GIR KNOW-HOW DATA PRIVACY & TRANSFER IN INVESTIGATIONS

Japan

Akira Matsuda, Koji Horita and Makoto Adachi
Iwata Godo

SEPTEMBER 2019

GIR INSIGHT

1 What laws and regulations in your jurisdiction regulate the collection and processing of personal data?

The laws and regulations in Japan regulating the collection and processing of Personal Data (defined in question 3) are as follows:

Laws and local regulations

- Act on the Protection of Personal Information (the APPI);
- Act on the Protection of Personal Information Held by Administrative Organs;
- Act on the Protection of Personal Information Held by Independent Administrative Agencies; and
- Local regulations (jourei) adopted by local governments.

Guidelines (the Guidelines)

- Guidelines on the principles of the APPI issued by the Personal Information Protection Committee (the PPC) (the Principle Guidelines);
- Guidelines on the protection of Personal Information in the financial sector issued by the PPC and the Financial Service Agency;
- Guidance on the protection of Personal Information in the medical sector issued by the PPC and the Ministry of Health, Labour and Welfare (the MHLW);
- Guidelines on the protection of personal information in the labour management sector issued by the MHLW; and
- Other guidelines issued by other ministries.

Tort law (which is incorporated in the Chapter 5, Part 1 of the Civil Code)

Tort law in Japan provides that a person who has infringed any right of others or the legally protected interest of others shall be liable to compensate for any resulting damage (subject to an adequate causal relationship). In this connection, the Japanese Supreme Court has recognised, pursuant to article 13 of the Constitution of Japan, the right to privacy (the privacy rights) as the right of persons not to have their private life disclosed,exposed or invaded without a legitimate reason. Therefore, business operators are advised not to infringe the privacy rights of the data subjects when collecting and handling information containing privacy-related information in the course of their investigation, in addition to complying with the data protection requirements, namely, the APPI and relevant regulations and guidelines cited above. A business operator is any entity handling a personal data database regardless of the size of the business or volume of personal data. See question 3 for its definition.

2 What other laws and regulations may prevent data sharing in the context of an investigation?

The APIPO Privacy Policy

An authorised or accredited personal information protection organisation (the APIPO) is an entity authorised by the PPC to handle complaints from individuals against business operators' handling personal information. The APIPOs have published their privacy policy (the APIPO Privacy Policy) and relevant business operators including members of the relevant APIPO must comply this such policy. The All Banks Personal Data Protection Council is the most well-known APIPO.

The APIPO Privacy Policy provides for more detailed and comprehensive requirements than the laws and regulations referred to in question 1, and impose obligations stricter than the "best effort" obligations contained in the laws and regulations.

Financial regulations

The financial regulations such as the Banking Act or the Insurance Business Act provide for specific obligations to be complied with by financial business operators relating to the collection and handling of personal data. In addition, such specific obligations applicable to the financial sector are also contained in the Comprehensive Guidelines for Supervision of Major Banks and the Comprehensive Guidelines for Supervision of Small to Medium or Local Banks (collectively, the Banking Guidelines).

Professionals duties and duty of confidentiality

The Attorney Act, Medical Practitioners' Act or certain other laws including provisions on professional duties may provide secrecy obligations and prohibit the transfer of certain data that may otherwise be regarded as lawful under the APPI. Furthermore, business operators in certain sectors such as the financial sector owe a duty of confidentiality to their clients.

Tort law (employee's privacy rights)

It is generally permissible for employers to investigate data saved in devices and equipment which employers provide to their employees for business use because employers are deemed to own and control such data. However, if such investigation went beyond what is fair and reasonable (which qualification would be determined in the light of current social standards considering

various factors such as the purpose of the investigation or the manner in which it is conducted), employers may infringe on the employee's privacy rights and may be liable for damages under tort law or labour laws. Employers will not contravene tort law or labour law as long as they have a legitimate reason to investigate and limit the scope and the manner of the investigation to an extent that is fair and reasonable. For example, employers should consider specifying a scope of investigation of their employees' emails as narrow as possible to mitigate risks of infringement on the employee's privacy rights (eg, by limiting the period of exchange of emails on which the investigation is focusing).

Unfair Competition Prevention Act

See question 15.

Other laws

In addition to the above, there are sector-specific regulations which provide for a prohibition of data sharing in the context of an investigation, such as the telecommunications sector or the medical care sector. For example, the Telecommunications Business Act prohibits telecommunication business operators from disclosing communications between the parties that should be kept secret, save in certain circumstances.

3 What can constitute personal data for the purposes of data protection laws?

The APPI defines two different concepts: "personal information" and "personal data". To better understand the concept of personal data, it is necessary to distinguish the two.

For a brief overview of these concepts, see below:

Personal information

- (i) Information relating to a living individual by which a specific individual is identified; and
- (ii) Information relating to a living individual containing an individual identification code (ie, passport number, driver's licence number);
- Including information that can be readily combined with other information and make the identification of a specific individual possible.

Personal data

- personal information that constitutes a "personal information database" (a collective body of information comprising personal information systematically organised to be able to retrieve personal information).

When you are handling personal information only (ie, without using personal Information in a systematically organised way), generally, you do not fall under the definition of "business operators". In this case, obligations on business operators such as the obligation to disclose the purpose of use of personal Information (the purpose of use) prior to its collection, and to limit the use of such information within the scope necessary to achieve the purpose of use (the scope of purpose) will not be applicable.

However, if you are using a personal information database for your business, this business entity will be classified as a business operator and various obligations will kick in under the APPI.

Examples of personal data are internal or external emails, email addresses, customer information and data extracted from business cards.

4 Does personal data protection relate only to natural persons or also legal persons?

Personal information and personal data only relate to a living individual. However, please note that the Banking Guidelines also cover the customer information of a legal entity as well as that of individuals.

5 To whom do data protection laws apply?

Business operators

The APPI does not use the "controller" or "processor" concepts. The obligation under the APPI generally applies to any business operator which is using personal data for its business, regardless of whether such business operator is performing its business in an equivalent "controller" or "processor" position.

If foreign entities have offices in Japan, such foreign entities will also fall under the business operator and obligations under the APPI are imposed, if it is using personal data for its business.

Extraterritorial application

Activities conducted by foreign entities located in foreign countries without offices in Japan but trading in, or with, Japan are generally not covered by the APPI. However, certain provisions of the APPI have extraterritorial applications and are relevant if the foreign entity is collecting personal information on individuals in Japan in connection with a supply of goods or services. Accordingly, such foreign entities must take measures to comply with certain provisions of the APPI.

6 What acts or operations on personal data are regulated by data protection laws?

The APPI covers acts or operations very broadly. Below are acts and operations covered by the APPI.

- handling (which is a very wide concept that covers most actions with respect to personal data and is basically similar to processing under the EU GDPR);
- collection;
- update and deletion;
- transfer to third parties (domestic or overseas);
- receipt from third parties; and
- disclosure to the data subject, rectification, deletion and discontinuity of use upon request of a data subject.

7 What are the principal obligations on data controllers to ensure the proper processing of personal data?

We describe obligations imposed on business operators below, since APPI does not use the "controller" concept (see question 5).

Collection

The APPI requires business operators to either publicly announce (including on their website) or notify the data subjects of the purposes of use before or upon collection of the personal information. Consent of the data subjects is not required generally, but consent is required in the case of sensitive personal data, the categories of which are listed in the APPI and its sub-legislation.

Handling

The APPI requires business operators to clarify the purpose of use and to make it specific as much as possible and not to use personal information without obtaining the prior consent of the data subjects beyond the scope of purpose (we refer to such consent as the consent to use), subject to exceptions such as:

- when the handling of personal information is based on laws and regulations;
- when the handling of personal information is necessary for the protection of the life, body, or property of an individual or the property of a legal entity and it is difficult to obtain the consent of the data subjects;
- when the handling of personal information is necessary for cooperating with a Japanese state organisation, a Japanese local government, or an individual or an entity entrusted by either of the former two in executing the affairs prescribed by laws and regulations and obtaining the consent of the person is likely to impede the execution of the affairs concerned; and
- when a business operator entrusts the handling of personal data in whole or in part within the scope of purpose (the entrustment).

Transfer to third parties

The APPI prohibits business operators from transferring personal data to a third party (the transfer to third parties) without obtaining the prior consent of the data subjects (the consent to transfer), subject to certain exceptions such as the ones listed in the preceding paragraph.

Data extraction by third parties for data collection purposes

8 Before data extraction by third parties commences, should steps be taken to ascertain whether non-locally generated data was lawfully transferred to, or within, your jurisdiction in the first instance?

Unlawful data

If a business operator commences an investigation by having third parties extract data from digital devices such business operator owns and controls (we refer to such business operator as the investigating operator) the investigating operator needs

to ascertain to the extent reasonable whether the data was lawfully obtained or transferred in the first instance. This is because inappropriate obtaining of the personal data from a data subject or a third party is prohibited under the article 17 of the APPI (we refer to this obtained personal data as the unlawful data) and the transfer of the unlawful data may lead to certain sanction under the civil law in Japan as well as the APPI. Any personal data may be deemed as the unlawful data in the case such as (i) where the personal data is saved in a company's mobile device together with the email that shows that such data were obtained in contravention of the local data protection regulation, including the cross-border transfer restriction (if any), or (ii) where the investigating operator did not confirm certain designated statutory items (eg, how the transferrer had obtained the personal data) pertaining to a receipt of such personal data in violation of the article 26 of the APPI, which provides ascertainment obligation of a business operator who receives personal data from a third party. In particular, if the third party obtained from the personal data from another third party located in the EU based on the European Commission's determination (and adequacy decision) that Japan offers an "adequate level of protection", the investigating operator needs to trace and check whether the third party located in the EU had obtained the personal data lawfully. Accordingly, the investigating operator should be more careful if the personal data was generated in a foreign jurisdiction.

However, the clearance procedure for distinguishing unlawful data from personal data should be conducted as "to the extent reasonable" basis, and if there are no peculiar clues showing the personal data was unlawfully obtained, the personal data is unlikely to be deemed as the unlawful data for this purpose.

When the investigating operator finds that the personal data contains unlawful data, it shall obtain a consent to use and consent to transfer for the investigation from the data subject, prior to the use and transfer of the unlawful data to a third party.

9 Are there additional requirements where third parties process the data on behalf of the entity to which data protection laws primarily apply?

No. There are no material and additional requirements where the third party processes the data on behalf of the entity to which the data protection laws primarily apply. However, the entity which entrusts processing of the personal data is required to adequately monitor and supervise the third party under the APPI (see question 14).

10 Is the consent of the data subject mandatory for the processing of personal data as part of an investigation? And how can consent be given by a data subject?

Consent is not always mandatory for handling of the personal data as part of an investigation (see question 7). However, in order to mitigate the risk of complaint by data subjects based on tort due to the infringement of their privacy rights, it is safer to obtain the consent of the data subjects when this is possible and realistic. Japanese practice follows this approach, especially for personal data obtained from the employees of the company that is conducting the investigation.

Any means used for obtaining the consent to use, consent to transfer and a consent to handling of the personal data relating to the privacy right (the consent regarding privacy right) including oral communication, emails, checking the corresponding box or items and clicking a button on the website will be permissible. It is desirable to use means allowing you to keep evidence of the consents. For example, if the consent is obtained orally, recording this consent in writing is strongly recommended.

11 If not mandatory, should consent still be considered when planning and carrying out an investigation?

See question 10.

12 Is it possible for data subjects to give their consent to such processing in advance?

It is possible for data subjects to give their consent to use in advance and through standard business terms and conditions provided that the purpose of use is sufficiently clear and specified. Insufficiently detailed purposes of use such as "investigation when necessary" cannot be regarded as sufficiently specified. From data protection regulation perspectives, a consent to use is not generally required in Japan, as long as the purpose of use is sufficiently disclosed beforehand. See question 7.

It is possible for data subjects to give their consent to transfer in advance and through standard business terms and conditions. The data subjects may give comprehensive consent to a transfer to third parties that they can expect at the moment. If the third party is located in a foreign country, the consent to transfer shall include consent to the cross-border third-party transfer.

The data subjects may give their consent regarding privacy rights in advance and through standard business terms and conditions. However, if the scope of consent is too wide and vague, such consent could be deemed to be void. Although this has

not been tested before the courts, if such prior consent is obtained, compared to a situation where no consent is given either prior or at the time of the investigation, this would reduce the risk of infringement of privacy rights.

13 What rights do data subjects have to access or verify their personal data, or to influence or resist the processing of their personal data, as part of an investigation?

If a business operator has the authority to disclose or correct (or add, delete, etc) personal data retained by such business operator for more than six months (the personal data in this case is referred to as the retained personal data), such business operator must cope with the various requests made by the individuals as a holder of retained personal data, such as disclosure, correction or ceasing to use. Personal data transferred from the EU based on the European Commission Determination, falls under retained personal data regardless of the retention period.

In connection with the data subject's right to object to the processing of retained personal data, the data subject may request a business operator to discontinue the handling, or transfer of retained personal data to third parties or to delete the retained personal data, if such handling or transfer of retained personal data is made in violation of the APPI. The business operator must discontinue the handling or transfer of retained personal data upon the request of the data subjects if the request has reasonable grounds.

Transfer for legal review and analysis

14 How are law firms, and legal process outsourcing firms, generally characterised in your jurisdiction?

Professionals

It is generally accepted that the transfer of personal data to attorneys, certified public accountants, legal process outsourcing firms or other similar professions (the professionals) does not fall within the definition of a transfer to third parties, because the transfer of personal data to the professionals is deemed to be an entrustment (see question 7). Thus, business operators may transfer data including personal data to be investigated to professionals without consent to transfer (the consent to use still needs to be obtained unless statutory exceptions are met).

These professionals will be business operators and therefore subject to the obligations imposed under the APPI upon business operators.

Furthermore, please note that when a business operator provides personal data to the professionals as part of an entrustment, it must exercise necessary and appropriate supervision over the professionals to ensure the security control of the entrusted personal data.

Attorney's inquiry

Attorneys have a statutory right through the bar association to request public offices or public or private organisations for information necessary in a case for which they have been retained under article 23-2 of the Attorney Act (the attorney's inquiry). Attorneys may request information that could include personal data from business operators. From the business operators' view, who are requested to submit such information by attorneys, giving such information could conflict with the regulations regarding purpose of use and transfer to third parties. One should carefully review whether giving such information containing personal data falls under the "based on laws and regulations" exception (see question 7). Lower court decisions in Japan suggest that a supply of information containing personal data according to the request would qualify as "based on laws and regulations" only when such provision is necessary and reasonable.

From the position of a business operator collecting personal data from third parties for investigation purposes, the attorney's inquiry could be utilised as a means for collecting information for investigation. However, for the above reasons, the request may be rejected by the third parties who receive such a request.

15 Are there any additional requirements, beyond those specified above, that regulate the disclosure of data to third parties within your jurisdiction for the purpose of reviewing the content of documents, etc?

Unfair Competition Prevention Act

If information to be investigated includes (i) a production method, sales method, or any other technical or operational information useful for business activities that is controlled as a secret and is not publicly known (the trade secret) or (ii) technical or business data (excluding data that is treated as confidential) which is handled as part of a business as data to be provided to

specific persons and is accumulated in substantial quantities by electric or other methods that cannot be recognised by human perception (the data for limited provision) and together with trade secrets, etc), which were provided by the holder of the trade secrets, etc, it can be unlawful to disclose such information for the purpose of making an illicit gain or harming the interest of the information holder (the illegal purpose disclosure).

Guidelines on Data for Limited Provision issued by Ministry of Economy, Trade and Industry make it clear that disclosure of trade secrets, etc, for the investigation being conducted under laws and regulations will not be an illegal purpose disclosure. Hence it seems possible that disclosure of the trade secrets, etc to professionals, forensic accountants or consultants for the purpose of conducting investigations will not fall on the illegal purpose disclosure because such disclosure is made for a legitimate reason.

16 What rules regulate the transfer of data held in your jurisdiction to a third party in another country for the purpose of reviewing the content of documents, etc?

If the personal data is transferred from a Japanese investigation officer to third parties in another country, a consent to use and a consent to transfer (including consent to cross-border third-party transfer) must be obtained in general. However, because the investigation is likely to be regarded as necessary for protecting the property of the investigation officer, if the transfer is reasonably necessary for the purpose of investigation and if it is difficult to obtain the consent of the data subject regarding a data transfer, these two consents are not required to be obtained.

Data sharing

Even if the above exemption requirement for cross-border transfer is not met, data sharing with third parties (commonly used for intra-group data sharing) could be permitted if (i) personal data is used jointly between the investigating operator and the third party, and the business operator meets prior notification requirements: the business operator must inform the data subjects in advance of five statutory elements, or ensure that the data subjects can easily become aware of these statutory elements, and (ii) if the third party is located in the EU (as currently a white-listed country for cross-border transfer), or appropriate measures have been taken between the business operator in Japan and the third party abroad to ensure appropriate protection of the personal data in such third party (ie, data transfer agreement or binding corporate rules). Accordingly, the investigating operator may share data with its group companies for the purpose of investigation by complying with these requirements.

Transfer to regulators or enforcement authorities

17 Under what circumstances is the transfer of personal data to regulators or enforcement authorities within your jurisdiction permissible?

The Regulations regarding Purpose of Use and Transfer to Third Party are also applicable to the transfer of personal data to Japanese regulators or enforcement authorities and there are no additional requirements in addition to the above. However, in most cases, the transfer of personal information will fall on exceptions where the consent to use and consent to transfer does not need to be obtained such as when such transfer of personal data is based on Japanese laws and regulations or when such transfer of personal data is necessary for cooperating with a state organisation (see question 7).

18 Under what circumstances is the transfer of personal data held within your jurisdiction to regulators or enforcement authorities in another country permissible?

The Regulations regarding Purpose of Use and Transfer to Third Parties are also applicable to the transfer of personal data to regulators or enforcement authorities in another country (section 2-2 of the of Principle Guidelines regarding the provisions to a third party located in a foreign country) and it is necessary for the transferor (including those who transfer personal data to foreign regulators) to obtain the consent to use and consent to transfer except when the transfer of personal information is necessary for the protection of the life, body, or property of an individual or the property of a legal entity and it is difficult to obtain the consent of the data subject.

It is NOT necessary to notify data transfers to the data protection authority in Japan (ie, PPC).

19 What are some recommended steps to take on receipt of a request from a regulator for disclosure of personal data?

Request from Japanese regulators

Upon receipt of a request from Japanese regulators, you should confirm which ground below would authorise you to disclose personal data to the regulator.

- the data transfer is based on the consent to use and consent to transfer;
- the data transfer is based on Japanese laws and regulations;
- the data transfer is necessary for the protection of the life, body, or property of an individual or the property of a legal entity and it is difficult to obtain the consent of the data subject; or
- the data transfer is necessary for cooperating with a state organisation, a local government, or an individual or an entity entrusted by either of the former two in executing the affairs prescribed by laws and regulations and obtaining the consent of the person is likely to impede the execution of the affairs concerned.

Request from foreign regulators

Upon receipt of a request from foreign regulators, you need to confirm whether either of the requirements below is met.

- the data transfer is based on consent to use and consent to transfer; or
- the data transfer is necessary for the protection of the life, body, or property of an individual or the property of a legal entity and it is difficult to obtain the consent of the subject.

20 What are the sanctions and penalties for non-compliance with data protection laws?

If a business operator has used personal data beyond the scope of purpose or disclosed personal data without taking the required steps under the APPI as described above, the PPC may recommend the business operator to rectify the violation of the APPI and take other necessary measures to cure the violation, and then order to take such measures if the recommendation was ignored. Failure to comply with a cease and desist order may be punished with imprisonment for up to six months or a fine of up to Y300,000.

Extraterritorial application

If a business operator located in a foreign country has used personal data beyond the scope of purpose or disclosed personal data without taking the required steps under the APPI as described above (see question 5), the PPC may recommend the business operator to rectify the violation of the APPI and to take other necessary measures to cure the violation, but cannot order the business operator to take the necessary measures. Failure to comply with such recommendation brings no criminal sanctions.

Continuing obligations on original and intervening data controllers

21 What are the continuing obligations on the original data controller that apply in an investigation?

We describe obligations imposed on business operators below, since APPI does not use the "controller" concept (see question 5).

Continuing obligations on the business operators are as follows: the principal obligations of business operators (see questions 5 and 7), the obligation to supervise the entrusted party (see question 14) and the obligation to keep a record of certain designated statutory items in the case of a transfer to third parties. However, these requirements could be exempted in many cases in an investigation context – please refer to questions 7, 14 and 16.

22 What are the continuing obligations on any intervening data controller that apply in an investigation?

We describe obligations imposed on business operators below, since APPI does not use "controller" concept (see question 5).

Assuming that the third party who receives personal data from the investigating operator is a business operator, the continuing obligations imposed on such third party are: the principal obligations of business operators (see questions 5 and 7) and the obligation to keep a record of certain designated statutory items in the case of a transfer to third parties. However, these requirements could be exempted in many cases in an investigation context – please refer to questions 7, 14 and 16.

Relevant materials

23 Provide a list of relevant materials, including any decisions or guidance of the data protection authority in your jurisdiction regarding internal and external investigations, and transfers to regulators or enforcement authorities within and outside your jurisdiction.

PPC's webpage https://www.ppc.go.jp/en/

APPI
https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf

Amendment to the Cabinet Order to Enforce the APPI
https://www.ppc.go.jp/files/pdf/Cabinet_Order.pdf

Enforcement Rules for the APPI
https://www.ppc.go.jp/files/pdf/PPC_rules.pdf

Overview of the APPI issued by PPC
https://www.ppc.go.jp/files/pdf/280222_outline_v2.pdf

Current Legal Framework for the Protection of Personal Information
https://www.ppc.go.jp/files/pdf/280222_Current_Legal_Framework_v2.pdf

Other relevant materials are available on the PPC's website (only in Japanese)
https://www.ppc.go.jp/personalinfo/legal/

Akira Matsuda

Iwata Godo

Akira Matsuda is an attorney-at-law (admitted in Japan and New York) and a partner at Iwata Godo heading the AI/TMT and data protection practice group. He is based in Tokyo and Singapore. His practice focuses on cross-border transactions, including mergers and acquisitions, as well as international disputes (litigation/arbitration), and advice on digital/TMT related matters. Mr Matsuda regularly advises Japanese and foreign clients on data security issues (Japanese laws, Singapore PDPA, and EU GDPR) including on the structuring of global compliance systems. He also advises complicated cross-border corporate investigation matters.

He is a graduate of the University of Tokyo (LLB) and Columbia Law School (LLM).

Koji Horita

Iwata Godo

Koji Horita is an attorney-at-law (admitted in Japan) and an associate at Iwata Godo and a member of the AI/TMT and Data Protection practice group. His practice focuses on digital/IT business. He regularly advises Japanese and foreign clients on data protection, data marketing, financial technology (Fintech), regulatory technology (Regtech) and other TMT related matters. His practice also includes the investigation of fraud and misconduct and he is well versed in computer forensics.

He graduated from the University of Tokyo (LLB).

Makoto Adachi

Iwata Godo

Makoto Adachi is an attorney-at-law (admitted in Japan) and associate at Iwata Godo and a member of the AI/TMT and Data Protection practice group. Mr Adachi has given advice on data security issues in a wide range of industries, including financial institutions. Mr Adachi is also advising on investigations regarding fraud and misconduct in a group's foreign subsidiaries and has experience interviewing foreign employees and business partner for investigation purposes.

He earned his JD in 2016 and LLB in 2014 from the University of Tokyo.

Iwata Godo is one of Japan's premier and oldest law firms. It was established in 1902 as one of the first business law firms by Chuzo Iwata, an attorney-at-law who subsequently held various positions, including serving as Minister of Justice and president of the Japan Federation of Bar Associations. It is a full-service firm with about 60 attorneys and each of its practice areas is highly regarded. It is the firm of choice for clients with respect to their most challenging legal issues, including in relation to data protection. Over the past few years, Iwata Godo has hosted a number of international seminars and conferences on data protection, often in coordination with "best friend" firms that are renowned firms and market leaders in their jurisdictions.

Marunouchi Building 10F
2-4-1 Marunouchi,
Chiyoda-ku,
Tokyo
100-6310,
Japan
Tel: +81-3-3214-6205

www.iwatagodo.com

Akira Matsuda
amatsuda@iwatagodio.com

Koji Horita
khorita@iwatagodo.com

Makoto Adachi
makoto.adachi@iwatagodo.com