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.

TABLE OF CONTENTS

Please be aware that the information on legal, tax and other matters contained in this book is merely descriptive and therefore not exhaustive. As a result of frequent changes in legislation and regulations from country to country, the situations as described throughout this book do not remain the same. Meritas® cannot, and does not, guarantee the accuracy or the completeness of information given, nor the application and execution of laws as stated.

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

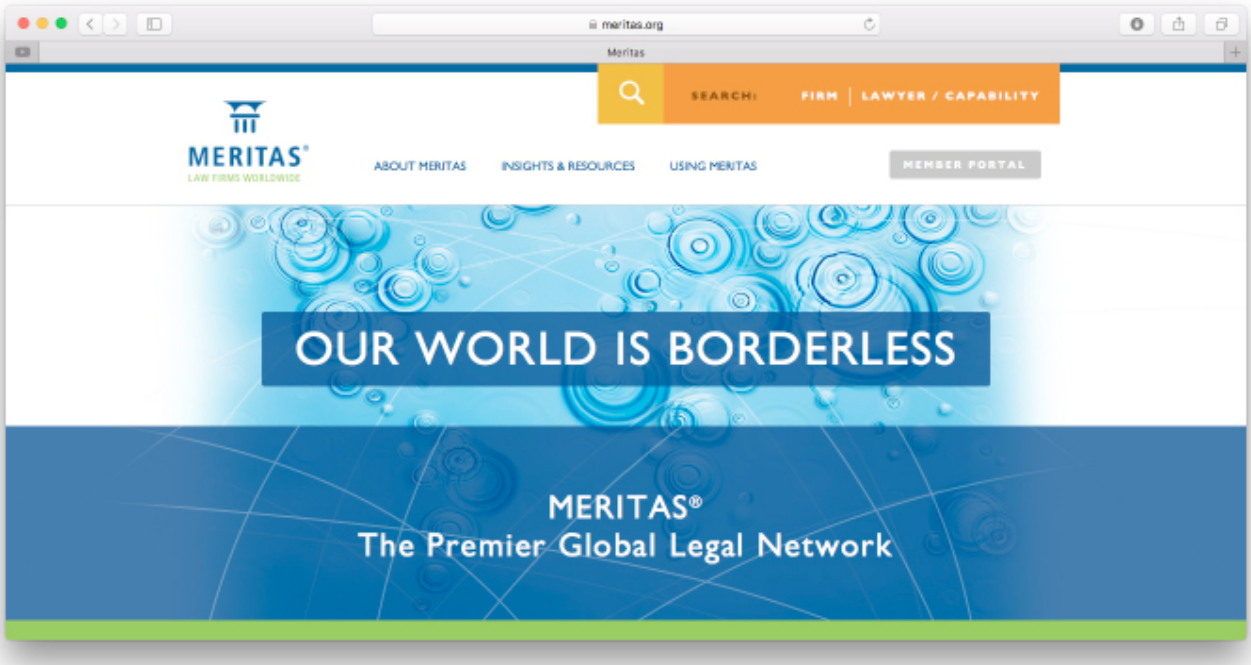
90+ COUNTRIES

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

CHINA

FIRM PROFILE:

汇 衡 律 师 事 务 所
HHP ATTORNEYS-AT-LAW

HHP Attorneys-at-Law is a law office on the frontier of providing its clients, both home and abroad, with professional solutions to help them achieve the best possible commercial outcome.

HHP has a corporate culture with a fully integrated team approach, under which specialist services are provided under a partner-hands-on working style. With an abundance of experience in our respective areas, we fully understand our clients' commercial needs, such that we are capable of creating innovative solutions for even the most discerning demands.

HHP primarily focuses on investment and financing, compliance and risk control, and dispute resolution. With a keen eye on the latest legal developments in China, we are known for developing unique perspectives on such legal matters as antitrust, taxation, employment, cross-border investment and finance. We have also actively participated in the promulgation of laws by relevant legislative agencies. Our ample experience has directly contributed to our vast exposure in the fields of banking, insurance, securities, trust, real estate, construction and infrastructure, pharmaceuticals, automobiles, commercial retail, Internet, education, food and mining among others.

CONTACT:

YAO RAO
yao.rao@hhp.com.cn

JINGDONG XU
jingdong.xu@hhp.com.cn

+86-21 5047 3330
www.hhp.com.cn

Introduction

Personal information protection does not have a long history in the Chinese legal system, but it is now one of the hottest legal topics in China. The legislation contains some broad, and sometimes confusing, definitions in respect of personal information protection. It also involves stringent regulations and severe legal penalties. The Chinese government is still exploring a feasible way to implement the relevant legal requirements, and this delays the process of issuing the implementing rules.

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

In China, laws protecting personal information mainly include:

(1) *The General Rules of the Civil Law of the PRC* (the "Civil Law"), which generally grants natural persons the right to the legal protection of their personal information;

(2) The *Criminal Law of the PRC and its Amendment VII and Amendment IX* (the "Criminal Law"), which govern the crime of illegally collecting or providing personal information;

(3) The *Cybersecurity Law of the PRC* (the "Cybersecurity Law"), only applying to network operators which are broadly defined as those who own, manage or provide service on networks (the "Network Operators"); and

(4) The *Consumer Rights Protection Law of the PRC* (the "Consumer Rights Protection Law"), only applying to business operators who sells products or services to consumers (collectively with Network Operators referred to as "Operators").

There are also some recommendatory national standards (GB/T) and technical guidance documents (GB/Z) already in place, which set forth more strict and detailed personal information protection requirements than the laws, but these standards or documents are not mandatory, such as the national standard *Personal Information Security Specification* (GB/T 35273-2017).

2. How is "personal information" defined?

Under the Cybersecurity Law and the regulations related to the Consumer Rights Protection Law, "personal information" means all kinds of information, whether electronically or otherwise recorded, that can be used separately or in combination with other information to identify a natural person. With this definition, the scope of personal information includes, for example, the name, date of birth, identity certificate number, personal biological identification information, addresses, telephone numbers, account names and passwords, property status, location, whereabouts, health and consumption activities of a natural person.

However, from the judicial view of enforcing the Civil Law and the Criminal Law, "personal information" is defined in a broader way. It embraces not only the information that is able to be used to identify a natural person but also all kinds of information reflecting the activities of a natural person, including information that involves personal privacy.

As shown in the above definitions, personal information protected by law means the information related to a natural person but excludes the information of corporations, companies, partnerships or other legal entities.

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

The Chinese laws explicitly establish the following key principles which, shall be obeyed in the course of collection, processing and use of personal information:

(1) **Lawfulness**. Personal information shall be collected, used, stored and processed in compliance with laws and administrative regulations.

(2) **Fairness**. The laws provide no official explanation for what "fairness" means. However, it should be understood that the principle of "fairness" may inherently embody, among other things, the requirements that the collection and use of personal information should be for a reasonable and justifiable purpose, and follow right and appropriate procedures.

(3) **Necessity**. As one of the requirements of the principle, Network Operators shall not collect personal information irrelevant to the services provided by them.

Apart from the above three principles, there are other important principles which may be implied by detailed compliance requirements, including information integrity and confidentiality protection, procedural transparency, accountability and so forth.

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

Under the Chinese laws, the collection of personal information, especially by Operators, shall comply with the following requirements:

(1) The personal information shall be collected with the consent of the information subject, before which the collection and use rules shall be publicly available, and the purposes, manners and extent of the personal information collection and use shall be explicitly noticed to the information subject;

(2) The personal information collected shall be limited to the information relating to the services provided or to be provided by the information collector;

(3) The personal information shall not be stolen, illegally bought, obtained by fraud, or otherwise collected in violation of the laws and administrative regulations; and

(4) The collection of the personal information shall be not in breach of any agreements with the information subject or the information provider.

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

The processing and use of personal information, especially by Operators, shall be in accordance with any agreements with the information subject or the information provider. The Operators are prohibited from sending commercial messages to a recipient by using the recipient's email address, phone number or other channels without the recipient's consent or request.

Operators are also legally obliged to protect the integrity and strict confidentiality of the personal information they collect, for which purpose the Operators shall:

(1) Not divulge, illegally sell or otherwise provide, tamper with or damage the personal information;

(2) Not disclose to any third party the personal information without the consent of the information subject, unless the information has been irreversibly anonymized or otherwise processed so that the information cannot be used to identify a natural person anymore;

(3) Establish a sound system and take necessary measures to ensure the security of the personal information; and

(4) In a situation where the personal information is or might be divulged, damaged or lost, take remedial measures immediately, notify their users of the situation in a timely manner and report the same to relevant competent authorities.

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

The existing laws and regulations in China impose no restriction or prohibition on personal information being transferred to other jurisdictions except for the following special personal information:

(1) The personal information collected or generated in China in the operation of critical information infrastructures (the "CII") shall be stored within China, and shall not be transferred outside of China unless a prior security assessment by the competent authorities has been passed. Under the Cybersecurity Law, the CII means the information infrastructures in the critical industries and fields such as public communication and information services, energy, transportation, water resources, finance, public services and e-government, and the information infrastructures

of which the damage, function loss or data leakage may endanger national security, people's livelihood or the public interest. The definition of the CII is broad and inclusive, however currently there is no practical rule or guidance in effect establishing how to identify a CII.

(2) The personal financial information collected by banking institutions, like assets, bank accounts, credit data and investment history of a natural person, shall be stored and processed only within China, unless otherwise provided by laws or regulations or the People's Bank of China.

(3) The personal information collected by online car hailing service providers shall be stored and used only within China, unless otherwise provided by laws or regulations.

(4) Other personal information that involves state secrets or that may affect the state economic security.

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?

In addition to the above rights, individuals also have the following rights under the Cybersecurity Law:

(1) **Erasure Right**. If Network Operators collect or use personal information of any individuals in violation of laws or administrative regulations or in breach of their agreement with the individuals, the individuals are entitled to require the Network Operators to erase their personal information.

(2) **Rectification Right**. Individuals are entitled to require relevant Network Operators to rectify any error in their personal information.

(3) **Right to Complaint**. The Network Operators shall establish a complaint system for their users, and the users have the right to obtain timely responses to their complaints from the Network Operators.

The individual users, to whom telecommunication services including Internet information services (the "Telecom Services") are provided, also have the right to cancellation of their phone numbers or accounts if they cease to use the Telecom Services.

Despite the above rights, no existing laws or regulations expressly provide any individuals with rights to withdraw their consent to collection, use or processing of their personal information. However, the withdrawal rights are recommended by the national standard GB/T 35273-2017; if any Operator is voluntarily committed to giving the withdrawal rights to its individual users, like WeChat, Taobao, and DiDi Chuxing did, its users may withdraw their consent as promised.

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?

There is no difference in personal information protection between an employee and any other person. No employer shall illegally collect, use, process, buy or sell, provide or publicly disclose any personal information of its existing or potential employees. If the employer applies an information system on an intranet or the Internet to manage its employees, the Cybersecurity Law may be applicable for the employer with respect to the personal information collected by it.

Except for the above, we see no other special legal protection for certain types of personal information.

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

In China, several governmental authorities, instead of a centralized agency, are simultaneously empowered to regulate and supervise the personal information protection in different respects, whose functions and authority may overlap each other. Those regulatory authorities mainly

include the following:

(1) **The Office of the Central Cyberspace Affairs Commission, namely the Cyberspace Administration of China, and its local offices**. Responsibilities - Coordination in supervision and regulation of cybersecurity, and management of the Internet information content. Contact - Hotline: 12377. Address: No. 11 Chegongzhuang Avenue, Xicheng District, Beijing 100044, China

(2) **The Ministry of Industry and Information Technology of the PRC and its local offices**. Responsibilities - Supervision and regulation of personal information protection regarding Telecom Services. Contact - Tel: 010- 68206133 Address: No. 13 West Chang'an Avenue, Beijing 100804, China

(3) **The State Administration for Market Regulation and its local offices**. Responsibilities - Supervision and regulation of protection of personal information of consumers. Contact - Hotline: 12315. Address: No. 8 East Sanlihe Road, Xicheng District, Beijing 100820, China

(4) **The People's Bank of China and its local offices**.

Responsibilities - Supervision and regulation of protection of personal financial information. Contact - Tel: 021-58845000. Address: No. 181 Lujiazui East Road, Pudong New District, Shanghai 200120, China.

(5) **The Ministry of Public Security of the PRC and its local offices**. Responsibilities - Investigation, detention, execution of arrests and preliminary inquiry in criminal cases regarding personal information; and public security administration regarding personal information. Contact - Hotline: 110. Address: No. 14 East Chang'an Avenue, Beijing 100741, China.

Apart from the above governmental authorities, the Procuratorates of all levels are responsible for procuratorial work, approval of arrests and initiating public prosecution of criminal cases regarding personal information, and the Courts of all levels are responsible for adjudication of all kinds of cases regarding personal information.

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

Any entity or individual who violates any of the personal information protection laws shall bear the following liabilities:

(1) **Civil Liability**

If personal information rights or privacy rights of individuals are infringed, the individuals may claim tort liability against the tortfeasor or if there is a relevant contract, claim liability for breach of the contract against the breaching party, by filing an arbitration or lawsuit.

In this civil case, the tortfeasor or the breaching party may be liable for, as the case may be,

- Ceasing the infringement;
- Eliminating any adverse impacts;
- Restoring the individual's reputation;
- Making an apology;
- Continuing to perform the contract;
- Taking remedial measures;
- Compensating for loss; and
- Other civil liabilities.

(2) **Administrative Liability**

If Operators violate the personal information protection laws or regulations, the competent authorities may impose administrative liabilities and penalties, mainly including the following on the Operators:

- Rectification of the violation;
- Warning;
- Confiscation of illegal gains;
- A fine not less than one time but not more than ten times the illegal gains, or if no illegal gains occur, a fine of up to RMB 1,000,000;
- Cessation of business for rectification;
- Closing of relevant websites;
- Keeping in credit records and publicly announcing the violations;
- Revocation of the business license or relevant business permits/fillings; and/or
- Detention of up to 20 days.

(3) **Criminal Liability**

Any entity or individual who

sells, illegally provides, steals or otherwise illegally obtains the personal information of others, in a severe case, may commit a crime of infringing personal information, and consequently imprisonment for up to 7 years and/or a fine may be imposed as a criminal penalty.

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?

The Chinese government is contemplating tougher and more comprehensive regulations and rules on personal information protection. For example, the following laws and regulations have been drafted and are currently under discussion:

(1) *The Measures for the Security Assessment of Personal Information and Important Data to be Provided Overseas* (Draft for Public Comments) dated 11 April 2017, which is to establish the principle that all the personal information collected in China by the Network Operators, not limited to the CII Operators, shall be stored within China, unless a prior security assessment has been passed.

(2) *The Regulation on Protection of Juveniles on Networks (Draft for Review)* dated 6 January 2017, which aims to provide special personal information protection for juveniles.

Conclusion

The personal information protection legislation in China is still in its early stage, and it remains to be seen how the personal information protection will be required and implemented in practice. For now, it is advisable for players in China's markets to keep a close watch on the rapidly changing and evolving legislation in China and get ready for the probably tougher and more comprehensive regulation and supervision on personal information protection.

MERITAS®
LAW FIRMS WORLDWIDE

HONG KONG

FIRM PROFILE:

Gallant

何 耀 棣 律 師 事 務 所

Our firm was established in 1977 and is one of the largest and most well-known local firms in Hong Kong with about 40 lawyers. We offer comprehensive legal services to individuals and corporate clients, covering various commercial, corporate and property related activities both contentious and non-contentious, ranging from banking finance, joint venture to project finance, mergers and acquisitions to listing of companies in Hong Kong.

Apart from banking, real estate and dispute resolution work, which have always been the backbone of our services, we are particularly noted for our cross-border legal services between Hong Kong and Mainland China.

Hong Kong is the common law jurisdiction most preferred by both foreign and Mainland Chinese investors and enterprises for in-bound and out-bound investments to and from Mainland China, in particular using Hong Kong corporate vehicles as a base for fund raising.

Our firm with over four decades of experience in cross-border work is in a privileged position to serve as a bridge for the foreign investors and enterprises in Mainland China.

CONTACT:

PHILIP WONG
philipwong@gallantho.com

BRENDA LEE
brendalee@gallantho.com

+852 2526 3336
www.gallantho.com

Introduction

Personal information is protected by the Personal Data (Privacy) Ordinance, Chapter 486, Laws of Hong Kong, enacted in 1995. It protects the whole lifecycle of personal data from their collection to destruction. The legislation obliges data users to comply with the six data protection principles (discussed below) and gives a data subject a right to know what personal data is held about them.

The Ordinance protects the privacy of individuals in relation to personal data, rather than the privacy of individuals generally. Other types of privacy interests extend beyond the scope of the Ordinance, such as the interest in controlling entry to one's personal territory, the interest in freedom from interference with one's personal privacy, and the interest in freedom from surveillance or interception of one's communications.

The law applies only to data users, not data processors. This means that where a data processor is retained by the data user, the obligation to comply with the law remains with the data user.

The Ordinance was amended in 2012 to tighten regulation of corporate data users on the application of customers' personal data in direct marketing to and sharing data with third parties. A data user may share with third parties the personal data collected for use in direct marketing only if—(a) it gives the prescribed information in writing to the data subjects, including the kinds of personal data to be used or provided, the classes of marketing subjects for which the data will be used for direct marketing, and (where appropriate) the classes of persons to whom it be provided for direct marketing purposes; and (b) the date subjects reply in writing indicating their consent or no objection. If the personal data is shared for profit, the data user must inform the data subject in writing. Data subjects may at any time require a data user to cease to use their personal data or share it with third parties for use in direct marketing. Upon the receipt of a request to cease to share personal data, the data user must notify any person with whom the data has been shared. Under the provisions as amended in 2012, the first person convicted was a real estate agent who obtained the complainant's name and mobile phone number in a social function. Without seeking the complainant's consent, he gave the name and phone number to a financial planner of an insurance company, who later contacted the complainant to market insurance products. The real estate agent was convicted for a criminal offence and fined.

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

The major personal information protection legislation in Hong Kong is the Personal Data (Privacy) Ordinance. In addition, there are various codes of practice issued pursuant to the Ordinance. The provisions of the codes of practice are not legally binding. A breach of a mandatory provision of the codes of practice by a data user, however, will give rise to a presumption against the data user in any legal proceedings under the Ordinance.

2. How is personal information defined?

Under the Personal Data (Privacy) Ordinance, "data" means "any representation of information (including an expression of opinion) in any document, and includes a personal identifier"; "personal data" means "any data—(a) relating directly or indirectly to a living individual; (b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and (c) in a form in which access to or processing of the data is practicable"; and "personal identifier" means "an identifier that is assigned to an individual by a data user for the purpose of the operations of the user; and that uniquely identifies that individual in relation to the data user, but does not include an individual's name used to identify that individual". The definitions are limited to the personal data of individuals. Information identifying legal entities such as corporations and companies is not included in the definition, but information identifying individual partners of a partnership is included.

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

The legislation protects personal data during their whole life cycle from their collection to destruction. It obliges data users to comply with six data protection principles, discussed in the answers to Questions 4 and 5 below. It protects the privacy of individuals in relation to personal data, rather than to protect the privacy of individuals generally. Any person, including the private sector and government departments, who controls the collection, holding, processing or use of the personal data must comply with the principles.

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

Personal data must be collected in a lawful and fair way for a legitimate purpose directly related to a function or activity of the data user. Data subjects must be notified of the purpose and the classes of persons to whom the data may be transferred. They must also be notified whether it is obligatory to supply the data and if so, the consequences of refusal. The data collected should be necessary but not excessive. For example, an individual's date of birth should not be requested when all is needed is the age range of the respondent or a declaration that he/she is over a certain age. "Collection" of data has been judicially interpreted: a person (a collector) is collecting personal data only if he or she is thereby compiling information about a living individual whom the collector has identified, or intends or seeks to identify. The identity of that living individual must be an important item of information to the collector.

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

Personal data must be accurate. It must not be kept for longer than necessary to fulfil the purpose for which it is collected and used. Personal data must be used for the specified purpose or a purpose directly related to it, unless voluntary and explicit consent with a new purpose is obtained from the data subject. There must be measures against unauthorized or unlawful access, processing, erasure, loss or use of personal data. There must be measures to make personal data policies and practices known to the public regarding the types of personal data it holds and how the data is used. Data subjects must be given access to their personal data and allowed to make corrections.

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

Where a data user engages a data processor, whether within or outside Hong Kong, to process personal data on the data user's behalf, the data user must adopt contractual or other means to prevent any personal data transferred to the data processor from being kept longer than is necessary for processing of the data, and to prevent unauthorized or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing. A data processor is defined to mean a person who processes personal data on behalf of another person; and does not process the data for any of the person's own purposes.

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?

Individuals have the right to:

(1) Make a data access request and know the reason for the refusal to such request;

(2) Request the correction of incorrect data and know the reason for the refusal to such request;

(3) Request the erasure of incorrect data;

(4) Require that their personal data is not used for direct marketing;

(5) Make a complaint to the Privacy Commissioner for Personal Data about any contravention of the legislation;

(6) Claim compensation in civil

proceedings where they have suffered damage as a result of a data user's failure to comply with the legislation and may ask the Commissioner for assistance in the proceedings; and

(7) Withdraw their consent to the retention of their personal information by a third party by informing the data user (ie, the person who collected their data) of their withdrawal.

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?

Employees are protected by the same legislation and data protection principles. Among the various codes of practice and guidelines issued pursuant to the Ordinance (see the answer to Question 1 above), there are some on human resource management and personal data privacy at work, providing specific guidelines on the protection of employees' personal information. There are other codes and guidelines on specific trades (eg, property management, banking industry, insurance industry, etc) or types of data (eg, consumer credit data, biometric data, etc).

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

The Privacy Commissioner for Personal Data is an independent statutory body set up to oversee and enforce the implementation of the legislation. The Commissioner investigates complaints and tries to resolve disputes through conciliation. Members of the public who wish to make an enquiry or lodge a complaint to the Commissioner should proceed to its office at Room 1303, 13/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong and/or reach them by email at enquiry@pcpd.org.hk. Further details of the Commissioner can be found on the website at https://www.pcpd.org.hk/.

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

The Privacy Commissioner for Personal Data has the power to issue enforcement notices, directing a person in breach of a requirement under any data protection principle to take steps to remedy and prevent any recurrence of the contravention. Contravention of an enforcement notice or intentionally doing the same act or making the same omission specified in the enforcement notice is an offence, which may result in a fine and imprisonment. Disclosing any personal data obtained from individuals without their consent with the intention to obtain gain in the form of money or other property or to cause loss to them is an offence. Furthermore, any such disclosure causing psychological harm to them is also an offence. In addition to criminal liability, a person in breach of the legislation may be faced with a civil claim. If necessary, the Commissioner may grant legal assistance to the aggrieved individual who intends to institute civil proceedings to seek compensation.

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?

There is no proposed legislation published at the moment. However, the new GDPR of the EU applies to data controllers and data processors without an establishment in the EU, so long as they offer goods or services to data subjects in the EU or monitor their behaviours in the EU. It has legal ramifications over businesses and individuals in Hong Kong, an international city having numerous multinational corporations and expatriates living and working here.

Conclusion

Data users should familiarize themselves with the Personal Data (Privacy) Ordinance, codes of practice, guidelines and guidance notes, all of which can be found

on the website of the Privacy Commissioner for Personal Data at https://www.pcpd.org.hk. The six data protection principles are the central feature of the Ordinance. Codes of practice are not legally binding, but any breach will give rise to a presumption against a data user in any legal proceedings under the Ordinance. Where it is essential to prove a contravention of the law, there is a rebuttable presumption that it is proved if the code of practice has not been observed. The presumption may be rebutted if there is evidence that the requirement under the Ordinance was actually complied with in a different way. Unlike the codes of practice, guidelines and guidance notes only indicate the manner in which the Privacy Commissioner proposes to perform its functions or exercise its powers under the law. They represent the best practices in the opinion of the Privacy Commissioner, but any breach will not necessarily give rise to legal liability or presumption.

Author: Walter Lee

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

MERITAS®
LAW FIRMS WORLDWIDE

PHILIPPINES

FIRM PROFILE:

ACCRALAW®

Angara Abello Concepcion Regala & Cruz Law Offices (ACCRALAW) is a leading full service Firm with about 150 lawyers. For 2017, it was recognized as an Outstanding Firm by Asialaw Profiles, Top Tier by the Legal 500, and Top Ranked by Chambers, Asian Mena Counsel, and Asian Business Law Journal. Its main offices are located at the ACCRALAW Tower in the newly developed Bonifacio Global City in Metro Manila. It has full service branches in the thriving commercial centers of Cebu City in the Visayas and Davao City in Mindanao. The Firm has an excellent track record in handling diverse, significant, and complex business projects and transactions for both local and multinational clients, and has been involved in landmark litigation cases.

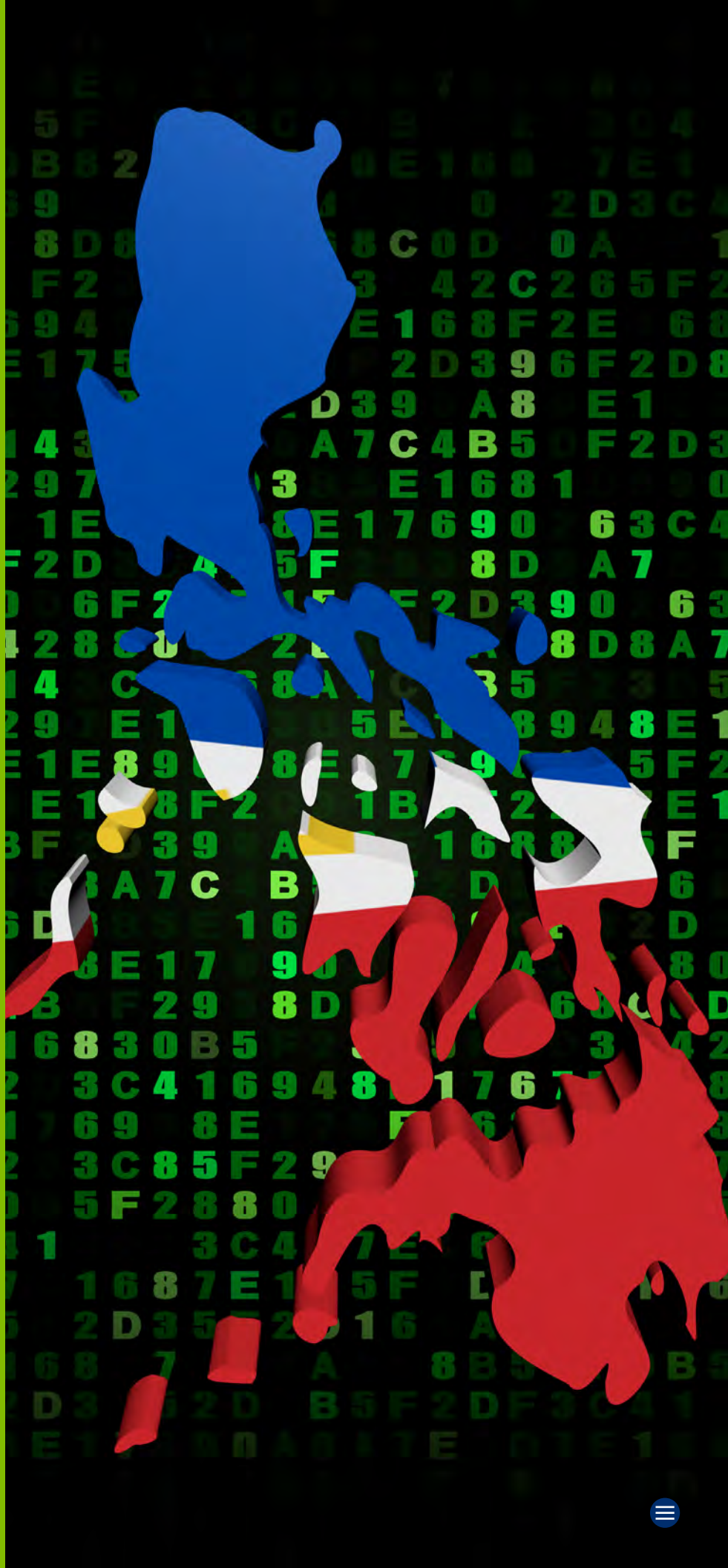
ACCRALAW's clientele represents the full spectrum of business and industry, and includes professional organizations and individuals. Servicing the Firm's clients are seven practice departments and its two branches, which offer timely, creative, and strategic legal solutions matched with cost-efficient administration and expert handling of clients' requirements.

CONTACT:

EMERICO O. DE GUZMAN
eodeguzman@accralaw.com

REGINA PADILLA-GERALDEZ
rpgeraldez@accralaw.com

+63 2 830 8000
www.accralaw.com



Introduction

The Data Privacy Act of 2012 or Republic Act No. 10173, with its Implementing Rules and Regulations, was promulgated in response to the freer exchange of personal data in the global stage and the setting of international standards for data protection. Prior to the Act, without so much as regulatory oversight for data collectors or protective measures for the data subject, the wealth of personal data available is subject to abuse and misuse — from the unmitigated use of contact details for purposes beyond those initially contemplated, to identity theft or security breaches of corporate data — to the detriment of the data subject's constitutionally guaranteed right to privacy. As this is a relatively new law in the Philippines and while initial enforcement measures have been implemented by the National Privacy Commission, it remains to be seen how robustly this new area of law will develop in the country.

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

The governing law on personal information protection in the Philippines is the Data Privacy Act of 2012 or Republic Act No. 10173, together with its Implementing Rules and Regulations.

2. How is personal information defined?

Personal information is defined as any information, whether recorded in a material form or not, from which the identity of an individual is apparent by the entity holding the information.[1] For example, if the data collected pertains to his birthdate, address, Social Security number, or employee number, even if the individual is not explicitly named, then each data point (since the identity of the individual will be apparent when these data points are taken in consideration with each other) will be considered as personal data and, thus protected by the Data Privacy Act.

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

Processing of personal information must adhere to the general principles of transparency, legitimate purpose, and proportionality. For example, if the personal data of an individual is being collected for purposes of a conducting a contest wherein an individual will win a raffle prize of a store, then the data subject must be informed that his data is being collected and processed only for the said purpose and will be retained by the store for only as long as necessary to fulfill the contest. The data must not be used for any other purpose (e.g., marketing other products of the store) or kept longer than necessary (e.g., an indefinite period after the contest). The data collected must also be proportionate to the purpose. For example, if the purpose of collecting the data is to identify the winner of the contest, then the individual's name, birthdate, and address should suffice. Considering the purpose of the data collection, there is no need to collect the individual's mother's name, educational attainment, and his current employer, and so doing will violate the principle of proportionality of the Data Privacy Act.

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

The processing of personal information is permitted if not prohibited by law and, generally, when the data subject has given his or her consent. The Data Privacy Act, however, recognizes situations wherein the nature or exigencies of the situation may not accommodate a situation wherein the individual can give his consent but his or her personal data still needs to be processed.[2] A good example of this will be a situation wherein the data subject's health is in danger and the data subject cannot give his or her consent in the form that the law requires (i.e., written). The Data Privacy Act, among other situations, recognizes this exception and allows for processing of personal data even without the data subject's consent.

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

Personal information controllers and personal information processors shall register with the National Privacy Commission their data processing systems or automated processing operations, subject to notification, if it employs at least two hundred fifty (250) employees, or if there is risk to the rights and freedoms of data subjects, or the processing is not occasional, or the processing includes sensitive personal information of at least one thousand (1,000) individuals.

In complying with the DPA-IRR's organizational security measures, the personal information controller must first:

(1) Have a compliance officer or data protection officer who shall ensure compliance with applicable rules and regulations for the protection of data privacy and security;

(2) Have data protection policies which provide for organizational, physical, and technical security measures;

(3) Maintain records that sufficiently describe its data processing system and identify the duties of individuals who have access to personal data;

(4) Hold capacity building, orientation, or training programs for employees who have access to personal data regarding privacy or security policies;

(5) Develop and implement procedures for collecting and processing personal data, access management, system monitoring, and protocols to follow during security incidents or technical problems, for data subjects to exercise their rights, and for a data retention schedule; and

(6) Ensure its contracts with personal information processors also implement the security measures required by the Data Privacy Act of 2012 and its IRR. [3]

Next, in complying with the DPA-IRR's physical security measures, the personal information controller must:

(1) Have policies/procedures to monitor and limit access to, and activities in, room, workstation or facility (including guidelines on use of and access to electronic media);

(2) Design office space and work stations to ensure privacy of processors of personal data;

(3) Define a clear description of duties, responsibilities and work schedules to processors of personal data to ensure only individuals actually performing duties are in the room at the given time;

(4) Implement policies and procedures on the transfer, removal, disposal, and re-use of electronic media; and

(5) Establish policies and procedures on the prevention of the mechanical destruction of files and equipment.[4]

Lastly, in complying with the DPA-IRR's technical security measures, the personal information controller must establish the following:

(1) A security policy with respect to processing personal data;

(2) Safeguards to protect computer networks against unauthorized access or to ensure data integrity and functioning of the system;

(3) The ability to ensure and maintain the confidentiality, integrity, availability, and resilience of their processing systems and services;

(4) Regular monitoring for security breaches, accessing vulnerabilities, and preventive, corrective, and mitigating action against data breaches;

(5) Ability to restore availability and access to personal data in a timely manner;

(6) Processes for testing the effectiveness of security measures; and

(7) Encryption of personal data during storage, transit, authentication process, or any measure that controls and limits access.[5]

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

In cases of "data sharing" agreements, a disclosure or transfer must have been upon the instructions of the personal information controller concerned.

The term excludes "outsourcing", or the disclosure or transfer of personal data by a personal information controller to a personal information processor.[6]

The DPA-IRR provides "General Principles for Data Sharing" and allows processing of personal data collected from a party other than the data subject if the data subject's *informed* consent is obtained.[7] Specifically, the data subject must be informed of the identity of the personal information controller, the purpose of the data sharing, the categories of data that will be collected, the intended recipient of the data, and his rights over his personal data. For example, if the data subject's personal data is collected by his Philippine employer, who is part of an affiliate of companies located in multiple jurisdictions, if the employer decides to transfer his data for storage to one of the affiliates located elsewhere, then the employer must first obtain the data subject-employee's informed consent before doing so.

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 rights of an individual whose personal information is collected, also known as the data subject, are: to be informed that his data is being processed, to know the extent of the processing of such data (e.g., scope, purpose, to whom the data may be disclosed, period for storage), to know their rights to access and correction over the data, to have reasonable access to the data, to dispute inaccuracies or errors in their data, to suspend the destruction of their data, and to be indemnified for damages due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal information.[8]

A data subject may withdraw the consent to the retention of his/her personal information by a third party,[9] although there is no specific process given in the DPA-IRR on withdrawing consent.

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?

Apart from exempting personal information which is necessary and desirable in the context of an employer-employee relationship from the requirement of prior notification before amendment (specifically as to any of the information listed under **Section 16 b of the Data Privacy Act**), an employee's personal information is not treated differently from that of the treatment accorded to personal information in general. However, a class of information that receives special protection is called sensitive personal information, wherein, among others, consent of the data subject must be specific to the purpose of processing.[10] Sensitive personal information refers to personal information:

(1) About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;

(2) About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;

(3) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or **current** health records, licenses or its denials, suspension or revocation, and tax returns; and

(4) Specifically established by an executive order or an act of Congress to be kept classified.[11]

For example, in interviewing applicants for a job, it is not enough to secure the data subject's general consent to collect their personal data and then include their Social Security or Tax Identification number in the collection and processing. The data subject-applicant must be informed, prior to consenting, that his personal and sensitive personal information will be collected and processed for determining his qualifications for the job and

to process employment-related requirements should he or she accept the job offer.

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

The National Privacy Commission is an independent body tasked to administer and implement the provisions of the Data Privacy Act, and to monitor and ensure compliance of the country with international standards set for data protection.

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

Yes, there are penalties in the form of fines ranging from One Hundred Thousand Pesos (Php100,000.00) to Five Million Pesos (Php5,000,000.00) and imprisonment ranging from six (6) months to six (6) years depending on the type of violation committed.[12]

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?

Apart from the Data Privacy Act and the DPA-IRR, no further legislation is in contemplation in the Philippines relating to personal information protection. However, it is worthy to note that the National Privacy Commission regularly issues Circulars and Advisories to further clarify the implementation of and for guidance of the public as to complying with the Data Privacy Act and the DPA-IRR. The National Privacy Commission likewise issues Advisory Opinions for queries, which it publishes on its website and is considered to have, at the very least, persuasive effect.

Conclusion

Based on the issuances of the National Privacy Commission, a company that wishes to comply with the provisions of the Data Privacy Act of 2012 must focus on the following requirements:

(1) Appoint a data protection officer who will ensure compliance with the Data Privacy Act of 2012 and the DPA-IRR;

(2) Conduct a Privacy Impact Assessment (with a template available at https://privacy.gov.ph/wp-content/uploads/NPC-PIA-Template-v2.pdf);

(3) Create a Privacy Manual which contains the protocols for each step in processing personal information with the goal of complying with complying with the Data Privacy Act of 2012, the DPA-IRR, and the issuances of the National Privacy Commission;

(4) Implement a privacy and data protection policy; and

(5) Install and maintain a breach reporting protocol.

Finally, in reference to the registration requirements for a personal information controller and personal information processors, as mandated by National Privacy Commission Circular 17-01, certain sectors or institutions wherein processing of personal data is likely to pose a risk to the rights and freedoms of data subjects and/or where the processing is not occasional, are required to register their data processing systems. While Phase 1 and 2 of the registration process has already lapsed (9 September 2017 and 9 March 2018, respectively), it is nevertheless prudent for companies who are mandated to register to comply, as the Commission will still accept late registrants, although they will be included in the list of priority organizations for a data privacy compliance check.

Authors: Neptali B. Salvanera and Franchesca C. Gesmundo.

Footnotes

[1]/ An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012] Republic Act No. 10173, Section 3 (g) (2012).

[2]/ *Id.* Section 12.

[3]/ National Privacy Commission, Implementing Rules and Regulations of Republic Act No. 10173, known as the "Data Privacy Act of 2012", Rule VI, Section 26 (2016) (hereafter, "DPA-IRR").

[4]/ *Id.* Rule VI, Section 27.

[5]/ *Id.* Rule VI, Section 28.

[6]/ *Id.* Rule I, Section 3, f.

[7]/ *Id.* Rule IV, Section 20.

[8]/ Data Privacy Act of 2012, Section 16.

[9]/ DPA-IRR, Rule IV, Section 19 a 1 and b 1.

[10]/ *Id.* Section 13.

[11]/ *Id.* Section 3 (l).

[12]/ *Id.* Sections 25-33.

MERITAS®
LAW FIRMS WORLDWIDE

SINGAPORE

FIRM PROFILE:

JOYCE A TAN & PARTNERS

The firm provides the full range of corporate and commercial legal services with particular strengths in intellectual property, information technology, telecommunications, media and entertainment.

The firm's service philosophy is aimed at bringing clarity to a situation and making the client experience a seamless, fuss-free encounter across multiple requirements that may arise. The firm does this by the pre-emptive, integrated and commercially realistic approach to the work and strategies it undertakes and ensuring alignment with its clients. The key areas of the firm's practice comprises work in:

- Corporate and Commercial Transactions
- Private Equity and Investment
- Business Financing
- Company Regulatory Compliance
- Employment and Immigration
- Intellectual Property
- Information Technology
- Telecommunications and Broadcasting
- Media and Publishing
- Entertainment
- Dispute Management and Litigation
- Arbitration, Mediation and Other Alternative Dispute Resolution
- Family and Personal Law

The firm routinely operates in a cross-border setting, managing local and foreign elements and dimensions as second nature, with its strong and keen multi-jurisdictional awareness and approach to the matters it handles.

CONTACT:

JOYCE A.TAN
joyce@joylaw.com

DANIEL LIM
daniel@joylaw.com

+65 6333 6383
www.joylaw.com

Introduction

In Singapore, the mandatory protection of "personal data" (as is the term used, rather than "personal information") under specific legislation only came into force in 2014, with the promulgation of the Personal Data Protection Act 2012 ("**PDPA**"). This protection regime seeks to address growing concerns from individuals about how their personal data is being used, maintain the trust of individuals in organisations that manage data, and strengthen Singapore's position as a trusted business hub.

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

Putting aside common law remedies (e.g. breach of confidence, etc.), sector-specific legislation (e.g. Official Secrets Act, Banking Act, etc.) and industry-specific self-regulatory codes (e.g. Singapore Code of Advertising Practice), personal data is primarily protected by the PDPA, which:

(1) Governs the collection, use, disclosure and care of personal data by an "organisation" (which includes any individual or legal entity) in a manner which recognises both –

- The needs of organisations to collect, use or disclose personal data for legitimate and reasonable purposes; and
- The rights of individuals to protect their personal data;

(2) Includes a national Do Not Call Registry, which allows individuals to opt out of receiving marketing phone calls, mobile text messages, and faxes from organisations; and

(3) Is supplemented by various –

- subsidiary legislation comprising the
  - Personal Data Protection (Do Not Call Registry) Regulations 2013;
  - Personal Data Protection (Composition of Offences) Regulations 2013;
  - Personal Data Protection Regulations 2014;
  - Personal Data Protection (Enforcement) Regulations 2014;
  - Personal Data Protection (Appeal) Regulations 2015;
- Practical tools issued by the Personal Data Protection Commission ("**PDPC**") comprising
  - Advisory Guidelines on PDPC's interpretation of PDPA provisions and handling of general and sector-specific issues; and
  - General Guides to assist organisations in complying with the PDPA.

2. How is "personal information" defined?

Under the PDPA, "personal data":

(1) Is defined as "data, whether true or not, about an individual who can be identified from that data, or from that data and other information to which the organisation has or is likely to have access";

(2) May include different types of data about an individual and from which an individual can be identified, such as the individual's passport number, facial image, voice, fingerprint, or DNA profile, regardless of such data being true or false or whether the data exists in electronic or other form; and

(3) Excludes –

- Business contact information e.g. position name or title, business telephone number, address, email and other similar information not provided by the individual solely for personal purposes; and
- Personal data contained in a record in existence for at least 100 years, or about an individual who has been dead for more than 10 years.

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

The PDPA is based on the following principles:

(1) ***Accountability***: An organisation is responsible for personal data in its possession or under its control. Where personal data is under the control of the organisation, the organisation shall designate one or more individuals to be responsible for compliance under the PDPA.

(2) ***Specified purpose/s***: The purpose/s for which personal data is collected by an organisation shall be specified by the organisation.

(3) ***Consent***: An individual's consent is required for the collection, use, or disclosure of his personal data, save in exceptional cases where the individual may be deemed to consent or where no consent is required.

(4) ***Reasonable* collection**: The collection of personal data shall be limited to that which is necessary for the specified purpose/s that a reasonable person would consider appropriate in the circumstances.

(5) ***Authorised use, disclosure, and retention***: Personal data shall not be used or disclosed to a third party for purposes other than the specified purpose/s for which it was collected, unless the individual consents to such use or disclosure, or unless exceptions allow for use or disclosure without consent. Personal data shall be retained only as long as necessary for the fulfillment of the specified purpose/s.

(6) ***Accuracy***: An organisation shall make a reasonable effort to ensure that personal data collected is accurate and complete if the personal data is likely to be used to make a decision affecting the individual to whom the data relates or is likely to be disclosed by the organisation to another organisation.

(7) ***Safeguards***: An organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal, or similar risks.

(8) ***Openness***: An organisation shall make available information about (a) policies and practices necessary for the organisation to meet its obligations under the PDPA; and (b) information about the complaint process to receive and respond to complaints that may arise.

(9) ***Individual access and correction***: An organisation shall, on the request of an individual, provide that individual with personal data about the individual in its possession or control and ways in which that personal data may have been used or disclosed within a year before the date of the request. There are exceptions where an organisation is not required to or shall not provide an individual with the requested personal data. An individual may request an organisation to correct an error or omission in personal data about him and which is in the possession or under the control of the organisation.

(10) ***Manageable compliance costs***: The PDPA aims to keep compliance costs manageable for businesses, especially Small and Medium Enterprises (SMEs). In line with this, a complaints-based approach rather than a more stringent audit-based regime will be adopted. There is no mandatory breach notification requirement under the law, but notification is recommended, as discussed below.

(11) ***Consistency with international standards***: The data protection regime is designed to be in line with international standards for data protection, such as the OECD Guidelines and the data protection frameworks in key jurisdictions, including Canada, New Zealand, Hong Kong, and the European Union.

(12) ***Facilitate cross-sector data flows***: The PDPA aims to be a general baseline law that applies across all sectors. It coexists with sector-specific regulations, which may impose more stringent data protection requirements. A baseline law engenders greater consumer trust in the private sector while at the same time facilitating data flows to achieve positive economic outcomes.

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

Unless the collection is required or authorised by law or under

certain prescribed exceptional circumstances e.g. an emergency that threatens the life, health or safety of the individual to whom the personal data relates or any other individual, an organisation which collects personal data about an individual is obliged to ensure that:

(1) The organisation shall have notified the individual of the purpose/s for which his personal data will be collected – the form and manner of such notification is to be determined by the organization as the best way of doing so, generally regarded as being in written form (whether electronic or other documented form) so that the individual is clear about the purpose/s and the parties have clear documentation on the matter to refer to in the event of any dispute;

(2) The individual's consent to the collection for such purpose/s has been given, which would be –

- Deemed to have been given if he voluntarily provides the personal data to the organisation, and it is reasonable that the individual would voluntarily provide the personal data;
- Invalid if the organisation –
  - As a condition of providing a product or service, had required the individual to consent to the collection of personal data beyond what is reasonable to provide the product or service to the individual; or
  - Had obtained or attempted to obtain the said consent by providing false or misleading information, or using deceptive or misleading practices.

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

(1) The requirements for the use and disclosure of personal data are identical to those set out at in the response to Question 4 above, in relation to the collection of personal data.

(2) In addition, an organisation in possession of personal data is obliged to:

- Make a reasonable effort to ensure that the personal data collected is accurate and complete, if the personal data is likely to be used by the organisation in making a decision that would affect the individual or to be disclosed by the organisation to another organisation;
- Make reasonable security arrangements to protect the personal data, such as preventing unauthorised access, use or disclosure; and
- Cease to retain documents containing personal data, or remove the means by which the personal data can be associated with the particular individual, as soon as it is reasonable to assume that –
  - The purpose for which the personal data was collected is no longer being served by retention of the personal data; and
  - Such retention is no longer necessary for legal or business purposes (there is no specified duration for this, which is assessed on a standard of reasonableness, having regard to the purposes for which the personal data was collected and other legal or business purposes for which its retention may be necessary).

(3) A data intermediary, i.e. an organisation which processes personal data on behalf of another organisation is also obliged to comply with the above security and removal obligations.

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

An organisation is not permitted to transfer an individual's personal data to another country or territory outside of Singapore unless it has taken appropriate steps to:

(1) Ensure that it will comply with its obligations on the collection, use and disclosure of the personal data (as set out in the responses to Questions 4 and 5 above), while the transferred personal data remains in its possession or under its control; and

(2) Ascertain whether, and ensure

that, the recipient in that country or territory outside Singapore is bound by legally enforceable obligations (e.g. by any law, contract or binding corporate rules) to protect that personal data at a standard that is at least comparable to that under the PDPA, an obligation which would be considered satisfied if –

- The transferring organisation
  - Duly obtained the individual's consent to the transfer after having provided the individual with a reasonable written summary of the extent to which the personal data transferred will be protected to a standard comparable to that under the PDPA; and
  - Had not required the individual's consent to the transfer as a condition of providing any product or services to the individual (unless the transfer is reasonably necessary to provide such product or service to the individual); and
  - Had not obtained nor attempted to obtain the individual's consent by providing false or misleading information about the transfer, or by using other deceptive or misleading practices; or
- The transfer is necessary for
  - The performance of a contract between the individual and the transferring organisation, or to do anything at the individual's request with a view to the individual entering into a contract with the transferring organisation; or
  - The conclusion or performance of a contract between the transferring organisation and a third party which is entered into at the individual's request or if a reasonable person would consider the contract to be in the individual's interest; or
  - The personal data transferred to be used or disclosed in certain prescribed exceptional circumstances where the consent of the individual is not required e.g. an emergency that threatens the life, health or safety of the individual to whom the personal data relates or any other individual, and the organisation has taken reasonable steps to ensure that the personal data will not be used or disclosed by the recipient for any other purpose.

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?

An individual is entitled to:

(1) Request (other than in exceptional circumstances, such as where the provision would threaten the safety of, or cause immediate harm to, another individual) an organisation, which would be obliged on such request (for which a reasonable fee may be charged), to ***provide the individual*** with –

- Personal data about the individual that is in the possession or under the control of the organisation; and
- Information about the ways in which that personal data has been or may have been used or disclosed by the organisation within a year before the date of the individual's request;

(2) Request an organisation in possession or control of his personal data, to ***correct an error or omission*** in such personal data, in which case, unless the organisation is satisfied on reasonable grounds that the correction should not be made, it must (without imposing any charge) –

- Correct the personal data as soon as practicable;
- Send the corrected personal data to every other organisation to which the personal data was disclosed by the organisation within a year before the date of the individual's request, unless that other organisation does not need the corrected personal data for any legal or business purpose; and

- Inform the individual in writing, within 30 days of receiving his request, of the time by which it will be able to correct the personal data, if it is unable to do so within such period of 30 days.

(3) ***Withdraw his consent*** given or deemed to have been given for an organisation's collection, use or disclosure of his personal data for any purpose, by giving reasonable notice of such withdrawal to the organisation, which –

- Must on receipt of the notice
  - Inform the individual of the likely consequences of withdrawing consent; and
  - Cease (and cause its data intermediaries and agents to cease) collecting, using or disclosing the personal data;
- Is, however, not required to delete or destroy the personal data upon request of the individual, but remains obliged to cease retention of, or to remove any means of associating the individual with, the personal data in the circumstances stated at point (2) under Question 5 above; and

(4) A right of action in civil proceedings in a court on account of any loss or damage suffered by the individual directly as a result of an organisation's contravention of its obligations in relation to the collection, use, disclosure, grant of access, correction and care of the individual's personal data –

- For relief, including
  - By way of injunction or declaration;
  - In the form of damages; and/or
  - Such other relief as the court thinks fit.
- Provided that if the PDPC has made a decision on the same contravention, such decision has become final after the right of appeal against that decision has been exhausted.

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?

(1) Subject to any applicable legal obligations, including confidentiality obligations and those under the employment contract:

- The PDPA allows an organisation to collect, use and/or disclose the personal data of an employee or prospective employee, as the case may be, without his consent where –
  - Such collection, use and/or disclosure is necessary for evaluative purposes, which includes determining the suitability, eligibility or qualifications of the employee for promotion or continuance in employment; or
  - Such collection, and subsequent use and/or disclosure, is reasonable for the purpose of managing or terminating the employment relationship with the employee.
- The Employment Act obliges an employer to –
  - Keep a record of complete and accurate information about its employment of every employee and former employee containing various prescribed particulars, including certain personal data ("**employee record**");
  - Retain such employee record relating to the personal data for the duration of employment, and if applicable, one year after the employment ends ("**retention period**"); and
  - Ensure that during such retention period, the employee record is readily accessible to the employee or former employee, as the case may be.

(2) Other than the above, the PDPA does not make any other differentiation of the types of personal data, although in its Advisory Guidelines and decisions, the PDPC has:

- Recognised that certain types of personal data, e.g. bank account details, would typically be more sensitive in

nature; and

- Recommended that organisations –
  - Accord a higher standard of protection to and take relevant precautions in the collection, use and/or disclosure of more sensitive personal data, when making security arrangements to protect personal data under its possession or control; and
  - Take extra steps to verify the accuracy of personal data where inaccuracy of the personal data would have severe consequences on the relevant individual e.g. a minor.

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

The PDPC is the authority responsible for the administration and enforcement of the PDPA, which may for such purpose, appoint the following:

(1) The Commissioner for Personal Data Protection; and

(2) Such number of Deputy Commissioners for Personal Data Protection, Assistant Commissioners for Personal Data Protection and inspectors, as the PDPC considers necessary.

More information about the PDPC, including its contact details, enforcement actions, etc. may be found at its website at https://www.pdpc.gov.sg.

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

Contravention of any personal data protection provisions in the PDPA may:

(1) Incur the PDPC's ***enforcement action*** in the form of such directions as the PDPC thinks fit to ensure compliance with the PDPA (which are subject to an appeal process) including requiring the non-compliant organisation to –
- Stop collecting, using or disclosing personal data in contravention of the PDPA;
- Destroy personal data collected in contravention of the PDPA;
- Comply with the PDPC's finding on the matter of a disputed request by an individual for access to or correction of his personal data as discussed at points (1) and (2) under Question 7 above; and/or
- Pay a financial penalty of an amount not exceeding SGD1 million.

(2) Open the non-compliant organisation to a ***civil suit*** in the court by an individual who suffers loss or damage directly as a result of the contravention, as discussed at point (4) under Question 7 above; and/or

(3) In specific instances, constitute an offence under the PDPA, such as where a person –
- Makes a request to an organisation in order to obtain access to or change the personal data of an individual without the authority of that individual, for which the guilty person would be liable on conviction to –
  - A fine not exceeding SGD5,000; and/or
  - Imprisonment for a term not exceeding 12 months; or
- Disposes of, alters, falsifies, conceals or destroys a record containing personal data or information about the collection, use or disclosure of personal data (or directs another person to do so), for which the guilty person would be liable on conviction to a fine not exceeding –
  - SGD5,000 in the case of an individual; or
  - SGD50,000 in the case of a non-individual.

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?

(1) The PDPC recently concluded, in June 2018, its conduct of a public consultation exercise on:
- A review of the Do Not Call provisions of the PDPA to ensure that these provisions

remain relevant in light of the increasing adoption of digital marketing tools such as social media and instant messaging platforms; and

- The introduction of an Enhanced Practical Guidance framework –
  - For the PDPC to provide guidance with regulatory certainty, which the current guidelines do not provide; and
  - Which is intended to facilitate the development of new and innovative data services, recognising the opportunities for innovations around the use of data as Singapore gears up to be a Digital Economy.

(2) Based on public feedback on the above issues, the PDPC might propose amendments to the PDPA, and/or the introduction of new regulations to put in place the Enhanced Practical Guidance framework.

MERITAS®
LAW FIRMS WORLDWIDE

TAIWAN

FIRM PROFILE:

泰運法律事務所
RUSSIN & VECCHI
INTERNATIONAL LEGAL COUNSELLORS

Russin & Vecchi's areas of specialized expertise include corporate transactions, asset management, private equity, M&A, competition law, franchising, banking, finance, securities, labor law, aviation, litigation and intellectual property. R&V-Taipei counsels both multinational and Taiwan corporations and financial institutions on all aspects of Taiwan law including representation before Taiwan government agencies and courts. R&V-Taipei attorneys also assist in the structuring and implementation of sophisticated commercial and financing transactions. R&V-Taipei's clientele includes international banks and financial institutions, manufacturers and computer and computer component suppliers.

CONTACT:

T. Y. LEE
tylee@russinvecchi.com.tw

THOMAS MCGOWAN
thmcgowan@russinvecchi.com.tw

+886-2-2712-8956
www.russinvecchi.com

Introduction

Taiwan was an early mover in recognizing the importance of data protection and has had a personal information protection regime in place for over 20 years. Taiwan initially adopted what was then called the "Computer Processed Personal Data Protection Law" ("CPPDPL") in 1995. The CPPDPL applied only (1) to data used within a specified list of industries (e.g. banks, hospitals etc.) which were required to register as data users and (2) to data that was "computer processed" such that manually processed data was not protected.

That original law was amended and replaced by the current Personal Data Protection Law ("PDPL"), which was enacted in 2010 and implemented in stages over the next few years after that.

The PDPL is now fully in effect and, among other changes, removes the data user registration requirement and expands data protection obligations to all industries in Taiwan and to all methods of processing. Thus, all business entities in Taiwan that collect, process or use data must comply with the PDPL. However, the PDPL does not extend to non-Taiwan business entities that collect, process or use data of Taiwan resident Protected Parties outside Taiwan.

The below responses set out brief highlights of the PDPL as currently in effect.

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

The major personal information protection laws and regulations in Taiwan are the PDPL and the Enforcement Rules of the Personal Data Protection Law ("Enforcement Rules").

2. How is personal information defined?

The PDPL defines "Personal Data" as: "the name, date of birth, identification card number, passport number, special traits, fingerprints, marital status, family, education, profession, medical history, medical treatment, genetic information, sexual life (including sexual orientation), health examination, criminal record, contact information, financial condition, and social activities of a natural person, as well as other data by which such person may be directly or indirectly identified."

The PDPL also defines certain personal data as "Sensitive Personal Data" and provides special protection for such data (see Response to Q8, below).

Specifically, "Sensitive Personal Data" is defined as medical records, medical treatment information, genetic information, sexual life information (including sexual orientation), health examination information, and criminal records.

The parties protected by the PDPL are "living natural persons" ("Protected Parties"). The PDPL does not protect companies, organizations or the deceased.

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

The key principles related to Taiwan personal information protection are:

(1) Collection, processing and use of Personal Data must be done in good faith and only for specified purposes notified to the Protected Party at the time of collection.

(2) A legitimate and reasonable connection must exist between the data collected and the purpose of collection.

(3) Protected Parties are entitled to be made aware of their rights to protect their data including the right to inspect, copy and revise as well as the right to require cessation of use. For example, a data notice will typically provide the data subject with a specific telephone number/email address as the contact point for requests to exercise such rights.

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

The core compliance requirement for the collection of personal information in Taiwan is that the data collector must, at the time of collection, notify the Protected Party of the purpose, category, and recipients of the Personal Data being collected; the geographical and temporal scope of its use; and the impact of choosing not

to provide Personal Data to the collector. The notification must also inform the Protected Party of his or her rights to inquire about, review, obtain copies of, supplement or correct, request the deletion of, and request the discontinuation of collection, processing or use of the Personal Data, as well as how to exercise those rights.

Further, consent is required for any use of Personal Data outside the scope of the purpose identified in the initial notification.

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

The key compliance requirements for the processing of personal information are to (1) Take proper security measures to protect the data and (2) Notify Protected Parties if a violation of the PDPL results in a data breach and the key compliance requirement for use and disclosure is that such must be within the scope of (1) The notice described in the response to Q4, above or (2) A separate consent from the Data Subject.

For certain industries such as financial institutions, there are detailed regulations setting out the specific technologies and methods required to be used to protect personal data.

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

There is no general prohibition on the transfer of Personal Data from Taiwan to other jurisdictions. However, cross-border transmissions of Personal Data may be restricted if a substantial interest of Taiwan is at stake (e.g. protecting national security); if an international treaty or agreement so requires; if the receiving country's laws or regulations do not adequately protect Personal Data; if transmission threatens the rights and interests of a Protected Party; or if the purpose of the transmission is to evade the application of the PDPL.

To date, no such restriction has been imposed except that the Taiwan National Communications Commission issued an order in 2012 prohibiting communications enterprises from transferring subscribers' Personal Data to Mainland China (defined as the People's Republic of China, excluding Hong Kong and Macau) on the grounds that the personal data protection laws in Mainland China are inadequate.

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?

A Protected Party in Taiwan has the right to inquire about, review, obtain copies of, supplement or correct, request the deletion of, and request the discontinuation of collection, processing or use of Personal Data and must be provided with information as to how to do so at the time the Personal Data is first collected. Data collectors will typically provide a contact telephone number or email address via which requests to exercise such rights may be made.

A Protected Party is also entitled to monetary or corrective compensation (e.g., to rectify damage to the Protected Party's reputation) for damages resulting from a collector's illegal or inaccurate use of Personal Data (see also responses to Q10, below).

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?

An employee's Personal Data is not treated differently than Personal Data of other Protected Parties.

Sensitive Personal Data receives special protection. For example, Article 6 of the PDPL provides that Sensitive Personal Data may not be collected, processed or used unless one of six specified exceptions applies, e.g., the Protected Party has voluntarily made such data available to the public or the data has been made public by other legal means.

Also, under various industry-specific regulations, particularly in the financial services industry, service providers have regulatory confidentiality obligations with respect to customers and customer transactions that apply to information beyond Personal Data and with respect to customers beyond natural persons. For example, banks are required by the Banking Law to keep all information regarding all customers (both individual and corporate) confidential and not to disclose such information without express customer consent.

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

The regulatory body with overall responsibility for data protection is the Ministry of Justice. However, the authority with jurisdiction over each relevant industry has primary enforcement responsibility within that industry. For example, the Taiwan Financial Supervisory Commission has responsibility for financial institutions and the Taiwan National Communications Commission has responsibility for communications enterprises.

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

There are administrative and criminal sanctions as well as civil liabilities to damaged Protected Parties.

Administrative sanctions are imposed by the regulatory authority having jurisdiction over the relevant industry (e.g. the Taiwan Financial Supervisory Commission if the violator is a bank) and range from NT$20,000 to NT$500,000 (approximately US$700 to US$17,500 at current exchange rates) per violation. Such fines may be imposed repeatedly until the violation is cured. The representative, managers or other persons having authority over the private regulated user that violates the PDPL are subject to the same administrative fines.

Criminal sanctions can include up to five years' imprisonment and/or fines up to NT$1,000,000 (approximately US$34,500 at current exchange rates).

Also, if a data collector or user intentionally or negligently violates any provision of the PDPL, and such violation causes the illegal collection, processing or use of Personal Data, or any other infringement of a Protected Party's rights (e.g., by way of a data breach), the data collector or user is liable to compensate the Protected Party for the damages suffered. Compensation may be both monetary and in the form of corrective measures (e.g., to rectify damage to the Protected Party's reputation).

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?

We are not aware of any current proposals to significantly change the methods by which Personal Data is protected in Taiwan or the scope of such protection. Thus, we do not anticipate any major changes from the current protection regime.

We do expect that, as public focus on data breaches and misuse increases, and as Protected Parties become more aware of their rights, the legal and commercial consequences for businesses of data breaches or other misuse of Personal Data will become more significant. For example, there have been a number of recent cases where data breaches have received a high level of media (including social media) attention resulting in potentially affected customers grouping together to take collective action via social media and otherwise to pressure the data user to pay compensation in amounts greater than what one could objectively expect via the court system but which the data user may effectively be forced to pay to preserve its reputation and avoid loss of business.

MERITAS®
LAW FIRMS WORLDWIDE

AUSTRALIA

FIRM PROFILE:

SWAAB

Swaab Attorneys is a Sydney based full service law firm. Established for well over 30 years, we pride ourselves on our ability to get on with business by providing great results, value for money and trusted advice, which is void of complexities, unnecessary delays and legal jargon, with a focus on building long-lasting and enduring relationships.

We do this because we're a passionate team of legal professionals who are committed to achieving exceptional results in everything we do and we believe that, with the spirit of generosity at our core, we can harness our strengths to overcome challenges together.

Our aim is to ensure the best possible and most rewarding experience for our clients. That is why we value our Swaab Brand of Service.

Our primary areas of law include: Corporate, Commercial, Property, planning & projects, Employment, Intellectual property & technology, Litigation and insolvency, Estate planning and Family law.

CONTACT:

MARY DIGIGLIO
med@swaab.com.au

JOHN HOVELMANN
jbh@swaab.com.au

+61 2 9233 5544
www.swaab.com.au

Introduction

Australian privacy law has national significance.

The main privacy law contains 13 principles, which have the force of law by virtue of the *Privacy Act* 1988 (Cth). The federal privacy regulator is the Australian Information Commissioner.

The 13 Australian Privacy Principles are:

(1) Open and transparent management of personal information

(2) Anonymity and pseudonymity

(3) Collection of solicited personal information

(4) Dealing with unsolicited personal information

(5) Notification of the collection of personal information

(6) Use or disclosure of personal information

(7) Direct marketing

(8) Cross-border disclosure of personal information

(9) Adoption, use or disclosure of government-related identifiers

(10) Quality of personal information

(11) Security of personal information

(12) Access to personal information

(13) Correction of personal information.

Some types of information and selected organisations are exempt. These include personal information about employees and the personal information dealings of most small businesses (those with an annual turnover of less than AU$3 million).

In addition some state laws regulate the personal information collection practices of certain sectors. For example, state laws may govern the personal information management practices of state government entities in the healthcare sector.

Major changes to Australian national privacy laws occurred in March 2014 (with the introduction of the Australian Privacy Principles) and in February 2018 (concerning the mandatory notification of certain types of data breaches, which are likely to cause serious harm to an individual).

Australia's statutory privacy law provisions do not generally provide for civil actions by affected individuals. However, some causes of action for breach of confidence exist.

There are some parallels between the concepts underlying Australia's notifiable data breach scheme and the personal data breach provisions under the GDPR (Articles 33, 34, 58 and 83). However, there are important differences. For example, the mandated "assessment phase" where one is not sure whether serious harm is likely, and the penalties attaching to failure to notify. The penalties are significantly higher in the EU.

Unlike the European GDPR, Australian privacy principles are not strictly based on statements of individuals' human rights and freedoms.

Australian privacy law does not include an express distinction between controllers and processors and does not mandate any particular terms for written contracts between controllers and processors.

Australia privacy law does not have an express equivalent of those provisions of the GDPR, which require at least one of six lawful bases for collection.

As to the territorial reach of the *Privacy Act* 1988 (Cth), it covers:

(1) Those who have some recognition under Australian law (for example are incorporated in Australia); and

(2) Those who do not have such recognition but who both carry on business in Australia and collect the relevant personal information in Australia.

As to cross-border disclosure of personal information, Australian law does not prohibit cross-border disclosures in circumstances where adequate protection of individuals' rights is not guaranteed. Instead, Australian law imposes, in effect, vicarious liability on the entity governed by the *Privacy Act* 1988 (Cth) for the data breaches of those to whom cross-border disclosures occur and who are not governed by that Act.

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

(1) Australian Privacy Principles

under Australian federal statutory law, the *Privacy Act* 1988 (Cth). Note: Some Australian states have enacted state-based privacy legislation and there is the law of confidential information, which is non-statutory law applying throughout Australia.

(2) A federal statutory law regulating commercial electronic messages (the *Spam Act* 2003 (Cth). While the Spam Act does not regulate personal information protection, there are overlaps with the Privacy Act because the Privacy Act regulates use of personal information for direct (including electronic) marketing.

The answers below are limited to the *Privacy Act* 1988 (Cth) position.

2. How is personal information defined?

The definition of "personal information" under the *Privacy Act* 1988 (Cth) is *information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) Whether the information or opinion is true or not; and (b) Whether the information or opinion is recorded in a material form or not.*

This definition is limited to the personal information of individuals. Information identifying legal entities such as corporations and companies is not within the definition. Information identifying members of an unincorporated partnership may be within the definition.

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

There are 5 key principles:

(1) Managing personal information in an open and transparent way;

(2) Giving notices to individuals regarding the collection of solicited and unsolicited personal information including unsolicited personal information;

(3) Limiting uses and disclosures of personal information to primary and related secondary purposes of collection;

(4) Maintaining the quality and security of personal information; and

(5) Responding to requests for access to, and the correction of, personal information.

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

Compliance requires:

(1) Creating the individual's awareness of the purposes of collection, holding, use and disclosure;

(2) Requiring consents where the collection, holding, use or disclosure is for marketing purposes and

(3) Taking reasonable security measures to guard against unauthorized access.

Australian law mandates the following:

Sensitive information: Obtaining consents to the collection of an individual's sensitive information. This is in addition to the requirement that the collection be reasonably necessary for one or more of the entity's functions or activities.

Contact information: Giving details of the entity's identity and contact details.

3rd party sources: Creating an awareness of this. This is particularly important as regards cookies and customer profiling.

Limited awareness circumstances: Taking such steps as are reasonable in the circumstances to ensure that individuals about whom the entity collects personal information are aware of it (in circumstances where they may not be otherwise – again important as regards cookies and customer profiling).

Purposes of collection: Taking such steps as are reasonable in the circumstances to ensure that there is an awareness of the purposes for which the entity collects personal information. This should be done in a way which enables the primary purpose of collection to be identified, a matter relevant to consents and secondary use. The manner of making individuals aware should be done in a way which is consistent with the entity's privacy policy. Where a purpose is direct marketing, a privacy policy/notice may not be sufficient. Opt ins may be needed. This might be done in separate legal terms or in specific opt in text to which the individual's attention is drawn in the relevant

communication channel. All direct marketing must be accompanied by a simple mechanism by which the individual may request not to receive direct marketing. An opt in is not required where the personal information is collected directly from the relevant individual in circumstances where the individual would reasonably expect the entity to use or disclose their personal information for that purpose. An opt in is always required for direct marketing use of sensitive information

Consequences: Disclosing the main consequences for individuals if some of their personal information is not collected by the entity.

Usual disclosures: Taking reasonable steps to make the individual aware of those entities to whom disclosures are usually made of the kind collected.

Access, correction and complaints: Giving the individual information about how they may access, correct and make complaints about the handling of their personal information.

Overseas disclosures: Outlining the likelihood of ex-Australian disclosures. Where practicable, the entity should specify the countries in which the overseas recipients are likely to be located.

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

See answer to Question 4.

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

Australian national privacy law does not prohibit overseas disclosures. However, the likelihood of overseas disclosures should be addressed in collection notices and there is transferor liability for transferee breaches where the transferee is not directly bound by the Australian *Privacy Act.*

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?

Individuals who complain to an entity about its personal information management practices have the right to be made aware of the entity's complaints procedures as part of the entity's privacy policy. In the absence of a contractual commitment to the contrary, individuals can withdraw their consent to the retention of their personal information by third party by communicating with the relevant data controller – contact details need to be disclosed as part of the entity's privacy policy. Consents to direct marketing may always be withdrawn. Complaints may be made by an individual directly to the Australian Information Commissioner, the contact details of which are at Question 9.

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?

Employee personal information is not regulated by the *Privacy Act* 1988 (Cth).

The privacy rules for credit information and sensitive information are more stringent than for other types of personal information.

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

The Australian Information Commissioner. Contact details for the Australian Information Commissioner are:

Email: enquiries@oaic.gov.au

Tel: 1300 363 992

Postal address: GPO Box 5218, Sydney NSW 2001, Australia.

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

The Australian Information Commissioner may seek to impose civil penalty provisions for interferences with privacy. These

can include financial penalties in the order of AU$0.5million.

The Australian Information Commissioner has broad supporting powers. These are to investigate and conciliate and to make ancillary orders, for example obtaining documents and carrying out "own motion" assessments.

The Commissioner's authorised actions are also:

(1) Examining proposed legislation, which would allow interference with privacy or may have any adverse effects on people's privacy;

(2) Researching and monitoring developments in data processing and computer technology to ensure that adverse effects on people's privacy are minimised, as well as promoting an understanding and acceptance of the Australian Privacy Principles and their objects;

(3) Preparing and publicising guidelines for agencies and organisations to follow to avoid breaches of privacy; and

(4) Encouraging industries to develop programs to handle personal information consistent with the Australian Privacy Principles.

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?

None has been published by the regulator. Australia introduced mandatory notifiable data breach laws in February 2018, which have close parallels with those under GDPR.

Conclusion

For those who are likely to be subject to Australian privacy law, advice should be taken on whether they have an Australian-law compliant privacy policy and whether their communications with relevant individuals provide the necessary forms of awareness and, if necessary, consent.

When seeking local counsel, key issues for instructions are:

(1) How personal information is collected, stored, used and disclosed, and from whom;

(2) The types of personal information in question;

(3) How the information may be used and disclosed (and by and to whom);

(4) The mechanisms available to the collector to provide opt-ins and opt-outs;

(5) The range of contracts entered into by the collector, which have personal information management implications; and

(6) The extent to which Australian collections involve ex-Australian dealings or customers or data flows.

As with the the GDPR no amount of legal text will render an organisation's personal information management practices compliant with Australian law in the absence of other appropriate management practices, important amongst which are:

(1) Informed awareness;

(2) Measures which protect personal information from misuse, interference, loss, unauthorised access, modification or disclosure;

(3) The giving of access to and rights to correct personal information; and

(4) Complaints management.

MERITAS®
LAW FIRMS WORLDWIDE

NEW ZEALAND

FIRM PROFILE:

Martelli McKegg lawyers

Martelli McKegg is an Auckland based full service law firm specialising in Overseas Investment (into New Zealand), Corporate/Commercial, Mergers and Acquisitions, Intellectual Property and Technology, Real Estate, Building and Construction, Litigation/Dispute Resolution, Employment, Trusts, Estates and Relationship Property.

Established in 1921, we are very well regarded in the market with a number of partners nationally recognised for their expertise.

Our clients range from small family-owned businesses and private clients, through to some of the largest organisations in Australia and New Zealand across a variety of industries. We have particular experience acting for clients in the following sectors: manufacturing, import/export, wine and beverage, hospitality, tourism, entertainment, advertising, technology, telecommunications, property-development, forestry and industrial services.

We work hard to get to know our clients and to understand what our clients want to achieve. Our focus is to provide our clients with positive, practical legal advice, on time and within budget.

CONTACT:

MELISSA HIGHAM
mh@martellimckegg.co.nz

MIKE WORSNOP
mcw@martellimckegg.co.nz

+64 9 379 7333
www.martellimckegg.co.nz

Introduction

The protection of personal information is seen as important in New Zealand with robust privacy laws which are generally observed and enforced. New Zealand privacy laws were traditionally seen as "adequate" under the European Union's 1995 Data Protection Directive, however with the advent of the GDPR, New Zealand now lags behind the EU. Consequently, New Zealand's privacy laws are under review with changes designed to ensure that New Zealand is aligned with the EU and other major trading partners likely to come into force next year.

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

The principal personal information protection law in New Zealand is the Privacy Act 1993 (Act). A number of more specific privacy Codes of Practice have been issued pursuant to the Act for certain industries; namely:

(1) Civil Defence National Emergencies (Information Sharing) Code;

(2) Credit Reporting Privacy Code;

(3) Health Information Privacy Code;

(4) Justice Sector Unique identifier Code;

(5) Superannuation Schemes Unique Identifier Code; and

(6) Telecommunications Information Privacy Code.

There are also relevant provisions in the Unsolicited Electronic Messages Act 2007, which prohibit address harvesting software or harvested-address lists being used in connection with unsolicited commercial electronic messages (i.e. spam emails). Our answers below do not focus on this aspect.

2. How is personal information defined?

Under the Act, "personal information" means "information about an identifiable individual". An "individual" is defined to mean a "natural person, other than a deceased natural person", which excludes legal entities such as companies but would include the individual partners of a partnership or the trustees of a trust.

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

The Act centers around 12 information privacy principles. The wording of these principles contains a number of qualifications and exceptions, but they can be summarised as follows:

(1) Principle 1: An agency may only collect personal information necessary for a lawful purpose which is connected with a function of the agency.

(2) Principle 2: An agency must collect personal information directly from the individual, unless one of several exceptions applies.

(3) Principle 3: An agency must take reasonable steps to ensure an individual is aware of a number of matters, including the fact that the personal information is being collected, the purpose of the collection, the recipients of the information, the name of the agencies which will collect and hold the information, whether the supply of information is voluntary or mandatory (and under what laws), and the individual's rights under the Act.

(4) Principle 4: Personal information must not be collected in a way which is unlawful, unfair or unreasonably intrusive.

(5) Principle 5: An agency that holds personal information must ensure it is securely stored and protected from loss or misuse.

(6) Principle 6: If readily retrievable, an individual is entitled to confirmation from an agency of whether it holds their personal information and to be given access to it.

(7) Principle 7: Individuals have the right to request correction of personal information held, and if no correction is made may have a statement attached to the information noting that a correction was sought and not made.

(8) Principle 8: An agency must not use personal information without first taking reasonable steps to ensure it is up to date, complete, relevant and not misleading.

(9) Principle 9: An agency must only hold personal information as long as required for lawful purposes.

(10) Principle 10: An agency cannot use information for any purpose other than the one that it was obtained for, unless an exception applies.

(11) Principle 11: An agency must not disclose collected personal information unless pursuant to one of the purposes for which it was collected, or another exception applies.

(12) Principle 12: A unique identifier (such as tax identifiers and passport numbers) cannot be assigned to an individual unless it is necessary for the agency to carry out one of its functions efficiently, and the sharing of these identifiers is restricted.

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

As per the privacy principles, an agency collecting personal information must ensure it is doing so for a legitimate purpose connected to its functions, should seek to obtain the information directly from the individual if possible, and must take steps to inform the individual about the collection and their rights in accordance with principle 3.

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

As a general rule, the use and disclosure of personal information must be connected to the legitimate purpose for which it was collected. An agency should have processes in place to ensure information is up to date and complete before being used. Information must be securely processed and stored, kept only for so long as necessary, and the agency needs to have the ability to correct and modify stored personal information in case a correction request is received from an individual.

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

There is no general restriction on the transfer of personal information to other jurisdictions. However, the Privacy Commissioner has authority to prohibit a transfer of information from New Zealand to another State if satisfied the information would not be adequately protected or the transfer would lead to a breach of the relevant OECD Guidelines.

Where personal health information is to be stored in the cloud, the Ministry of Health requires that the agency undertake a cloud service risk assessment and for certain agencies there are enhanced requirements.

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?

As per privacy principles 6 and 7, individuals have the right to know whether an agency holds their information, to access the information, and to request that corrections be made. Agencies must notify individuals of these rights. There is no right to have information deleted or to withdraw consent to its retention.

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

Employees' personal information is not protected differently and is subject to the same privacy principles.

There are specific Codes of Practice issued by the Privacy

Commissioner in relation to certain industries, which override the privacy principles under the Act. These resemble the privacy principles but are tailored to the relevant area. These are specified above.

9. Which regulatory authorities are responsible for the implementation and enforcement of personal information protection laws in New Zealand?

The Act establishes the Office of the Privacy Commissioner, an independent Crown Entity which is responsible for implementing and enforcing the Act. In particular, the Privacy Commissioner has a role in receiving and determining privacy complaints, investigating breaches and authorising specific exemptions from the privacy principles. The Office of the Privacy Commissioner maintains a comprehensive website at https://www.privacy.org.nz with links to the relevant legislation and Codes of Practice.

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

Complaints regarding breaches of privacy are to be made in first instance to the Privacy Commissioner, which will review the complaint, investigate if necessary and if possible settle the complaint between the individual and the agency. The role of the Privacy Commissioner is to facilitate or mediate a settlement; the Privacy Commissioner cannot force the parties to settle. Most settlements take the form of an apology or release of information. Financial settlements are relatively uncommon.

If it is not possible to settle the complaint, or the agency contravenes an earlier assurance not to repeat a breach of the privacy principles, the Privacy Commissioner may refer the matter to the Director of Human Rights Proceedings for a civil action in the Human Rights Review Tribunal (essentially a specialist court). If the Privacy Commissioner or Director of Human Rights Proceedings decline to take action, the individual may bring the claim themselves.

The Human Rights Review Tribunal has a broad discretion in the orders it can make, which include an order restraining the defendant, costs and damages. There is no stated limit to the maximum damages awardable on a claim, but the awards to date are modest. Perhaps the most high-profile case to date has involved the internet tycoon, Kim Dotcom. In this 2018 case the Human Rights Review Tribunal made an award of NZ$90,000 plus costs in favour of Mr Dotcom.

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?

In March 2018, a new Privacy Bill was introduced to replace the existing Act and is currently working its way through Parliament. Much of the new Bill is remaining the same, with updates and clarification to the wording. The key amendments are:

(1) Mandatory reporting of privacy breaches that pose a risk of harm.

(2) A new requirement for New Zealand agencies to take reasonable steps to ensure personal information disclosed overseas will be subject to acceptable privacy standards.

(3) New powers for the Privacy Commissioner, including strengthened information gathering powers, an ability to issue enforceable compliance notices to agencies, and the ability to make binding decisions on access to information complaints.

(4) New criminal offences of misleading an agency in a way that affects a third party's information, and knowingly destroying documents containing personal information where a request has been made for it.

As the Bill is still at an early stage it is possible there will be further amendments before it is enacted. The Bill is currently with the Select Committee (the main opportunity for submissions

to be made and amendments recommended), with the Report of the Select Committee due in October 2018.

Conclusion

Agencies handling the personal information of New Zealand residents must ensure that they are properly acquainted with New Zealand privacy laws, implement appropriate policies around the collection, storage, use and dissemination of such information and have relevant contract documentation vetted for compliance. They must also ensure that they keep abreast of developments in what is currently an evolving area of the law.

MERITAS®
LAW FIRMS WORLDWIDE

GERMANY, EUROPE

FIRM PROFILE:

ARNECKE SIBETH DABELSTEIN

ARNECKE SIBETH DABELSTEIN - The commercial law firm. 12 areas of expertise - focused, reliable, premium! As a leading commercial law firm, we are internationally recognized for our core competencies in real estate, maritime industry, and the transportation/aviation/logistics market.

ARNECKE SIBETH DABELSTEIN provides comprehensively focused legal advice building on a foundation of a total of 12 outstanding areas of expertise. Our expertise is on par with specialized competitors and will continue to grow in the future. We plan to strategically develop the fields of insurance, energy, and sports/media/entertainment to become further core competencies.

ARNECKE SIBETH DABELSTEIN is innovative, dynamic and modern. Proven valuable and successful for decades, as authentic advisors at the highest level we have a proven record of success and value.

Our international network is multi-layered and tightly-knit. As a member of Meritas we are a reliable partner for our international clients.

CONTACT:

HANS GEORG HELWIG
h.helwig@asd-law.com

+49 30 8145913-42
www.asd-law.com

MERITAS®
LAW FIRMS WORLDWIDE

FRANCE, EUROPE

FIRM PROFILE:

BignonLebray

Founded in 1982, Bignon Lebray specializes in all areas of company law.

Our firm brings together more than one hundred legal professionals, including 25 partners, specialising in 11 practice areas.

Our cultural and professional diversity reflects our history: we are an independent French law firm that has evolved with its clients as they seek growth in today's globalized business world.

We provide services to companies ranging from small start-ups to large listed firms and to public authorities and not-for-profit organizations. Central to our legal focus in all matters, legal and contentious, is a thorough understanding of our clients' business activities and projects.

Through our 4 offices in France (Paris, Lyon, Lille and Aix-Marseille), we endeavor to bring clients the most efficient, cost effective and case-specific answers to their business needs.

CONTACT:

ÉLISE DUFOUR
edufour@bignonlebray.com

+33 (0)1 44 17 17 44
www.bignonlebray.com

Introduction

On May 25, 2018, the European General Data Protection Regulation (GDPR) came into force. As legislation directly binding all EU member states, the GDPR is a true paradigm shift. In the past, while statutory provisions did protect data subjects' rights, a violation was not a barrier because fines for international enterprises were small. Now, any infringement could cost businesses up to 4% of their worldwide revenue or up to 20m EUR. Protection of personal data must now be taken seriously. Below is a general outline based on 11 questions we are asked regularly about the new regulation. Also rendered are references to how German and French law will apply the GDPR in the respective countries. As an EU regulation the GDPR is directly applicable and takes direct effect in each EU member state, superseding contradictory national laws. Yet, in some aspects the GDPR allows for the member states to implement individual national provisions that are stricter than the GDPR.

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

The REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation – GDPR).

The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way organizations across the region approach data privacy. Its key points of impact are:

(1) Extended jurisdiction of the GDPR, as it applies to all companies processing the personal data of data subjects residing in the Union, regardless of the company's location;

(2) Severe penalties (see above).

(3) Stricter conditions for valid consent given by a data subject.

(4) Right to be forgotten, data portability.

(5) Mandatory data protection officers to be appointed by enterprises.

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

Although directly applicable, this regulation has been incorporated into domestic law on June 20th, 2018.

The Federal Data Protection Act 2018 (abbr. BDSG), implements the GDPR.

Where permissible by the GDPR the BDSG stipulates even stricter rules.

2. How is personal information defined?

Art. 4 (1) : (1) "personal data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Information about corporations or companies is not included in the definition, which is limited to the personal information of individuals, but information identifying members of a corporation can be.

Personal data of deceased persons is not protected under the GDPR (Recital 27). Member states may, however, stipulate rules with respect to such data and its continuous protection after a person's death.

According to Art. 2 of the law, the same definition as in GDPR applies.

BDSG refers to Art. 4 GDPR and therefore does not stipulate a more detailed definition. According to German case law, however, the business email address of an individual is considered 'personal data'.

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

Chapter III GDPR: Data concerning individuals can be collected, provided that they have been informed of this operation. (Art. 13)

Art. 5: personal data shall be:

(1) Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(2) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (…);

(3) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(4) Accurate and, where necessary, kept up to date (…) ('accuracy');

(5) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; (…) ('storage limitation');

(6) Processed in a manner that ensures appropriate security of the personal data ('integrity').

Recital 39 with respect to the storage time stipulates: What requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted.

According to article Art. 6 of the law, the same rights are stipulated.

BDSG refers to the GDPR and therefore stipulates the same rights.

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

Art. 6 GDPR: Processing shall be lawful only if and to the extent that at least one of the following applies:

(1) The data subject has given consent to the processing of his or her personal data for one or more specific purposes [according to Art. 7 and recital 32 – consent does not have to be given in writing; whereby the controller should demand consent in writing to be able to prove that consent has been given, Art. 7 Sec. 1 GDPR];

(2) Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(3) Processing is necessary for compliance with a legal obligation to which the controller is subject;

(4) Processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(5) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(6) Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Art. 13 GDPR: the data subject should be informed at the time of:

(1) The identity of the data controller;

(2) The purpose;

(3) The compulsory or optional nature of the answers;

(4) Possible consequences for him of a failure to reply;

(5) Recipients or categories of recipients of the data;

(6) The rights the data subject has according to the law;

(7) Where appropriate, transfers of personal data to a non-member State of the European Community;

(8) The retention period of the categories of data processed.

According to Art. 32 of the law, the same requirements are provided.

Sec. 32 to 37 of Germany's Federal Data Protection Act establishes the same regime.

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

See answer to Q4.

The disclosure of personal data shall only be admissible with the consent of the data subject.

According to Art. 34 of the law, the data controller should take all appropriate precautions, in view of the nature of the data and the risks presented by the processing, to preserve the security of the data and, in particular, to prevent them from being distorted, damaged, or that unauthorized third parties have access.

See answer to Q4.

If personal data are obtained not from the data subject but a third party, Art. 14 GDPR and Sec. 33 BDSG stipulate specific rights of information vis-à-vis the controller, such as:

(1) Identity and contact details of the controller and data protection officer;

(2) Purpose for processing of personal data and legal basis;

(3) Categories of data concerned;

(4) Recipients of data;

(5) Ensure fair and transparent processing, which includes,

- Period of storage
- Rights according to Art. 5 GDPR
- Right to lodge a complaint with a supervisory authority
- Source personal data originates from

(6) Such information must be provided within a reasonable time after obtaining the data.

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

Art. 44 to 50 GDPR.

The transfer is not possible, provided safeguards are taken such as:

(1) Standard EU agreement (Data Controller to Data Controller and Data Controller to Data Processor);

(2) Binding corporate rules;

(3) Transfers or disclosures to a country with an adequate level of protection.

If the controller fails to take such measures of an adequate level of data security, it shall be personally liable towards the data subject according to Art. 82 GDPR. In addition, an infringement of Art. 44 to 49 GDPR is subject to administrative fines up to 20m EUR or up to 4% of the yearly turnover according to Art. 83 Sec. 5 GDPR.

According to Art. 69 to 70 of the law, the data controller may not transfer personal data to a State that is not a Member of the European Union if this State does not provide a sufficient level of protection of individuals' privacy, liberties and fundamental rights.

Some exceptions exist.

The BDSG provides for a very elaborate regime of prerequisites for the transfer of data to third countries in Sec. 78 to 81. This includes:

(1) The transfer of personal data to a third country law enforcement authority if the data subject's fundamental rights are not deemed to be more protectable;

(2) The transfer on the basis of a adequacy decision of the EU commission, based on Art. 36 (3) of the Directive (EU) 2017/680, i.e. the Commission has resolved that the third country in question meets EU data protection standards (the EU commission upholds a regularly updated list on its respective resolutions and states recognized as "adequate").

(3) Without such resolution the transfer to a third country is admissible, if this country has given a legally binding guarantee to give sufficient protection to an individual's personal data, e.g. the US-EU Privacy Shield.

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?

Art. 12 to 23: GDPR.

(1) Transparent information, communication and modalities for the exercise of the rights of the data subject.

(2) Disclosure of and access to personal data.

(3) Information to be provided where personal data are collected from the data subject, and where personal data have not been obtained from the data subject.

(4) Right to restriction of processing, data portability, of access by the data subject, to rectification, to erasure (right to be forgotten).

(5) Notification obligation regarding rectification or erasure of personal data or restriction of processing data portability.

(6) Right to object and automated individual decision-making.

According to Art. 7 Sec. 3 GDPR the data subject shall have the right to withdraw consent at any time; whereby lawfulness of processing based on the consent before its withdrawal is not affected. Withdrawal further only affects lawfulness of data processing based on consent according to Art. 6 (1) (a) GDPR.

According to Art. 38, 39 and 40 of the law, same rights, but France have an additional right: according to article 40-1 of the law, the data subject also has the right to define guidelines on the fate of his personal data after his death.

Rights of the data subject are stipulated in Sec. 32 et seq. BDSG and resemble the standards of the GDPR.

Besides the general principles laid out in Art. 5 and 6 GDPR (see Q3 and 4) a fundamental change is the establishment of the data subject's right of information according to Art. 13 GDPR, such as (e.g.),

(1) Identity and the contact details of the controller;

(2) Contact details of the data protection officer;

(3) The purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(4) Where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(5) Recipients or categories of recipients of the personal data;

(6) Basis for transfer to a third country;

(7) Period of storage;

(8) Existence of right to object and right of erasure;

(9) Right to withdraw consent at any time, when processing is based on consent (Art. 6 (1) (a) GDPR;

(10) Right to file a complaint to the supervisory authority.

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?

Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context (Art. 88 GDPR).

The law does not define a specific frame for employees' personal information protection. However, according to the CNIL's decisions, the consent of an employee should be collected with additional safeguards. Indeed, the CNIL considers that the consent of the employee is not freely given and hence not a valid legal ground for processing the data of an employee. Hence the employer should collect data only with regard of the execution of the employment contract or its legitimate interest.

Sec. 26 BDSG implements the provision in the GDPR.

In addition to codified law, within an employment relationship a basis for data processing may also be provided for in collective bargaining and shop agreements.

For example, collective agreements often define rules for the use of IT, especially Internet and email devices. This includes the accessibility of employee's accounts. Without an employee's consent, the employer shall not access the employee's email account, whereas a shop or collective bargaining agreement may stipulate such a right for the employer, which then supersedes a missing consent.

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

The European Data Protection Supervisor (EDPS) is an independent supervisory authority whose primary objective is to ensure that European institutions and bodies respect the right to privacy and data protection when they process personal data and develop new policies.

Postal address: Rue Wiertz 60, B-1047 Brussels

Office address: Rue Montoyer 30, B-1000 Brussels

Telephone: +32 2 283 19 00

Email: edps@edps.europa.eu

Website: www.edps.europa.eu

The CNIL, "Commission Nationale de l'Informatique et des Libertés", is responsible for implementation and enforcement of personal information protection laws in France. CNIL's details are:

CNIL

3, Place de Fontenoy

75007 Paris, FRANCE

Tel: 01 53 73 22 22

The state data protection commissioner – each of the 16 states in Germany has its own commissioner responsible.

Further the Federal Data Protection Commissioner as the national supervisory authority established a so-called single point of contact (ZASt. - www.bfdi.bund.de/ZASt/EN). In the federal German system, which is unique throughout Europe, and which includes data protection supervisory authorities of the Federal Government and of the 16 Länder (Federal States), the single contact point coordinates the cross-border cooperation with the other Member States of the European Union, the European Data Protection Board (EDPB) and the European Commission. The ZASt is established at the Federal Commissioner for Data Protection and Freedom of Information, but organizationally separated from that authority.

As a single contact point, the ZASt shall enable the supervisory authorities of the other Member States, the EDPB and the European Commission, to communicate

effectively with the German supervisory authorities.

It is not active in the external relationship vis-à-vis citizens, authorities and companies.

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

Art. 83 GDPR administrative provides penalties up to 10 or 20 million euros or 2% to 4% of the global turnover (GDPR) depending on the offence.

Article 45

The CNIL can pronounce administrative penalties up to 10 or 20 million euros or 2% to 4% of the global turnover depending on the offence.

In addition, certain offenses are punishable by criminal law and are punishable by five years of imprisonment and a € 300,000 fine (multiplied by 5 for legal entities) (article 226-16 to 226-24 of the criminal code).

Art. 83 GDPR is directly applicable according to Sec. 41 BDSG. Further Sec. 43 BDSG limits the fine to a maximum of 50.000 EUR for infringements of rights of information of the data subject acc. to Sec. 30 BDSG.

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?

European Union data protection affects every business and organization and cannot be ignored. The scope of data protection and implementing regulations is likely to increase in the coming years throughout the European Union..

In addition to the GDPR the ePrivacy Regulation is expected to come into force within the first six months 2019. This more towards e-commerce directed regulation was originally intended to be effective parallel to the GD PR on May 25, 2018.

Certainly, all of Europe can expect an increase in jurisdiction relating to violation of the GDPR as the immense fines will force controllers to take legal action against imposed fines.

A recent law for the protection of personal information has recently been adopted: The law n°2018-493 of June 20, 2018, promulgated June 21, 2018, modified the law Informatique et Libertés of January 6, 1978.

The decree implementing the law has been adopted on August 1 2018.

The GDPR has been implemented with the BDSG. ePrivacy will follow.

Conclusion

The European Union is currently composed of twenty-eight countries. Using France and Germany as examples, this outline illustrates how GDPR compliance and obligations may vary from country to country because of differences in national transition laws of EU members and the EU members' different interpretations of the GDPR provisions.

We recommend that your business strictly comply with all standards set by the GDPR. Your obligations may extend beyond what is contained in this outline. For example, your records of processing activities and obligations to delete incorrect information as well as technical and organizational measures should be established immediately.

A violation or non-compliance with GDPR standards and national requirements will expose your business to significant fines. In addition, it may endanger cross-border relations as your business partners will look to you for verification of compliance with all GDPR provisions.

MERITAS®
LAW FIRMS WORLDWIDE

USA

FIRM PROFILE:

MEYER UNKOVIC SCOTT
ATTORNEYS AT LAW

Meyer, Unkovic & Scott established in 1943 is a full service law firm with a diverse clientele including Fortune 100 companies, significant financial institutions, business enterprises, and individuals. Our firm has extensive experience handling international matters for its clients across the globe.

We advise on legal matters, including structuring a variety of business transactions, mergers & acquisitions, foreign direct investments, intellectual property and data protection, real estate and banking law, insolvency law, employment law, international law, immigration issues, tax planning, and commercial litigation and arbitration.

We strive to understand each client's unique goals and needs. Our most important priority is clear, concise, and regular communications.

Dennis Unkovic served as the world-wide Chair of Meritas® from April 2015 to May 2018. Meyer, Unkovic & Scott has been an active member of Meritas® since October 11, 1999.

CONTACT:

DENNIS UNKOVIC
du@muslaw.com

MICHAEL G. MONYOK
mgm@muslaw.com

+1-011-412-456-2800
www.muslaw.com

Introduction

Data privacy is an important and evolving issue in the United States. Various national and state-level laws and regulations protect the collection, storage, and use of personal information. At the national level, there are several federal agencies charged with the enforcement of applicable laws and regulations, including the Federal Trade Commission (the "FTC"), the Department of Health and Human Services (the "DHS"), and the Consumer Financial Protection Bureau (the "CFPB"). The distributed enforcement duties among various agencies results from the lack of a single, comprehensive law relating to the protection of personal information.

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

The following is an overview of the current law and regulations of most concern to businesses operating in the US:

(1) Federal Trade Commission Act (15 USC §§ 41-58): Provides general authority to the FTC to regulate deceptive and unfair trade practices. The FTC has interpreted its charter to include the authority to regulate cybersecurity practices and the unauthorized disclosure of personal information. A federal court has confirmed the FTC's authority in an enforcement proceeding brought by the FTC against Wyndham Hotels. The FTC initiated the enforcement proceeding, alleging that Wyndham Hotels unfairly exposed the payment card information of hundreds of thousands of guests to hackers in three separate breaches by failing to implement a reasonable security program. Wyndham Hotels paid a significant fine to settle the suit.

(2) HIPAA Regulations (45 CFR 160): This Rule regulates the collection and use of protected health information by hospitals, healthcare providers, doctors, healthcare clearinghouses, and any business associate of the foregoing.

(3) Children's Online Privacy Protection Rule (FTC Regulation 16 CFR 312): This rule prohibits unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the internet. Under this rule, parents have control over what information can be collected about their child.

(4) Privacy of Consumer Financial Information (FTC Regulations 16 CFR 313): Pursuant to this section of the FTC regulations, financial institutions are required to provide notice to customers about their privacy policies and practices. In addition, the rules describe situations where a financial institution may disclose nonpublic personal information about customers to nonaffiliated third parties.

(5) Standards for Safeguarding Customer Information (FTC Regulations 16 CFR 314): Entities that are subject to FTC regulations "shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards" to protect the security, confidentiality, and integrity of customer information. Covered entities include financial institutions, which is broadly defined, and any service provider to a covered entity.

(6) CAN-SPAM Rule (FTC Regulations (16 CFR 316): Regulates the collection and use of email addresses.

(7) Electronic Communications Privacy Act (15 USC § 2510) and Computer Fraud Abuse Act (18 USC § 1030): These laws restrict the intercept of electronic data, whether in transmission or stored, and prohibits access to a computer without authorization.

(8) State Privacy Laws: Nearly all 50 states have laws requiring notification to an individual whose personal information was involved in a security breach.

2. How is personal information defined?

The definition of personal information will vary depending on the particular law or regulation

being applied. In general, the term typically relates to information that can be used to identify an individual, whether alone or in combination with other pieces of information. For example, the FTC considers a person's name, address, social security number, credit card number, account information, and other similar data as "personally identifiable information." Many states take a similarly open-ended approach, where a person's name or additional piece of information that could be used to identify a person is considered personal information. The HIPAA Regulations apply to any "individually identifiable health information", stored in any form, whether, electronic, paper, or oral. The laws and regulations typically reference "customers" or "individuals", so the protections afforded to personal information likely applies to citizens and non-citizens alike. In addition, many of the regulations aim to protect data associated with an individual, rather than a corporation.

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

The key principles in relating to personal information protection in the United States are: (1) Creating and following a privacy policy for the collection and use of information from customers; (2) Using reasonable safeguards for the protection of personal or sensitive information; and (3) Providing notice of a breach to every individual whose information has been compromised.

While the term "reasonable" can be ambiguous, federal agencies in the United States have adopted as official policy the Cybersecurity Framework ("Framework"; available at <https://www.nist.gov/cyberframework>) created by the National Institute of Standards and Technology, a federal agency that promotes innovation and industrial competitiveness. The Framework consists of standards, guidelines, and best practices to manage cybersecurity-related risks. Adherence to the Framework satisfies the "reasonableness" standard used by the FTC in determining whether a company's activities are deceptive or unfair and also satisfies the HIPAA requirements. For example, in an enforcement action brought by the FTC, it alleged that Petco Animal Supplies, a large national retail chain, failed to implement policies and procedures to safeguard consumers' information. Establishing an organizational information security policy, as suggested in the Framework, would have addressed this issue.

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

Collection of personal information is generally not subject to regulation. In this regard, Europe is far ahead of the United States in regulating the collection of personal information with the implementation of the General Data Protection Regulation. Although not a requirement, the FTC, in its self-regulatory principles for online behavioral advertising, suggests that websites disclose their data collection practices and provide a customer the ability to opt-out.

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

As noted above, the compliance requirements for the processing, use, and disclosure of personal information is dependent on which law or regulation applies. Except for most health or some financial information, the processing, use and disclosure of personal information is not prohibited. With respect to health and financial information, an entity can disclose such information only as permitted in the regulations. For example, a doctor can transmit health information to an insurance company. To ensure the security of information transmitted in these situations, the entity is usually required to have a contractual relationship with the receiving party in which the receiving party agrees to be bound to the same security requirements as the disclosing party.

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

There are few restrictions on the transfer of personal information to foreign jurisdictions. However, an entity may still be subject to FTC authority for activities that

involve information transferred outside of the US. For example, Facebook is being probed by the FTC for allowing a consulting firm in the UK to access the profiles of millions of US-based Facebook users. Facebook's actions have also subjected it to investigations led by the attorneys general of New York and Massachusetts.

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?

An individual does not have specific rights to their information. Further, since consent is not required for the retention of information, an individual cannot withdraw consent. Notwithstanding the foregoing, a parent has certain rights to information about their child under the Children's Online Privacy Protection Act. In addition, if an individual's personal information is used fraudulently, that individual may have recourse against the person or entity that misused or leaked the data. The fraudulent actor may also be subject to criminal penalties.

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?

An employee's personal information is generally not treated differently under federal law or state law. Although, an employer cannot engage in discriminatory hiring practices based on information collected or made available to the employer, such as a person's medical history, family status, race, or religion. If this occurs, the individual who is denied employment would have a cause of action against the employer. In addition, as previously noted, financial and health information is treated differently than general personal information in terms of how the information can be disclosed or shared.

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

The FTC, DHS (related to HIPAA regulations), and the CFPB are the main federal agencies responsible for the enforcement of personal information protection laws in the US. In addition, various state agencies are responsible for state-level laws and regulations related to personal information.

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

Violation of laws and regulations related to personal information can result in fines from government agencies, civil lawsuits brought by individuals whose information was misused, and liabilities that are merely related to the data breach. As an example of a penalty resulting from an enforcement action brought by the FTC, LifeLock (a company who provides identity protection services, ironically) agreed to pay a $100 million fine for failing to secure consumers' personal information. The large size of the fine resulted because LifeLock violated a previous court order requiring it to implement such practices and failed to keep records of its efforts to protect its customers' data.

As an example of how a data breach can lead to liabilities that extend beyond the damages caused by the breach itself, the Securities and Exchange Commission (the "SEC") recently fined Yahoo $35 million for failing to disclose to investors a data breach involving the unauthorized access to hundreds of millions of user accounts, which included the usernames, email addresses, passwords, birthdates, phone numbers, and answers to security questions. Given the extent of the breach, the SEC determined that Yahoo misled investors since the breach was likely to have significant financial and legal implications.

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?

In response to recent breaches involving the unauthorized disclosure of personal information, the United States Congress has proposed legislation that would provide individuals with greater control over their personal information. For example, the Social Media Privacy Protection and Consumer Rights Act of 2018 would require operators of websites to provide users a copy of the data that has been collected about them. Under the proposed legislation, the website operators would also be required to provide details on how the data is being used by the website, to indicate if it has been made available to third parties, and to notify users within 72 hours if their data has been misused in any manner.

Similarly, the state of California has recently enacted the California Consumer Privacy Act, which requires websites to show users the data that is collected about them, how the data will be used, and to identify third parties that will have access to the data. The law does not take effect until 2020 and is receiving criticism from many technology companies, so the data privacy law may change before it is implemented.

Conclusion

As discussed above, the US Congress has proposed legislation protecting user's information collected by website operators. The legislation is one of many currently being considered. Further, US regulations, which are implemented by a particular agency and do not require additional authorization from Congress, continue to evolve as the type of data and the nature of its use continues to change. Even if regulations did not evolve, enforcement actions brought by the FTC and other agencies continue to help define acts that are considered "unlawful" under existing laws and regulations. As a result of the divided enforcement responsibilities, lack of unification, and changing legislative and enforcement landscape, those operating in the United States would benefit from staying abreast of the current standards for protecting personal information.

Author: Michael Monyok

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