OVERVIEW OF THE REVISED PERSONAL INFORMATION PROTECTION ACT OF JAPAN AND ITS MAIN IMPACT ON FOREIGN GROUPS

Akira Matsuda, Takaki Sato and Landry Guesdon
Iwata Godo

March 2, 2017

1. INTRODUCTION

The Act on the Protection of Personal Information ("**APPI**") of Japan originally came into force in 2005. The APPI had not been amended since then, in spite of the fact rapid technological developments and globalization have brought new challenges for the protection of personal data, with the scale of the collection and sharing of personal data having increased significantly. Technology allows private and public players to make use of personal data on an unprecedented scale to conduct their activities, and natural persons increasingly make personal information available publicly and globally. New rules had become necessary to deal with these new challenges (including cloud computing and Big Data).

The bill to amend the APPI was adopted in 2015. The amended APPI will come into effect on 30 May 2017. Part of the new APPI is already in force and the Personal Information Protection Commission ("**PPC**") was established in 2016 as a fully integrated supervisory authority and regulatory watchdog. The PPC has already issued general guidelines applicable to all sectors aiming to clarify certain provisions of the APPI. The PPC is expected to release sector specific guidelines and Q&As to deal with practical issues which are still unclear. This is intended to supplement the sketchy provisions of APPI and its sub-regulations and enable private organizations to understand the changes better and adequately reflect them in their operational rules. An English translation of the APPI and its sub-regulations is available on the PPC's website but no English translation of the guidelines is available as of the date of this newsletter.

In this article, we would like to draw the attention of foreign groups to the significant impact the amended APPI will have on them, especially on those companies which have so far paid little attention to the APPI.

Contents

Inquiry contact:
newsmail@iwatagodo.com

2. OVERVIEW- MAIN IMPACT ON FOREIGN ENTITIES

What is the impact of the amended APPI by type of foreign group?

A. Foreign groups which have an office in Japan (with a data base regarding less than 5,000 individuals over the past period of 6 months)

Prior to the amendment, entities handling a relatively small volume of personal data in Japan were exempted from the strictures of the APPI. Generally speaking, an entity with a data base concerning less than 5,000 data subjects over the past 6 months did not have to comply with the obligations imposed by the APPI on Business Operators (as defined below). This is about to change, and as from May 30, 2017, all entities collecting, processing and keeping personal data will become subject to the APPI. This will be a major change for entities handling small volumes of personal data.

Because these entities will have obligations as Business Operators under the revised APPI, they will have to put into place proper APPI-compliant compliance systems (in particular by prescribing internal rules regarding the handling of personal information and personal data).

B. Foreign groups which have an office in Japan (handling personal data on more than 5,000 data subjects in the past 6 months)

Entities handling personal data on 5,000 or more data subjects in the past 6 months were already covered by the APPI and they already had to abide by their obligations as Business Operators (as defined below) under the APPI. They will have to continue to do so after the amended APPI comes into force.

These entities will have to update their internal rules regarding the handling of personal information and personal data to reflect the newly introduced obligations, in particular, the traceability requirement and cross-border transfer restrictions in a disclosure context, as explained below.

C. Foreign groups without an office in Japan

Most of the activities conducted by foreign groups without an office in Japan but trading in, or with, Japan were not covered by the APPI. However, after the amendment, certain provisions of the APPI will have extra-territorial applications and be relevant if the foreign entity has collected personal information on an individual in Japan in connection with a supply of goods or services to such individual. Accordingly, entities which do not have an office in Japan must take measures to comply with these provisions of the APPI (see Note 6 in Page 4).

3. THREE KEY CONCEPTS

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 (i.e. passport number, driver's license number)
- Including information which can be readily combined with other information and make the identification of a specific individual possible

Personal Data

Personal Information which constitutes a "Personal Information Database" (a collective body of information comprising Personal Information systematically organized to be able to retrieve Personal Information)

Retained Personal Data

Personal Data which a Business Operator has the authority to disclose, correct, etc. and continuously retains over at least 6 months

In order to better understand the APPI, it is necessary to grasp 3 key concepts underpinning the Japanese laws and regulations governing data protection. The 3 concepts have not been drastically revised, but it is important to understand these concepts, because a more extensive set of obligations will be imposed on entities handling such types of information under the revised APPI. For a brief overview of the concepts and corresponding obligations, please see the chart in the Appendix.

It is important for foreign groups not only to understand these concepts, but to conduct internal audits to determine how these categories of data/information are to be dealt with under the revised APPI.

When the foreign group is handling Personal Information only (i.e. doesn't use Personal Information in a systematically organized way), generally speaking, the obligation to disclose Purpose of Use (as defined below) prior to its collection, and to use such information within the scope of the Purpose of Use will be imposed.

However, if the foreign group is using a Personal Information Database (i.e. Personal Information organized systematically (defined under Note 3 in page 4)) for its business, such business entity will be classified as a Business Operator, and various obligations under the APPI will kick in (to be explained in detail in "5. Obligations Imposed on Business Operators").

Furthermore, if a Business Operator has the authority to disclose or correct (or add, delete, etc.) the Personal Data retained by such Business Operator for more than 6 months, such Business Operator must deal with the various requests made by the individuals as a holder of Personal Data, such as disclosure, correction or ceasing to utilize.

4. APPLICABILITY OF APPI OBLIGATIONS TO FOREIGN GROUPS

The APPI mainly imposes obligations on "Personal Information handling business operators" ("**Business Operators**"). A Business Operator is defined as "an entity using a Personal Information Database for use in its business."[1] Public entities are expressly excluded from such definition. However, there is no similar carve-out for the benefit of companies incorporated in a foreign country[2] or entities having their head office located in a foreign country (hereinafter collectively referred to as a "**Foreign Company**"). This definition reflects the official position of the PPC that APPI obligations and provisions equally apply to Foreign Companies, if these Foreign Companies fall under the definition of a "Business Operator" in Japan. The PPC takes the view that a Foreign Company is a "Business Operator" if it uses a Personal Information Database[3] for its business conducted in Japan[4]. This is regardless of the place of incorporation or the location of the head office[5].

Therefore, if a Foreign Company has a branch office or a business office in Japan, or if a Foreign Company conducts its business in Japan, and uses a Personal Information Database for its business in Japan, such Foreign Company will fall under the definition of a "Business Operator" and will have to abide by the provisions of the APPI. In addition, if a Foreign Company has a subsidiary in Japan using a Personal Information Database for its business in Japan, this subsidiary will be deemed to be a Business Operator (although the Foreign Company itself might not necessarily be covered by the APPI). Accordingly, if a Foreign Company has an office in Japan, which falls under the definition of "Business Operator", regardless of whether such office is branch, business office or subsidiary, APPI-complaint compliance systems must be put in place.

Even if a Foreign Company has no office in Japan, in the event this Foreign Company is collecting Personal Information from individuals in Japan in connection with a supply of goods or services to these individuals, certain obligations under the APPI would apply to them on an extra-territorial basis[6]. Accordingly, such entities must take measures to comply with these provisions of the APPI.

In the next section, we will go into the details of the obligations imposed on Business Operators under the APPI.

---

[1] Article 2(5) of the APPI.
[2] A foreign country means a country or region located outside Japan.
[3] "Personal Information Database" means a collective body of information comprising Personal Information systematically organized so as to be able to retrieve particular Personal Information (Article 2 (4) of the APPI).
[4] "Business" includes profit and non-profit activities (i.e. NGOs).
[5] Section 2-2 of the Guideline on the transfer of Personal Data to a third party in a foreign country ("Cross-Border Transfer Guideline").
[6] Obligations include: (i) Specifying a Purpose of Use; (ii) Restriction due to Purpose of Use; (iii) Notification of Purpose of Use upon Collection; (iv) Assurance about the Accuracy of Data Contents; (v) Security Control Action; (vi) Supervision of Employees; (vii) Supervision of Data Trustees; (viii) Restriction on Third Party Disclosure; (ix) Restriction on Transfers to Third Parties in a Foreign Country; (x) Keeping Records of Third-Party Disclosures; (xi) Public Disclosure of Matters relating to Retained Personal Data; (xii) Disclosure; (xiii) Correction; (xiv) End of Use; (xv) Explanation of Reasons; (xvi) Procedure for Responding to a Demand for Disclosure; (xvii) Fee; (xviii) Business Operator's Dealing with Complaints; and (xix) Production of Anonymously Processed Information.

5. OBLIGATIONS IMPOSED ON BUSINESS OPERATORS

A. Summary

This section provides an overview of the obligations imposed on Business Operators under the APPI. The following chart provides a brief outline of the obligations imposed on Business Operators for each phase during which information is handled.

Phase		Type of information	Summary of duties
Phase I	Collection	Personal Information	• Disclosure of the Purpose of Use prior to collection of Personal Information. • No need to obtain the individual's consent (except for Sensitive Personal Information).
Phase II	Utilization	Personal Information/Personal Data	• No need to obtain the individual's consent, when utilizing within the scope of a previously disclosed Purpose of Use. • Duty to take reasonable security measures when handling Personal Data.
Phase III	Disclosure (to a third party)	Personal Data only	**Consent Requirement** • In principle, the individual's consent is required for disclosure to a third party. • Consent requirement is exempted in case of (i) entrustment of Personal Data, (ii) disclosure upon business succession (i.e. M&A), and (iii) joint use. • If the Business Operator meets the Opt-out process requirements, no need to obtain the individual's consent upon each disclosure of Personal Data. **Traceability Requirement** • An entity disclosing Personal Data to a third party must keep track (i.e., records) of such disclosure. • An entity receiving Personal Data from a third party must confirm the status of the disclosing party and keep track of such disclosure. **Cross-border Transfer Restrictions** • Cross-border Personal Data transfer restrictions are newly introduced.

B. Phase I – Collection of Personal Information

APPI rules governing the collection of Personal Information deal with (a) the purpose of use of Personal Information ("**Purpose of Use**"); and (b) the requirement to obtain the individual's prior consent in the case of Sensitive Personal Information.

a. Purpose of Use

The key points in the APPI with respect to the Purpose of Use when collecting Personal Information can be summarized as follows: (i) specification of the Purpose of Use; and (ii) notification to the individual / public disclosure of the Purpose of Use.

(i) A Business Operator must specify the Purpose of Use as explicitly as possible[7].

(ii) A Business Operator having collected Personal Information (except where the Purpose of Use has been disclosed in advance to the public) must promptly inform the individual of, or disclose to the public, the Purpose of Use[8].

b. Prior Consent

Under the APPI, it is not required to obtain the individual's consent when collecting personal information from such individual (although that may be recommended in many cases (i.e. a retailer collecting individual customer data)).

However, if the entity is collecting Sensitive Personal Information from the individual, such entity must obtain individual's consent. Sensitive Personal Information is defined as Personal Information requiring special care, i.e., information which is sensitive by nature, including but not limited to the individual's race, creed, social status, medical history, criminal record, status as the victim of a crime.

C. Phase II – Utilization / Handling of Personal Information / Personal Data

The regulations governing the utilization and handling of Personal Information vary depending on whether such Personal Information is just Personal Information or part of Personal Data. If Personal Information is systematically organized and can be easily retrieved, e.g., by computer (i.e. database), such Personal Information is treated as Personal Data.

The regulations relevant to the utilization of Personal Information can be summarized as follows: utilization is permitted only within the limits of the Purpose of Use which was set when collecting the Personal Information.

Furthermore, if Personal Information is contained in Personal Data, the APPI imposes an extra obligation on Business Operators which can be summarized as follows: the Business Operator must take necessary and appropriate action to control the security of the Personal Data ("**Security Control Action**").

[7] Article 15(1) of the APPI.
[8] Article 18(1) of the APPI.

a. Personal Information – Purpose of Use

A Business Operator must not handle Personal Information beyond the necessary scope of what is needed to achieve the specified Purpose of Use[9] without obtaining the individual's prior consent.

Further, in the course of its business and subsequent to the collection of Personal Information, a Business Operator might find it necessary to utilize the collected Personal Information for purposes other than the specified Purpose of Use. In such cases, the Business Operator may alter the Purpose of Use if the revised purpose is reasonably relevant to the original Purpose of Use. If the alteration of Purpose of Use goes beyond this limit, the Business Operator must inform the individual of, or disclose to the public, the revised Purpose of Use[10].

b. Personal Data – Security Control Action

When handling Personal Data, a Business Operator must take Security Control Action including preventing the leakage, loss of, or damage to, the Personal Data it is handling[11].

According to the Guideline on general rules (the general Guideline), the Business Operator must develop and implement certain actions based on four pillars: (i) organizational security; (ii) personnel security; (iii) physical security; and (iv) technological security. The general Guideline also enumerates examples of good practices for each pillar.

Under the general Guideline, small and medium sized entities (i.e., with not more than 100 employees) handling Personal Data on less than 5,000 individuals in the past 6 months and which are not entrusted with the processing of Personal Data, are allowed to take less stringent measures than other entities handling larger volumes of Personal Data.

D. Phase III – Disclosure of Personal Data

Next, we will explain rules under the APPI on disclosure of Personal Data to a third party. The criterion to qualify as a "third party" under the APPI is whether the disclosing party and the receiving party are separate legal entities. For example, the wholly-owned subsidiary of a parent company is a separate legal entity from the parent, and consequently treated as a "third party" for the purposes of the APPI.

a. Domestic Disclosure within Japan

In principle, a Business Operator must not disclose Personal Data to a third party without obtaining the individual's prior consent[12]. Article 23 (5) of the APPI provides for three cases where the recipient of Personal Data does not fall under the "third party" definition and the Business Operator is allowed as a consequence to disclose Personal Data to the recipient without individual's prior consent.

[9] Article 16(1) of the APPI.
[10] Article 18(3) of the APPI.
[11] Article 20 of the APPI.
[12] Article 23(1) of the APPI.

Carve Outs of recipients from "third party" definition	
Carve out (i)	Entrustment of handling of the Personal Data
Carve out (ii)	Business Succession (i.e. M&A)
Carve out (iii)	Joint Utilization

These three cases can be summarized as follows:

(i) cases where a Business Operator discloses Personal Data in the course of entrusting all or part of the handling of Personal Data;

(ii) cases where Personal Data is disclosed in the course of a business succession caused by a merger or for some other types of transaction; and

(iii) cases where Personal Data is "jointly utilized" with a specified party.

Case (iii) is important in practice from a corporate group management standpoint. For example, based on this provision, a parent company and its subsidiary can jointly utilize Personal Data originally collected by the subsidiary, without obtaining any prior consent to the disclosure, provided that such utilization is within the limits of the specified Purpose of Use[13]. However, a Business Operator planning to rely on this provision must meet prior notification requirements: the Business Operator must inform the individual in advance of five statutory elements, or ensure that the individual can easily become aware of these statutory elements[14].

A Business Operator can also rely on the Opt-out process to disclose Personal Data without obtaining prior consent from the individual[15]. In order to meet Opt-out process requirements, a Business Operator must be prepared to cease the disclosure of Personal Data if requested by the individual. Furthermore, the Organization must inform the individual in advance of a few statutory elements such as the method of transfer of the Personal Data, or ensure that the individual can easily become aware of these statutory elements, as well as give notification to the PPC. However, Foreign Companies should note that the implementation of an Opt-out process cannot lead to the discharge of the prior consent requirement for transfers of Personal Data by a Business Operator to a third party located in a foreign country[16].

b. Cross-Border Transfer of Personal Data

As described above, restrictions on cross-border transfers of Personal Data will be newly introduced by the amendment. Unless exemption requirements are met, a Business Operator disclosing Personal Data to a third party in a foreign country must obtain the individual's prior consent to ensure that the data subject approves of the transfer to a third party in a foreign country[17].

[13] Section 3-4-3 of the Guideline on the general Guideline.
[14] These five statutory elements are: (i) the fact that Personal Data would be jointly utilized; (ii) the categories of jointly utilized Personal Data; (iii) the scope of a jointly utilizing party; (iv) the Purpose of Use for the utilizing party; and (v) the name or appellation of the person responsible for controlling Personal Data.
[15] Article 23(2) of the APPI.
[16] Section 2 of the Cross-Border Transfer Guideline.
[17] Article 24 of the APPI.

Summary Chart for Cross-Border Transfer Exemption	
Exemption (i)	Transfer to a country which is designated by rules of the PPC as a foreign country having established a Personal Information protection system recognized as being subject to equivalent standards to those applicable in Japan with respect to the protection of an individual's rights and interests (currently, no country is designated as such)
Exemption (ii)	The disclosing Business Operator and the recipient ensure that the recipient develops and implements arrangements through appropriate and reasonable measures for the handling of Personal Data to be performed consistently with the APPI obligations provisions. Such measures may include: 1) Contracts between the disclosing Business Operator and the recipient; or 2) Internal rules that are commonly applied to the disclosing Business Operator and the recipient
Exemption (iii)	The recipient receives certification based on the APEC cross-border privacy rules framework (CBPR)

The first exemption is a transfer to a country which is designated by the PPC rules as a foreign country having established a Personal Information protection system recognized as being subject to equivalent standards to those applicable in Japan with respect to the protection of an individual's rights and interests. However, as of the date of this newsletter, no country has been designated as such. Accordingly, this exemption is currently not available.

The second exemption applies where the disclosing Business Operator and the recipient ensure that the recipient develops and implements arrangements through appropriate and reasonable measures for the handling of Personal Data to be performed consistently with the APPI obligations provisions. According to the PPC, "appropriate and reasonable measures" should be construed on a case-by-case basis, but the PPC still attempts to clarify the meaning of the expression by giving a few examples of measures in the Cross-Border Transfer Guideline (Section 3-1). Based on these examples, "appropriate and reasonable measures" includes a contract between the disclosing Business Operator and the recipient. However, the Cross-Border Transfer Guideline and the Public Comment are still unclear as to whether such contract should be in writing and legally binding[18]. It should be noted that a contract simply including language such as "the recipient shall comply with the APPI of Japan" does not meet the "appropriate and reasonable measures" requirement[19]. Given the uncertainties regarding what constitutes "appropriate and reasonable measures", it is desirable to entrench wording based on professional legal advice. Where a Business Operator transfers Personal Data to another company belonging to the same corporate group, "appropriate and reasonable measures" would include corporate rules or privacy policy rules commonly applicable to both the disclosing Business Operator and the recipient.

The third exemption is where the Recipient receives "recognition based on a cross-border privacy rules framework." The PPC explicitly accepts the APEC-CBPR certification[20] as qualified to meet the standards for "recognition based on a cross-border privacy rules framework." However, the APEC-CBPR certification scheme has only been adopted by a very small number of APEC countries to date.

[18] No. 748 and 754 of the Public Comment for the Cross-Border Transfer Guideline.
[19] No. 752 of the Public Comment for the Cross-Border Transfer Guideline.
[20] Under the APEC-CBPR certification framework, registered Accountability Agent will certify the entities that are compatible with CBPR standards.

c. Traceability

In order to ensure the traceability of the flow of Personal Data, the APPI imposes obligations to maintain a record of disclosures. This recordkeeping obligation is unique to Japan, and was introduced in light of a huge data breach by the educational service provider company that has occurred several years ago in Japan. In this particular case, the authorities could not sufficiently trace the flow of Personal Data.

The parties on which such traceability obligations are imposed differ in a domestic disclosure and a cross-border transfer context. For disclosure within Japan, such obligations are imposed on both the disclosing Business Operator and the receiving Business Operator. For cross-border transfers, such obligations are only imposed on the disclosing Business Operator in Japan and not on the recipient based in a foreign country. This is because, from an international law perspective, Japan has no ground to apply its law to the foreign entity just based on the fact that such entity is receiving Personal Data from a Business Operator based in Japan.

More precisely, when a Business Operator discloses Personal Data to a third party or receives Personal Data from a third party, the Business Operator must (i) make a record of certain designated statutory items (e.g. the name of the recipient) relevant to such disclosure or receipt of Personal Data, and (ii) keep such record for a prescribed period between 1 to 3 years, depending on the type of record[21].

Practically, the traceability requirement would impose a high burden on Business Operators, especially where a large amount of Personal Data is handled by them. The PPC therefore admits a very wide exemption and simplified method for making records (the detail is covered in specific PPC guidelines on traceability requirements). The instructions made by the PPC under the guidelines and related public comments are complicated and sketchy (hopefully soon to be clarified in the Q&A to be issued by the PPC in the near future). We will not go into detail, but it is advisable for a Business Operator to structure its internal record keeping system in coordination with Japanese legal counsels.

E. Obligations relevant to Retained Personal Data

The main extra obligations relevant to Retained Personal Data are that the Business Operators must deal with the various requests made by the individuals as a holder of Personal Data.

For example, a Business Operator must:

- disclose Retained Personal Data to the individual in response to the individual's request[22];
- correct, add or delete Retained Personal Data in response to the individual's request when it is inaccurate[23]; and
- cease to utilize or disclose Retained Personal Data in response to the individual's request when it has become clear that the Business Operator violates the relevant APPI obligation provisions[24].

[21] Article 25 and 26 of the APPI.
[22] Article 28(2) of the APPI.
[23] Article 29(2) of the APPI.
[24] Articles 30(2) and (4) of the APPI.

Appendix[25]

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 (i.e. passport number, driver's license number)

- Including information which can be readily collated with other information and make the identification of a specific individual possible

Personal Data: Personal Information which constitutes a "Personal Information Database" (a collective body of information comprising Personal Information systematically organized to be able to retrieve Personal Information)

Retained Personal Data: Personal Data which a Business Operator has the authority to disclose, correct, etc. and continuously retains over 6 months

In addition to Obligations (A)

In addition to Obligations (A+B)

[Obligations (A) : corresponding to Personal Information]

Article 15:
Specifying a Purpose of Use

Article 16:
Restriction due to a Purpose of Use

Article 17:
Proper Collection

Article 18:
Notification etc. of a Purpose of Use when Collecting

Article 35:
Business Operator's Dealing with a Complaint

[Obligations (B): corresponding to Personal Data]

Article 19:
Assurance etc. about the Accuracy of Data Contents

Article 20:
Security Control Action

Article 21:
Supervision over Employees

Article 22:
Supervision over a Trustee

Article 23:
Restriction on Third Party Disclosures

Article 24:
Restriction on Transfers to Third Party in a Foreign Country

Article 25:
Keeping etc. of a Record of Third-Party Disclosures

Article 26:
Confirmation etc. when Receiving a Third Party Disclosure

[Obligations (C): corresponding to Retained Personal Data]

Article 27:
Public Disclosure etc. of Matters relating to Retained Personal Data

Article 28:
Disclosure

Article 29:
Correction etc.

Article 30:
Ceasing to Utilize etc.

Article 31:
Explanation of Reason

Article 32:
Procedure for Responding to a Demand etc. for Disclosure etc.

Article 33:
Fee

[25] Based on the Ministry of Economy, Trade and Industry of Japan website: http://www.meti.go.jp/policy/it_policy/privacy/downloadfiles/01kaiseikojinjohopamphlet.pdf

Akira Matsuda (amatsuda@iwatagodo.com)

Akira Matsuda is a senior associate at Iwata Godo, currently seconded to Drew & Napier in Singapore. His practice focuses on cross-border transactions, including mergers and acquisitions and capital markets, as well as international disputes (litigation/arbitration). Mr. Matsuda is also advising many Japanese and Foreign clients for data security issues, both in terms of Japanese laws and Singapore PDPA, including structuring of global compliance system.

Mr. Matsuda obtained his LL.M. from Columbia Law School in 2015 (awarded Harlan Fiske Stone Scholar) and passed NY Bar in the same year. He earned LL.B. from the University of Tokyo in 2006.

Takaki Sato (tsato@iwatagodo.com)

Takaki Sato is a senior associate at Iwata Godo. His practice focuses on mergers and acquisitions as well as litigation. Mr. Sato has experience with U.S. government cartel investigations. He has also given advice on data security issues in a wide range of industries, including financial institutions.

Mr. Sato obtained his LL.M. from Columbia Law School in 2016 and passed NY Bar in the same year. He earned his J.D., cum laude, in 2009 and LL.B. in 2007 from the University of Tokyo.

Landry Guesdon (lguesdon@iwatagodo.com)

Landry Guesdon is a foreign registered lawyer who focuses his practice on M&A, foreign direct investment, and other corporate and commercial matters. He has extensive experience advising overseas and local public and private companies from a wide spectrum of industries in local and cross-border transactions and projects, and other general corporate matters in Europe, Africa, Japan and other parts of Asia.

About Iwata Godo

IWATA GODO
Established 1902

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 Bldg. 10th floor, 2-4-1, Marunouchi, Chiyoda-ku, Tokyo, 100-6310, Japan www.iwatagodo.com/en
For Inquirires: E-mail: newsmail@iwatagodo.com Tel: +81-3-3214-6205