EUROPEAN
COMMISSION

Brussels, 23.1.2019
C(2019) 304 final

ANNEXES 1 to 2

ANNEXES

to the

Commission Implementing Decision

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

ANNEX 1

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

Table of Contents

[Terms]

"Act"	The Act on the Protection of Personal Information (Act No. 57, 2003)
"Cabinet Order"	Cabinet Order to Enforce the Act on the Protection of Personal Information (Cabinet Order No. 507, 2003)
"Rules"	Enforcement Rules for the Act on the Protection of Personal Information (Rules of the Personal Information Protection Commission No. 3, 2016)

"General Rules Guidelines"	Guidelines for the Act on the Protection of Personal Information (Volume on General Rules) (Notice of the Personal Information Protection Commission No. 65, 2015)
“EU”	European Union, including its Member States and, in the light of the EEA Agreement, Iceland, Liechtenstein and Norway
“GDPR”	Regulation of the European Parliament and of the Council 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）
“adequacy decision”	The European Commission’s decision that a third country or a territory within that third country, etc. ensures an adequate level of protection of personal data pursuant to Article 45 of the GDPR

The Personal Information Protection Commission, for the purpose of conducting mutual and smooth transfer of personal data between Japan and the EU, designated the EU as a foreign country establishing a personal information protection system recognized to have equivalent standards to that in Japan in regard to the protection of an individual's rights and interests based on Article 24 of the Act and the European Commission concurrently decided that Japan ensures an adequate level of protection of personal data pursuant to Article 45 of the GDPR.

Hereby, mutual and smooth transfer of personal data will be conducted between Japan and the EU in a way that ensures a high level of protection of an individual's rights and interests. In order to ensure that high level of protection regarding personal information received from the EU based on an adequacy decision and in light of the fact that, despite a high degree of convergence between the two systems, there are some relevant differences, the Personal Information Protection Commission has adopted these Supplementary Rules, based on the provisions of the Act concerning implementation etc. of cooperation with the governments in other countries and in view of ensuring appropriate handling of personal information received from the EU based on an adequacy decision by a personal information handling business operator and proper and effective implementation of the obligations laid down in such rules (*1).

In particular, Article 6 of the Act provides for the power to take necessary legislative and other action with a view to ensure the enhanced protection of personal information and construct an internationally conformable system concerning personal information through stricter rules that supplement and go beyond those laid down in the Act and the Cabinet Order. Therefore, the Personal Information Protection Commission, as the authority competent for governing the overall administration of the Act, has the power to establish pursuant to Article 6 of the Act stricter regulations by formulating the present Supplementary Rules providing for a higher level of protection of an individual's rights and interests regarding the handling of personal data received from the EU based on an adequacy decision, including with respect to the definition of special care-required personal information pursuant to Article 2, paragraph (3), of the Act and retained personal data pursuant to Article 2, paragraph (7), of the Act (including as to the relevant retention period).

On this basis, the Supplementary Rules are binding on a personal information handling business operator that receives personal data transferred from the EU based on an adequacy decision which is thus required to comply with them. As legally binding rules, any rights and obligations are enforceable by the Personal Information Protection Commission in the same way as the provisions of the Act that they supplement with stricter and/or more detailed rules.

In case of infringement of the rights and obligations resulting from the Supplementary Rules, individuals can also obtain redress from courts in the same way as with respect to the provisions of the Act that they supplement with stricter and/or more detailed rules.

As regards enforcement by the Personal Information Protection Commission, in case a personal information handling business operator does not comply with one or several obligations under the Supplementary Rules, the Personal Information Protection Commission has the power to adopt measures pursuant to Article 42 of the Act. Regarding generally personal information received from the EU based on an adequacy decision, failure by a personal information handling business operator to take action in line with a recommendation received pursuant to Article 42, paragraph (1), of the Act, without legitimate ground (*2), is considered as a serious infringement of an imminent nature of an individual's rights and interests within the meaning of Article 42, paragraph (2), of the Act.

(*1) Article 4, Article 6, Article 8, Article 24, Article 60 and Article 78 of the Act, and Article 11 of the Rules.

(*2) Legitimate ground shall be understood as meaning an event of an extraordinary nature outside the control of the personal information handling business operator which cannot be reasonably foreseen (for example, natural disasters) or when the necessity to take action concerning a recommendation issued by the Personal Information Protection Commission pursuant to Article 42, paragraph (1), of the Act has disappeared because the personal information handling business operator has taken alternative action that fully remedies the violation

(1) Special care-required personal information (Article 2, paragraph (3) of the Act)

Article 2 (paragraph 3) of the Act

(3) Special care-required personal information" in this Act means 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.

Article 2 of the Cabinet Order

Those descriptions etc. prescribed by cabinet order under Article 2, paragraph (3) of the Act shall be those descriptions etc. which contain any of those matters set forth in the following (excluding those falling under a principal's medical record or criminal history)

(i) the fact of having physical disabilities, intellectual disabilities, mental disabilities (including developmental disabilities), or other physical and mental functional disabilities prescribed by rules of the Personal Information Protection Commission;

(ii) the results of a medical check-up or other examination (hereinafter referred to as a "medical check-up etc." in the succeeding item) for the prevention and early detection of a disease conducted on a principal by a medical doctor or other person engaged in

duties related to medicine (hereinafter referred to as a “doctor etc.” in the succeeding item);

(iii) the fact that guidance for the improvement of the mental and physical conditions, or medical care or prescription has been given to a principal by a doctor etc. based on the results of a medical check-up etc. or for reason of disease, injury or other mental and physical changes;

(iv) the fact that an arrest, search, seizure, detention, institution of prosecution or other procedures related to a criminal case have been carried out against a principal as a suspect or defendant;

(v) the fact that an investigation, measure for observation and protection, hearing and decision, protective measure or other procedures related to a juvenile protection case have been carried out against a principal as a juvenile delinquent or a person suspected thereof under Article 3, paragraph (1) of the Juvenile Act.

Article 5 of the Rules

Physical and mental functional disabilities prescribed by rules of the Personal Information Protection Commission under Article 2, item (i) of the Order shall be those disabilities set forth in the following.

(i) physical disabilities set forth in an appended table of the Act for Welfare of Persons with Physical Disabilities (Act No.283 of 1949)

(ii) intellectual disabilities referred to under the Act for the Welfare of Persons with Intellectual Disabilities (Act No.37 of 1960)

(iii) mental disabilities referred to under the Act for the Mental Health and Welfare of the Persons with Mental Disabilities (Act No.123 of 1950) (including developmental disabilities prescribed in Article 2, paragraph (1) of the Act on Support for Persons with Development Disabilities, and excluding intellectual disabilities under the Act for the Welfare of Persons with Intellectual Disabilities)

(iv) a disease with no cure methods established thereof or other peculiar diseases of which the severity by those prescribed by cabinet order under Article 4, paragraph (1) of the Act on Comprehensive Support for Daily and Social Lives of Persons with Disabilities (Act No. 123 of 2005) is equivalent to those prescribed by the Minister of Health, Labor and Welfare under the said paragraph

If personal data received from the EU based on an adequacy decision contains data concerning a natural person's sex life or sexual orientation or trade-union membership, which are defined as special categories of personal data under the GDPR, personal information handling business operators are required to handle that personal data in the same manner as special care-required personal information within the meaning of Article 2, paragraph (3) of the Act.

(2) Retained personal data (Article 2, paragraph (7) of the Act)

Article 2 (paragraph 7) of the Act

(7) "Retained personal data" in this Act means personal data which a personal information handling business operator has the authority to disclose, correct, add or delete the contents of, cease the utilization of, erase, and cease the third-party provision of, and which shall be neither those prescribed by cabinet order as likely to harm the public or other interests if their presence or absence is made known nor those set to be deleted within a period of no longer than one year that is prescribed by Cabinet Order.

Article 4 of the Cabinet Order

Those prescribed by cabinet order under Article 2, paragraph (7) shall be those set forth in the following.

(i) 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 harm a principal or third party's life, body or fortune;

(ii) 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 encourage or induce an illegal or unjust act;

(iii) 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 undermine national security, destroy a trust relationship with a foreign country or international organization, or suffer disadvantage in negotiations with a foreign country or international organization;

(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.

Article 5 of the Cabinet Order

A period prescribed by Cabinet Order under Article 2, paragraph (7) of the Act shall be six months.

Personal data received from the EU based on an adequacy decision is required to 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.

If personal data received from the EU based on an adequacy decision falls within the scope of personal data prescribed by Cabinet Order as being "likely to harm the public or other interests if their presence or absence is made known," such data is not required to be handled as retained personal data (see Article 4 of the Cabinet Order; General Rules Guidelines, "2-7. Retained personal data").

(3) Specifying a utilization purpose, restriction due to a utilization purpose (Article 15, paragraph (1), Article 16, paragraph (1) and Article 26, paragraphs (1) and (3) of the Act)

Article 15 (paragraph 1) of the Act

(1) A personal information handling business operator shall, in handling personal information, specify the purpose of utilizing the personal information (hereinafter referred to as a "utilization purpose") as explicitly as possible.

Article 16 (paragraph 1) of the Act

(1) A personal information handling business operator shall not handle personal information without obtaining in advance a principal's consent beyond the necessary scope to achieve a utilization purpose specified pursuant to the provisions under the preceding Article.

Article 26 (paragraphs 1 and 3) of the Act

(1) A personal information handling business operator shall, when receiving the provision of personal data from a third party, confirm those matters set forth in the following pursuant to rules of the Personal Information Protection Commission. (omitted)
  (i) (omitted)
  (ii) circumstances under which the said personal data was acquired by the said third party

(3) A personal information handling business operator shall, when having confirmed pursuant to the provisions of paragraph (1), keep a record pursuant to rules of the Personal Information Protection Commission on the date when it received the provision of personal data, a matter concerning the said confirmation, and other matters prescribed by rules of the Personal Information Protection Commission.

If personal information handling business operators handle personal information beyond the necessary scope to achieve a utilization purpose specified under Article 15, paragraph (1) of the Act, they shall obtain the relevant principal's consent in advance (Article 16, paragraph (1) of the Act). When receiving the provision of personal data from a third party, personal information handling business operators shall, pursuant to the Rules, confirm matters such as the circumstances under which the said personal data was acquired by the said third party, and record these matters (Article 26, paragraphs (1) and (3) of the Act).

In the case where a personal information handling business operator receives personal data from the EU based on an adequacy decision, the circumstances regarding the acquisition of the said personal data which shall be confirmed and recorded as prescribed by Article 26, paragraphs (1) and (3), include the utilization purpose for which it was received from the EU.

Similarly, in the case where a personal information handling business operator receives from another personal information handling business operator personal data previously

transferred from the EU based on an adequacy decision, the circumstances regarding the acquisition of the said personal data which shall be confirmed and recorded as prescribed by Article 26, paragraphs (1) and (3), include the utilization purpose for which it was received.

In the above-mentioned cases, the personal information handling business operator is required to specify the purpose of utilizing the said personal data within the scope of the utilization purpose for which the data was originally or subsequently received, as confirmed and recorded pursuant to Article 26, paragraphs (1) and (3), and utilize that data within the said scope (as prescribed by Articles 15, paragraph (1) and Article 16, paragraph (1) of the Act).

(4) Restriction on provision to a third party in a foreign country (Article 24 of the Act; Article 11-2 of the Rules)

Article 24 of the Act
A personal information handling business operator, except in those cases set forth in each item of the preceding Article, paragraph (1), shall, in case of providing personal data to a third party (excluding a person establishing a system conforming to standards prescribed by rules of the Personal Information Protection Commission as necessary for continuously taking action equivalent to the one that a personal information handling business operator shall take concerning the handling of personal data pursuant to the provisions of this Section; hereinafter the same in this Article) in a foreign country (meaning a country or region located outside the territory of Japan; hereinafter the same) (excluding those prescribed by rules of the Personal Information Protection Commission as a foreign country establishing a personal information protection system recognized to have equivalent standards to that in Japan in regard to the protection of an individual's rights and interests; hereinafter the same in this Article), in advance obtain a principal's consent to the effect that he or she approves the provision to a third party in a foreign country. In this case, the provisions of the preceding Article shall not apply.

Article 11-2 of the Rules
Standards prescribed by rules of the Personal Information Protection Commission under Article 24 of the Act are to be falling under any of each following item.
(i) a personal information handling business operator and a person who receives the provision of personal data have ensured in relation to the handling of personal data by the person who receives the provision the implementation of measures in line with the purport of the provisions under Chapter IV, Section 1 of the Act by an appropriate and reasonable method
(ii) a person who receives the provision of personal data has obtained a recognition based on an international framework concerning the handling of personal information

A personal information handling business operator, in cases of providing a third party in a foreign country with personal data that it has received from the EU based on an adequacy decision, shall obtain in advance a principal's consent to the effect that he or she approves the

provision to a third party in a foreign country pursuant to Article 24 of the Act, after having been provided information on the circumstances surrounding the transfer necessary for the principal to make a decision on his/her consent, excluding the cases falling under one of the following (i) through (iii).

(i) when the third party is in a country prescribed by the Rules as a foreign country establishing a personal information protection system recognized to have equivalent standards to that in Japan in regard to the protection of an individual's rights and interests

(ii) when a personal information handling business operator and the third party who receives the provision of personal data have, in relation to the handling of personal data by the third party, implemented together measures providing an equivalent level of protection to the Act, read together with the present Rules, by an appropriate and reasonable method (meaning a contract, other forms of binding agreements, or binding arrangements within a corporate group).

(iii) in cases falling under each item of Article 23, paragraph (1) of the Act

(5) Anonymously processed information (Article 2, paragraph 9 and Article 36, paragraphs (1) and (2) of the Act)

Article 2 (paragraph 9) of the Act

(9) "Anonymously processed information" in this Act means information relating to an individual that can be produced from processing personal information so as neither to be able to identify a specific individual by taking action prescribed in each following item in accordance with the divisions of personal information set forth in each said item nor to be able to restore the personal information.

(i) personal information falling under paragraph (1), item (i);
Deleting a part of descriptions etc. contained in the said personal information (including replacing the said part of descriptions etc. with other descriptions etc. using a method with no regularity that can restore the said part of descriptions etc.)

(ii) personal information falling under paragraph (1), item (ii);
Deleting all individual identification codes contained in the said personal information (including replacing the said individual identification codes with other descriptions etc. using a method with no regularity that can restore the said personal identification codes)

Article 36 (paragraph 1) of the Act

(1) A personal information handling business operator shall, when producing anonymously processed information (limited to those constituting anonymously processed information database etc.; hereinafter the same), process personal information in accordance with standards prescribed by rules of the Personal Information Protection Commission as those necessary to make it impossible to identify a specific individual and restore the personal information used for the production.

Article 19 of the Rules

Standards prescribed by rules of the Personal Information Protection Commission under Article 36, paragraph (1) of the Act shall be as follows.

(i) deleting a whole or part of those descriptions etc. which can identify a specific individual contained in personal information (including replacing such descriptions etc. with other descriptions etc. using a method with no regularity that can restore the whole or part of descriptions etc.)

(ii) deleting all individual identification codes contained in personal information (including replacing such codes with other descriptions etc. using a method with no regularity that can restore the individual identification codes)

(iii) deleting those codes (limited to those codes linking mutually plural information being actually handled by a personal information handling business operator) which link personal information and information obtained by having taken measures against the personal information (including replacing the said codes with those other codes which cannot link the said personal information and information obtained by having taken measures against the said personal information using a method with no regularity that can restore the said codes)

(iv) deleting idiosyncratic descriptions etc. (including replacing such descriptions etc. with other descriptions etc. using a method with no regularity that can restore the idiosyncratic descriptions etc.)

(v) besides action set forth in each preceding item, taking appropriate action based on the results from considering the attribute etc. of personal information database etc. such as a difference between descriptions etc. contained in personal information and descriptions etc. contained in other personal information constituting the personal information database etc. that encompass the said personal information

Article 36 (paragraph 2) of the Act

(2) A personal information handling business operator, when having produced anonymously processed information, shall, in accordance with standards prescribed by rules of the Personal Information Protection Commission as those necessary to prevent the leakage of information relating to those 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 pursuant to the provisions of the preceding paragraph, take action for the security control of such information.

Article 20 of the Rules

Standards prescribed by rules of the Personal Information Protection Commission under Article 36, paragraph (2) of the Act shall be as follows.

(i) defining clearly the authority and responsibility of a person handling information relating to those descriptions etc. and individual identification codes which were deleted from personal information used to produce anonymously processed

information and information relating to a processing method carried out pursuant to the provisions of Article 36, paragraph (1) (limited to those which can restore the personal information by use of such relating information) (hereinafter referred to as "processing method etc. related information" in this Article.)

(ii) establishing rules and procedures on the handling of processing method etc. related information, handling appropriately processing method etc. related information in accordance with the rules and procedures, evaluating the handling situation, and based on such evaluation results, taking necessary action to seek improvement

(iii) taking necessary and appropriate action to prevent a person with no legitimate authority to handle processing method etc. related information from handling the processing method etc. related information

Personal information received from the EU based on an adequacy decision shall only be considered anonymously processed information within the meaning of Article 2, paragraph (9) of the Act 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 (meaning information relating to those descriptions etc. and individual identification codes which were deleted from personal information used to produce anonymously processed information and information relating to a processing method carried out pursuant to the provisions of Article 36, paragraph (1) of the Act (limited to those which can restore the personal information by use of such relating information)).

ANNEX 2

Her Excellency Ms. Věra Jourová, Commissioner for Justice, Consumers and Gender Equality of the European Commission

Your Excellency,

I welcome the constructive discussions between Japan and the European Commission aiming at building the framework for mutual transfer of personal data between Japan and the EU).

Upon the request from the European Commission to the government of Japan, I am sending a document attached herewith providing an overview of the legal framework concerning access to information by the government of Japan.

This document concerns many ministries and agencies of the government of Japan, and regarding the contents of the document, the relevant ministries and agencies (Cabinet Secretariat, National Police Agency, Personal Information Protection Commission, Ministry of Internal Affairs and Communications, Ministry of Justice, Public Security Intelligence Agency, Ministry of Defense) are responsible for the passages within the scope of their respective competences. Please find below the relevant ministries and agencies and respective signatures.

The Personal Information Protection Commission accepts all inquiries on this document and will coordinate the necessary responses among the relevant ministries and agencies.

I hope that this document would be helpful in making decisions at the European Commission. ·

I do appreciate your great contribution to date in this matter.

Sincerely yours,

Yoko Kamikawa
Minister of Justice

This Document was drawn up by Ministry of Justice and the following ministries and agencies concerned.

Koichi Hamano

Counsellor, Cabinet Secretariat

Schunichi Kuryu

Commissioner General of National Police Agency

Mari Sonoda

Secretary General, Personal Information Protection Commission

Mitsuru Yasuda

Vice-Minister, Ministry of Internal Affairs and Communication

Seimei Nakagawa

Public Security Intelligence Agency

Kenichi Takahashi

Administrative Vice-Minister of Defense

September 14, 2018

Collection and use of personal information by Japanese public authorities for criminal law enforcement and national security purposes

The following document provides an overview of the legal framework for the collection and use of personal (electronic) information by Japanese public authorities for criminal law enforcement and national security purposes (hereinafter referred to as "government access"), in particular as regards the available legal bases, applicable conditions (limitations) and safeguards, including independent oversight and individual redress possibilities. This representation is addressed to the European Commission with a view to express the commitment and provide assurances that government access to personal information transferred from the EU to Japan will be limited to what is necessary and proportionate, subject to independent oversight and that concerned individuals will be able to obtain redress in case of any possible violation of their fundamental right to privacy and data protection. This representation also provides for the creation of a new redress mechanism, administrated by the Personal Information Protection Commission (PPC), to handle complaints by EU individuals concerning government access to their personal data transferred from the EU to Japan.

I. The general legal principles relevant for government access

As an exercise of public authority, government access must be carried out in full respect of the law (legality principle). In Japan, personal information is protected across both the private sector and the public sector by a multi-layered mechanism.

A. Constitutional framework and reservation of law principle

Article 13 of the Constitution and case law recognize the right to privacy as a constitutional right. In this respect, the Supreme Court has held that it is natural that individuals do not want others to know their personal information without good reason, and that this expectation should be protected.[1] Further protections are enshrined in Article 21(2) of the Constitution, which ensures respect for the secrecy of communications, and Article 35 of the Constitution, which guarantees the right not to be subject to search and seizure without warrant, meaning that the collection of personal information, including access, by compulsory means must always be based on a court warrant. Such a warrant may only be issued for the investigation of an already committed crime. Therefore, in the legal framework of Japan, information

[1] Supreme Court , Judgement of September 12, 2003(2002 (Ju) No.1656)

collection by compulsory means for the purpose of (not a criminal investigation but) national security is not allowed.

Moreover, in accordance with the reservation of law principle, compulsory information collection must be specifically authorised by law. In case of non-compulsory/voluntary collection, information is obtained from a source that can be freely accessed or received based on a request for voluntary disclosure, i.e. a request that cannot be enforced against the natural or legal entity holding the information. However, this is only permissible to the extent the public authority is competent to carry out the investigation, given that each public authority can only act within the scope of its administrative jurisdiction prescribed by the law (irrespective of whether or not its activities interfere with the rights and freedoms of individuals). This principle applies to the authority's ability to collect personal information.

B. Specific rules on the protection of personal information

The Act on the Protection of Personal Information (APPI) and the Act on the Protection of Personal Information Held by Administrative Organs (APPIHAO), which are based on and further detail the constitutional provisions, guarantee the right to personal information in both the private and public sectors.

Article 7 of the APPI stipulates that the PPC shall formulate the "Basic Policy on the Protection of Personal Information" (Basic Policy). The Basic Policy, which is adopted through decision of the Cabinet of Japan as central organ of the Japanese government (Prime Minister and Ministers of State), shall set the direction for the protection of personal information in Japan. In this way, the PPC, as an independent supervisory authority, serves as the "command centre" of Japan's personal information protection system.

Whenever administrative organs collect personal information, and irrespective of whether they do so by compulsory means or not, they in principle[2] have to comply with the requirements of the APPIHAO. The APPIHAO is a general law applicable to the processing of "retained personal Information"[3] by "administrative organs" (as defined in Article 2(1) of the APPIHAO). It therefore also covers data processing in the area of criminal law enforcement and national security. Among the public authorities authorized to implement government access, all authorities, except the Prefectural Police, are national government authorities that fall under the definition of "administrative organs". The handling of personal information by the Prefectural Police is governed by prefectural ordinances[4] that stipulate

[2] For exceptions with respect to Chapter 4 of the APPIHAO, see below at p.16.

[3] Retained Personal Information" in Article 2(5) of the APPIHAO means personal information prepared or obtained by an employee of an administrative organ in the course of that employee's duties and held by that administrative organ for organizational use by its employees.

[4] Every prefecture has its own "prefectural ordinance" applicable to the protection of personal information by the Prefectural Police. No English translations for these prefectural ordinances exist.

principles for the protection of personal information, rights and obligations equivalent to the APPIHAO.

II. Government access for criminal law enforcement purposes

A) Legal bases and limitations

1) Collection of personal information by compulsory means

a) Legal bases

According to Article 35 of the Constitution, the right of all persons to be secure in their homes, papers and effects against entries, searches and seizures shall not be impaired except upon a warrant issued for "adequate cause" and particularly describing the place to be searched and things to be seized. Consequently, the compulsory collection of electronic information by public authorities in the context of a criminal investigation can only take place based on a warrant. This applies to both the collection of electronic records containing (personal) information and the real-time interception of communications (so-called wiretapping). The only exception to this rule (which however is not relevant in the context of an electronic transfer of personal information from abroad) is Article 220(1) of the Code of Criminal Procedure[5], according to which a public prosecutor, a public prosecutor's assistant officer or a judicial police official may, when arresting a suspect or "flagrant offender", if necessary carry out a search and seizure "on the spot at the arrest".

Article 197(1) of the Code of Criminal Procedure provides that compulsory measures of investigation "shall not be applied unless special provisions have been established in this Code". With respect to the compulsory collection of electronic information, the relevant legal bases in this regard are Article 218(1) of the Code of Criminal Procedure (according to which a public prosecutor , a public prosecutor's assistant officer or a judicial police official may, if necessary for the investigation of an offense, conduct a search, seizure or inspection upon a warrant issued by a judge) and Article 222-2 of the Code of Criminal Procedure (according to which compulsory measures for the interception of electronic communications without the consent of either party shall be executed based upon other Acts). The latter provision refers to the Act on Wiretapping for Criminal Investigation (Wiretapping Act), which in its Article

[5] Article 220(1) of the Code of Criminal Procedure provides that when a public prosecutor, a public prosecutor's assistant officer or a judicial police official arrests a suspect, (s)he may, if necessary, take the following measures: (a) entry into the residence of another person etc. to search for the suspect; (b) search, seizure or inspection on the spot at the arrest.

3(1) stipulates the conditions under which communications relating to certain serious crimes can be wiretapped based on a wiretapping warrant issued by a judge. [6]

Regarding the police, the investigate authority lies in all cases with the Prefectural Police, whereas the National Police Agency (NPA) does not conduct any criminal investigations based on the Code of Criminal Procedure.

b) Limitations

The compulsory collection of electronic information is limited by the Constitution and empowering statutes, as interpreted in case law, which in particular provide for the criteria to be applied by courts when issuing a warrant. In addition, the APPIHAO imposes a number of limitations applicable to both the collection and handling of information (while local ordinances reproduce essentially the same criteria for the Prefectural Police).

(1) Limitations following from the Constitution and the empowering statute

According to Article 197(1) of the Code of Criminal Procedure, compulsory dispositions shall not be applied unless special provisions have been established in this Code. Article 218(1) of the Code of Criminal Procedure then stipulates that seizure, etc. may be carried out based on a warrant issued by a judge only "if necessary for the investigation of an offense". Although the criteria for judging necessity are not further specified in statutory law, the Supreme Court[7] has ruled that, when assessing the necessity of dispositions, the judge should make an overall assessment, taking into consideration notably the following elements:

(a) Gravity of the offense and how it was committed;
(b) Value and importance of the seized materials as evidence;
(c) Probability of concealment or destruction of seized materials;

---

[6] More specifically, this provision prescribes that “the public prosecutor or the judicial police may, in the cases falling under any of the following items, when there is a situation sufficient to suspect that communications will take place concerning commitment, preparations, conspiracies on follow-up actions such as suppression of evidence, etc., instructions and other intercommunication of the crime prescribed in each of the said items (hereinafter referred to as “a series of crimes” in the second and third items), as well as communications containing the matters related to the said crime (hereinafter referred to as "communications relating to crime" in this paragraph) and in the cases where it is extremely difficult to identify the criminal or clarify the situations/details of the perpetration by any other ways, wiretap communication relating to crime, based on the wiretapping warrant issued by a court judge, regarding a means of communications, which is specified by phone number and other numbers/codes to identify source or destination of the phone and is used by the suspect based on the contract with telecommunications carriers, etc. (except those which can be regarded as there is no suspicion to be used as “communications relating to crime”) , or those on which there are grounds to suspect to be used as “communications relating to crime”, wiretapping of the communications relating to crime by this means of communications can be conducted.”

[7] Judgement of March 18th, 1969 (1968 (Shi) No.100).

(d) Extent of the disadvantages caused by a seizure;
(e) Other related conditions.

Limitations follow also from the requirement in Article 35 of the Constitution to show "adequate cause". Under the "adequate cause" standard, warrants can be issued if: [1] there is the necessity for criminal investigation (see the Supreme Court Ruling on March 18, 1969 (1968 (Shi) No.100) mentioned above), [2] there is a situation where the suspect (the accused) is considered to have committed an offense (Article 156 (1) of the Rules of Criminal Procedure) [8][3] The warrant on investigation for body, articles, residence or any other place of a person other than the accused should be issued only when it is reasonably supposed that articles which should be seized exist .(Article 102 (2) of the Code of Criminal Procedure). When a judge considers that the documentary evidence submitted by investigative authorities presents insufficient grounds to suspect a crime, he/she will dismiss the request for a warrant. It should be noted in this regard that under the Act on Punishment of Organized Crimes and Control of Crime Proceeds, "preparatory acts to commit" a planned crime (e.g. preparation of money for committing a terrorism crime) themselves constitute a crime and can thus be subject to compulsory investigation based on a warrant.

Finally, where the warrant concerns the investigation of the body, articles, residence or any other place of a person other than the suspect or accused, it shall only be issued when it can reasonably be assumed that the articles which shall be seized exist (Article 102(2) and 222(1) of the Code of Criminal Procedure).

As regards specifically the interception of communications for the purpose of criminal investigations based on the Wiretapping Act, it may be conducted only when the strict requirements provided in its Article 3(1) are satisfied. According to that provision, the interception always requires a court warrant in advance, which may only be issued in limited situations[9].

(2) Limitations following from the APPIHAO

As regards the collection[10] and further handling (including notably the retaining, managing and using) of personal information by administrative organs, the APPIHAO stipulates in particular the following limitations:

(a) According to Article 3(1) of the APPIHAO, administrative organs may retain personal information only when the retention is necessary for performing the duties falling

[8] Article 156(1) of the Rules of Criminal Procedure provides: "In filing the request set forth in paragraph (1) of the preceding Article, the requester shall provide materials based on which the suspect or the accused should be considered to have committed an offense."

[9] See footnote 6.

[10] Article 3(1) and (2) of the APPIHAO restrict the extent of retention and, thereby, also the collection of personal information.

within their jurisdiction as provided by laws and regulations. Upon retention, they are also required to specify (as much as possible) the purpose of use of personal information. According to Article 3(2), (3) of the APPIHAO, administrative organs shall not retain personal information beyond the scope necessary for the achievement of the purpose of use thus specified, and shall not change the purpose of use beyond what can reasonably be considered as appropriately relevant for the original purpose.

(b) Article 5 of the APPIHAO provides that the head of an administrative organ shall endeavour to maintain the retained personal information accurate and up to date, within the scope necessary for the achievement of the purpose of use.

(c) Article 6(1) of the APPIHAO provides that the head of an administrative organ shall take the measures necessary for the prevention of leakage, loss, or damage, as well as for the proper management of the retained personal information.

(d) According to Article 7 of the APPIHAO, no (including: former) employee shall disclose the acquired personal information to another person without a justifiable ground, or use such information for an unjust purpose.

(e) Moreover, Article 8(1) of the APPIHAO provides that the head of an administrative organ shall not, except as otherwise provided by laws and regulations, use or provide another person with retained personal information for purposes other than the specified purpose of use. While Article 8(2) contains exceptions from this rule in specific situations, these only apply if such exceptional disclosure is not likely to cause "unjust" harm to the rights and interests of the data subject or a third party.

(f) According to Article 9 of the APPIHAO, where retained personal information is provided to another person, the head of an administrative organ shall, if necessary, impose restrictions on the purpose or method of use, or any other necessary restrictions; it may also request the receiving person to take measures necessary for the prevention of leakage and for the proper management of the information.

(g) Article 48 of the APPIHAO provides that the head of an administrative organ shall endeavour to process any complaints regarding the handling of personal information properly and expeditiously.

2) Collection of personal information through requests for voluntary cooperation (Voluntary investigation)

a) Legal basis

Aside from using compulsory means, personal information is obtained either from a source that can be freely accessed or based on voluntary disclosure, including by business operators holding such information.

As regards the latter, Article 197(2) of the Code of Criminal Procedure empowers the prosecution and judicial police to make "written inquiries on investigative matters" (so-called "enquiry sheets"). Under the Code of Criminal Procedure, the inquired persons are requested to report to investigative authorities. However, there is no way to force them to report, if the public offices, or the public and/or the private organizations, who received the inquiries, refuse to comply. If they do not report for the inquiries, no criminal punishment or other sanction can be imposed. If the investigative authorities consider the requested information indispensable, they will need to obtain the information through search and seizure based on a court warrant.

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[11]. In deciding whether to cooperate, business operators in particular take into account the nature of the information requested, their relationship with the person whose information is at stake, risks to their reputation, litigation risks, etc.

b) Limitations

As for the compulsory collection of electronic information, voluntary investigation is limited by the Constitution, as interpreted in case law, and the empowering statute. In addition, business operators are not legally allowed to disclose information in certain situations. Finally, the APPIHAO provides for a number of limitations applicable to both the collection and handling of information (while local ordinances reproduce essentially the same criteria for the Prefectural Police).

(1) Limitations following from the Constitution and the empowering statute

By taking the purpose of Article 13 of the Constitution into consideration, the Supreme Court in two decisions of December 24th, 1969 (1965 (A) No.1187) and April 15th, 2008 (2007 (A) No.839) has imposed limits to voluntary investigations conducted by investigatory authorities. While these decisions concerned cases where personal information (in the form of images) was collected through photography/filming, the findings are relevant for voluntary (non-compulsory) investigations interfering with an individual's privacy in general. They therefore apply, and have to be complied with, as regards the collection of personal

[11] See also the notification issued by the National Police Agency on December 7th, 1999 (below at p.9) which states the same point.

information through voluntary investigation, taking into account the specific circumstances of each case.

According to these decisions, the legality of voluntary investigation depends on the fulfilment of three criteria, namely:

- "suspicion of a crime" (i.e. it must be assessed whether a crime has been committed);

- "necessity of investigation" (i.e. it must be assessed whether the request stays within the scope of what is necessary for the purposes of the investigation); and

- "appropriateness of methods" (i.e. it must be assessed whether voluntary investigation is "appropriate" or reasonable in order to achieve the purpose of the investigation).[12]

In general, taking into account the above three criteria, the legality of voluntary investigation is judged from the viewpoint of whether it can be considered reasonable in accordance with socially accepted conventions.

The requirement for the investigation to be "necessary" also follows directly from Article 197 of the Code of Criminal Procedure, and has been confirmed in the instructions issued by the National Police Agency (NPA) to the Prefectural Police as regards the use of "enquiry sheets". The NPA Notification of 7th December 1999 stipulates a number of procedural limitations, including the requirement to use "enquiry sheets" only if necessary for the purposes of the investigation. In addition, Article 197(1) of the Code of Criminal Procedure is limited to criminal investigations, and can thus be applied only where there is a concrete suspicion of an already committed crime. Conversely, this legal basis is not available for the collection and use of personal information where no violation of the law has yet occurred.

(2) Limitations with respect to certain business operators

Additional limitations apply in certain areas based on the protections provided in other laws.

First, investigative authorities as well as telecommunication carriers holding personal information have a duty to respect the secrecy of communications as guaranteed by Article

[12] Gravity of the crime and urgency are relevant factors to assess the "appropriateness of methods".

21(2) of the Constitution.[13] Besides, telecommunication carriers have same duty under Article 4 of the Telecommunication Business Act[14]. According to the "Guidelines on Personal Information Protection in Telecommunications Business", which have been issued by the Ministry of Internal Affairs and Communications (MIC) based on the Constitution and the Telecommunication Business Act, in cases where the secrecy of communications is at stake, telecommunication carriers must not disclose personal information regarding the secrecy of communication to third parties, except where they have obtained the individual's consent or if they can rely on one of the "justifiable causes" for non-compliance with the Penal Code. The latter relate to "justifiable acts" (Article 35 of the Penal Code), "Self-Defense" (Article 36 of the Penal Code) and "Averting Present Danger" (Article 37 of the Penal Code). "Justifiable acts" under the Penal Code are only those acts of a telecommunication carrier by which it complies with compulsory measures of the State, which excludes voluntary investigation. Therefore, if the investigative authorities request personal information based on an "enquiry sheet" (Article 197(2) of the Code of Criminal Procedure), a telecommunication carrier is prohibited from disclosing the data.

Second, business operators are bound to refuse requests for voluntary cooperation where the law prohibits them from disclosing personal information. As an example, this includes cases where the operator has a duty to respect the confidentiality of information, for instance pursuant to Article 134 of the Penal Code[15].

(3) Limitations based on the APPIHAO

As regards the collection and further handling of personal information by administrative organs, the APPIHAO provides for limitations as explained above in section II.A.1) b) (2). Equivalent limitations follow from the prefectural ordinances applicable to the Prefectural Police.

B) Oversight

[13] Article 21(2) of the Constitution states: "No censorship shall be maintained, nor shall the secrecy of any means of communication be violated."

[14] Article 4 of the Telecommunication Business Act states: "(1) The secrecy of communications being handled by a telecommunications carrier shall not be violated. (2) Any person who is engaged in a telecommunications business shall not disclose secrets obtained, while in office, with respect to communications being handled by a telecommunications carrier. The same shall apply even after he/she has left office."

[15] Article 134 of the Penal Code states: "(1) When a physician, pharmacist, pharmaceuticals distributor, midwife, attorney, defense counsel, notary public or any other person formerly engaged in such a profession discloses, without justifiable grounds, another person's confidential information which has come to be known in the course of such profession, imprisonment with work for not more than 6 months or a fine of not more than 100,000 yen shall be imposed. (2) The same shall apply to the case where a person who is or was engaged in a religious occupation discloses, without justifiable grounds, another person's confidential information which has come to be known in the course of such religious activities."

1) Judicial oversight

As regards collection of personal information by compulsory means, it must be based on a warrant[16] and is thus subject to the prior examination by a judge. In case the investigation was illegal, a judge may exclude such evidence in the subsequent criminal trial of the case. An individual may request such exclusion in his/her criminal trial claiming that the investigation was illegal.

2) Oversight based on the APPIHAO

In Japan, the Minister or Head of each ministry or agency has the authority of oversight and enforcement based on the APPIHAO, while the Minister of Internal Affairs and Communications may investigate the enforcement of the APPIHAO by all other ministries.

If the Minister of Internal Affairs and Communications – based for instance on the investigation on the status of the enforcement of the APPIHAO[17], the processing of complaints, or inquiries directed to one of its Comprehensive Information Centres –find it necessary for achieving the purpose of the APPIHAO, he/she may request the head of an administrative organ to submit materials and explanations regarding handling of personal information by the concerned administrative organ based on Article 50 of the APPIHAO. The Minister may address opinions to the head of administrative organ regarding processing of personal information in the administrative organ when he or she finds it necessary for achieving the purpose of this Act. In addition, the Minister may, for instance, request a revision of the measures through the actions he/she can take pursuant to Articles 50 and 51 of the Act when it is suspected that a violation or inappropriate operation of the Act has occurred. This helps to ensure the uniform application of and compliance with the APPIHAO.

3) Oversight by the Public Safety Commissions as regards the police

[16] Regarding the exception to this rule, see footnote 5.

[17] To ensure transparency and facilitate the oversight by the MIC, the head of an administrative organ is required, pursuant to Article 11 of the APPIHAO, to record each item prescribed in Article 10(1) of the APPIHAO, such as the name of the administrative organ which retains the file, purpose of use of the file, method of collection of the personal information, etc. (so-called "Personal Information File Register"). However, personal information files which fall under Article 10(2) of the APPIHAO, such as those prepared or obtained as part of a criminal investigation or concerning matters relevant for national security, are exempted from the obligation to notify the MIC and to include them in the public register. However, pursuant to Article 7 of the Public Records and Archives Management Act, the head of an administrative organ is always required to record the classification, title, retention period and storage location, etc. of administrative documents ("Administrative Document File Management Register"). The index information for both registers is published on the internet and allows individuals to check what kind of personal information the file contains and which administrative organ retains the information.

Regarding the police administration, the NPA is subject to oversight by the National Public Safety Commission, while the Prefectural Police is subject to oversight by one of the Prefectural Public Safety Commissions established in each prefecture. Each of these oversight bodies secures democratic management and political neutrality of the police administration.

The National Public Safety Commission is in charge of the affairs which fall under its jurisdiction pursuant to the Police Law and other laws. This includes the appointment of the Commissioner General of the NPA and local senior police officers as well as the establishment of comprehensive policies which lay out basic directions or measures with respect to the administration of the NPA.

The Prefectural Public Safety Commissions are composed of members representing the people in the respective prefecture based on the Police Law and manage the Prefectural Police as an independent council system. Members are appointed by the prefectural governor with the consent of the prefectural assembly based on Article 39 of the Police Law. Their term of office is three years and they can only be dismissed against their will for specific reasons enumerated in law (such as incapacity to perform their duties, violation of duties, misconduct etc.), thus ensuring their independence (see Articles 40, 41 of the Police Law). Furthermore, in order to guarantee their political neutrality, Article 42 of the Police Law prohibits a member of the Commission from concurrently serving as a member of a legislative body, becoming an executive member of a political party or any other political body, or actively engaging in political movements. While each Commission falls under the jurisdiction of the respective prefectural governor, this does not entail any authority of the governor to issue instructions as to the exercise of its functions.

Pursuant to Article 38(3) in conjunction with Article 2 and 36(2) of the Police Law, the Prefectural Public Safety Commissions are responsible for "the protection of rights and freedom of an individual". To that end, they shall receive reports from the Chiefs of the Prefectural Police concerning the activities within their jurisdiction, including at regular meetings held three or four times a month. The Commissions provides guidance on these matters through the establishment of comprehensive policies.

Moreover, as part of their supervisory function, the Prefectural Public Safety Commissions may issue directions to the Prefectural Police in concrete, individual cases when they consider this necessary in the context of an inspection of the activities of the Prefectural Police or misconduct of its personnel. Also, the Commissions may, when they consider this necessary, have a designated Commission member review the state of implementation of the issued direction (Article 43-2 of the Police Law).

4) Oversight by the Diet

The Diet may conduct investigations in relation to the activities of public authorities and to this end request the production of documents and the testimony of witnesses (Article 62 of the Constitution). In this context, the competent committee in the Diet may examine the appropriateness of information collection activities conducted by the Police.

These powers are further specified in the Diet Act. Pursuant to its Article 104, the Diet may require the Cabinet and public agencies to produce reports and records necessary for carrying out its investigation. Furthermore, Diet members may submit "written inquiries" under Article 74 of the Diet Act. Such inquiries must be approved by the Chair of the House and, in principle, must be answered by the Cabinet in writing within seven days (when it is impossible to reply within that period, this must be justified and a new deadline set, Article 75 of the Diet Act). In the past, written inquiries by the Diet have also covered the handling of personal information by the administration.[18]

C) Individual Redress

According to Article 32 of the Constitution of Japan, no person shall be denied the right of access to the courts. In addition, Article 17 of the Constitution guarantees every person the right to sue the State or a public entity for redress (as provided by law) in case he/she has suffered damage through the illegal act of a public official.

1) Judicial redress against compulsory collection of information based on a warrant (Article 430 Code of Criminal Procedure)

According to Article 430(2) of the Code of Criminal Procedure, an individual who is dissatisfied with the measures undertaken by a police official concerning a seizure of articles (including if they contain personal information) based on a warrant may file a request (so-called "quasi-complaint") with the competent court for such measures to be "rescinded or altered".

Such a challenge can be brought without the individual having to wait for the conclusion of the case. If the court finds that the seizure was not necessary, or that there are other reasons to consider the seizure illegal, it may order such measures to be rescinded or altered.

[18] See e.g. written enquiry of the House of Councillors no. 92 of 27 March 2009 regarding handling information collected in the context of criminal investigations including violations of confidentiality obligations by police and prosecutorial authorities.

2) Judicial redress under the Code of Civil Procedure and State Redress Act

If they consider that their right to privacy under Article 13 of the Constitution has been violated, individuals can bring a civil action requesting that personal information collected through a criminal investigation be deleted.

Also, an individual can bring an action for the compensation of damages based on the State Redress Act in combination with relevant articles of the Civil Code if he/she considers that his/her right to privacy has been infringed and he/she has suffered harm as a result of the collection of his/her personal information or surveillance[19]. Given that the "damage" which is subject to a claim for compensation is not limited to damage to property (Article 710 of the Civil Code), this may also cover "mental distress". The amount of compensation for such moral harm will be assessed by the judge based on a "free evaluation in consideration of various factors in each case"[20].

Article 1(1) of the State Redress Act grants a right to compensation where (i) the public officer who exercises public authority of the State or of a public entity has (ii) in the course of his/her duties (iii) intentionally or negligently (iv) unlawfully (v) inflicted damage on another person.

The individual must file the lawsuit in accordance with the Code of Civil Procedure. According to the applicable rules, he/she may do so with the court that has jurisdiction over the place where the tort was committed.

3) Individual redress against unlawful/improper investigations by the Police: complaint to the Prefectural Public Safety Commission (Article 79 Police Law)

According to Article 79 of the Police Law[21], as further clarified in an instruction by the Head of the NPA to the Prefectural Police and Prefectural Public Safety Commissions[22],

---

[19] An example for such an action is “The Case of Defense Agency’s List” (Niigata District Court, decision of May 11, 2006 (2002(Wa) No.514)). In this case, an official of the Defense Agency prepared, kept, and distributed a list of those individuals who had filed requests for disclosure of administrative documents with the Defense Agency. There were descriptions of the plaintiff's personal information on that list. Insisting that his privacy, right to know, etc. were infringed, the plaintiff requested the defendant to pay compensation for damages under Article 1(1) of the State Redress Act. This request was partially granted by the court that awarded the plaintiff a partial compensation.

[20] Supreme Court, decision of April 5, 1910 (1910(O) No.71).

[21] Article 79 of the Police Law (excerpt):
1. Whoever has a complaint against the execution of duties by the personnel of the Prefectural Police may lodge a complaint in writing to the Prefectural Public Safety Commission through the procedure prescribed in the National Public Safety Commission Ordinance.

individuals may lodge a written complaint[23] with the competent Prefectural Public Safety Commission against any illegal or improper behaviour by a police officer in the execution of his/her duties; this includes duties with respect to the collection and use of personal information. The Commission shall faithfully handle such complaints in accordance with laws and local ordinances, and shall notify the result of the investigation to the complainant in writing.

Based on its supervisory authority according to Article 38(3) of the Police Law, the Prefectural Public Safety Commission shall issue an instruction to the Prefectural Police to investigate the facts, implement the necessary measures according to the result of the examination and report the results to the Commission. Where it deems this necessary, the Commission may also issue an instruction on the handling of the complaint, for instance if it considers the investigation carried out by the police to be insufficient. This implementation is described in the Notice issued by the NPA to the heads of the Prefectural Police.

The notification to the complainant of the result of the investigation is made in light also of the reports from the police concerning the investigation and the measures taken on request of the Commission.

4) Individual redress under the APPIHAO and the Code of Criminal Procedure

a) APPIHAO

Under Article 48 of the APPIHAO, administrative organs must endeavour to properly and expeditiously process any complaints on the handling of personal information. As a means to provide consolidated information to individuals (e.g. on the available rights to disclosure, correction and suspension of use under the APPIHAO) and as a contact point for inquiries, the MIC has established Comprehensive Information Centres on Information Disclosure/Personal Information Protection in each of the prefectures based on Article 47(2) of the APPIHAO. Inquiries by non-residents are also possible. As an example, in FY2017 (April 2017 to March

---

2. The Prefectural Public Safety Commission which received a complaint provided for in the previous paragraph shall faithfully handle it in accordance with laws and local ordinances, and shall notice its result to the complainant in writing, except in the following cases:
(1) The complaint can be recognized as brought in order to obstruct the lawful execution of the duties of the Prefectural Police;
(2) The current residence of the complainant is unknown;
(3) The complaint can be recognized as brought jointly with other complainants and other complainants have already been notified with the result of the joint complaint.

[22] NPA, Notice on the proper handling of complaints on the execution of duties by police officers, April 13th, 2001, with Attachment 1 "Standards on interpretation/implementation of Article 79 of the Police Act".

[23] According to the NPA Notice (see previous footnote), individuals with difficulties in formulating a complaint in writing shall receive assistance. This expressly includes the case of foreigners.

2018), the total number of cases in which the comprehensive information centres responded to inquiries, etc. was 5,186.

Articles 12 and 27 of the APPIHAO grant individuals the right to request disclosure and correction of retained personal information. Furthermore, pursuant to Article 36 of the APPIHAO, individuals may request the suspension of use or deletion of their retained personal information where the administrative organ has not obtained the retained personal information lawfully, or retains or uses such information in violation of law.

However, as regards personal information collected (either based on a warrant or by way of an "enquiry sheet") and retained for criminal investigations[24], such information generally falls within the category of "personal information recorded in documents relating to trials and seized articles". Such personal information is therefore excluded from the scope of application of the individual rights in Chapter 4 of the APPIHAO pursuant to Article 53-2 of the Code of Criminal Procedure[25]. The processing of such personal information and the rights of the individual to access and correction are instead subject to special rules under the Code of Criminal Procedure and Act on Final Criminal Case Records (see below).[26] This exclusion is justified by various factors such as the protection of the privacy of persons concerned, the secrecy of investigations and the proper conduct of the criminal trial. This been said, the provisions of Chapter 2 of the APPIHAO governing the principles for the handling of such information remain applicable.

b) Code of Criminal Procedure

Under the Code of Criminal Procedure, the possibilities for access to personal information collected for the purposes of a criminal investigation depend both on the stage of the procedure and the role of the individual in the investigation (suspect, accused, victim, etc.).

As an exception to the rule in Article 47 of the Code of Criminal Procedure that documents relating to the trial shall not be made public prior to the commencement of the trial (as this

[24] On the other hand, there would be documents which are not classified as "documents relating to trials" as they are not themselves information obtained by a warrant or written inquiries on investigative matters but created on the basis such documents. This would be a case where private information is not subject to Article 45 (1) of the APPIHAO, and therefore such information would not be excluded from the application of Chapter 4 of the APPIHAO.

[25] Article 53-2(2) of the Code of Criminal Procedure prescribes that the provisions of Chapter IV of the APPIHAO shall not apply to the personal information recorded in documents relating to trials and seized articles.

[26] Under the Code of Criminal Procedure and the Act on Final Criminal Case Records, access to and the correction of seized articles as well as documents/personal information regarding criminal trials are subject to a unique and distinctive system of rules that aims at protecting the privacy of persons concerned, the secrecy of investigations and the proper conduct of the criminal trial, etc.

could violate the honor and/or privacy of the individuals concerned and hinder the investigation/trial), the inspection of such information by the victim of a crime is in principle permitted to the extent that it is deemed reasonable by taking into account the purpose of the provision of Article 47 of the Code of Criminal Procedure.[27]

As regards suspects, they will typically learn about the fact that they are subject to a criminal investigation upon interrogation by either the judicial police or public prosecutor. If subsequently the public prosecutor decides not to institute prosecution, he/she shall promptly notify the suspect of this fact upon his/her request (Article 259 of the Code of Criminal Procedure).

In addition, following the institution of prosecution, the public prosecutor shall give the accused or his/her counsel an opportunity to inspect the evidence in advance before requesting its examination by the court (Article 299 of the Code of Criminal Procedure). This allows the accused to check his/her personal information collected through criminal investigation.

Finally, the protection of personal information collected in the context of a criminal investigation, be it of a suspect, the accused or any other person (e.g. a crime victim) is guaranteed through the confidentiality obligation (Article 100 of the National Public Service Act) and the threat of penalty in case of leakage of confidential information handles in the course of the exercise of public service duties (Article 109 (xii) of the National Public Service Act).

5) Individual redress against unlawful/improper investigations by public authorities: complaint to the PPC

According to Article 6 of the APPI, the Government shall take necessary action in collaboration with the governments of third countries to construct an internationally conformable system concerning personal information through fostering cooperation with international organizations and other international frameworks. Based on this provision, the Basic Policy on the Protection of Personal Information (adopted by Cabinet Decision) delegates to the PPC, as the authority competent for the overall administration of the APPI, the power to take the necessary action to bridge differences of the systems and operations between Japan and the concerned foreign country in view of ensuring the appropriate handling of personal information received from such country.

[27] More specifically, the inspection of information related to objective evidence is in principle permitted for crime victims regarding the non-prosecution records on the cases subject to the victim participation stipulated in Article 316-33 thereafter of the Code of Criminal Procedure in order to make the protection of crime victims more satisfactory.

Furthermore, as provided for under Article 61, items (i) and (ii) of the APPI, the PPC is entrusted with the task of formulating and promoting a basic policy, as well as with the mediation of complaints lodged against business operators. Finally, administrative organs shall closely communicate and cooperate with one another (Article 80 of the APPI).

Based on these provisions, the PPC will deal with complaints lodged by individuals as follows:

a) An individual who suspects that his/her data transferred from the EU has been collected or used by public authorities in Japan, including the authorities responsible for the activities referred to in Chapter II and Chapter III of the present "Representation", in violation of the applicable rules, including those subject to this "Representation", can submit a complaint to the PPC (individually or though his/her DPA).

b) The PPC handles the complaint, including by making use of its powers under Article 6, 61(ii), and 80 of the APPI, and informs the competent public authorities, including the relevant oversight bodies, of the complaint.

   These authorities are required to cooperate with the PPC under Article 80 of the APPI, 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. In carrying out its evaluation, the PPC will cooperate with the MIC.

c) If the evaluation shows that an infringement of the applicable rules has occurred, cooperation by the concerned public authorities with the PPC includes the obligation to remedy the violation.

   In case of unlawful collection of personal information under the applicable rules, this shall include the deletion of the personal information collected.

   In case of a violation of the applicable rules, the PPC will also confirm, before concluding the evaluation, that the violation has been fully remedied.

d) 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. Through this notification, the PPC shall also inform the individual about the possibility of seeking a confirmation of the outcome from the competent public authority and about the authority to which such a request for confirmation shall be made.

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.

Where the complaint concerns the collection or use of personal data in the area of criminal law enforcement, the PPC will, in the event that the evaluation reveals that a case involving the personal information of the individual has been opened and that the case is concluded, inform the individual that the case record can be inspected pursuant to Article 53 of the Code of Criminal Procedure and Article 4 of the Act on Final Criminal Case Records.

Where the evaluation reveals that an individual is a suspect in a criminal case, the PPC will inform the individual about that fact and about the possibility to make a request pursuant to Article 259 of the Code of Criminal Procedure.

e) If an individual is still dissatisfied with the outcome of this procedure, he/she can address the PPC which shall inform the individual of the various possibilities and detailed procedures for obtaining redress under Japanese laws and regulations. The PPC will provide the individual with support, including counselling and assistance in bringing any further action to the relevant administrative or judicial body.

III. Government access for national security purposes

A. Legal bases and limitations for the collection of personal information

1) Legal bases for information collection by concerned ministry/agency

As indicated above, the collection of personal information for the purpose of national security by administrative organs needs to be within the scope of their administrative jurisdiction.

In Japan, no law exists that enables information collection by compulsory means for the purpose of national security only. Pursuant to Article 35 of the Constitution, it is possible to collect personal information forcibly only on the basis of a warrant issued by a court for the investigation of an offence. Such a warrant can thus only be issued for the purpose of a criminal investigation. This means that, in the Japanese legal system, collection of/access to information by compulsory means for national security reasons is not allowed. Instead, in the area of national security, concerned ministries or agencies can only obtain information from sources that can be freely accessed, or receive information from business operators or individuals through voluntary disclosure. Business operators receiving a request for voluntary cooperation are under no legal obligation to provide such information and, hence, face no negative consequences if they refuse to cooperate.

A number of different ministerial departments and agencies have responsibilities in the area of national security.

(1) Cabinet Secretariat

The Cabinet Secretariat conducts information collection and research concerning important policies of the Cabinet [28] prescribed in Article 12-2 of the Cabinet Law.[29] However, the Cabinet Secretariat has no power for collecting personal information directly from business operators. It collects, incorporates, analyses and assesses information from open source materials, other public authorities, etc.

(2) The NPA/Prefectural Police

In each prefecture, the Prefectural Police is empowered to collect information within the scope of its jurisdiction under Article 2 of the Police Law. It can happen that the NPA directly collects information within the scope of its jurisdiction under the Police Law. This concerns in particular the activities of the NPA's Security Bureau and the Foreign Affairs and Intelligence Department. Pursuant to Article 24 of the Police Law, the Security Bureau is in charge of matters concerning the security police[30] and the Foreign Affairs and Intelligence Department is in charge of the affairs concerning foreign nationals as well as Japanese nationals whose bases of activity are located in foreign countries.

(3) Public Security Intelligence Agency (PSIA)

The application of the Subversive Activities Prevention Act (SAPA) and the Act on the Control of Organizations Which Have Committed Acts of Indiscriminate Mass Murder (ACO) falls mainly under the authority of the Public Security Intelligence Agency (PSIA). This is an agency of the Ministry of Justice.

SAPA and the ACO stipulate that administrative dispositions (i.e. measures ordering the limitation of the activities of such organisations, their dissolution, etc.) can be adopted, under strict conditions, against organisations committing certain serious acts (“Terroristic Subversive Activity” or “Act of Indiscriminate Mass Murder”) in violation of “public security” or the "fundamental system of society" under the Constitution. “Terroristic

[28] It is conducted by the Cabinet Intelligence and Research Office based on Article 4 of the Cabinet Secretariat Organization Order.

[29] This includes "the collection and research of intelligence concerning important policies of the Cabinet".

[30] The security police is responsible for crime-control activities relating to public safety and the interest of the Nation. This includes crime-control and information gathering on illegal acts related to extreme leftist groups, rightist groups and harmful anti-Japan activities.

Subversive Activities" fall within the scope of SAPA (see Article 4 covering activities such as insurrection, instigation of foreign aggression, homicide with political intent, etc.), while the ACO addresses "Acts of Indiscriminate Mass Murder" (see Article 4 of the ACO). Only precisely identified organisations posing specific internal or external threats to public security can be subject to dispositions under SAPA or ACO.

To this end, SAPA and ACO provide legal authority of investigation. The fundamental investigative powers of the officers of the PSIA (PSIO) are set out in Article 27 of SAPA and Article 29 of ACO. Investigations by the PSIA under these provisions are conducted to the extent they are necessary with respect to the above organization-control dispositions (e.g. Radical Leftist Groups, the *Aum Shinrikyo* sect and certain domestic group closely linked to North Korea have been exemplified as a subject of investigation in the past). However, these investigations cannot rely on compulsory means and thus an organisation holding personal information cannot be compelled to provide such information.

Collection and use of information disclosed to the PSIA on a voluntary basis is subject to the relevant safeguards and limitations provided by law such as, *inter alia*, the secrecy of communication guaranteed by the Constitution and the rules on the handling of personal information under the APPIHAO.

(4) Ministry of Defense (MOD)

As for the information collection by the Ministry of Defense (MOD), the MOD collects information based on Article 3 and 4 of the Act for the Establishment of the MOD to the extent necessary for the exercise of its administrative jurisdiction affairs, including with respect to defence and guard, action to be taken by the Self-Defense Forces as well as the deployment of the Ground, Maritime and Air Self-Defense Forces. The MOD can only collect information for these purposes through voluntary cooperation and from freely accessible sources. It does not collect information on the general public.

2) Limitations and safeguards

a) Statutory limitations

(1) General limitations based on the APPIHAO

The APPIHAO is a general law that applies to the collection and handling of personal information by administrative organs in any field of activity of such organs. Therefore, the limitations and safeguards described in section II.A.1) b)(2) also apply to the retention, storage, use etc. of personal information in the area of national security.

(2) Specific limitations applicable to the police (both NPA and Prefectural Police)

As specified above in the section dealing with the collection of information for law enforcement purposes, the police may only collect information within the scope of its jurisdiction and when doing so it may, pursuant to Article 2(2) of the Police Law, only act to an extent "strictly limited" to the performance of its duties and in a way which is "impartial, nonpartisan, unprejudiced and fair". Moreover, its powers "shall never be abused in any way such as to interfere with the rights and liberties of an individual guaranteed in the Constitution of Japan".

(3) Specific limitations applicable to the PSIA

Both Article 3 of the SAPA and Article 3 of the ACO stipulate that investigations carried out under these acts shall be conducted only to the minimum extent necessary to achieve the purpose pursued and shall not be carried out in a way that unreasonably restricts fundamental human rights. Moreover, pursuant to Article 45 of the SAPA and Article 42 of the ACO, if an officer of the PSIA abuses his/her authority, this constitutes a crime that is punishable by heavier criminal sanctions than "general" abuses of authority in other fields of the public sector.

(4) Specific limitations applicable to the MOD

As regards information collection/organization by the MOD, as referred to in Article 4 of the Act for the Establishment of the MOD, this Ministry's activity to collect information is limited to what is "necessary" to conduct its duties concerning (1) defense and guard, (2) action to be taken by the Self-Defense Forces, (3) the organizations, number of personnel, structure, equipment, and deployment of the Ground, Maritime and Air Self-Defense Forces.

b) Other limitations

As explained earlier in section II.A.2) b) (1) concerning criminal investigations, 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.

The combination of the above limitations ensures that 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. This excludes mass and indiscriminate collection or access to personal information for national security reasons.

B. Oversight

1) Oversight based on the APPIHAO

As explained above in section II.B.2), in Japan's public sector, the Minister or the Head of each ministry or agency is vested with the power to oversee and enforce compliance with the APPIHAO in his/her ministry or agency. Moreover, the Minister of Internal Affairs and Communications may investigate the status of enforcement of the Act, request each Minister to submit materials and explanations based on Article 49 and 50 of the Act, address opinions to each Minister based on Article 51 of the Act. For example, he/she may request a revision of the measures through the actions pursuant to Article 50 and 51 of the Act.

2) Oversight over the police by the Public Safety Commissions

As explained in the above section "II. Information collection for criminal law enforcement purpose", the independent Prefectural Public Safety Commissions supervise the activities of the Prefectural Police.

As regards the National Police Agency (NPA), supervisory functions are exercised by the National Public Safety Commission. Pursuant to Article 5 of the Police law, this Commission is responsible, in particular, for "the protection of rights and freedom of an individual". To that end, it shall notably establish comprehensive policies which set out regulations for the administration of affairs prescribed in each item of Article 5(4) of the Police Law and lay out other basic directions or measures that should be relied on to carry out the said activities. The National Public Safety Commission (NPSC) has the same degree of independence as the Prefectural Public Safety Commissions (PPSCs).

3) Oversight of the MOD by the Inspector General's Office of Legal compliance

The Inspector General's Office of Legal Compliance (IGO) is an independent office in the Ministry of Defense (MOD), which is under the direct supervision of the Minister of Defense pursuant to Article 29 of the Act for the Establishment of the MOD. The IGO can carry out inspections of compliance with laws and regulations by officials of the MOD. These inspections are called "Defense Inspections".

The IGO conducts inspections from the standpoint of an independent office so as to ensure legal compliance across the entire ministry including the Self-Defense Forces (SDF). It performs its duties independently from MOD's operational departments. Following an inspection, the IGO reports its findings, together with the necessary ameliorative measures, directly to the Minister of Defense without delay. On the basis of the IGO's report, the Minister of Defense may issue orders to implement the measures necessary to remedy the situation. The Deputy Vice-Minister is responsible for implementing these measures and must report to the Minister of Defense on the status of such implementation.

As a voluntary transparency measure, the findings of Defense Inspections are now made public on the MOD's website (although this is not required by law).

There are three categories of Defense Inspections:

(i) Regular Defense Inspections, which are conducted periodically[31];
(ii) Defense Inspections for checks, which are conducted to check whether ameliorative measures have been effectively taken; and
(iii) Special Defense Inspections, which are conducted for specific matters ordered by the Minister of Defense.

In the context of such inspections, the Inspector General can request reports from the concerned office, request the submission of documents, enter sites to conduct the inspection, request explanations from the Deputy Vice-Minister, etc. In consideration of the nature of the inspection tasks of the IGO, this office is headed by very senior legal experts (former Superintending Prosecutor).

[31] As an example of an inspection relevant to the issues covered by this Representation, reference can be made to the 2016 Regular Defence Inspection with respect to "Awareness/Preparation for Legal Compliance" as personal information protection was one of the focal points of the inspection. More specifically, the inspection concerned the status of management, storage, etc. of personal information. In its report, the IGO identified several inappropriate aspects in the management of personal information that should be improved, such as the failure to protect the data through a password. The report is available on the website of the MOD.

4) Oversight of the PSIA

The PSIA carries out both regular and special inspections on the operations of its individual bureaus and offices (Public Security Intelligence Bureau, Public Security Intelligence Offices and Sub Offices, etc.). For the purposes of the regular inspection, an Assistant Director General and/or a Director is designated as inspector(s). Such inspections also concern the management of personal information.

5) Oversight by the Diet

As for information collection for law enforcement purposes, the Diet, through its competent committee, may examine the lawfulness of information collection activities in the area of national security. The Diet's investigatory powers are based on Article 62 of the Constitution and Articles 74, 104 of the Diet Act.

C. Individual redress

Individual redress can be exercised through the same avenues as in the area of criminal law enforcement. This also includes the new redress mechanism, administrated and supervised by the PPC, for handling and resolving complaints lodged by EU individuals. In this regard, please see the relevant passages of section II.C.

In addition, there are specific individual redress avenues available in the area of national security.

Personal information collected by an administrative organ for national security purposes is subject to the provisions of Chapter 4 of the APPIHAO. This includes the right to request disclosure (Article 12), correction (including addition or deletion) (Article 27) of the individual's retained personal information as well as the right to request suspension of use of the personal information in case the administrative organ has obtained the concerned information unlawfully (Article 36). That said, in the national security area, the exercise of such rights is subject to certain restrictions: requests for disclosure, correction or suspension will not be granted when they concern “information for which there are reasonable grounds for the head of an administrative organ to find that disclosure is likely to cause harm to national security, cause damage to the relationship of mutual trust with another country or an international organization, or cause a disadvantage in negotiations with another country or an international organization" (Article 14(iv)). Hence, not all voluntary collection of information related to national security falls with this exemption as the latter always requires a concrete assessment of the risks involved in their disclosure.

Furthermore, if the request of the individual is rejected on the grounds that the concerned information is considered non-disclosable within the meaning of Article 14(iv), the individual

may lodge an administrative appeal for the review of such decision, claiming for example that the conditions set forth in Article 14(iv) are not fulfilled in the case at issue. In that case, before taking a decision, the Head of the concerned administrative organ shall consult the Information Disclosure and Personal Information Protection Review Board. This Board will review the appeal from an independent standpoint. The Board is a highly specialized and independent body whose members are appointed by the Prime Minister, with consent of both Houses of the Diet, amongst people with outstanding expertise.[32] The Board enjoys strong investigative powers, including the possibility to request documents and the disclosure of the personal information in question, hold in-camera deliberation, and apply the Vaughn index procedure[33]. The Board then establishes a written report which is communicated to the concerned individual.[34] The findings contained in the report are made public. Although the report is not formally speaking legally binding, almost all the reports are complied with by the concerned administrative organ.[35]

Finally, pursuant to Article 3(3) of the Administrative Case Litigation Act, the individual may bring a court action seeking the revocation of the decision taken by the Administrative Organ not to disclose the personal information.

IV. Periodic review

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.

[32] See Article 4 of the Act for Establishment of the Information Disclosure and Personal Information Protection Review Board.

[33] See Article 9 of the Act for Establishment of the Information Disclosure and Personal Information Protection Review Board.

[34] See Article 16 of the Act for Establishment of the Information Disclosure and Personal Information Protection Review Board.

[35] Over the last 3 years, there is no precedent where the concerned administrative organ took a decision that differed from the Board's conclusions. Going back in the years, there are extremely few cases where this happened: only two instances out of total 2,000 cases between 2005 (the year in which the APPIHAO entered into force). When the administrative organ makes a determination/decision which differs from the Board's conclusions, pursuant to Article 50(1), item 4 of the Administrative Complaint Review Act as applied with the replacement of Article 42(2) of the APPIHAO, it shall clearly indicate the reasons for that.