Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information (notified under document C(2019) 304) (Text with EEA relevance)

COMMISSION IMPLEMENTING DECISION (EU) 2019/419

of 23 January 2019

pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information

(notified under document C(2019) 304)

(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] ('GDPR'), 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.

Changes to legislation: *There are outstanding changes not yet made to Commission Implementing Decision (EU) 2019/419. Any changes that have already been made to the legislation appear in the content and are referenced with annotations. (See end of Document for details) View outstanding changes*

(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, 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

***Changes to legislation:** There are outstanding changes not yet made to Commission Implementing Decision (EU) 2019/419. Any changes that have already been made to the legislation appear in the content and are referenced with annotations. (See end of Document for details) View outstanding changes*

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." 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.

Changes to legislation: *There are outstanding changes not yet made to Commission Implementing Decision (EU) 2019/419. Any changes that have already been made to the legislation appear in the content and are referenced with annotations. (See end of Document for details) View outstanding changes*

(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 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)].

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

***Changes to legislation:** There are outstanding changes not yet made to Commission Implementing Decision (EU) 2019/419. Any changes that have already been made to the legislation appear in the content and are referenced with annotations. (See end of Document for details) View outstanding changes*

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 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.