation of the APPI or the Numbers Use Act; (iii) conviction to a prison sentence without labour or an even more severe sentence; (iv) incapacity to execute duties due to mental or physical disorder or misconduct.

[58] See Article 62 of the APPI.

recommendation, paragraph 3 allows for the direct adoption of an order in cases of urgency.

(99) Although not all provisions of Chapter IV, Section 1 of the APPI are listed in Article 42(1) – which also determines the scope of application of Article 42(2) – this can be explained by the fact that certain of those provisions do not concern obligations of the PIHBO[59] and that all essential protections are already afforded by other provisions that are included in that list. For instance, although Article 15 (requiring the PIHBO to set the utilisation purpose and process the relevant personal information exclusively within its scope) is not mentioned, failure to observe this requirement can give ground to a recommendation based on a violation of Article 16(1) (prohibiting the PIHBO to process personal information beyond what is necessary to achieve the utilisation purpose, unless it obtains the data subject's consent).[60] Another provision not listed in Article 42(1) is Article 19 of the APPI on data accuracy and retention. Non-compliance with that provision can be enforced either as a violation of Article 16(1) or based on a violation of Article 29(2), if the individual concerned asks for the correction or deletion of erroneous or excessive data and the PIHBO refuses to satisfy the request. As regards the *rights* of the data subject according to Articles 28(1), 29(1) and 30(1), oversight by the PPC is ensured by granting it enforcement powers with respect to the corresponding *obligations* of the PIHBO laid down in those Articles.

(100) Pursuant to Article 42(1) of the APPI, the PPC can, if it recognizes that there is a "need for protecting an individual's rights and interests in cases where a [PIHBO] has violated" specific APPI provisions, issue a recommendation to "suspend the act of violating or take other necessary action to rectify the violation". Such a recommendation is not binding, but opens the way for a binding order pursuant to Article 42(2) of the APPI. Based on this provision, if the recommendation is not followed "without legitimate grounds" and the PPC "recognises that a serious infringement of an individual's rights and interests is imminent", it can order the PIHBO to take action in line with the recommendation.

(101) The Supplementary Rules further clarify and strengthen the PPC's enforcement powers. More specially, in cases involving data imported from the European Union, the PPC will always consider a PIHBO's failure to take action in line with a recommendation issued by the APPI pursuant to Article 42(1), without legitimate ground, as a serious infringement of an imminent nature of an individual's rights and interests within the meaning of Article 42(2), and therefore as an infringement warranting the issuance of a binding order. Moreover, as a "legitimate ground" for not complying with a recommendation the PPC will only accept an "event of an extraordinary nature [preventing compliance] outside the control of the [PIHBO] which cannot be reasonably foreseen (for example, natural disasters)" or cases where the necessity to take action concerning a recommendation "has disappeared because the [PIHBO] has taken alternative action that fully remedies the violation".

---

[59] For instance, certain provisions concern PIHBO actions that are optional (Article 32, 33 of the APPI), or "best effort" obligations that are, as such, not enforceable (Articles 31, 35, 36(6) and 39 of the APPI). Certain provisions are not addressed to the PIHBO but other actors. This is the case, for instance, with respect to Articles 23(4), 26(2) and 34 of the APPI (however, enforcement of Article 26(2) of the APPI is ensured through the possibility of criminal sanctions pursuant to Article 88(i) of the APPI).

[60] Moreover, as explained above in recital (48), in a transfer context the "utilisation purpose" will be specified by the EU data exporter, which in this respect is bound by the obligation pursuant to Article 5(1)(b) of Regulation (EU) 2016/679. That obligation is enforceable by the competent DPA in the European Union.

(102) Non-compliance with a PPC order is considered as a criminal offence under Article 84 of the APPI and a PIHBO found guilty can be punished by imprisonment with labour for up to six months or a fine of up to 300,000 yen. Furthermore, pursuant to Article 85(i) of the APPI, lack of cooperation with the PPC or obstruction to its investigation is punishable with a fine of up to 300,000 yen. These criminal sanctions apply in addition to those that may be imposed for substantive violations of the APPI (see recital 108).

2.4.2. Judicial redress

(103) In order to ensure adequate protection and in particular the enforcement of individual rights, the data subject should be provided with effective administrative and judicial redress, including compensation for damages.

(104) Before or instead of seeking administrative or judicial redress, an individual may decide to submit a complaint about the processing of his/her personal data to the controller itself. Based on Article 35 of the APPI, PIHBOs shall endeavour to deal with such complaints "appropriately and promptly" and establish internal complaint-handling systems to achieve this objective. In addition, under Article 61(ii) of the APPI the PPC is responsible for the "necessary mediation on a lodged complaint and cooperation offered to a business operator who deals with the complaint", which in both cases includes complaints submitted by foreigners. In this regard, the Japanese legislator has also entrusted the central government with the task of taking "necessary action" to enable and facilitate the resolution of complaints by PIHBOs (Article 9), while local governments shall endeavour to ensure mediation in such cases (Article 13). In that respect, individuals may lodge a complaint with one of the more than 1,700 consumer centres established by local governments based on the Consumer Safety Act[61], in addition to the possibility of lodging a complaint with the National Consumer Affairs Centre of Japan. Such complaints may also be brought with respect to a violation of the APPI. Under Article 19 of the Basic Consumer Act[62], local governments shall endeavour to engage in mediation with respect to complaints and provide the parties with necessary expertise. Those dispute resolution mechanisms appear quite effective, with a resolution rate of 91.2% concerning more than 75,000 complaint cases in 2015.

(105) Violations of the provisions of the APPI by a PIHBO can give rise to civil actions as well as criminal proceedings and sanctions. First, if an individual considers that his/her rights under Articles 28, 29 and 30 of the APPI have been infringed, (s)he may seek injunctive relief by asking the court to order a PIHBO to satisfy his/her request under one of these provisions, i.e. to disclose retained personal data (Article 28), to rectify retained personal data that is incorrect (Article 29) or to cease unlawful processing or third party provision (Article 30). Such an action may be brought without the need to rely on Article 709 of the Civil Code[63] or otherwise on tort law.[64] In particular, this means that the individual does not have to prove any harm.

(106) Second, in the case where an alleged infringement does not concern individual rights under Articles 28, 29 and 30 but general data protection principles or obligations of

[61] Act No. 50 of 5 June 2009.

[62] Act No. 60 of 22 August 2012.

[63] Article 709 of the Civil Code is the main ground for civil litigation for damages. According to this provision, "a person who has intentionally or negligently infringed any right of others, or legally protected interest of others, shall be liable to compensate any damages resulting in consequence".

[64] Tokyo High Court, judgment of 20 May 2015 (not published); Tokyo District Court, judgment of 8 September 2014, Westlaw Japan 2014WLJPCA09088002. See also Article 34(1), (3) of the APPI.

the PIHBO, the concerned individual may bring a civil action against the business operator based on the torts provisions of the Japanese Civil Code, especially Article 709. While a lawsuit under Article 709 requires, aside from fault (intention or negligence), a demonstration of harm, according to Article 710 of the Civil Code such harm may be both material and immaterial. No limitation is imposed as to the amount of compensation.

(107) As regards the available remedies, Article 709 of the Japanese Civil Code refers to monetary compensation. However, Japanese case law has interpreted this article as also conferring the right to obtain an injunction.[65] Therefore, if a data subject brings an action under Article 709 of the Civil Code and claims that his/her rights or interests have been harmed by an infringement of an APPI provision by the defendant, that claim may include, besides compensation for damage, a request for injunctive relief, notably aiming at stopping any unlawful processing.

(108) Third, in addition to civil law (tort) remedies, a data subject may file a complaint with a public prosecutor or judicial police official with respect to APPI violations that can lead to criminal sanctions. Chapter VII of the APPI contains a number of penal provisions. The most important one (Article 84) relates to non-compliance by the PIHBO with PPC orders pursuant to Article 42(2) and (3). If a business operator fails to comply with an order issued by the PPC, the PPC Chair (as well as any other government official)[66] may forward the case to the public prosecutor or judicial police official and in that way trigger the opening of a criminal procedure. The penalty for the violation of a PPC order is imprisonment with labour for up to six months or a fine of up to 300,000 yen. Other provisions of the APPI providing for sanctions in case of APPI violations affecting the rights and interests of data subjects include Article 83 of the APPI (regarding the "providing or using by stealth" of a personal information database "for the purpose of seeking […] illegal profits") and Article 88(i) of the APPI (regarding the failure by a third party to correctly inform the PIHBO when the latter receives personal data in accordance with Article 26(1) of the APPI, in particular on the details of the third party's own, prior acquisition of such data). The applicable penalties for such violations of the APPI are, respectively, imprisonment with work for up to one year or a fine of up to 500,000 yen (in case of Article 83) or an administrative fine of up to 100,000 yen (in case of Article 88(i)). While the threat of a criminal sanction is already likely to have a strong deterrent effect on the business management that directs the PIHBO's processing operations as well as on the individuals handling the data, Article 87 of the APPI clarifies that when a representative, employee or other worker of a corporate body has committed a violation pursuant to Articles 83 to 85 of the APPI, "the actor shall be punished and a fine set forth in the respective Articles shall be imposed on the said corporate body". In this case, both the employee and the company can be imposed sanctions up to the full maximum amount.

(109) Finally, individuals may also seek redress against the PPC's actions or inactions. In this respect, Japanese law provides several avenues of administrative and judicial redress.

(110) Where an individual is not satisfied with a course of action undertaken by the PPC, (s)he may file an administrative appeal under the Administrative Complaint Review

[65] See Supreme Court, judgment of 24 September 2002 (Hanrei Times vol. 1106, p.72).
[66] Article 239 (2) of the Code of Criminal Procedure.

Act[67]. Conversely, where an individual considers that the PPC should have acted but failed to do so, an individual may request the PPC pursuant to Article 36-3 of that Act to make a disposition or provide administrative guidance if (s)he considers that "a disposition or administrative guidance necessary for the correction of the violation has not been rendered or imposed".

(111) As regards judicial redress, under the Administrative Case Litigation Act, an individual who is not satisfied with an administrative disposition made by the PPC may file a *mandamus* suit[68] asking the Court to order the PPC to take further action[69]. In certain cases, the court may also issue a provisional order of *mandamus*, so as to prevent irreversible harm.[70] Furthermore, under the same Act, an individual may seek revocation of a PPC decision.[71]

(112) Finally, an individual may also file an action for State compensation against the PPC under Article 1(1) of the State Redress Act in case (s)he has suffered damages due to the fact that an order issued by the PPC to a business operator was unlawful or the PPC has not exercised its authority.

3. Access and use of personal data transferred from the European Union by public authorities in Japan

(113) The Commission has also 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 to business operators in Japan by public authorities for public interest, in particular criminal law enforcement and national security purposes ("government access"). In this respect, the Japanese government has provided the Commission with official representations, assurances and commitments signed at the highest ministerial and agency level that are contained in Annex II to this Decision.

3.1. General legal framework

(114) As an exercise of public authority, government access in Japan must be carried out in full respect of the law (legality principle). In this regard, the Constitution of Japan contains provisions limiting and framing the collection of personal data by public authorities. As already mentioned with respect to processing by business operators, basing itself on Article 13 of the Constitution which among others protects the right to liberty, the Supreme Court of Japan has recognised the right to privacy and data protection.[72] One important aspect of that right is the freedom not to have one's personal information disclosed to a third party without permission.[73] This implies a right to the effective protection of personal data against abuse and (in particular) illegal access. Additional protection is ensured by Article 35 of the Constitution on the

---

67 Act No. 160 of 2014.

68 Article 37-2 of the Administrative Case Litigation Act.

69 According to Article 3(6) of the Administrative Case Litigation Act, the term "mandamus action" refers to an action seeking an order from the court against an administrative agency to make an original administrative disposition that it "should" have made but failed to.

70 Article 37-5 of the Administrative Case Litigation Act.

71 Chapter II, Section 1 of the Administrative Case Litigation Act.

72 See for instance Supreme Court, judgment of 12 September 2003, Case No. 1656 (2002 (Ju)). In particular, the Supreme Court has held that "every individual has the liberty of protecting his/her own personal information from being disclosed to a third party or made public without good reason."

73 Supreme Court, judgment of 6 March 2008 (Juki-net).

right of all persons to be secure in their homes, papers and effects, which requires from public authorities to obtain a court warrant issued for "adequate cause"[74] in all cases of "searches and seizures". In its judgment of 15 March 2017 (GPS case), the Supreme Court has clarified that this warrant requirement applies whenever the government invades ("enters into") the private sphere in a way that suppresses the individual's will and thus by means of a "compulsory investigation". A judge may only issue such warrant based on a concrete suspicion of crimes, i.e. when provided with documentary evidence based on which the person concerned by the investigation can be considered as having committed a criminal offence.[75] Consequently, Japanese authorities have no legal authority to collect personal information by compulsory means in situations where no violation of the law has yet occurred[76], for example in order to prevent a crime or other security threat (as is the case for investigations on grounds of national security).

(115) Under the reservation of law principle, any data collection as part of a coercive investigation must be specifically authorised by law (as reflected, for instance, in Article 197(1) of the Code of Criminal Procedure ("CCP") regarding the compulsory collection of information for the purposes of a criminal investigation). This requirement applies also to access to electronic information.

(116) Importantly, Article 21(2) of the Constitution guarantees the secrecy of all means of communication, with limitations only allowed by legislation on public interest grounds. Article 4 of the Telecommunications Business Act, according to which the secrecy of communications handled by a telecommunications carrier shall not be violated, implements this confidentiality requirement at the level of statutory law. This has been interpreted as prohibiting the disclosure of communications information, except with the consent of users or if based on one of the explicit exemptions from criminal liability under the Penal Code.[77]

(117) The Constitution also guarantees the right of access to the courts (Article 32) and the right to sue the State for redress in the case where an individual has suffered damage through the illegal act of a public official (Article 17).

(118) As regards specifically the right to data protection, Chapter III, Sections 1, 2 and 3 of the APPI lays down general principles covering all sectors, including the public sector. In particular, Article 3 of the APPI provides that all personal information must be handled in accordance with the principle of respect for the personality of individuals. Once personal information, including as part of electronic records, has been collected ("obtained") by public authorities[78], its handling is governed by the Act on the

---

74 "Adequate cause" only exists where the individual concerned (suspect, accused) is considered to have committed an offence and the search and seizure is necessary for the criminal investigation. See Supreme Court, judgment of 18 March 1969, Case No. 100 (1968 (Shi)).

75 See Article 156(1) of the Rules of Criminal Procedure.

76 It should be noted, however, that the Act on Punishment of Organized Crimes and Control of Crime Proceeds of 15 June 2017 creates a new offence criminalizing the preparation of acts of terrorism and certain other forms of organized crime. Investigations may only be initiated in case of a concrete suspicion, based on evidence, that all three necessary conditions constituting the offence (involvement of an organized crime group, "act of planning" and "act of preparation for implementation" of the crime) are met. See also e.g. Articles 38-40 of the Subversive Activities Prevention Act (Act No. 240 of 21 July 1952).

77 Article 15(8) of the Guidelines on the Protection of Personal Information in the Telecommunication Sector.

78 Administrative Organs as defined in Article 2(1) of the APPIHAO. According to the information received from the Japanese government, all public authorities, except for the Prefectural Police, fall under the definition of "Administrative Organs". At the same time, the Prefectural Police operates within the legal framework set by the Prefectural Personal Information Protection Ordinances (see Article 11 of the APPI

Protection of Personal Information held by Administrative Organs ("APPIHAO").[79] This includes in principle[80] also the processing of personal information for criminal law enforcement or national security purposes. Among others, the APPIHAO provides that public authorities: (i) may only retain personal information to the extent this is necessary for carrying out their duties; (ii) shall not use such information for an "unjust" purpose or disclose it to a third person without justification; (iii) shall specify the purpose and not change that purpose beyond what can reasonably be considered as relevant for the original purpose (purpose limitation); (iv) shall in principle not use or provide a third person with the retained personal information for other purposes and, if they consider this necessary, impose restrictions on the purpose or method of use by third parties; (v) shall endeavour to ensure the correctness of the information (data quality); (vi) shall take the necessary measures for the proper management of the information and to prevent leakage, loss or damage (data security); and (vii) shall endeavour to properly and expeditiously process any complaints regarding the processing of the information.[81]

3.2. Access and use by Japanese public authorities for criminal law enforcement purposes

(119) Japanese law contains a number of limitations on the access and use of personal data for criminal law enforcement purposes as well as oversight and redress mechanisms that provide sufficient safeguards for that data to be effectively protected against unlawful interference and the risk of abuse.

3.2.1. Legal basis and applicable limitations/safeguards

(120) In the Japanese legal framework, the collection of electronic information for criminal law enforcement purposes is permissible based on a warrant (compulsory collection) or a request for voluntary disclosure.

3.2.1.1. Compulsory investigation based on a court warrant

(121) As indicated in recital (115), any data collection as part of a coercive investigation must be specifically authorised by law and may only be carried out based on a court warrant "issued for adequate cause" (Article 35 of the Constitution). As regards the investigation of criminal offences, this requirement is reflected in the provisions of the

---

and the Basic Policy) which stipulate provisions for the protection of personal information equivalent to the APPIHAO. See Annex II, Sec. I.B. As explained by PPC, according to the "Basic Policy" these Ordinances have to be enacted based on the content of the APPIHAO and the MIC issues notices to give the local governments the necessary directions in this regard. As stressed by PPC, "[w]ithin these limits, the personal information protection ordinance in each prefecture is to be established […] based on the Basic Policy and the content of the notices."

[79] Personal information obtained by officials of an Administrative Organ in the course of the exercise of their duties and held by said Administrative Organ for organisational use falls under the definition of "Retained Personal Information" within the meaning of Article 2(3) of the APPIHAO, as long as it is recorded in "Administrative Documents". This includes electronic information collected and then further processed by such bodies, given that the definition of "Administrative Documents" in Article 2(2) of the Act on Access to Information Held by Administrative Organs (Act No. 42 of 1999) covers electromagnetic records.

[80] However, according to Article 53-2 of the Code of Criminal Procedure, Chapter IV of the APPIHAO is excluded for "documents relating to trials", which according to the information received includes electronic information obtained based on a warrant or request for voluntary cooperation as part of a criminal investigation. Likewise, as regards information collected in the area of national security, individuals will not be able to successfully invoke their rights under the APPIHAO if the head of the public authority has "reasonable grounds" to consider that disclosure "is likely to cause harm to national security" (see Article 14(iv)). This being said, public authorities are required to grant at least partial disclosure, whenever possible (Article 15).

[81] See the specific references to the APPIHAO in Annex II, Sec. II.A.1)(b)(2).

Code of Criminal Procedure ("CCP"). According to Article 197(1) of the CCP, compulsory measures "shall not be applied unless special provisions have been established in this Code". With respect to the collection of electronic information, the only relevant[82] legal bases in this regard are Article 218 of the CCP (search and seizure) and Article 222-2 of the CCP, according to which compulsory measures for the interception of electronic communications without the consent of either party shall be executed based upon other acts, namely the Act on Wiretapping for Criminal Investigation ("Wiretapping Act"). In both cases, the warrant requirement applies.

(122) More specifically, pursuant to Article 218(1) of the CCP, a public prosecutor, a public prosecutor's assistant officer or a judicial police official may, if necessary for the investigation of an offence, conduct a search or seizure (including ordering records) upon a warrant issued by a judge in advance.[83] Among others, such a warrant shall contain the name of the suspect or accused, the charged offence[84], the electromagnetic records to be seized and the "place or articles" to be inspected (Article 219(1) of the CCP).

(123) As regards the interception of communications, Article 3 of the Wiretapping Act authorises such measures only under strict requirements. In particular, the public authorities have to obtain a prior court warrant that may only be issued for the investigation of specific serious crimes (listed in the Annex to the Act)[85] and when it is "extremely difficult to identify the criminal or clarify the situations/details of the perpetration by any other ways".[86] Under Article 5 of the Wiretapping Act, the warrant is issued for a limited period of time and additional conditions may be imposed by the judge. Moreover, the Wiretapping Act provides for a number of further guarantees, such as for instance the necessary attendance of witnesses (Articles 12, 20), the prohibition to wiretap the communications of certain privileged groups (e.g. doctors, lawyers) (Article 15), the obligation to terminate the wiretapping if it is no longer justified, even within the period of validity of the warrant (Article 18), or the general requirement to notify the individual concerned and allow access to the records within thirty days after the wiretapping has been terminated (Articles 23, 24).

(124) For all compulsory measures based on a warrant, only such an examination "as is necessary to achieve its objective" – that is to say where the objectives pursued with the investigation cannot be achieved otherwise – may be conducted (Article 197(1) CCP). Although the criteria for determining necessity are not further specified in statutory law, the Supreme Court of Japan has ruled that the judge issuing a warrant should make an overall assessment taking into consideration in particular (i) the gravity of the offence and how it was committed; (ii) the value and importance of the

---

82 While Article 220 of the CCP authorises a search and seizure "on the spot" without a warrant where a public prosecutor, public prosecutor's assistant or judicial police official arrests a suspect/flagrant offender, this is not relevant in a transfer context and thus for the purposes of this Decision.

83 According to Article 222(1) in conjunction with Article 110 of the CCP, the search/seizure warrant for records must be shown to the person that is to undergo the measure.

84 See also Article 189(2) of the CCP, according to which a judicial police officer shall investigate the offender and evidence thereof "when he/she deems that an offence has been committed." Likewise, Article 155(1) of the Rules of Criminal Procedure requires that a written request for a warrant shall, among others, contain the "charged offence" and a "summary of the facts of the crime".

85 The Annex refers to 9 types of crimes, e.g. crimes related to drugs and firearms, human trafficking and organised murder. It should be noted that the newly introduced offence of the "preparation of acts of terrorism and other organized crimes" (see footnote 76) is not included in this restrictive list.

86 Moreoever, according to Article 23 of the Wiretapping Act, the investigatory authority has to notify the individual whose communications have been intercepted (and thus included in the interception record) of this fact in writing.

materials to be seized as evidence; (iii) the probability (risk) that evidence may be concealed or destroyed; and (iv) the extent to which the seizure may cause prejudice to the individual concerned.[87]

3.2.1.2. Request for voluntary disclosure based on an "enquiry sheet"

(125) Within the limits of their competence, public authorities may also collect electronic information based on requests for voluntary disclosure. This refers to a non-compulsory form of cooperation where compliance with the request cannot be enforced,[88] thus relieving the public authorities from the duty of obtaining a court warrant.

(126) To the extent such a request is directed at a business operator and concerns personal information, the business operator has to comply with the requirements of the APPI. According to Article 23(1) of the APPI, business operators may disclose personal information to third parties without consent of the individual concerned only in certain cases, including where the disclosure is "based on laws and regulations"[89]. In the area of criminal law enforcement, the legal basis for such requests is provided by Article 197(2) of the CCP according to which "private organisations may be asked to report on necessary matters relating to the investigation." Since such an "enquiry sheet" is permissible only as part of a criminal investigation, it always presupposes a concrete suspicion of an already committed crime.[90] Moreover, since such investigations are generally carried out by the Prefectural Police, the limitations pursuant to Article 2(2) of the Police Law[91] apply. According to that provision, the activities of the police are "strictly limited" to the fulfilment of their responsibilities and duties (that is to say the prevention, suppression and investigation of crimes). Moreover, in performing its duties, the police shall act in an impartial, unprejudiced and fair manner and must never abuse its powers "in such a way as to interfere with the rights and liberties of an individual guaranteed in the Constitution of Japan" (which include, as indicated, the right to privacy and data protection).[92]

(127) Specifically with respect to Article 197(2) of the CCP, the National Police Agency ("NPA") – as the federal authority in charge, among others, of all matters concerning the criminal police – has issued instructions to the Prefectural Police[93] on the "proper use of written inquiries in investigative matters". According to this Notification, requests must be made using a pre-established form ("Form No. 49" or so-called "enquiry sheet"),[94] concern records "regarding a specific investigation" and the requested information must be "necessary for [that] investigation". In each case, the

87 See Annex II, Sec. II.A.1)(b)(1).

88 According to the information received, business operators that fail to cooperate do not face negative consequences (including sanctions) under any law. See Annex II, Sec. II.A.2)(a).

89 According to the PPC Guidelines (General Rule Edition), Article 23(1)(i) provides the basis for the disclosure of personal information in reaction to both a warrant (Article 218 of the CCP) and an "enquiry sheet" (Article 197(2) of the CCP).

90 This means that the "enquiry sheet" may be used only to collect information in individual cases and not for any large-scale collection of personal data. See also Annex II, Sec. I.A.2)(b)(1).

91 As well as the regulations of the Prefectural Public Safety Commission, see Article 189(1) of the CCP.

92 See also Article 3 of the Police Law, according to which the oath of office taken by all police officers is "to be faithful to the obligation to defend and uphold the Constitution and laws of Japan, and perform their duties impartially, equitably, fairly and without prejudice."

93 According to Articles 30(1) and 31(2) of the Police Law, the Director-General of the Regional Police Bureaus (local branches of the NPA) shall "direct and supervise" the Prefectural Police.

94 The enquiry sheet must also specify the contact information of the "handler" ("name of section [position], name of the handler, phone number of the office, extension number, etc.").

chief investigator shall "fully examine the necessity, content, etc. of [the] individual enquiry" and must receive internal approval from a high-ranking official.

(128) Moreover, in two judgments from 1969 and 2008,[95] the Supreme Court of Japan has stipulated limitations with respect to non-compulsory measures that interfere with the right to privacy.[96] In particular, the court considered that such measures must be "reasonable" and stay within "generally allowable limits", that is to say they must be necessary for the investigation of a suspect (collection of evidence) and carried out "by appropriate methods for achieving the purpose of [the] investigation."[97] The judgments show that this entails a proportionality test, taking into account all the circumstances of the case (e.g. the level of interference with the right to privacy, including the expectation of privacy, the seriousness of the crime, the likelihood to obtain useful evidence, the importance of that evidence, possible alternative means of investigation, etc.).[98]

(129) Aside from these limitations for the exercise of public authority, business operators themselves are expected to check ("confirm") the necessity and "rationality" of the provision to a third party.[99] This includes the question whether they are prevented by law from cooperating. Such conflicting legal obligations may in particular follow from confidentiality obligations such as Article 134 of the Penal Code (concerning the relationship between a doctor, lawyer, priest, etc. and his/her client). Also, "any person engaged in the telecommunication business shall, while in office, maintain the secrets of others that have come to be known with respect to communications being handled by the telecommunication carrier" (Article 4(2) of the Telecommunication Business Act). This obligation is backed-up by the sanction stipulated in Article 179 of the Telecommunication Business Act, according to which any person that has violated the secrecy of communications being handled by a telecommunications carrier shall be guilty of a criminal offence and punished by imprisonment with labour of up to two years, or to a fine of not more than one million yen.[100] While this requirement is not absolute and in particular allows for measures infringing the secrecy of communications that constitute "justifiable acts" within the meaning of Article 35 of

---

95 Supreme Court, judgment of 24 December 1969 (1965(A) 1187); judgment of 15 April 2008 (2007(A) 839).

96 While these judgments did not concern the collection of electronic information, the Japanese government has clarified that the application of the criteria developed by the Supreme Court extends to any interference by public authorities with the right to privacy, including to all "voluntary investigations", and thus the criteria bind the Japanese authorities also when making requests for voluntary disclosure of information. See Annex II, Sec. II.A.2)(b)(1).

97 According to the information received, these factors have to be considered "reasonable in accordance with socially accepted conventions." See Annex II, Sec. II.A.2)(b)(1).

98 For similar considerations in the context of compulsory investigations (wiretapping) see also Supreme Court, judgment of 16 December 1999, 1997 (A) 636.

99 In this respect, the Japanese authorities have pointed to the PPC Guidelines (General Rule Edition) and point 5/14 of the "Q&A" prepared by PPC for the application of the APPI. According to the Japanese authorities, "given the growing awareness of individuals as regards their privacy rights, as well as the workload created by such requests, business operators are more and more cautious in answering such requests". See Annex II, Sec. II.A.2), also with reference to the 1999 Notification by the NPA. According to the information received, there have indeed been cases where business operators have refused to cooperate. For instance, in its 2017 transparency report, LINE (the most popular messaging app in Japan) states the following: "After receiving requests from investigative agencies etc., we […] verify the appropriateness from the viewpoints of legality, user protection, etc. In this verification, we will refuse the request at that time if there is a legal deficiency. If the scope of the claim is too broad for the purpose of investigation, we ask the investigation agency for explanation. If explanation is without reason, we will not respond to that request." Available on the internet at: https://linecorp.com/en/security/transparency/top.

100 The penalties are 3 years of imprisonment with labour or a fine of not more than 2 million yen for any person who "engages in the telecommunications business".

the Penal Code[101], this exception does not cover the response to non-compulsory requests by public authorities for the disclosure of electronic information pursuant to Article 197(2) of the CCP.

3.2.1.3. Further use of the information collected

(130) Upon collection by the Japanese public authorities, personal information falls within the scope of application of the APPIHAO. That Act regulates the handling (processing) of "retained personal information", and insofar imposes a number of limitations and safeguards (see recital (118)).[102] Moreover, the fact that an Administrative Organ may retain personal information "only when the retention is necessary for performing the affairs under its jurisdiction provided by laws and regulations" (Article 3(1) of the APPIHAO) also imposes restrictions – at least indirectly – on the initial collection.

3.2.2. Independent oversight

(131) In Japan, the collection of electronic information in the area of criminal law enforcement foremost[103] falls within the responsibilities of the Prefectural Police[104], which in this regard is subject to various layers of oversight.

(132) First, in all cases where electronic information is collected by compulsory means (search and seizure), the police has to obtain a prior court warrant (see recital (121)). Therefore, the collection in those cases will be checked ex ante by a judge, based on a strict "adequate cause" standard.

(133) While there is no ex-ante check by a judge in the case of requests for voluntary disclosure, business operators to whom such requests are addressed can object to them without risking any negative consequences (and will have to take into account the privacy impact of any disclosure). Moreover, according to Article 192(1) of the CCP, police officials shall always cooperate and coordinate their actions with the public prosecutor (and the Prefectural Public Safety Commission).[105] In turn, the public prosecutor may give the necessary general instructions setting forth standards for a fair investigation and/or issue specific orders with respect to an individual investigation (Article 193 of the CCP). Where such instructions and/or orders are not followed, the prosecution may file charges for disciplinary action (Article 194 of the CCP). Hence, the Prefectural Police operates under the supervision of the public prosecutor.

(134) Second, according to Article 62 of the Constitution, each House of the Japanese parliament (the Diet) may conduct investigations in relation to the government, including with respect to the lawfulness of information collection by the police. To that end, it may demand the presence and testimony of witnesses, and/or the production of records. Those powers of inquiry are further specified in the Diet Law,

---

101 "Justifiable acts" under the Penal Code are in particular those acts of a telecommunication carrier by which it complies with measures of the State that have legal force (compulsory measures), for instance when investigation authorities take measures based on a warrant issued by a judge. See Annex II, Sec. II.A.2)(b)(2), with reference to the Guidelines on Personal Information Protection in Telecommunications Business.

102 As regards the rights of the individuals concerned, see section 3.1.

103 In principle, a public prosecutor – or public prosecutor's assistant officer under the orders of a public prosecutor – may, if (s)he deems it necessary, investigate an offence (Article 191(1) of the CCP).

104 According to the information received, the National Police Agency does not conduct individual criminal investigations. See Annex II, Sec. II.A.1)(a).

105 See also Article 246 of the CCP, according to which the judicial police is under an obligation to send the case file to the public prosecutor once it has conducted the investigation of a criminal offence ("Principle of sending in all cases").

in particular Chapter XII. In particular, Article 104 of the Diet Law provides that the Cabinet, public agencies and other parts of the government "must comply with the requests of a House or any of its Committees for the production of reports and records necessary for consideration of investigation." Refusal to comply is allowed only if the government provides a plausible reason found acceptable by the Diet, or upon issuance of a formal declaration that the production of the reports or records would be "gravely detrimental to the national interest"[106]. In addition, Diet members may ask written questions to the Cabinet (Articles 74, 75 of the Diet Law), and in the past such "written inquiries" have also addressed the handling of personal information by the administration.[107] The Diet's role in supervising the executive is supported by reporting obligations, for instance pursuant to Article 29 of the Wiretapping Act.

(135) Third, also within the executive branch the Prefectural Police is subject to independent oversight. That includes in particular the Prefectural Public Safety Commissions established at prefectural level to ensure democratic administration and political neutrality of the police.[108] These commissions are composed of members appointed by the Prefectural Governor with the consent of the Prefectural Assembly (from among citizens with no public servant position in the police in the five preceding years) and have a secure term of office (in particular only dismissal for good cause).[109] According to the information received, they are not subject to instructions, and thus can be considered as fully independent.[110] As regards the tasks and powers of the Prefectural Public Safety Commissions, pursuant to Article 38(3) in conjunction with Articles 2 and 36(2) of the Police Law they are responsible for "the protection of [the] rights and freedom of an individual". To this effect, they are empowered to "supervise"[111] all investigatory activities of the Prefectural Police, including the collection of personal data. Notably, the commissions "may direct the [P]refectural [P]olice in detail or in a specific individual case of inspection of police personnel's misconduct, if necessary."[112] When the Chief of the Prefectural Police[113] receives such a direction or by him-/herself becomes aware of a possible case of misconduct (including the violation of laws or other neglect of duties), (s)he has to promptly inspect the case and report the inspection result to the Prefectural Public Safety Commission (Article 56(3) of the Police Law). Where the latter considers this necessary, it may also designate one of its members to review the status of implementation. The process continues until the Prefectural Public Safety Commission is satisfied that the incident has been appropriately addressed.

---

106 Alternatively, the Diet may request that the Board of Oversight and Review of Specially Designated Secrets conduct an investigation into the refusal to respond. See Article 104-II of the Diet Law.

107 See Annex II, Sec. II.B.4).

108 In addition, according to the provisions of Article 100 of the Local Autonomy Act, the local assembly has the authority to investigate the activities of enforcement authorities established at prefectural level, including the Prefectural Police.

109 See Articles 39-41 of the Police Law. As regards political neutrality, see also Article 42 of the Police Law.

110 See Annex II, Sec. II.B.3) ("independent council system").

111 See Articles 5(3) and 38(3) of the Police Law.

112 See Articles 38(3), 43-2(1) of the Police Law. In case it "makes a direction" within the meaning of Article 43-2(1), the Prefectural Public Safety Commission may order a committee nominated by the Commission to monitor its implementation (paragraph 2). Also, the Commission may recommend disciplinary action or dismissal of the Chief of the Prefectural Police (Article 50(2)) as well as other police officers (Article 55(4) of the Police Law).

113 The same applies to the Superintendent General in the case of the Tokyo Metropolitan Police (see Article 48(1) of the Police Law).

(136) In addition, with respect to the correct application of the APPIHAO, the competent minister or agency head (e.g. the Commissioner General of the NPA) has enforcement authority, subject to the supervision by the Ministry of Internal Affairs and Communications (MIC). According to Article 49 APPIHAO, the MIC "may collect reports on the status of enforcement of this Act" from the heads of Administrative Organs (Minister). That oversight function is supported by input from MIC's 51 "comprehensive information centres" (one in each Prefecture throughout Japan) that each year handle thousands of inquiries from individuals[114] (which, in turn, may reveal possible violations of the law). Where it considers this necessary for ensuring compliance with the Act, MIC may 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).

3.2.3. Individual redress

(137) In addition to ex officio oversight, individuals also have several possibilities for obtaining individual redress, both through independent authorities (such as the Prefectural Public Safety Commissions or the PPC) and the Japanese courts.

(138) First, with respect to personal information collected by Administrative Organs, the latter are under an obligation to "endeavour to properly and expeditiously process any complaints" regarding its subsequent processing (Article 48 of the APPIHAO). While Chapter IV of the APPIHAO on individual rights is not applicable with respect to personal information recorded in "documents relating to trials and seized articles" (Article 53-2(2) of the CCP) – which covers personal information collected as part of criminal investigations – individuals may bring a complaint to invoke the general data protection principles such as for instance the obligation to only retain personal information "when the retention is necessary for performing [law enforcement functions]" (Article 3(1) of the APPIHAO).

(139) In addition, Article 79 of the Police Law guarantees individuals who have concerns with respect to the "execution of duties" by police personnel the right to lodge a complaint with the (competent) independent Prefectural Public Safety Commission. The Commission will "faithfully" handle such complaints in accordance with laws and local ordinances and shall notify the complainant in writing of the results. Based on its authority to supervise and "direct" the Prefectural Police with respect to "personnel's misconduct" (Articles 38(3), 43-2(1) of the Police Law), it may request the Prefectural Police to investigate the facts, take appropriate measures based on the outcome of this investigation and report on the results. If it considers that the investigation carried out by the Police has not been adequate, the Commission may also provide instructions on the handling of the complaint.

(140) In order to facilitate complaint handling, the NPA has issued a "Notice" to the Police and Prefectural Public Safety Commissions on the proper handling of complaints regarding the execution of duties by police officers. In this document, the NPA stipulates standards for the interpretation and implementation of Article 79 of the Police Law. Among others, it requires the Prefectural Police to establish a "system for handling complaints" and to handle and report all complaints to the competent Prefectural Public Safety Commission "promptly". The Notice defines complaints as claims seeking correction "for any specific disadvantage that has been inflicted as the

[114] According to the information received, in FY2017 (April 2017 to March 2018) a total of 5,186 inquiries from individuals were handled by the "comprehensive information centres".

result of an illegal or inappropriate behaviour"[115] or "failure to take a necessary action, by a police officer in his/her execution of duty"[116], as well as any "grievance/discontent about inappropriate mode of duty execution by a police officer". The material scope of a complaint is thus broadly defined, covering any claim of unlawful collection of data, and the complainant does not have to demonstrate any harm suffered as a result of a police officer's actions. Importantly, the Notice stipulates that foreigners (among others) shall be provided with assistance in formulating a complaint. Following a complaint, the Prefectural Public Safety Commissions are required to ensure that the Prefectural Police examines the facts, implements measures "according to the result of the examination" and reports on the results. Where the Commission considers the examination to be insufficient, it shall issue an instruction on the handling of the complaint, which the Prefectual Police is required to follow. Based on the reports received and the measures taken, the Commission notifies the individual indicating, among others, the measures taken to address the complaint. The NPA Notice stresses that complaints should be handled in a "sincere manner" and that the result should be notified "within the scope of time […] deemed appropriate in the light of the social norms and common sense."

(141) Second, given that redress will naturally have to be sought abroad in a foreign system and in a foreign language, in order to facilitate redress for EU individuals whose personal data is transferred to business operators in Japan and then accessed by public authorities, the Japanese government has made use of its powers to create a specific mechanism, administered and supervised by PPC, for handling and resolving complaints in this field. That mechanism builds on the cooperation obligation imposed on Japanese public authorities under the APPI and the special role of the PPC with respect to international data transfers from third countries under Article 6 of the APPI and the Basic Policy (as established by the Japanese government through Cabinet Order). The details of this mechanism are set out in the official representations, assurances and commitments received from the Japanese government and attached to this Decision as Annex II. 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.

(142) Under the mechanism, an individual who suspects that his/her data transferred from the European 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 though his/her data protection authority within the meaning of Article 51 of the GDPR). The PPC will be under an obligation to 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 the subsequent use of personal information has taken place in compliance with the applicable rules."[117] This obligation, derived from Article 80 of the APPI (requiring Japanese public authorities to co-operate with PPC), applies in general and hence

[115] The condition of a "specific disadvantage" merely suggests that the complainant needs to be individually concerned by the police conduct (or inaction), not that (s)he has to demonstrate any harm.

[116] Observance of the law, including the legal requirements for the collection and use of personal data, is part of those duties. See Article 2(2), 3 of the Police Law.

[117] In carrying out its evaluation, the PPC will cooperate with the MIC which, as explained in recital (136), may request the submission of explanations and materials, and issue opinions, concerning the handling of personal information by the respective Administrative Organ (Articles 50, 51 APPIHAO).

extends to the review of any investigatory measures taken by such authorities, which moreover have committed to such cooperation through written assurances from the competent ministries and agency heads, as reflected in Annex II.

(143) If the evaluation shows that an infringment of the applicable rules has occurred, "cooperation by the concerned public authorities with the PPC includes the obligation to remedy the violation", which in case of the unlawful collection of personal information covers the deletion of such data. Importantly, this obligation is carried out under the supervision of the PPC which will "confirm, before concluding the evaluation, that the violation has been fully remedied."

(144) Once the evaluation is concluded, the PPC shall notify the individual within a reasonable period of time of the outcome of the evaluation, including any corrective action taken where applicable. At the same time, the PPC shall also inform the individual about the possibility of seeking a confirmation of the outcome from the competent public authority and the identity of the authority to which such a request for confirmation should be made. The possibility to receive such a confirmation, including the reasons underpinning the decision of the competent authority, may be of assistance to the individual in taking any further steps, including when seeking judicial redress. Detailed information on the outcome of the evaluation can be restricted as long as there are reasonable grounds to consider that communicating such information is likely to pose a risk to the ongoing investigation.

(145) Third, an individual who disagrees with a seizure decision (warrant)[118] concerning his/her personal data by a judge, or with the measures by the police or prosecution executing such a decision, may file a request for that decision or such measures to be rescinded or altered (Articles 429(1), 430(1), (2) of the CCP, Article 26 of the Wiretapping Act).[119] In the case where the reviewing court considers that either the warrant itself or its execution ("procedure for seizure") is illegal, it will grant the request and order the seized articles to be returned.[120]

(146) Fourth, as a more indirect form of judicial control, an individual who considers that the collection of his/her personal information as part of a criminal investigation was illegal may, at his/her criminal trial, invoke this illegality. If the court agrees, this will lead to the exclusion of the evidence as inadmissible.

(147) Finally, under Article 1(1) of the State Redress Act a court may grant compensation where a public officer who exercises the public authority of the State has, in the course of his/her duties, unlawfully and with fault (intentionally or negligently) inflicted damage on the individual concerned. According to Article 4 of the State Redress Act, the State's liability for damages is based on the provisions of the Civil Code. In this respect, Article 710 of the Civil Code stipulates that liability also covers damages other than those to property, and hence moral damage (for instance in the form of

---

[118] This includes a wiretapping warrant, for which the Wiretapping Act stipulates a specific notification requirement (Article 23). According to that provision, the investigatory authority has to notify the individuals whose communications have been intercepted (and thus included in the interception record) of this fact in writing. Another example is Article 100(3) of the CCP according to which the court, when it has seized postal items or telegrams sent to or by the accused, shall notify the sender or recipient unless there is a risk that such notification would obstruct court proceedings. Article 222(1) of the CCP cross-references this provision for searches and seizures carried out by an investigatory authority.

[119] While such a request does not have the automatic effect of suspending the execution of the seizure decision, the reviewing court may order the suspension until it has rendered a decision on substance. See Articles 429(2), 432 in conjunction with Article 424 of the CCP.

[120] See Annex II, Sec. II.C(1).

"mental distress"). This includes cases where the privacy of an individual has been invaded by unlawful surveillance and/or the collection of his/her personal information (e.g. the illegal execution of a warrant).[121]

(148) In addition to monetary compensation, individuals may under certain conditions also obtain injunctive relief (e.g. the deletion of personal data collected by public authorities) based on their privacy rights under Article 13 of the Constitution.[122]

(149) With respect to all those redress avenues, the dispute resolution mechanism created by the Japanese government provides that an individual who is still dissatisfied with the outcome of the procedure can address the PPC "which shall inform the individual of the various possibilities and detailed procedures for obtaining redress under Japanese laws and regulations." Moreover, the PPC "will provide the individual with support, including counselling and assistance in bringing any further action to the relevant administrative or judicial body."

(150) This includes making use of the procedural rights under the Code of Criminal Procedure. For instance, "[w]here the evaluation reveals that an individual is a suspect in a criminal case, the PPC will inform the individual about that fact"[123] as well as the possibility pursuant to Article 259 of the CCP to ask the prosecution to be notified once the latter has decided not to initiate criminal proceedings. Also, if the evaluation reveals that a case involving the personal information of the individual has been opened and that the case is concluded, the PPC will inform the individual that the case record can be inspected pursuant to Article 53 of the CCP (and Article 4 of the Act on Final Criminal Case Records). Gaining access to his/her case record is important as it will help the individual to better understand the investigation carried out against him/her and thus to prepare an eventual court action (e.g. a damages claim) in case (s)he considers his/her data was unlawfully collected or used.

3.3. Access and use by Japanese public authorities for national security purposes

(151) According to the Japanese authorities, there is no law in Japan permitting compulsory requests for information or "administrative wiretapping" outside criminal investigations. Hence, on national security grounds information may only be obtained from an information source that can be freely accessed by anyone or by voluntary disclosure. Business operators receiving a request for voluntary cooperation (in the form of disclosure of electronic information) are under no legal obligation to provide such information.[124]

(152) Also, according to the information received only four government entities are empowered to collect electronic information held by Japanese business operators on national security grounds, namely: (i) the Cabinet Intelligence & Research Office (CIRO); (ii) the Ministry of Defence ("MOD"); (iii) the police (both National Police

---

[121] See Annex II, Sec. II.C.2).

[122] See, e.g., Tokyo District Court, judgment of 24 March 1988 (No. 2925); Osaka District Court, judgment of 26 April 2007 (No. 2925). According to the Osaka District Court, a number of factors will need to be balanced, such as for instance: (i) the nature and content of the personal information at issue; (ii) the way it has been collected; (iii) the disadvantages to the individual in case the information is not deleted; and (iv) the public interest, including the disadvantages to the public authority in case the information is deleted.

[123] In any event, after the initiation of criminal proceedings the accused shall be given an opportunity by the prosecution to inspect that evidence (see Articles 298-299 of the CCP). As regards the victims of crimes, see Articles 316-333 of the CCP.

[124] Therefore, business operators can freely choose not to cooperate, without any risk for sanctions or other negative consequences. See Annex II, Sec. III.A.1).

Agency (NPA)[125] and Prefectural Police); and (iv) the Public Security Intelligence Agency ("PSIA"). However, the CIRO never collects information directly from business operators, including by means of interception of communications. Where it receives information from other government authorities in order to provide analysis to the Cabinet, these other authorities in turn have to comply with the law, including the limitations and safeguards analysed in this Decision. Its activities are thus not relevant in a transfer context.

3.3.1. Legal basis and applicable limitations/safeguards

(153) According to the information received, the MOD collects (electronic) information on the basis of the MOD Establishment Act. Pursuant to its Article 3, the mission of the MOD is to manage and operate the military forces and "to conduct such affairs as related thereto in order to secure national peace and independence, and the safety of the nation." Article 4(4) provides that the MOD shall have jurisdiction over the "defence and guard", over the actions to be taken by the Self-Defence Forces as well as over the deployment of the military forces, including the collection of information necessary to conduct those affairs. It only has authority to collect (electronic) information from business operators through voluntary cooperation.

(154) As for the Prefectural Police, its responsibilities and duties include the "maintenance of public safety and order" (Article 35(2) in conjunction with Article 2(1) of the Police Law). Within this scope of jurisdiction, the police may collect information, but only on a voluntary basis without legal force. Moreover, the activities of the police shall be "strictly limited" to what is necessary to perform its duties. Moreover, it shall act in an "impartial, nonpartisan, unprejudiced and fair" manner and never abuse its powers "in any way such as to interfere with the rights and liberties of an individual guaranteed in the Constitution of Japan" (Article 2 of the Police Law).

(155) Finally, the PSIA may carry out investigations under the Subversive Activities Prevention Act ("SAPA") and the Act on the Control of Organisations Which Have Committed Acts of Indiscriminate Mass Murder ("ACO") where such investigations are necessary to prepare the adoption of control measures against certain organisations.[126] Under both Acts, upon request by the Director-General of the PSIA the Public Security Examination Commission may issue certain "dispositions" (surveillance/prohibitions in the case of the ACO[127], dissolution/prohibitions in the case of the SAPA[128]) and in this context the PSIA may carry out investigations.[129] According to the information received, these investigations are always conducted on a voluntary basis, meaning that the PSIA may not force an owner of personal

[125] However, according to the information received, the main role of the NPA is to coordinate investigations by the various Prefectural Police departments and to exchange information with foreign authorities. Even in this role the NPA is subject to oversight by the National Public Safety Commission, responsible among others for the protection of the rights and freedoms of individuals (Article 5(1) of the Police Law).

[126] See Annex II, Sec. III.A.1)(3). The respective scope of application of these two laws is limited, with SAPA referring to "terroristic subversive activities" and ACO to the "act of indiscriminate mass murder" (meaning a "terroristic subversive activity" under SAPA "through which a large number of persons are indiscriminately murdered").

[127] See Articles 5, 8 ACO. A surveillance disposition also entails a reporting obligation for the organisation concerned by the measure. For the procedural safeguards, in particular transparency requirements and the prior authorisation by the Public Security Examination Commission, see Articles 12, 13, 15-27 ACO.

[128] See Articles 5, 7 SAPA. For the procedural safeguards, in particular transparency requirements and the prior authorisation by the Public Security Examination Commission, see Articles 11-25 SAPA.

[129] See Article 27 SAPA and Articles, 29, 30 ACO.

information to provide such information.[130] Each time, controls and investigations shall be conducted only to the minimum extent necessary to achieve the control purpose and shall not under any circumstances be carried out to "unreasonably" restrict the rights and freedoms guaranteed under the Constitution of Japan (Article 3(1) of SAPA/ACO). Moreover, according to Article 3(2) of the SAPA/ACO, the PSIA must under no circumstances abuse such controls, or the investigations carried out to prepare such controls. If a Public Security Intelligence Officer has abused his/her authority under the respective Act by forcing a person to do anything which the person is not required to, or by interfering with the exercise of a person's rights, (s)he may be subject to criminal sanctions pursuant to Article 45 SAPA or Article 42 ACO. Finally, both Acts explicitly prescribe that their provisions, including the powers granted therein, shall "not under any circumstances be subject to an expanded interpretation" (Article 2 of SAPA/ACO).

(156) In all cases of government access on national security grounds described in this section, the limitations stipulated by the Japanese Supreme Court for voluntary investigations apply, which means that the collection of (electronic) information must conform with the principles of necessity and proportionality ("appropriate method").[131] As explicitly confirmed by the Japanese authorities, "the collection and processing of information takes place only to the extent necessary to the performance of specific duties of the competent public authority as well as on the basis of specific threats". Therefore, "this excludes mass and indiscriminate collection or access to personal information for national security reasons"[132].

(157) Also, once collected, any personal information retained by public authorities for national security purposes will fall under and thus benefit from the protections under the APPIHAO when it comes to its subsequent storage, use and disclosure (see recital (118)).

3.3.2. Independent oversight

(158) The collection of personal information for national security purposes is subject to several layers of oversight from the three branches of government.

(159) First, the Japanese Diet through its specialised committees may examine the lawfulness of investigations based on its powers of parliamentary scrutiny (Article 62 of the Constitution, Article 104 of the Diet Law; see recital (134)). This oversight function is supported by specific reporting obligations on the activities carried out under some of the aforementioned legal bases.[133]

(160) Second, several oversight mechanisms exist within the executive branch.

---

130 See Annex II, Sec. III.A.1)(3).

131 See Annex II, Sec. III.A.2)(b): "It follows from the case law of the Supreme Court that, in order to address a request for voluntary cooperation to a business operator, such a request must be necessary for the investigation of a suspected crime and must be reasonable in order to achieve the purpose of the investigation. Although investigations conducted by investigative authorities in the area of national security differ from investigations conducted by investigative authorities in the area of law enforcement as regards both their legal basis and purpose, the central principles of "necessity for investigation" and "appropriateness of method" similarly apply in the area of national security and have to be complied with taking appropriate account of the specific circumstances of each case."

132 See Annex II, Sec. III.A.2)(b) .

133 See e.g. Article 36 SAPA/Article 31 ACO (for the PSIA).

(161) As regards MOD, oversight is exercised by the Inspector General's Office of Legal Compliance (IGO)[134] that has been established based on Article 29 of the MOD Establishment Act as an office within the MOD under the supervision of the Minister of Defence (to which it reports) but independent from MOD's operational departments. The IGO has the task of ensuring compliance with laws and regulations as well as the proper execution of duties by MOD officials. Among its powers is the authority to carry out so-called "Defence Inspections", both at regular intervals ("Regular Defence Inspections") and in individual cases ("Special Defence Inspections"), which in the past have also covered the proper handling of personal information.[135] In the context of such inspections, the IGO may enter sites (offices) and request the submission of documents or information, including explanations by the Deputy Vice-Minister of the MOD. The inspection is concluded through a report to the Minister of Defence setting out the findings and measures for improvement (the implementation of which can again be checked through further inspections). The report in turn forms the basis for instructions from the Minister of Defence to implement the measures necessary to address the situation; the Deputy Vice-Minister is charged with carrying out such measures and has to report on the follow-up.

(162) As regards the Prefectural Police, oversight is ensured by the independent Prefectural Public Safety Commissions, as explained in recital (135) with respect to criminal law enforcement.

(163) Finally, as indicated, the PSIA may only carry out investigations to the extent this is necessary with respect to the adoption of a prohibition, dissolution or surveillance disposition under the SAPA/ACO, and for these dispositions the independent[136] Public Security Examination Commission exercises ex ante oversight. In addition, regular/periodic inspections (which in a comprehensive manner look at PSIA's operations)[137] and special internal inspections[138] on the activities of individual departments/offices etc. are carried out by specifically designated inspectors and may lead to instructions to the heads of relevant departments etc. to take corrective or improvement measures.

(164) These oversight mechanisms, which are further strengthened through the possibility for individuals to trigger the intervention of the PPC as an independent supervisory authority (see below section 168), provide adequate guarantees against the risk of abuse by Japanese authorities of their powers in the area of national security, and against any unlawful collection of electronic information.

---

134 The head of the IGO is a former public prosecutor. See Annex II, Sec. III.B.3).

135 See Annex II, Sec. III.B.3. According to the example provided, the Regular Defence Inspection 2016 with respect to "Consciousness/Preparedness for Legal Compliance" among other things covered the "status of personal information protection" (management, storage, etc.). The resulting report found instances of inappropriate data management and called for improvements in this regard. The MOD published the report through its website.

136 According to the Act on the Establishment of the Public Security Examination Commission, the Chairperson and members of the Commission "shall independently exercise their authority" (Article 3). They are appointed by the Prime Minister with the consent of both Houses of the Diet and may only be dismissed "for cause" (e.g. imprisonment, misconduct, mental or physical disorder, opening of bankruptcy proceedings).

137 Regulation of the Public Security Intelligence Agency's Periodic Inspection (Director-General of the PSIA, Instruction No. 4, 1986).

138 Regulation of the Public Security Intelligence Agency's Special Inspection (Director-General of the PSIA, Instruction No. 11, 2008). Special inspections will be carried out when the Director-General of the PSIA deems it necessary.

3.3.3. Individual redress

(165) As regards individual redress, with respect to personal information collected and thus "retained" by Administrative Organs, the latter are under an obligation to "endeavour to properly and expeditiously process any complaints" regarding such processing (Article 48 APPIHAO).

(166) Moreover, unlike for criminal investigations, individuals (including foreign nationals living abroad) have in principle a right to disclosure[139], correction (including deletion) and suspension of use/provision under the APPIHAO. This being said, the head of the Administrative Organ may refuse disclosure with respect to information "for which there are reasonable grounds […] to find that disclosure is likely to cause harm to national security" (Article 14(iv) APPIHAO) and may even do so without revealing the existence of such information (Article 17 APPIHAO). Likewise, while an individual may request suspension of use or deletion pursuant to Article 36(1)(i) APPIHAO in case the Administrative Organ has obtained the information unlawfully or retains/uses it beyond what is necessary to achieve the specified purpose, the authority may reject the request if it finds that the suspension of use "is likely to hinder the proper execution of the affairs pertaining to the Purpose of Use of the Retained Personal Information due to the nature of the said affairs" (Article 38 APPIHAO). Still, where it is possible to easily separate and exclude portions that are subject to an exception, Administrative Organs are required to grant at least partial disclosure (see e.g. Article 15(1) APPIHAO).[140]

(167) In any event, the Administrative Organ has to take a written decision within a certain period (30 days, which under certain conditions can be extended by an additional 30 days). If the request is rejected, only partially granted, or if the individual for other reasons considers the conduct of the Administrative Organ to be "illegal or unjust", the individual may request administrative review based on the Administrative Complaint Review Act.[141] In such a case, the head of the Administrative Organ deciding on the appeal shall consult the Information Disclosure and Personal Information Protection Review Board (Articles 42, 43 APPIHAO), a specialised, independent board whose members are appointed by the Prime Minister with consent of both Houses of the Diet. According to the information received, the Review Board may carry out an examination[142] and in this respect request the Administrative Organ to provide the retained personal information, including any classified content, as well as further information and documents. While the ultimate report sent to the complainant as well as the Administrative Organ and made public is not legally binding, it is in almost all cases followed.[143] Moreover, the individual has the possibility to challenge the appeal decision in court based on the Administrative Case Litigation Act. This opens the way

139 This refers to the right to receive a copy of the "Retained Personal Information".

140 See also the possibility for "discretionary disclosure" even in a case where "Non-Disclosure Information" is included in the "Retained Personal Information" for which disclosure is sought (Article 16 APPIHAO).

141 Administrative Complaint Review Act (Act No. 160 of 2014), in particular Article 1(1).

142 See Article 9 of the Act for the Establishment of the Information Disclosure and Personal Information Protection Review Board (Act No. 60 of 2003).

143 According to the information received, in the 13 years since 2005 (when the APPIHAO entered into force), in only two out of more than 2,000 cases did the Administrative Organ not follow the report, despite the fact that administrative decisions have been contradicted by the Review Board on a number of occasions. Moreover, where the Administrative Organ takes a decision that departs from the findings in the report, it has to indicate clearly the reasons for doing so. See Annex II, Sec. III.C, with reference to Article 50(1), item (iv) of the Administrative Complaint Review Act.

for judicial control of the use of the national security exception(s), including of whether such an exception has been abused or is still justified.

(168) In order to facilitate the exercise of the above-mentioned rights under the APPIHAO, the MIC has established 51 "comprehensive information centres" that provide consolidated information on those rights, the applicable procedures to make a request and possible avenues for redress.[144] As regards the Administrative Organs, they are required to provide "information that contributes to specifying the Retained Personal Information held"[145] and to take "other adequate measures in consideration of the convenience of the person who intends to make the request" (Article 47(1) of the APPIHAO).

(169) As is the case for investigations in the area of criminal law enforcement, also in the area of national security individuals may obtain individual redress by directly contacting the PPC. This will trigger the specific dispute resolution procedure that the Japanese government has created for EU individuals whose personal data is transferred under this Decision (see detailed explanations in recitals (141) to (144), (149)).

(170) In addition, individuals may seek judicial redress in the form of a damage action under the State Redress Act, which also covers moral harm and under certain conditions the deletion of the collected data (see recital (147)).

4. Conclusion: adequate level of protection for personal data transferred from the European Union to business operators in Japan

(171) The Commission considers that the APPI as complemented by the Supplementary Rules contained in Annex I, together with the official representations, assurances and commitments contained in Annex II, ensure a level of protection for personal data transferred from the European Union that is essentially equivalent to the one guaranteed by Regulation (EU) 2016/679.

(172) Moreover, the Commission considers that, taken as a whole, the oversight mechanisms and redress avenues in Japanese law enable infringements by recipient PIHBOs to be identified and punished in practice and offer legal remedies to the data subject to obtain access to personal data relating to him/her and, eventually, the rectification or erasure of such data.

(173) Finally, on the basis of the available information about the Japanese legal order, including the representations, assurances and commitments from the Japanese government contained in Annex II, the Commission considers that any interference with the fundamental rights of the individuals whose personal data are transferred from the European Union to Japan by Japanese public authorities for public interest purposes, in particular criminal law enforcement and national security purposes, will be limited to what is strictly necessary to achieve the legitimate objective in question, and that effective legal protection against such interference exists.

---

[144] The Comprehensive Information Centres – one in each Prefecture – provide citizens with explanations on personal information collected by public authorities (e.g. existing databases) and the applicable data protection rules (APPIHAO), including how to exercise the rights to disclosure, correction or suspension of use. At the same time, the centres work as a contact point for queries/complaints from citizens. See Annex II, Sec. II.C.4)(a).

[145] See also Articles 10, 11 APPIAHO on the "Personal Information File Register", which however contain broad exceptions when it comes to "Personal Information Files" prepared or obtained for criminal investigations or that contain matters concerning the security and other important interests of the State (see Article 10(2), items (i) and (ii), of the APPIHAO).

(174) Therefore, in the light of the findings of this Decision, the Commission considers that Japan ensures an adequate level of protection for personal data transferred from the European Union to PIHBOs in Japan that are subject to the APPI, except in those cases where the recipient falls within one of the categories listed in Article 76(1) APPI and all or part of the purposes of processing correspond(s) to one of the purposes prescribed in that provision.

(175) On this basis, the Commission concludes that the adequacy standard of Article 45 of Regulation (EU) 2016/679, interpreted in light of the Charter of Fundamental Rights of the European Union, in particular in the *Schrems* judgment[146], is met.

5. Action of data protection authorities and information to the Commission

(176) According to the case law of the Court of Justice[147], and as recognized in Article 45(4) of Regulation (EU) 2016/679, the Commission should continuously monitor relevant developments in the third country after the adoption of an adequacy decision in order to assess whether Japan still ensures an essentially equivalent level of protection. Such a check is required, in any event, when the Commission receives information giving rise to a justified doubt in that respect.

(177) Therefore, the Commission should on an on-going basis monitor the situation as regards the legal framework and actual practice for the processing of personal data as assessed in this Decision, including compliance by the Japanese authorities with the representations, assurances and commitments contained in Annex II. To facilitate this process, the Japanese authorities are expected to inform the Commission of material developments relevant to this Decision, both as regards the processing of personal data by business operators and the limitations and safeguards applicable to access to personal data by public authorities. This should include any decisions adopted by the PPC under Article 24 of the APPI recognising a third country as providing an equivalent level of protection to the one guaranteed in Japan.

(178) Moreover, in order to allow the Commission to effectively carry out its monitoring function, the Member States should inform the Commission about any relevant action undertaken by the national data protection authorities ("DPAs"), in particular regarding queries or complaints by EU data subjects concerning the transfer of personal data from the European Union to business operators in Japan. The Commission should also be informed about any indications that the actions of Japanese public authorities responsible for the prevention, investigation, detection or prosecution of criminal offences, or for national security, including any oversight bodies, do not ensure the required level of protection.

(179) Member States and their organs are required to take the measures necessary to comply with acts of the Union institutions, as the latter are presumed to be lawful and accordingly produce legal effects until such time as they are withdrawn, annulled in an action for annulment or declared invalid following a reference for a preliminary ruling or a plea of illegality. Consequently, a Commission adequacy decision adopted pursuant to Article 45(3) of Regulation (EU) 2016/679 is binding on all organs of the Member States to which it is addressed, including their independent supervisory authorities. At the same time, as explained by the Court of Justice in the *Schrems*

[146] See above footnote 3.
[147] *Schrems*, paragraph 76.

judgment[148] and recognised in Article 58(5) of the Regulation, where a DPA questions, including upon a complaint, the compatibility of a Commission adequacy decision with the fundamental rights of the individual to privacy and data protection, national law must provide it with a legal remedy to put those objections before a national court which, in case of doubts, must stay proceedings and make a reference for a preliminary ruling to the Court of Justice.[149]

6. Periodic review of the adequacy finding

(180) In application of Article 45(3) of Regulation (EU) 2016/679[150], and in the light of the fact that the level of protection afforded by the Japanese legal order may be liable to change, the Commission, following the adoption of this Decision, should periodically check whether the findings relating to the adequacy of the level of protection ensured by Japan are still factually and legally justified.

(181) To this end, this Decision should be subject to a first review within two years after its entry into force. Following that first review, and depending on its outcome, the Commission will decide in close consultation with the Committee established under Article 93(1) of the GDPR whether the two-year-cycle should be maintained. In any case, the subsequent reviews should take place at least every four years.[151] The review should cover all aspects of the functioning of this Decision, and in particular the application of the Supplementary Rules (with special attention paid to protections afforded in case of onward transfers), the application of the rules on consent, including in case of withdrawal, the effectiveness of the exercise of individual rights, as well as the limitations and safeguards with respect to government access, including the redress mechanism as set out in Annex II to this Decision. It should also cover the effectiveness of oversight and enforcement, as regards the rules applicable to both PIHBOs and in the area of criminal law enforcement and national security.

(182) To perform the review, the Commission should meet with the PPC, accompanied, where appropriate, by other Japanese authorities responsible for government access, including relevant oversight bodies. The participation in this meeting should be open to representatives of the members of the European Data Protection Board (EDPB). In the framework of the Joint Review, the Commission should request the PPC to provide comprehensive information on all aspects relevant for the adequacy finding, including on the limitations and safeguards concerning government access.[152] The Commission should also seek explanations on any information relevant for this Decision that it has received, including public reports by Japanese authorities or other stakeholders in

---

148 *Schrems*, paragraph 65.

149 *Schrems*, paragraph 65: "It is incumbent upon the national legislature to provide for legal remedies enabling the national supervisory authority concerned to put forward the objections which it considers well founded before the national courts in order for them, if they share its doubts as to the validity of the Commission decision, to make a reference for a preliminary ruling for the purpose of examination of the decision's validity."

150 According to Article 45(3) of Regulation (EU) 2016/679, "[t]he implementing act shall provide for a mechanism for a periodic review, at least every four years, which shall take into account all relevant developments in the third country or international organisation."

151 Article 45(3) of Regulation (EU) 2016/679 provides that a periodic review must take place at least every four years. See also EDPB, Adequacy Referential, WP 254 rev. 01.

152 See also Annex II, Sec. IV: "In the framework of the periodic review of the adequacy decision, PPC and the European Commission will exchange information on the processing of data under the conditions of the adequacy finding, including those set out in this Representation."

Japan, the EDPB, individual DPAs, civil society groups, media reports, or any other available source of information.

(183) On the basis of the Joint Review, the Commission should prepare a public report to be submitted to the European Parliament and the Council.

7. Suspension of the adequacy decision

(184) Where, on the basis of the regular and ad hoc checks or any other information available, the Commission concludes that the level of protection afforded by the Japanese legal order can no longer be regarded as essentially equivalent to that in the European Union, it should inform the competent Japanese authorities thereof and request that appropriate measures be taken within a specified, reasonable timeframe. This includes the rules applicable to both business operators and Japanese public authorities responsible for criminal law enforcement or national security. For example, such a procedure would be triggered in cases where onward transfers, including on the basis of decisions adopted by the PPC under Article 24 of the APPI recognising a third country as providing an equivalent level of protection to the one guaranteed in Japan, will no longer be carried out under safeguards ensuring the continuity of protection within the meaning of Article 44 of the GDPR.

(185) If, after the specified time period, the competent Japanese authorities fail to demonstrate satisfactorily that this Decision continues to be based on an adequate level of protection, the Commission should, in application of Article 45(5) of Regulation (EU) 2016/679, initiate the procedure leading to the partial or complete suspension or repeal of this Decision. Alternatively, the Commission should initiate the procedure to amend this Decision, in particular by subjecting data transfers to additional conditions or by limiting the scope of the adequacy finding only to data transfers for which the continuity of protection within the meaning of Article 44 of the GDPR is ensured.

(186) In particular, the Commission should initiate the procedure for suspension or repeal in case of indications that the Supplementary Rules contained in Annex I are not complied with by business operators receiving personal data under this Decision and/or are not effectively enforced, or that the Japanese authorities fail to comply with the representations, assurances and commitments contained in Annex II to this Decision.

(187) The Commission should also consider initiating the procedure leading to the amendment, suspension or repeal of this Decision if, in the context of the Joint Review or otherwise, the competent Japanese authorities fail to provide the information or clarifications necessary for the assessment of the level of protection afforded to personal data transferred from the European Union to Japan or compliance with this Decision. In this respect, the Commission should take into account the extent to which the relevant information can be obtained from other sources.

(188) On duly justified grounds of urgency, such as a risk of serious infringment of data subjects' rights, the Commission should consider adopting a decision to suspend or repeal this Decision that should apply immediately, pursuant to Article 93(3) of Regulation (EU) 2016/679 in conjunction with Article 8 of Regulation 182/2011.

8. Final considerations

(189) The European Data Protection Board published its opinion[153], which has been taken into consideration in the preparation of this Decision.

(190) The European Parliament has adopted a resolution on a digital trade strategy that calls on the Commission to prioritise and speed up the adoption of adequacy decisions with important trading partners under the conditions laid down in Regulation (EU) 2016/679, as an important mechanism to safeguard the transfer of personal data from the European Union.[154] The European Parliament has also adopted a resolution on the adequacy of the protection of personal data afforded by Japan.[155]

(191) The measures provided for in this Decision are in accordance with the opinion of the Committee established under Article 93(1) of the GDPR.

HAS ADOPTED THIS DECISION:

Article 1

1. For the purposes of Article 45 of Regulation (EU) 2016/679, Japan ensures an adequate level of protection for personal data transferred from the European Union to personal information handling business operators in Japan subject to the Act on the Protection of Personal Information as complemented by the Supplementary Rules set out in Annex I, together with the official representations, assurances and commitments contained in Annex II.

2. This decision does not cover personal data transferred to recipients falling within one of the following categories, to the extent all or part of the purposes of processing of the personal data corresponds to one of the listed purposes, respectively:

(a) broadcasting institutions, newspaper publishers, communication agencies or other press organisations (including any individuals carrying out press activities as their business) to the extent they process personal data for press purposes;

(b) persons engaged in professional writing, to the extent this involves personal data;

(c) universities and any other organisations or groups aimed at academic studies, or any person belonging to such an organisation or group, to the extent they process personal data for the purpose of academic studies;

(d) religious bodies to the extent they process personal data for purposes of religious activity (including all related activities); and

(e) political bodies to the extent they process personal data for the purposes of their political activity (including all related activities).

---

153 Opinion 28/2018 regarding the European Commission Draft Implementing Decision on the adequate protection of personal data in Japan, adopted on 5 December 2018.

154 European Parliament, Resolution of 12 December 2017 "Towards a digital trade strategy" (2017/2065(INI)). See in particular point 8 ("…recalls that personal data can be transferred to third countries without using general disciplines in trade agreements when the requirements – both at present and in the future – enshrined in […] Chapter V of Regulation (EU) 2016/679 are fulfilled; recognises that adequacy decisions, including partial and sector-specific ones, constitute a fundamental mechanism in terms of safeguarding the transfer of personal data from the EU to a third country; notes that the EU has only adopted adequacy decisions with four of its 20 largest trading partners…") and point 9 ("Calls on the Commission to prioritise and speed up the adoption of adequacy decisions, provided that third countries ensure, by reason of their domestic law or their international commitments, a level of protection 'essentially equivalent' to that guaranteed within the EU…").

155 European Parliament, Resolution of 13 December 2018 "Adequacy of the protection of personal data afforded by Japan" (2018/2979(RSP)).

Article 2

Whenever the competent authorities in Member States, in order to protect individuals with regard to the processing of their personal data, exercise their powers pursuant to Article 58 of Regulation (EU) 2016/679 leading to the suspension or definitive ban of data flows to a specific business operator in Japan within the scope of application set out in Article 1, the Member State concerned shall inform the Commission without delay.

Article 3

1. The Commission shall continuously monitor the application of the legal framework upon which this Decision is based, including the conditions under which onward transfers are carried out, with a view to assessing whether Japan continues to ensure an adequate level of protection within the meaning of Article 1.

2. The Member States and the Commission shall inform each other of cases where the Personal Information Protection Commission, or any other competent Japanese authority, fails to ensure compliance with the legal framework upon which this Decision is based.

3. The Member States and the Commission shall inform each other of any indications that interferences by Japanese public authorities with the right of individuals to the protection of their personal data go beyond what is strictly necessary, or that there is no effective legal protection against such interferences.

4. Within two years from the date of the notification of this Decision to the Member States and subsequently at least every four years, the Commission shall evaluate the finding in Article 1(1) on the basis of all available information, including the information received as part of the Joint Review carried out together with the relevant Japanese authorities.

5. Where the Commission has indications that an adequate level of protection is no longer ensured, the Commission shall inform the competent Japanese authorities. If necessary, it may decide to suspend, amend or repeal this Decision, or limit its scope, in particular where there are indications that:

(a) business operators in Japan that have received personal data from the European Union under this Decision do not comply with the additional safeguards set out in the Supplementary Rules contained in Annex I to this Decision, or there is insufficient oversight and enforcement in this regard;

(b) the Japanese public authorities do not comply with the representations, assurances and commitments contained in Annex II to this Decision, including as regards the conditions and limitations for the collection of and access to personal data transferred under this Decision by Japanese public authorities for criminal law enforcement or national security purposes.

The Commission may also present such draft measures if the lack of cooperation of the Japanese government prevents the Commission from determining whether the finding in Article 1(1) of this Decision is affected.

Article 4

This Decision is addressed to the Member States.

Done at Brussels, 23.1.2019

For the Commission
Věra JOUROVÁ
Member of the Commission

CERTIFIED COPY
For the Secretary-General,

Jordi AYET PUIGARNAU
Director of the Registry
EUROPEAN COMMISSION