A GLOBAL ROADMAP TO PERSONAL DATA PROTECTION

Asia Pacific, Europe & USA

First Edition

MERITAS®
LAW FIRMS WORLDWIDE

A GLOBAL ROADMAP TO PERSONAL DATA PROTECTION

Asia Pacific, Europe & USA

Dennis Unkovic, Editor

du@muslaw.com
Tel: +1-412-456-2833

Meyer, Unkovic & Scott LLP
www.muslaw.com

Not so long ago, "data protection" meant a locked filing cabinet and a good shredder. No longer. In a single generation, protecting data went from safeguarding documents to securing information of almost every kind, both tangible and in electronic form. Although everyone understands what it means to protect a hard copy document, it is much harder to conceptualize protecting intangible information. To make matters worse, a data breach today can cause far more serious consequences than in years past. To cite just one example, the improper disclosure of one's personal data can easily result in identity theft, with the victim often left unaware of the crime until it is far too late to stop it.

With the endless march of technology and an increasingly connected world, protecting personal data is clearly more important than ever. In response, governments around the world have focused on enacting legislation to keep up with the fast pace of change. The EU's recent implementation of the General Data Protection Regulation (GDPR) is just the latest development in this crucial area of law. Outside the EU, however, there is little uniformity in how different regions and countries protect personal data. To help make sense of this, Meritas® has produced this guide by leveraging its top quality member firms from around the world, specifically our firms in Asia Pacific, Europe and the USA. The guide employs a straightforward question-and-answer format to be as simple and as easy to use as possible. The authors hope that this guide will provide readers with a convenient and practical starting point to understand a complicated yet vitally important subject to businesses everywhere.

Special thanks go out to Meritas® Board Member Yao Rao (China), who was the inspiration behind this publication, as well as to Meritas® Board Member Darcy Kishida (Japan) and Eliza Tan (Meritas® Asia Regional Representative), who provided crucial support. Without their hard work and dedication, this global look at the critical issue of Data Privacy would not have been published.

ABOUT MERITAS®

Founded in 1990, Meritas® is the premier global alliance of independent law firms working collaboratively to provide businesses with qualified legal expertise. Our market-leading member firms offer a full range of high-quality, specialized legal services, allowing you to confidently conduct business anywhere in the world.

As an invitation-only alliance, Meritas® firms must adhere to our uncompromising service standards to retain membership status. Unlike any other network or law firm, Meritas® collects peer-driven reviews for each referral, and has for more than 25 years.

7,500+ EXPERIENCED LAWYERS

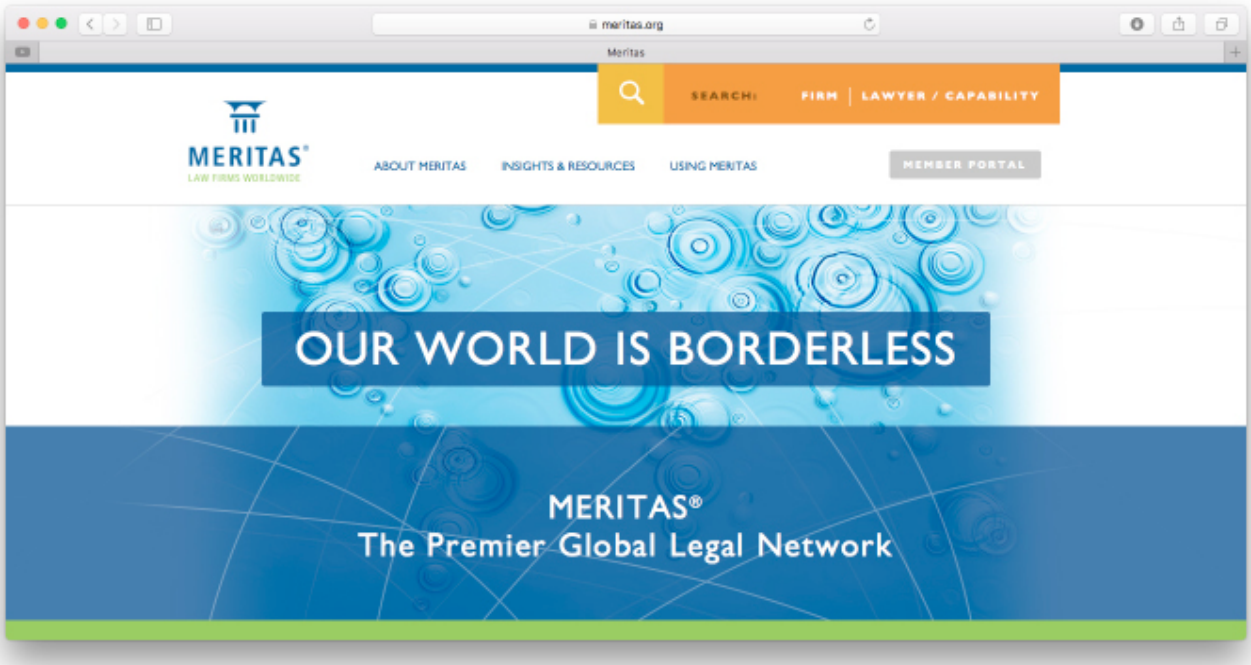
90+ COUNTRIES

180+ LAW FIRMS

240+ GLOBAL MARKETS

Using this exclusive ongoing review process, Meritas® ensures quality, consistency and client satisfaction.

With 180+ top-ranking law firms spanning more than 90 countries, Meritas® delivers exceptional legal knowledge, personal attention and proven value to clients worldwide.



For more information visit:

MERITAS®
LAW FIRMS WORLDWIDE

www.meritas.org

MERITAS®
LAW FIRMS WORLDWIDE

JAPAN

FIRM PROFILE:

Kojima Law Offices

Kojima Law Offices (KLO) handles all types of commercial transactions and corporate legal matters, including assisting American, European and other foreign corporations and individuals with inbound investments. We guide our clients through the intricacies of doing business in Japan's unique legal and business culture.

KLO assists clients in a broad range of areas, including Foreign Direct Investment (FDI) for Japan-bound investors. For over three decades, KLO has guided a wide variety of foreign clients—from an international beverage company to foreign governments to start-up businesses—to successfully establish operations in Japan. In the early 1990s, KLO was the first law firm to establish a legal mechanism to assist Japanese companies investing in India. KLO has extensive experience establishing joint ventures, creating strategic alliances, and handling mergers and acquisitions. We work with foreign companies to solve day-to-day problems, including regulatory compliance and employment issues.

With its strong litigation department, KLO has represented foreign governments before the Japanese courts, and has extensive experience representing both Japanese and foreign clients in international arbitrations.

CONTACT:

HIROMASA OGAWA
ogawa@kojimalaw.jp

DARCY KISHIDA
kishida@kojimalaw.jp

+81-3-3222-1401
www.kojimalaw.jp/en

Introduction

In 2016, Japan significantly amended its Personal Information Protection Act almost a decade and a half after its enactment in 2003 (the act went into full effect on May 30, 2017). The amendment was part of a global push to protect personal information, especially in response to the EU's General Data Protection Regulation (GDPR). In addition, Japan needed to update the law to cover such new developments as IoT (Internet of Things) and big data. One of the objectives of the amendment was to convince the EU to formally recognize Japan as providing "essentially equivalent" data protection as EU countries do. This status would allow EU countries to share personal data with Japan without requiring any further safeguards. Japan and the EU recently agreed on a framework that should pave the way for the EU to provide Japan with formal recognition as early as this fall.

1. What are the major personal information protection laws or regulations in your jurisdiction?

Japan's main personal information protection law is the Act on the Protection of Personal Information. In order to flesh out the act, Japan has issued general guidelines clarifying how the act applies in a variety of business areas. In addition to these general guidelines, there are specific guidelines covering the following seven business areas: (1) Financial services; (2) Medical services; (3) Telecommunications; (4) broadcasting; (5) Postal services provided by Japan Post; (6) Letter delivery services; and (7) Personal genetic information. A company that provides any of the seven services in Japan will therefore need to comply with the act itself, the general guidelines, and the specific guidelines.

2. How is personal information defined?

The act defines "personal information" as either: (1) Information about a living individual that contains a name, date of birth, or other description that can identify a person (including separate pieces of information that can collectively identify an individual); or (2) Information containing the unique individual identification number that the government issues to all residents of Japan (this is analogous to social security numbers in the US). The "other description" in (1) means anything stated, recorded or otherwise expressed through voice, motion or other methods in a document, a drawing, or in electronic form.

Because the act specifically applies to "living individuals", it does not protect information of the deceased, nor does it protect a corporation's information. On the other hand, because the act protects information that can identify a specific individual, fingerprints, irises and specific DNA sequences may be protected as personal information.

An example of how separate pieces of information can collectively identify an individual can be seen in the unique numbers that some companies assign to their customers as part of the product registration process. When customers register products with a company, they typically provide the company with certain information such as their name, address, and telephone number. Many companies use this information to create a customer database to notify customers about new products or special offers. Because this unique number is linked to the customer's personal information, the act considers the number itself to be personal information.

3. What are the key principles relating to personal information protection?

The key principle of the act is balancing the obvious usefulness of personal information with the need to protect it. This balance is evident in the act itself. For example, the act acknowledges that the use of personal information can be helpful in providing society with a variety of useful goods and services. At the same time, the act recognizes that in an advanced information society, there is a risk of serious human rights violations resulting from the improper use of personal information. The act therefore requires that personal information be stored and handled appropriately.

4. What are the compliance requirements for the collection of personal information?

The act obviously prohibits using deceptive or inappropriate means to obtain an individual's personal information. Beyond that, the act requires either informing individuals themselves how their data will be used, or disclosing the use of the data to the general public (As discussed in more detail below in Question 5).

In addition, the act recognizes a special class of personal information that requires an individual's prior consent before it can be obtained. This information includes a person's race, religion, ideology, social status, medical history, criminal record, and the fact that one has been the victim of a crime.

Protecting information about one's "social status" may seem odd to non-Japanese because social status typically refers to a person's overall position in society as determined by one's wealth, job, and education level, factors not easily captured in a single data point. However, the act specifically includes "social status" in order to protect certain groups of people in Japan who have historically faced unique forms of discrimination as a result of being born into a certain class.

5. What are the compliance requirements for the processing, use and disclosure of personal information?

Main Requirements

The act requires identifying in as much detail as possible how personal information will be used. This step needs to be taken at the time the personal information is obtained. Once obtained, the personal information must be used within a reasonable scope of the disclosed use. If the scope of use is changed in any meaningful way, individuals must be informed of those changes, either individually or through public disclosure. These requirements also apply when a company acquires personal information from another company as part of a merger or similar action. In that case, the acquiring company can use the personal information only to the extent that the company being acquired was authorized to prior to the merger.

To illustrate how the "reasonable scope" use requirement can apply in practice, suppose a company obtains a customer's contact information and specifically informs the customer that they will use that information only for product maintenance and repair. If the company subsequently uses that information to contact the customer to promote a new product or service, the company would be in violation of the act because the promotion is not reasonably related to maintaining or repairing the product. The company would need to obtain consent from the relevant individuals if it wanted to expand the scope of use beyond the original purpose of maintenance and repair.

It may happen that a company inadvertently fails to identify how it will use the personal information and/or fails to notify the relevant individuals about that use at the time it obtains the information. If so, the company is required to rectify the failure either by promptly informing the individual how it will use the information, or by promptly making the required public disclosure, e.g., by explaining on its homepage how it will use the personal information.

Personal Information in Contracts

The act protects personal information contained in contracts. Specifically, the use of any personal information obtained through entering into a contract with an individual is permitted, but only if that individual is explicitly informed in writing how that information will be used. The personal information covered by this requirement is not limited to information contained in the contract itself, but also includes information that may be found in related documents.

Duty to Keep Personal Information Accurate and Up-To-Date

Moreover, the act requires holders of personal information to endeavor to keep that information accurate and up to date to the extent necessary in light of how that information is being (or will be) used. For example, whenever an employee provides their company with their new residential address, the company is required to update its list of employee addresses. In addition, personal information must be

promptly deleted when the holder of that information no longer needs it. For instance, a company hosting a sporting event may obtain an attendee's personal information solely to verify that customer's identity when the customer enters the venue where the event is being held. In that case, the company will be required to delete the customer's information after the event ends.

Duty to Keep Personal Information Secure

Lastly, the act requires holders of personal information to take any necessary and appropriate steps to keep that personal information secure, including preventing the information from being lost, damaged, or improperly disclosed. Under the act and the guidelines, some of these steps include: (1) Employee education and training in how to appropriately and safely handle personal information; (2) Implementing and, when necessary, improving an organization's internal regulations for the protection of personal information; and (3) Introducing and using technical measures such as technological restrictions on the access to information, and countermeasures to guard against malware and other malicious software.

6. Are there any restrictions on personal information being transferred to other jurisdictions?

The act does not specifically address the transfer of personal information to other jurisdictions. As a result, the act treats those transfers the same as it treats transfers within Japan. Therefore, an individual's prior consent is generally required to provide personal information to a third party in a foreign country. This consent can be obtained as part of the consent requirement described above in the response to Question 5. However, prior consent is not required if providing the personal information to a third party in a foreign country:

(1) Is required by that country's laws and regulations;

(2) Is necessary to prevent death, injury, or property damage, and it is difficult to obtain the individual's consent; and

(3) Is necessary to improve public health or to promote the welfare of children, and it is difficult to obtain the individual's consent.

These exceptions apply equally to personal information transferred within Japan.

7. What are the rights of an individual whose personal information is collected? Can he/she withdraw the consent to the retention of his/her personal information by a third party, and if so, how?

The act gives individuals three basic rights in connection with their personal information. First, the act allows an individual to require a company to disclose any personal information that the company has on them. If the company receives such a request, the company is required to promptly disclose that personal information to the person making the request. Second, an individual has the right to have any incorrect personal information corrected. Third, if an individual's personal information is being handled in violation of the act, that person has the right to force a company to either stop using or to delete the individual's personal information.

8. Is an employee's personal information protected differently? If so, what's the difference? Apart from the personal information of employees, are there any other types of personal information that receive special protection?

The act does not offer an employee's personal information any special protection, except to the extent that the information constitutes the special class of personal information discussed above in the response to Question 4.

9. Which regulatory authorities are responsible for implementation and enforcement of personal information protection laws in your jurisdiction?

The amended act made the Personal Information Protection Commission the exclusive authority to handle matters involving the protection of personal information. Their website provides information on

whether any special guidelines apply to a given business in Japan (see https://www.ppc.go.jp/en/).

10. Are there any penalties, liabilities or remedies if any of the personal information protection laws is violated?

There are penalties for violating the requirements of the act. For example, knowingly selling a database of personal information to a third party without obtaining the required consent is punishable by up to one year imprisonment or a fine of up to 500,000 yen. A holder of personal information that fails to follow an order issued by the Personal Information Protection Commission to protect that information faces up to six months imprisonment or a fine of up to 300,000 yen.

It is the usual practice of the Japanese authorities to first issue "administrative guidance" to violators, especially first-time violators. This administrative guidance is essentially a warning, as the authorities generally avoid imposing penalties without first giving the violator a chance to resolve any issues that caused the violation. Typically, only if the violator fails to comply with the administrative guidance do the authorities impose penalties. Of course, the only way to completely eliminate the risk of punishment is to strictly comply with the law.

11. Is your jurisdiction planning to pass any new legislation to protect personal information? How is the area of personal information protection expected to develop in your jurisdiction?

As noted above, the act went into full effect just last year on May 30, 2017. As a result, there are no revisions currently planned.

Conclusion

The Japanese Personal Information Protection Act and related rules should be viewed as an opportunity instead of an obstacle. For starters, the act does not prohibit the use of personal information, nor does it make using that information especially onerous. The act instead provides reasonable protections for individuals, which is especially important in an era where information can easily be disseminated and abused. In this way, the law balances the need for privacy with the benefits of data usage. As a result, one should not fear using personal information as long as that information is used responsibly and in compliance with the act. Furthermore, if the act manages to achieve its goal of having the EU formally recognize Japan as providing adequate data protection, that recognition should in turn promote greater cross-border sharing of data and increased business opportunities.

Authors: Osamu Ishida and Darcy Kishida

Prepared by Meritas Law Firms

Meritas is an established alliance of 180+ full-service law firms serving over 240 markets – all rigorously qualified, independent and collaborative. Connect with a Meritas law firm and benefit from local insight, local rates and world-class service.

www.meritas.org enables direct access to Meritas law firms through a searchable database of lawyer skills and experience.

MERITAS®
LAW FIRMS WORLDWIDE

www.meritas.org

800 Hennepin Avenue, Suite 600
Minneapolis, Minnesota 55403 USA
+1.612.339.8680