A GLOBAL ROADMAP TO PERSONAL DATA PROTECTION

Asia Pacific, Europe & USA

Second Edition

MERITAS®

LAW FIRMS WORLDWIDE

A GLOBAL ROADMAP TO PERSONAL DATA PROTECTION

Second Edition

Asia Pacific, Europe & USA

Dennis Unkovic, Editor

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

Meyer, Unkovic & Scott LLP
www.muslaw.com

One year ago, Meritas member law firms created A Global Roadmap to Personal Data Protection in response to widely-growing interest in the impact of the European Union's General Data Protection Regulations (GDPR). The GDPR sparked a global movement of addressing the concerns of individuals who feel the need to safeguard and enhance protection of their private information. This trend has come amidst massive data breaches affecting hundreds of millions of people worldwide involving companies such as Marriott, Twitter, Under Armour, Facebook, and just recently Capital One, which may have affected over 100 million customers. In 2018, there were 1,244 publicly reported data breaches affecting US companies and consumers. Those breaches alone exposed about 446 million personal data records.

Because these events are occurring more and more frequently, Meritas is pleased to release the second edition of this well-received publication. In this new edition, the chapter on Europe was expanded to highlight the varying views of individual European countries on GDPR, and all chapter contributors have included updated privacy developments in Question 11.

We hope you will enjoy A Global Roadmap to Personal Data Protection (2nd edition). Feel free to contact any of the Meritas member firms listed if you would like more specific commentaries on this important issue.

Special thanks go out to Meritas board member Yao Rao (China) as well as to Meritas board member Darcy Kishida (Japan), Jeffrey Lim (Singapore) and Eliza Tan (Meritas Asia Regional Representative), all of whom provided crucial support. Without their hard work and dedication, this publication examining the critical issue of data privacy would not have been possible.

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

ASIA

PROFILE:

The Meritas Asia Data Security & Privacy Group is member-firm led group whose focus is data protection, privacy and data security issues in the complex multi-jurisdictional legal and regulatory landscape in Asia.

The group consolidates expertise and resources so as to provide a single robust platform to meet clients' domestic and cross-border needs as Asia prospers and becomes increasingly connected to the global economy and each unique jurisdiction adds to its body of law.

Access to the Meritas Asia Data Security & Privacy Group gives clients and other member firms access to expertise, including:

- Establishment of locally-compliant execution of data protection/privacy governance frameworks;
- Execution of data protection impact assessments
- Roll out and execution of data protection and privacy impact assessments and audits;
- Advice and practical solutions on data transfer or data export controls;
- Data breach advisory support
- Advice on use of personal data in data analytics and related projects

The following firms can provide assistance with your data protection needs in Asia:

CHINA

Yao Rao
HHP Attorneys-at-Law
Shanghai
yao.rao@hhp.com.cn
www.hhp.com.cn

Hongchuan Liu
Broad & Bright
Beijing
hongchuan_liu@broadbright.com
www.broadbright.com

HONG KONG

Philip Wong
Gallant
Hong Kong
philipwong@gallantho.com
www.gallantho.com

INDIA

Chakrapani Misra
Khaitan & Co.
Bangalore, Kolkata,
Mumbai, and New Delhi
chakrapani.misra@khaitanco.com
www.Khaitanco.com

INDONESIA

Milanti T. Kirana
HHR Lawyers
Jakarta
milantikirana@hhrlawyers.com
www.hhrlawyers.com

JAPAN

Hiromasa Ogawa
Kojima Law Offices
Tokyo
ogawa@kojimalaw.jp
www.kojimalaw.jp/en

PHILIPPINES

Emerico de Guzman
ACCRALAW
Cebu City, Davao City, and
Metro Manila
eodeguzman@accralaw.com
www.accralaw.com

SINGAPORE

Joyce A. Tan
Joyce A. Tan & Partners
Singapore
joyce@joylaw.com
www.joylaw.com

THAILAND

Palawi Bunnag
ILCT Advocates & Solicitors
Bangkok
palawib@ilct.co.th
http://www.ilct.co.th/

VIETNAM

Nhut Nguyen
Russin & Vecchi
Ho Chi Minh City
nhmnhut@russinvecchi.com.vn
www.russinvecchi.com

***Each firm is an active member of the Meritas Privacy and Data Security Group.**

MERITAS®
LAW FIRMS WORLDWIDE

CHINA
Shanghai

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, automotive, commercial retail, Internet, education, food and mining among others.

CONTACT:

YAO RAO
yao.rao@hhp.com.cn

SHUAIJIE LU
shuaijie.lu@hhp.com.cn

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

MERITAS®
LAW FIRMS WORLDWIDE

CHINA
Beijing

FIRM PROFILE:

世澤律師事務所
Broad & Bright

Broad & Bright is a prestigious, full-service Chinese firm providing a broad range of legal services for domestic and international clients, and with particular expertise and outstanding achievements in cross-border business transactions. Broad & Bright was founded by a group of highly accomplished lawyers from different practice fields. The firm's key partners received training in the most prestigious law schools both in China and overseas and have substantial work experience from top-notch international law firms. Most of them have over 10 years of experience serving multinational companies on investment and operation in China. We have four offices in China (Beijing, Shanghai, Guangzhou, Hong Kong) and one in Japan with about 100 professionals.

Broad & Bright is constantly recognized by Chambers and Partners, International Financial Law Review, The Legal 500 Asia Pacific, Asialaw Profiles, China Business Law Awards, Legalband and Asian Legal Business as one of the leading Chinese law firms in the areas of Anti-trust, M&A, PE/VC, energy and financing.

CONTACT:

HONGCHUAN LIU
hongchuan_liu@broadbright.com

FANG (HELEN) LIU
fang_liu@broadbright.com

+86 10 8513 1818
www.broadbright.com

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 current legislation contains broad, and sometimes confusing, definitions as to personal information protection. It also contains stringent regulations and in some cases severe legal penalties. The Chinese government is now still exploring the best way to implement the legal requirements. This has delayed the process of issuing the implementing rules.

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

China laws protecting personal information include:

(1) The General Rules of the Civil Law of the PRC (the "Civil Law"), 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") governs the crime of illegally collecting or providing personal information;

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

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

There are some recommendatory national standards (GB/T), technical guidance documents (GB/Z) and regulatory guidelines currently in place. They set forth stricter and detailed personal information protection requirements than the laws. However, these standards, documents and guidelines are not mandatory, such as the recommendatory national standard Personal Information Security Specification (GB/T 35273-2017) and the Internet Personal Information Security Protection Guidelines (the "Protection Guidelines") published by the Ministry of Public Security of the PRC in April, 2019.

2. How is "personal information" defined?

Under the Cybersecurity Law and the regulations related to the Consumer Rights Protection Law, "personal information" refers to 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 able to be used to identify a natural person, but it also covers all kinds of information reflecting activities of a natural person, including that involves personal privacy.

In addition, under the recommendatory GB/T 35273-2017, "personal sensitive information" refers to personal information which, upon disclosure, illegal provision, or abuse, may endanger personal and property safety, could easily lead to damaging personal reputation, physical and mental health, or discriminatory treatment. Under the Regulations on Protection of Personal Information of Children on Networks in force, personal information of children under 14 years of age is treated as sensitive personal information and granted much special protection.

As demonstrated in the above definitions, personal information protected by existing laws covers 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?

Chinese laws explicitly establish the following key principles which must 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 several other important principles which may be implied by detailed compliance requirements, including information integrity and confidentiality protection, procedural transparency, and accountability.

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, manner and extent of the personal information collection and use shall be explicitly notified 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.

In addition, GB/T 35273-2017 sets more compliance responsibilities on those who collect sensitive personal information. Express consent is required and must be voluntary, specific and clear on the basis of full knowledge of the information subject. A company's compliance program on collection, transmission, storage and sharing of sensitive personal information must be designed accordingly.

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. 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. Furthermore, the E-commence Law of the PRC requires e-commence Operators to make available to consumers the option of rejecting precision targeting of commodities using personal preference.

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?

Generally speaking, 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 to outside China unless

prior security assessment by the competent authorities has been granted. Under the Cybersecurity Law, the term 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, a person's livelihood and 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 Chinese state secrets or that may affect China's economic security.

Nevertheless, the Protection Guidelines encourages that not only the above items but all personal information collected or generated in China should be stored within China.

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 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, have the right to cancellation of their phone numbers or accounts after they cease to use the Telecom Services. The Ministry of Industry and Information Technology of the PRC examines the performance of Telecom Services in the market and will announce any uncovered violations of the aforesaid rights on a regular basis.

It should be understood, 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, 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), 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 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 with 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.

To enforce the mandatory legal requirements for the collection and use of personal information, starting from 23 January 2019, four governmental authorities, including the Cyberspace Administration of China, the Ministry of Industry and Information Technology, the State Administration for Market Regulation and the Ministry of Public Security, teamed up to launch a special investigation into illegal collection and use of personal information against mobile applications. Findings of the investigation against over one hundred mobile applications were published, plenty of which (such as TripAdvisor, and BOC Mobile Banking) were found to not have conformed to legal requirements regarding personal information protection and were ordered to make corrections.

Apart from the above governmental authorities, the Procuratorates at 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 impact,
- restoring the reputation of the aggrieved individual,
- 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; and/or
- revocation of the business license or relevant business permits/fillings; and/or
- detention of up to 20 days.

For example, in May 2018, the Shanghai Communications Administration imposed a fine of RMB 250,000 on LinkSure since the mobile application "Wi-Fi Master Key" operated by LinkSure failed to take reliable measures to ensure that the sharing of Wi-Fi passwords was conducted or authorized by the owner.

(3) Criminal Liability

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

11. Is there any recent notable development(s) in China or cases which you think is likely to affect data privacy/data protection in the future? E.g. 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 legislature, the National People's Congress of the PRC, is contemplating legislation of the Personal Information Protection Law and the Data Security Law, the drafts of which are expected to be formed and reviewed before the year 2023 according to the published legislation planning.

Simultaneously, since the Cybersecurity Law came into force, the Chinese government has remained active in drafting and bringing up for public discussion those intended regulatory regulations and detailed rules for implementing protection of personal information, such as:

- The Measures for the Security Assessment of Cross-border Transfer of Personal Information and Important Data (Draft for Public Comments) dated 11 April 2017;
- The Judgment Methods of Illegal Collection and Use of Personal Information by Mobile Applications (Draft for Public Comments) dated 5 May 2019;
- The Measures for Data Security Administration (Draft for Public Comments) dated 28 May 2019 (the "Data Security Measures Draft"); and
- The Measures for the Security Assessment of Cross-border Transfer of Personal Information (Draft for Public Comments) dated 13 June 2019 (the "Cross-border Transfer Measures Draft").

The above draft proposals aim at providing tougher regulation on and more comprehensive protection of personal information. For instance, the Data Security Measures Draft pays attention to individuals' right to withdrawal consent and right to be forgotten, requires special protection for personal sensitive information, and addresses the attribution of liability for damages in data security incidents; the Cross-border Transfer Measures Draft extends the prerequisite governmental security assessment to all the personal information collected in China before it is transferred outside China.

However, the above drafts have not been brought into force, and more discussion and amendments are expected as they are highly controversial now in China.

Summary

The personal information protection legislation in China is still in its early stage. It remains to be seen what kind of personal information protection will be required and how it will be 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 more than 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 and tax planning.

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 the data subjects 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. Some of those interests are regulated by other statutes.

The law focuses on 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 data subjects must 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. A new offence was created on unauthorized transfer of personal data to others for direct marketing. The first individual convicted for the offence 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 said 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 of 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 it's 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, date of birth should not be requested when all that 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 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:

(i) make a data access request and know the reason for the refusal to such request;

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

(iii) request the erasure of incorrect data;

(iv) require that their personal data is not used for direct marketing;

(v) make a complaint to the Privacy Commissioner for Personal Data about contravention of the legislation;

(vi) 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

(vii) 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 protection of employees' personal information. There are other codes and guidelines on other 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, currently at 13th Floor, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong 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 there any recent notable development(s) in Hong Kong or cases which you think is likely to affect data privacy/data protection in the future? E.g. 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 General Data Protection Regulation (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. The current Hong Kong legislation and the GDPR share certain common features, partly because when the former was drafted in the 1990s, reference was made to the Organization for Economic Co-operation and Development (OECD) Privacy Guidelines 1980 and the then EU Directive. In view of the new features introduced by the GDPR, the Privacy Commissioner for Personal Data, as Hong Kong's regulator on data protection, has published a booklet on the GDPR in the local context to assist local data users in complying with it. Apart from that, the Commissioner has recently published papers on data protection issues relating to blockchain, internet of things (IoT) and the digital ecosystem generally. It is generally believed that references will be made to all these new trends, discussed by the Commissioner, published at https://www.pcpd.org.hk, in the next round of legislative amendments.

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. Guidelines and guidance notes indicate the manner in which the Privacy Commissioner for Personal Data proposes to perform its functions or exercise its powers under the law. They represent the best practices in the opinion of the Commissioner, but any breach will not necessarily give rise to legal liability.

MERITAS®
LAW FIRMS WORLDWIDE

INDIA

FIRM PROFILE:

KHAITAN &CO
Advocates since 1911

Khaitan & Co is a heritage firm of lawyers advising leading business houses, multinational corporations, global investors, financial institutions and the government since 1911.

Service Philosophy
Our ambition is to be a respectable law firm providing efficient and courteous service, to act with fairness, integrity and diligence, to be socially responsible and to enjoy life.

Main Areas of Practice
- Banking and Finance
- Capital Markets
- Competition/Antitrust
- Corporate/Commercial advisory
- Data Privacy
- Dispute Resolution
- Energy, Infrastructure and Resources
- Employment, Labour & Benefits
- Environment Law
- Funds
- Intellectual Property
- Private Client and Trusts
- Real Estate
- Tax
- Technology, Media & Telecom
- White Collar Crime

Data Privacy: The firm has a robust data privacy practice ranging from advice on legal requirements, review and drafting of documentation (contracts, notices and disclaimers) and processes, compliance assessment, and dispute resolution.

Local and International Experience
Khaitan & Co has widespread domestic and foreign clientele serviced from across locations – Mumbai, Delhi, Bengaluru and Kolkata.

CONTACT:

HARSH WALIA
harsh.walia@khaitanco.com

+91 22 6636 5000
www.Khaitanco.com

Introduction

At present, India does not have an exclusive and comprehensive data protection legislation. Certain provisions pertaining to data protection are incorporated in the Information Technology Act, 2000 (IT Act) and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules) framed under the IT Act. Additionally, there are sector specific regulations, e.g. in relation to payment systems, telecom, healthcare etc. that stipulate certain obligations in relation to protection of personal data and information.

In recent times, the Government has laid considerable emphasis on the formulation of a comprehensive data protection legislation, which in many ways is a necessity in the present-day scenario and a key indicator for a country from the perspective of foreign investment and cross-border trade. This sentiment led to the formation of an expert committee for devising a data protection framework for India (Expert Committee), which was spearheaded by Justice (Retd.) B.N. Srikrishna. The Expert Committee released a draft of the Personal Data Protection Bill 2018 (Draft PDP Bill), which is being considered by the Indian Government at present. Earlier, in 2017, the 'right to privacy' was also declared by the Supreme Court of India as a fundamental right guaranteed by the Constitution of India, which has provided much needed impetus to this initiative.

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

India currently does not have an exclusive legislation governing protection of personal data or information. Currently, the data protection framework is encapsulated under the provisions of the IT Act and SPDI Rules. Data protection related obligations are also incorporated in sector specific regulations, e.g. in relation to payment systems, telecom and healthcare etc.

It is important to point out that the IT Act and SPDI Rules broadly classify personal information under two categories, viz. 'personal information' (PI) and 'sensitive personal data or information' (SPDI) and afford different degrees of protection to each kind of personal information. The SPDI Rules primarily grant protection to the provider of SPDI and therefore we have provided our responses to all questions raised below from the perspective of SPDI only.

2. How is personal information defined?

Under the SPDI Rules, PI is defined as any information that relates to a natural person, which either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.

Please note that the SPDI Rules primarily afford protection to SPDI and therefore, it is important to consider the definition of SPDI. SPDI is a subset of PI and means such "personal information which consists of information relating to (i) password (ii) financial information (iii) physical, physiological and mental health condition (iv) sexual orientation (v) medical records (vi) biometric information (vii) any detail relating to above as provided to a body corporate for providing services (viii) any of the information received under above clauses for processing, stored or processed under lawful contract or otherwise". The definition of SPDI excludes any information that is freely available or accessible in the public domain or furnished under the Right to Information Act, 2005 or any other law.

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

The provisions of the IT Act and SPDI Rules do not formally lay down principles relating to protection of PI and SPDI. However, certain conditions and requirements have been prescribed in cases where an entity collects, receives, possesses, stores, deals with, handles, discloses or transfers SPDI. We have touched upon these conditions and requirements in our responses to the questions raised below.

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

The following sets out the mandatory compliance requirements for the collection of SPDI under the SPDI Rules:

- Conditions for collection: An entity or any person collecting SPDI on its behalf is required to obtain consent in writing (through letter, fax or email) from the provider of the SPDI regarding the purpose of usage before the collection of such information. Further, SPDI shall not be collected unless it is collected for a lawful purpose connected with the function or activity of the body corporate, and the collection of SPDI is considered necessary for that purpose.
- Safeguards for collection: At the time of collecting SPDI, the collector of SPDI must take reasonable steps to ensure that the provider of SPDI has knowledge of the fact that SPDI is being collected, the purpose for which it is being collected, who are the intended recipients of their SPDI and the name and address of the agency collecting and retaining their SPDI.

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

Please note that the IT Act and SPDI Rules do not define the term 'processing'. Generally speaking, the applicability of SPDI Rules is triggered when an entity or any person/ entity on behalf of such entity "collects, receives, possesses, stores, deals with or handles" SPDI. Bearing this in mind, please note the following compliance requirements under the SPDI Rules relating to "processing" and use of SPDI:

- Privacy Policy: According to the SPDI Rules, in case a body corporate (which means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities) deals with or handles SPDI of any other person, then it must provide a privacy policy to providers of SPDI and ensure that the same is "available for view". The privacy policy must provide for the type of PI or SPDI collected by the entity, the purpose of collection and usage of such information, disclosure of information (including SPDI) and reasonable security practices and procedures implemented by the entity.
- Purpose limitation: Upon collection, a body corporate has to ensure that SPDI is used for the purpose for which it has been collected.
- Storage limitation: Further, SPDI should be retained by the body corporate only so long as it is necessary for the fulfilment of the specified purpose(s), unless the law requires retention of such information for a longer duration.

As far as disclosure of SPDI to third parties is concerned, please note that it is only permitted with the prior permission of the provider of SPDI, unless such disclosure has already been agreed to by the provider in the contract pursuant to which she/ he provides her/ his SPDI or where such disclosure is necessary for compliance of a legal obligation. The third party receiving the SPDI is not entitled to further disclose such information. Further, SPDI can be shared with government agencies (pursuant to a request made in writing) without prior consent from the provider of SPDI, for the purpose of verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution and punishment of offences. As a part of the written request, the government agency shall also state that the information so obtained shall not be published or shared with any other person.

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

According to SPDI Rules, SPDI may be transferred by the body corporate collecting SPDI to any body corporate or person within India or any other country that ensures the same level of data protection that is adhered to by the former as provided in the SPDI Rules. Further, the transfer is allowed only if it is necessary for the performance of a lawful contract or where the provider of SPDI has consented to such data transfer.

Separately, please note that there are restrictions on transfer of certain types of data outside India under some sectoral regulations (which are applicable on payment system providers and telecom service providers). Therefore, to the extent such types of data comprise of PI and SPDI, it is possible that the transfer of PI and SPDI to other jurisdictions can be impacted.

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 provider of SPDI have the following rights under SPDI Rules:

- The right to be informed about (a) the fact that SPDI is being collected, (b) purpose for which it is being collected, (c) who are the intended recipients of their SPDI and (d) the name and address of the agency collecting and retaining their SPDI
- The right to review the information provided to collecting entities and the right to request for correction of any SPDI, found to be inaccurate or deficient
- The right to not provide any SPDI that is sought to be collected
- The right to withdraw her/ his consent that was provided earlier for use or retention of her/ his SPDI any time while availing the relevant services
- The right of redress of grievances in connection with the processing of her/ his SPDI

As noted above, the SPDI Rules do enable the provider of SPDI to withdraw her/his consent, which has been provided earlier. The notice of withdrawal must be in writing and can be sent at any time while availing the services. It is important to note that as a corollary, the body corporate will have an option to not provide goods and services for which the SPDI was sought after the provider has withdrawn her/ his 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?

No, there is no special provision for the protection of an employee's PI or SPDI. We have not come across any other types of personal information that receive special protection. However, it is possible that certain types of PI and SPDI are also regulated by sector specific regulations, to the extent that they form part of the data or information that is sought to be protected or covered by such sector specific regulation.

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

At present, there is no specifically constituted regulatory authority that is responsible for implementation and enforcement of laws relating to protection of personal information in India.

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

Yes, the IT Act prescribes certain penalties, liabilities and remedies in case of violation of relevant provisions relating to protection of PI and SPDI. The following may be noted in this regard:

- In case of negligence in implementing and maintaining reasonable security practices and procedures which results in wrongful loss or wrongful gain to any person, such entity shall be liable to pay damages by way of compensation to the person so affected.
- Any person who has secured access to any material containing PI about another person and who discloses such material to another person with the intent to cause or knowing that he/she is likely to cause wrongful loss or wrongful gain and without the consent of the person concerned, or in breach of a lawful contract, may be punished with imprisonment that may extend to three years, or with a fine which may extend to INR 500,000 (Indian Rupees five hundred thousand) or with both.

11. Is there any recent notable development(s) in India or cases which you think is likely to affect data privacy/data protection in the future? E.g. 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?

Yes, a new, comprehensive personal data protection legislation is in the pipeline. The Expert Committee formed by the Government of India released the Draft PDP Bill in July 2018 after a process of public consultation. The efforts to create a robust data protection framework for India were catapulted by a landmark decision of the Supreme Court of India in 2017 (Privacy Judgment) where the right to privacy was declared as a fundamental right, guaranteed by the Constitution of India. In the Privacy Judgment, the Supreme Court emphasised on informational privacy and the importance of establishing a robust data protection regime for balancing of privacy interests of individuals with imperatives of the State and information needs of the economy.

The Draft PDP Bill is heavily inspired by the European Union's General Data Protection Regulation (GDPR) and aims to strengthen the data protection framework in India by introducing comparatively stringent requirements with respect to consent, cross-border transfer and disclosure to third parties. Some of the salient features of the Draft PDP Bill are set out below:

- Unlike the SPDI Rules (which primarily afford protection to SPDI), the Draft PDP Bill envisages protection to both 'personal data' (PD) as well as 'sensitive personal data' (SPD).
- The Draft PDP Bill postulates several core data protection principles such as fair and reasonable processing, purpose limitation, collection limitation, data quality, data storage limitation and accountability.

- The Draft PDP Bill provides certain grounds for processing of PD/ SPD, which include (i) consent, (ii) function of the State, (iii) prompt action (e.g. medical emergency or natural disasters), (iv) compliance with law or order/ judgment passed by a court, (v) employment (where obtaining consent is not appropriate or obtaining consent involves disproportionate efforts) and (vi) reasonable purposes that may be specified by the Data Protection Authority of India (DPAI).
- The Draft PDP Bill also grants certain unprecedented rights to data principals (such as right to data portability, right to erasure etc.). It also requires data fiduciaries and data processers to adhere to data transparency and accountability measures (such as implementing privacy by design, appointing data protection officers and conducting data protection impact assessments).
- The Draft PDP Bill prescribes comparatively stricter rules for cross border transfers and also imposes data localisation requirements in respect of certain types of PD and SPD.
- The Draft PDP Bill contemplates the constitution of DPAI for enforcement of the provisions of the Draft PDP Bill.
- The Draft PDP Bill envisages a stringent penalty scheme, which is in line with the provisions of the GDPR and also prescribes criminal penalties in respect of certain offences.

The Draft PDP Bill is likely to be presented in the lower house of the Indian Parliament soon, after undergoing minor modifications. In order to become law, the final version of the Draft PDP Bill will have to be passed by the lower and upper house of Parliament and thereafter receive the assent of the President of India. Further, if the Draft PDP Bill is enacted in its present form, its implementation will be carried out in a phase-wise manner, which will provide a moratorium to entities for re-engineering their practices and procedures to bring them in compliance with the new law. Some of the requirements laid down under the Draft PDP Bill are likely to have a significant impact on the cost of operations of entities.

In a follow up to the Privacy Judgment, the Supreme Court in another significant ruling in 2018 (Aadhaar Judgement) examined various principles of data protection (including data minimisation, purpose limitation, data retention and data security) and applied the same to uphold the legality of a Government sanctioned unique identification scheme, i.e. Aadhaar. Recently, the Telecom Disputes Settlement and Appellate Tribunal, which is also seized with the powers of the Cyber Appellate Tribunal, has also issued some rulings relating to payment of compensation for failure to protect data under the IT Act. Broadly speaking, courts in India have been relatively proactive in adjudicating cases that raise concerns of violation of data privacy and protection in recent times.

Conclusion

The legal framework relating to personal data and information protection in India is currently undergoing a meta-morphosis. The need for an effective data protection framework is imminent in the present day scenario, especially with increasing adoption of digital technologies. The existing legal framework, which is embodied in the IT Act and SPDI Rules, requires a major face-lift to meet the standards set by data protection legislations of other major countries. It is expected that the Draft PDP Bill, if enacted in its present form, will help bridge that gap. Consequently, it will also lead to additional compliances for entities and require them to undertake a thorough re-evaluation of their current data protection practices.

MERITAS®
LAW FIRMS WORLDWIDE

INDONESIA

FIRM PROFILE:

HHR
LAWYERS

HHR Lawyers was established in 1996 and is a reputable Indonesia commercial law firm with a global reach. For more than 20 years of experience and its multi-years of practice, our firm has evolved and demonstrated its ability to provide superior legal works and client services which are fully supported by almost 30 experienced Indonesian lawyers with skills across a broad range of their respective areas of specialty.

Our firm's legal services have been acknowledged in various professional circles, namely in: (i) Capital Markets, Banking and Finance; (ii) Commercial Dispute Resolution; (iii) Corporate and M&A; (iv) Energy and Natural Resources; (v) Infrastructure Development; (vi) Manpower & Industrial Relations; (vii) Real Estate; (viii) Trade and Competition & Intellectual Property.

With sustaining its ability through providing a full range of legal services to its clients, HHR Lawyers is consistently ranked as a leading and dynamic law firm in Indonesia by independent surveys and international legal publications.

CONTACT:

MILANTI T. KIRANA
milantikirana@hhrlawyers.com

M. FATHAN NAUTIKA
fathannautika@hhrlawyers.com

+62 2988 5988
www.hhrlawyers.com

Introduction

Indonesia has various sectoral laws and regulations related to data protection, for example in banking, telecommunication, public information and civil administration sector. Up until today, the specific law which accommodates private data protection is still under the legislation process and is expected to be enacted by the end of 2019. For reference, the following are several sectors which already established the data protection arrangement.

Telecommunication

In 1999, the government of Indonesia enacted Law No. 36 of 1999 on Telecommunication ("Telecommunication Law"). In spite of the generality of the provisions on confidentiality information, the Telecommunication Law can be considered as the first law which adopted the data privacy protection. Under the Telecommunication Law, any person is prohibited from tapping any information through the telecommunication system, and that the telecommunication service provider is obligated to keep confidential any information received or transmitted through its system. Under the provisions of the Telecommunication Law, tapping means adding a certain gadget within the telecommunication tools for purposes of obtaining certain information from the other person illegally.

Residents Administration

In 2006, Law No. 23 of 2006 on Residents Administration – as lastly amended by Law No. 24 of 2013 – ("Residents Administration Law") provides the residents data protection arrangement. Whereby, the government of Indonesia is obliged and is held responsible in storing and protecting the residents' personal data. Under the Residents Administration Law, the residents' personal data shall contain the information on mental/physical disabilities, fingerprints, eyes irises, signatures, and other elements that may cause great embarrassment and shame to the person. Recently, the implementing regulation of Residents Administration Law, i.e. Government Regulation No. 40 of 2019 ("GR 40/2019") has been enacted.

Electronic Information and Technology

In 2008, the government of Indonesia enacted Law No. 11 of 2008 on Electronic Information and Transaction which was lastly amended by Law No. 19 of 2016 ("EIT Law"). EIT Law stipulates that personal data is a part of the privacy rights and requires the electronic system providers to conduct the protection of information in their system. EIT Law was further followed up by the issuance of the Government Regulation No. 82 of 2012 on Implementation of Electronic System and Transaction ("GR 82/2012"), which is not only established certain obligations to the electronic system provider but also granting the individuals rights to give consent whether their respective personal data can be used by the electronic system provider or not in the future. At the end of 2016, Indonesia issued the implementing regulation of GR 82/2012, i.e. the Minister of Communications and Information Regulation No. 20 of 2016 on the Guidelines Regarding Protection of Personal Data in The Electronics System ("MOCR 20/2016").

Public Information

Under the provisions of Law No. 14 of 2008 on Disclosure of Public Information ("Disclosure of Public Information Law"), personal rights cannot be disclosed by any public institutions. Furthermore, the Disclosure of Public Information Law also prohibits the disclosure of private information of any person, particularly relating to information about a person's family, medical and psychological records, earnings, bank records, educational records and other relevant private information.

Banking and Financial Institutions

Aside from the aforementioned regulations, other sectors which have specific arrangements on data protection are banking and financial institution. The arrangements are as particularly regulated under: (i) Indonesian Central Bank Regulation No. 7/6/PBI/2005 ("ICBR 7/2005"), which regulates the transparency of banking products and the use of customer's personal data for banking activities; and (ii) Financial Service Authority Regulation No. 1/POJK.07/2013 ("FSAR 1/2013"), which specifically regulates the consumer protection in the financial service sector, including the consumer's data.

Having considered the above, it is a fact that the data protection arrangement in Indonesia has spread in many sectors and needs to be accommodated and synchronized with one another.

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

In line with the current development in this digital era, the most conversed issue now is the personal data relating to the electronic information and transaction. That being said, the major personal information protection laws or regulations in Indonesia are the EIT Law and its implementing regulations, in this matter GR 82/2012 and MOCR 20/2016. In addition, another sector that is heavily relied on the personal data protection arrangement is their banking sector. It is important to note that ICBR 7/2005 requires that banks must obtain a written notice from the customer, in the event that the bank will provide and distribute any of their customers Personal Data for a commercial purpose, unless otherwise regulated by the prevailing laws and regulations.

2. How is "personal information" defined?

Personal information in Indonesia shall be referred to as the Personal Data, which under the GR 82/2012 and MOCR 20/2016, is defined as:

"Certain individual data, of which: (i) the accuracy is stored, maintained, and retained, and (ii) the confidentiality is protected."

Furthermore, the definition of "certain individual data" itself shall be referred to as any true and actual information attached to, and identifiable towards, whether directly or indirectly, the respective individual of which utilization is in accordance with the prevailing laws and regulations.

Prior to the enactment of EIT Law and MOCR 20/2016, the Residents Administration Law has formerly set out the definition of Personal Data. However, its protection is narrowed down to "personal data of residents" only, for example: physical or mental disability records, fingerprints and signatures.

Considering that MOCR 20/2016 has defined "certain individual data" as broadly as possible, we believe that the current Indonesian data protection law has been reaching out and covering all attached information of each individual. Even though these regulations are equipped with administrative sanctions should the electronic system provider fail to protect the personal data, such as temporary suspension in doing business – however, its enforcement is still in limbo.

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

Referring to the provisions of the Telecommunication Law, EIT Law, MOCR 20/2016, ICBR 7/2005 and FSAR 1/2013, the key principle with regards to personal information is basically the consent of the respective person. Under the aforementioned laws and regulations, the prohibition from using and/or sharing any personal data/information may be waived based on a specific consent of the relevant person.

In addition, MOCR 20/2016 has specifically listed down the "principles of good personal data protection" as follows:

a. respect for the personal data as a matter of privacy;
b. confidentiality in accordance with the specific consent and/or the provision of laws and regulations (lawful basis);
c. must be based on a specific consent;
d. relevant with the objective of the process of acquiring, collecting, processing, analysing, storing, displaying, announcing, delivering and distributing of personal data;
e. feasibility of the electronic system being used;
f. the good faith to immediately notify the owner of personal data in the event of any failure of personal data protection;
g. the availability of internal rules in managing personal data;
h. responsibility towards the personal data that is in the possession of the user;
i. easy access and correction of the personal data by the owner of such personal data;
j. wholeness, accuracy, and validity as well as updates of the personal data.

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

Compliance in acquiring and collecting personal information must be limited to relevant information only and it must be in accordance with the purpose of acquiring and collecting the data. The other important aspect is the process of acquiring and collecting data must be done accurately. Referring to the answer in Q3 above, the process of acquiring and collecting of data must respect privacy rights over Personal Data; therefore, the data collector must reserve the individual rights by stating that the data could be served as confidential or not. Subsequently, the data collector has the obligation to verify the accuracy of the data directly to its owner. If it is acquired or collected indirectly, the data must be verified based on the results of various processed data sources.

After the verification process, the acquired and collected data must be gathered in a compatible and legal electronic system, as part of mitigation from the service provider that the data will be maintained properly.

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

The compliance requirement for processing, using and disclosing personal data is that the electronic service provider may only do so by firstly informing the data owner (from the beginning) that they will process, use and disclose the data. According to the basic privacy principle, the personal data owner may give their consent if their data can be processed, used and disclosed or not. If the data owner has confirmed and granted their consent, the verified data shall be the only data that is allowed to be processed, used and disclosed. Therefore, consent is the key in personal data protection – without it – the electronic service provider will be imposed with liability should they decide to process, use and disclose the personal data. However, for purposes of law enforcement, the electronic service provider must provide the personal data that resulted from the electronic system process as per request of the law enforcer. Although, only relevant and related data to a police investigation that can be requested by and to be provided for the law enforcers.

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

Transmission of personal data from Indonesia to other jurisdictions is allowed, for so long as the electronic service provider follows the necessary steps and complies with the prevailing requirements. Transmission of personal data that is managed by the electronic system provider from the Indonesian territory to private parties domiciled outside of Indonesia, must comply with the following requirements: (i) must be in coordination with the relevant Minister or official/institution authorized for this purpose; and (ii) apply the prevailing laws and regulations regarding the exchange of personal data across national borders.

Coordination shall be in the form of reporting the transmission of personal data plan, which at least contains a clear name of the destination, the recipient's name, the date of transmission, and the reason/purpose of sending; seeking for advocacy, if needed; and reporting the results of the transmission.

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?

Yes, individuals do have the right to to withdraw their consent and request the electronic service provider to destroy their data that is under the electronic service provider's retention.

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 shall be defined also as personal data. Therefore, there will be no difference in protecting the employee's personal information. Additionally, the Residents Administration Law can be seen as a special protection of resident's data, which specifically defines what kind of data that the law's protecting.

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

The regulation itself was prepared and issued by the Minister of Telecommunication and Information of the Republic of Indonesia. Furthermore, the Directorate General and/or a Supervision Institution or Sectoral Regulator will conduct the implementation and enforcement.

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

Yes, Indonesian laws and regulations have determined penalties and liabilities if any of the personal information protection obligations is violated. For example, there is an administrative sanction if every person who acquires, collects, processes, analyzes, stores, displays, announces, transfers, and / or destroys personal data without the right to do so, or does not comply with the provisions in laws and regulations in the form of:

a. a verbal warning;

b. a written warning;

c. a temporary suspension of activities; and/or

d. announcements in online media on the violation.

the Administrative sanctions above will be imposed by the Minister of Telecommunication and Information of the Republic of Indonesia, or the Directorate General and/or the Supervision Institution or Sectoral Regulator, in accordance with statutory provisions.

Besides the supervision and enforcement functions in the government institutions, the individuals also have the right to submit complaints to the Minister for the failure to protect the confidentiality of their Personal Data by the electronic service provider. Such complaints are intended as an effort to resolve any disputes by deliberation or through other alternative resolution efforts. In addition to the deliberation or alternative resolution process, the Directorate General and/or the Supervision Institution or Sectoral Regulator may give recommendations to the Minister to impose any administrative sanction to the electronic service provider, regardless of whether the parties reach a consensus from the deliberation or alternative resolution or not.

In the event that deliberation or alternative resolution have not been able to resolve the disputes, the personal data owner may file a civil lawsuit for the failure of confidential protection by the electronic service provider.

However, there is no clear remedy against the electronic service provider that fails to comply with the laws and regulations. Unlike in consumer protection law, where a product is defective, the producer must immediately make a remedial effort such as recalling the product or compensate the damage; there is no remedial effort that must be taken into account by the electronic service provider prior to any arising disputes.

11. Is there any recent notable development(s) in Indonesia or cases which you think is likely to affect data privacy/data protection in the future? E.g. 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?

Yes. For the past few years, the government of Indonesia has been preparing a bill and set out as the priority by the Indonesian House of Representative. We expect to have a new law on data protection by the end of this year. The new law is important and shall serve as the bridging law on the implementation and enforcement of data protection, by connecting all parties involved in the collection, processing, retention and even dissemination of personal data, electronically or non-electronically. By the enactment of this new law, we expect any misuse of personal data can be reduced and mitigated.

The recent case in Indonesia that most likely affects the data protection arrangement is the leak of Indonesian resident data that was shared and sold online, which case is currently under police investigation. This case indicates the necessity of the government of Indonesia to immediately enact the new law on data protection. The collection, processing, analysis and retention of electronic or non-electronic personal data, obviously involves various stakeholders e.g. government institutions, electronic service providers, outsourced companies hired to process the data, or even record management service providers. Personal data protection must be accommodated under an umbrella regulation to synergize all parties involved in the usage of personal data.

Summary

Data protection arrangement in Indonesia must also cover the protection in both electronic and non-electronic systems. To enforce data protection with legal certainty, the new law on data protection which accommodates all relevant sectors is necessary to be enacted as soon as possible. All stakeholders including investors and law enforcer should anticipate a major change with regards to the data protection arrangement in Indonesia.

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, which the EU did on January 23, 2019. As a result, the EU and Japan can now freely transfer personal data with each other without requiring any further safeguards.

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: (i) financial services; (ii) medical services; (iii) telecommunications; (iv) broadcasting; (v) postal services provided by Japan Post; (vi) letter delivery services; and (vii) 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: (i) 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 (ii) 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 (i) 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 now specifically addresses the transfer of personal information to other jurisdictions, and 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:

(i) is required by that country's laws and regulations;

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

(iii) 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 there any recent notable development(s) in Japan or cases which you think is likely to affect data privacy/data protection in the future? E.g. 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 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, as mentioned above, the EU formally recognized Japan as providing adequate data protection in January 2019. That recognition should promote greater cross-border sharing of data and increased business opportunities.

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 2019/2018, it was recognized as an Outstanding Firm 2019 by Asialaw Profiles, Philippine Law Firm of the Year & Outstanding Client Service Award by Asialaw Regional Awards 2019, 2019 Law Firm Award by Benchmark Litigation Asia Pacific, Top Tier Law Firm and Leading Firm by The Legal 500, Top Ranked Firm by Chambers Asia Pacific, Firm of the Year 2018 by Asian Mena Counsel, and the Philippine Law Firm of the Year 2018 by 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 DE GUZMAN
eodeguzman@accralaw.com

ANA LOURDES TERESA ARNALDO-ORACION
aaoracion@accralaw.com

+63 2 830 8000
www.accralaw.com

Introduction

The Philippine Data Privacy Act of 2012 or Republic Act No. 10173 ("DPA"), 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 enactment of the DPA in 2012, without no centralized regulatory oversight for personal data processing or comprehensive protective measures for the data subjects, the wealth of personal data at that time was subject to abuse and misuse — from the unmitigated use and sharing of contact details for purposes beyond those initially contemplated, to identity theft or security breaches— to the detriment of the data subject's constitutionally guaranteed right to privacy. The DPA had its origins as early as 2006 when the Philippine Department of Trade & Industry ("DTI") issued DTI Administrative Order No. 8-2006 on the "Guidelines on the Protection of Personal Data". Said DTI issuance was patterned after the European Union's ("EU") Data Protection Directive of 1995 (officially Directive 95/46/EC) – the predecessor of the current EU Genenal Data Protection Regulation ("GDPR"). Hence, the Philippine DPA is deeply rooted in the standards and principles espoused by the EU GDPR.

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 ("DPA"), together with its Implementing Rules and Regulations ("IRR"). Apart from the DPA and its IRR, the National Privacy Commission ("NPC") – the lead government agency tasked to administer privacy laws in the Philippines – issues circulars and advisories that further flesh out and implement the provisions of the DPA and its IRR.

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 home address, mobile 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 information and, thus protected by the DPA. From this legal definition, information pertaining to juridical entities (such as corporations, companies, and partnerships) are not covered by law. This exclusion of "corporate information" from the scope of the DPA notwithstanding, in instances where records or documents pertaining to juridical entities contain personal information (for example, names and contact details of incorporators/corporate officers in company registration documents), portions of such records or documents containing personal information should be treated as covered by the DPA.

From the universe of "Personal Information", our law carves two "special" sets of personal information – "Sensitive Personal Information" and "Privileged Information". "Privileged Information" is defined as "refers to any and all forms of data which under the Rules of Court and other pertinent laws constitute privileged communication".[2] Under Rule 130, Section 24 of our Rules of Court, the following constitute "privileged communication": (1) marital or spousal communication; (2) lawyer-client communication; (3) doctor-patient communication; (4) priest-penitent communication; and (5) public official communication. Meanwhile, "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." [3]

The foregoing list under the DPA outlining what constitutes "Sensitive Personal Information" is exhaustive – those personal data not included in the enumeration is considered "non-sensitive" but nonetheless still "Personal Information" covered by the DPA (e.g., name, contact details such as phone numbers, e-mail addresses, etc.). Under the DPA, both "Privileged Information" and "Sensitive Personal Information" are treated the same.

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

Similar to the principles espoused by the EU GDPR, "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 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 requirements. 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 declared to the data subject. For example, if the purpose of collecting the data is to identify the winner of the contest, then the individual's name and contact information should suffice. Hallmark of the principle of transparency under the DPA is the need to have either the clear, expressed consent of the data subject or a valid legal ground to the processing of personal information. Primarily, the data subject must be informed as to how his personal information will be used or "processed" – who are the parties involved (e.g., data controllers, data processors, third parties), the purposes why such personal information is needed, how long shall personal information be maintained, appropriate security measures being implemented to protect the data, and contact details as to how data subjects can reach out to the data controller in case he has any concerns. Absent any of the foregoing, "processing of personal information" can be generally considered as unauthorized under the DPA.

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 clear, expressed consent. This notwithstanding, the DPA recognizes situations wherein the nature or exigencies thereof may not accommodate a situation wherein the individual can give consent but his or her personal data still needs to be processed.[4] A good example is when 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 DPA, among other situations, recognizes this exception and allows for processing of personal data even without the data subject's consent.

The foregoing exempted situations as outlined in the DPA only exempt such instances of processing personal information from the consent requirement. It does not exclude data controllers and/or data processors from complying with the rest of the requirements and standards under the DPA, such as, but not limited to, implementing reasonable and adequate security measures to protect the "confidentiality, integrity, and availability" of personal information.

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

Generally, Personal Information Controllers ("PIC") and Personal Information Processors ("PIP") are required to appoint or designate a Data Protection Officer ("DPO"). For certain PICs and PIPs, they are required to register their DPO and their data processing systems ("DPS") with the NPC. These PICs and PIPs that are required to register with the NPC are the following:

(1) Those that employ at least two hundred fifty (250) employees; or

(2) Those that undertake operations or personal information processing activities which are likely to pose a risk to the rights and freedoms of the data subjects, or such processing is not occasional, regardless of the number of employees; or

(3) Those that process sensitive personal information of at least one thousand (1,000) individuals; or

(4) Regardless of the number of employees or data subjects, those that belong to sectors / industries which the NPC classified as "critical sectors", e.g., banks and non-bank financial institutions; hospitals, medical centers, and health-related organizations; schools and universities; research institutions; business process outsourcing companies (including those acting as "shared service" providers or have a "captive market"); telecommunication companies.

Regardless of whether one is covered by the NPC registration requirement or not, all PICs and PIPs must implement the appropriate and reasonable security measures to ensure protection of the "confidentiality, integrity, and availability" of personal information. The DPA's IRR enumerates these specific security measures, and categorizes them into three (3) groups, namely: (1) organizational; (2) physical; and (3) technical security measures. The following are the organization security measures that PICs and PIPs must implement:

1) Designation of 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) Creation of 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) Conduct 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 contracts with PIPs (i.e., third party suppliers/vendors) also implement the security measures required by the DPA and its IRR. [5]

The following are the physical security measures:

1) Establish policies/procedures to monitor and limit access to, and activities in, rooms, workstations or facilities (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. [6]

Finally, the following are the technical security measures:

1) Establish a security policy with respect to processing personal data;
2) Establish safeguards to protect computer networks against unauthorized access or to ensure data integrity and functioning of the system;
3) Ensure and maintain the confidentiality, integrity, availability, and resilience of their processing systems and services;
4) Conduct regular monitoring for security breaches, accessing vulnerabilities, and preventive, corrective, and mitigating action against data breach;

5) Develop a capability to restore availability and access to personal data in a timely manner;
6) Establish processes and protocols for testing the effectiveness of security measures; and
7) Implement encryption measures of personal data during storage, transit, authentication process, or any measure that controls and limits access.[7]

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

Generally, the DPA does not restrict cross-border transfers of personal information, provided that: (1) the relevant data subjects are sufficiently informed/notified of such transfer and that they consent to such transfer; and (2) in the event that the personal information shall be transferred to a third party, the relevant agreement (whether the same be an "outsourcing/subcontracting" agreement or a "data sharing" agreement) must be in place. With respect to the agreement referred to in the second item, the DPA and its IRR require the inclusion of "mandatory clauses" to ensure that the third party will, among others, comply with the requirements of the DPA and implement the appropriate security measures. Under the DPA, affiliated or related companies or entities belonging to the same group of companies are considered "third party" to each other.

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 or processed, 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.

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]

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, an employee's personal information is not treated differently from that of the treatment accorded to personal information in general.

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

The NPC is an independent body tasked to administer and implement the provisions of the DPA and its IRR, 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?

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.[10] Apart from fines and imprisonment (both of which are mandatory), a complaining data subject can seek civil damages (e.g., actual damages, moral damages, exemplary damages, etc.).

11. Is there any recent notable development(s) in the Philippines or cases which you think is likely to affect data privacy/data protection in the future? E.g. 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 DPA and its IRR, no further legislation is in contemplation in the Philippines relating to personal information protection. Nonetheless, under its legal mandate, the NPC regularly issues Circulars and Advisories to further clarify the implementation of the DPA and its IRR. The NPC likewise issues Advisory Opinions for queries, which it publishes on its website and are considered to have, at the very least, persuasive effect. Recently, the NPC issued its Rules on Compliance Checks outlining the procedure for the conduct of web privacy sweeps, compliance document submissions by covered entities, and on-site compliance inspections. Moreover, the NPC has categorically declared that single professional practitioners, such as lawyers and medical professionals, are required to register with the NPC (separate registration process and forms were established by the NPC to cater to this requirement).

Conclusion

To ensure that all individuals and entities (i.e., PICs and PIPs) comply with the requirements of the DPA, its IRR, and NPC's issuances, the NPC enunciated what it called the "Five Pillars of Pivacy Compliance", namely:

1. Appoint a DPO;
2. Conduct a Privacy Impact Assessment;
3. Create a Privacy Manual which contains the protocols for each step in processing personal information with the goal of complying with the prevailing privacy law and regulations;
4. Implement a privacy and data protection policy; and
5. Install and maintain a breach reporting protocol.

Finally, in reference to the registration requirements, covered PICs and PIPs can still register with the NPC (initially, the registration of the DPO – Phase I registration); no penalty for late filing is imposed. However, to date, the registration of the DPS – Phase II registration is still suspended by the NPC until further notice.

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 3(k).*

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

[4]/ *Id. Section 12 with respect to processing "Personal Information" (i.e., those that are not classified as "Sensitive Personal Information" and "Privileged Information"; and Section 13 with respect to processing "Sensitive Personal Information" and "Privileged Information".*

[5]/ *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").*[6]/ *Id.* Rule I, Section 3, f.

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

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

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

[10]/ *Id. Sections 25 to 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.

Service Philosophy

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.

Main Areas of Practice

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

Local and International Experience

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:

JEFFREY LIM
jeffrey@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?

The PDPA applies concurrently with common law remedies (e.g. breach of confidence, etc.), and defers to sector-specific Singapore legislation (e.g. Official Secrets Act, Banking Act, etc.). It is "hard law" (i.e. having the force of law for which legal rights and remedies are accorded) as opposed to industry-specific self-regulatory codes (e.g. Singapore Code of Advertising Practice). Except where sector-specific Singapore legislation applies, 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 (which distinguish between Main Advisory Guidelines and Sector-specific 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 or in the case of a Singapore citizen or resident, his/her national registration identity card or NRIC number (collectively, the "National Identification Numbers" or "NIN"), 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 principle of fostering accountability on the part of an organisation in its handling of personal data, having been developed partly with a view to providing some broad consistency with international standards on data protection and providing a framework for the regulation of cross border flows of personal data.

The PDPA does this by imposing the following key data protection obligations:

(1) Consent Obligation –An organisation must ensure that personal data is only collected, used or disclosed with the consent of the data subject (unless it is exempt from the consent obligation or where consent is deemed to have been given). Where consent is withdrawn by a data subject, the organisation must take steps to ensure that requirements arising from the data subject's withdrawal of consent are complied with.

(2) Notification Obligation –An organisation must give adequate notification of the purposes for which personal data is collected, used or disclosed by the organisation.

(3) Purpose Limitation Obligation –An organisation must limit the collection, use or disclosure of personal data to the purposes for which consent is given and notified, or to the purposes for which an exemption from the consent obligation applies, as the case may be.

(4) Protection Obligation –An organisation must take reasonable steps to protect the personal data that it collects, uses, discloses or processes from unauthorized access, use or disclosure, to a level of protection commensurate with the risk of harm posed by such unauthorized access, use or disclosure.

(5) Retention Obligation –An organisation must not retain personal data for longer than is necessary to meet its business or legal purposes. Once all business and legal purposes have been met, that personal data should be anonymized or disposed of securely.

(6) Transfer Obligation –An organisation may only transfer personal data out of Singapore in accordance with specific requirements under the PDPA that are intended to ensure adherence to a standard of protection of personal data that is comparable to the protection under the PDPA.

(7) Access & Correction Obligation – An organisation must provide each data subject with information about that data subject's personal data which it has possession or control of and about the way it has collected, used or disclosed that personal data up to a year before the request. Concurrently, if a data subject wishes to correct an inaccuracy in relation to his/her personal data in the possession of an organisation, the organization is obliged to make that correction, and to inform other parties who have previously received (within the last year) that erroneous personal data of such correction. This obligation is limited and qualified by certain exclusions prescribed in relation to access or correction requests in certain situations.

(8) Accuracy Obligation –An organisation must take reasonable steps to ensure the accuracy of personal data it uses in making a decision affecting the data subject to whom the personal data relates or in disclosing such personal data to another organization.

(9) Transparency Obligation –An organization must make available information about its collection, use or disclosure of personal data, and provide means by which a data subject may place inquiries or complaints in relation to such collection, use or disclosure.

(10) Do-Not-Call Registry Obligation - An organisation is prohibited from conducting telemarketing activities relating to (and the sending of specified messages, which are essentially for marketing purposes, to) Singapore telephone numbers which have been registered with the Singapore Do-Not-Call Registry.

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 exceptions (i.e. 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, etc.), 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; and

(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 comply with the obligations referred to earlier in Question 3 above, including the obligation 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?

In line with the Transfer Obligation referred to at item (6) in the answer to Question 3, 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 of 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:

(1) In line with the Access Obligation referred to at item (7) in our answer to Question 3, to 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, and

(2) In line with the Correction Obligation referred to at item (7) in our answer to Question 3, to 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) To 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) To 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;
  - 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 contains provisions which address employee personal data including those that limit the Consent Obligation under specified conditions, for example, 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, so long as the employee is notified in advance of that purpose and of the business contact information of a person from the employer organisation to whom the that employee's questions may be directed; and
- the Employment Act further obliges an employer to

- collect and 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 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 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;
- 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 there any recent notable development(s) in Singapore or cases which you think is likely to affect data privacy/data protection in the future? E.g. 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?

Since the last update of this guide:

(1) The PDPC has -

- promulgated Advisory Guidelines on the Personal Data Protection Act for NRIC and Other National Identification Numbers, which amongst others, clarifies the general prohibition against and the applicable standard for permissible collection, use or disclosure and retention of the unique NRIC (i.e. national identification registration card) issued by the Singapore government to every Singapore citizen and resident and other NIN. These Advisory Guidelines are intended to reduce the excessive collection, use or disclosure of NRICs, passport numbers and other NIN (see item (2) of the answer to Question 2 above); and
- published certain additional guides (all accessible from https://www.pdpc.gov.sg Legislation-and-Guidelines/Guidelines/Other Guides) such as:
  - Guide to Developing a Data Protection Management Programme
  - Technical Guide to Advisory Guidelines on the Personal Data Protection Act for NRIC and Other National Identification Numbers;
  - Guide to Managing Data Breaches 2.0;
  - Guide On Active Enforcement;
  - Guide to Data Protection by Design for ICT Systems; and
  - Guide to Accountability under the Personal Data Protection Act;

(2) The PDPC is also expected to implement

- mandatory breach reporting, the framework for which has been published and public consultation on this concluded; and
- data portability and data innovation provisions, which will provide data subjects with rights to require an organisation to transfer certain personal data stored in digital form, to another organization on request under specified conditions and fulfilment of certain requirements, the public consultation on which has recently concluded and pending publication; and

(3) The PDPC has interestingly ventured into the realm of data analytics and artificial intelligence ("A.I."), by its publication of the Proposed Model Artificial Intelligence Governance Framework in January 2019 ("Model A.I. Framework"). Although the Model A.I. Framework is not legally binding and is not strictly about personal data, it is relevant as to providing insight to the PDPC's expectations and thinking in relation to the collection, use, disclosure or processing of personal data in A.I. applications.

MERITAS®
LAW FIRMS WORLDWIDE

THAILAND

FIRM PROFILE:

ILCT

advocates & solicitors

International Legal Counsellors Thailand Ltd. (ILCT) is the leading law office in Bangkok, Thailand which was founded in 1966 and has grown to become a full-service law firm. ILCT was one of the pioneer law offices engaging in the business law practice in Thailand. We have earned our reputation by consciously practicing in a group format and using personnel of diverse educational backgrounds to form teams to deal with each matter by applying maximum diversified expertise.

We are a full-service law firm. Among the types of matters handled by our lawyers in Bangkok are the following:

- Banking and Finance;
- Corporate;
- Entertainment Industry;
- Expatriate Services;
- Factory and Environmental Regulations;
- FinTech;
- Food & Drugs;
- Infrastructure and Privatization Projects;
- Insurance;
- IP;
- Labor;
- Litigation & Arbitration;
- M&A, Take-Overs and JV;
- Mineral Resources and Energy;
- Real Estate;
- Taxation.

CONTACT:

PALAWI BUNNAG
palawib@ilct.co.th

ANONG SEEHAPAN
anongs@ilct.co.th

+66 2 679 6005
http://www.ilct.co.th/

Introduction

Personal information is protected by the Personal Data Protection Act B.E. 2562 (2019) ("PDPA") which was finally published in the Royal Gazette on 27 May 2019 and then came into force on 28 May 2019. However, at present there are only provisions under Chapter 1 (Personal Data Protection Commission) that came into effect, whereas provisions under Chapter 2 (Personal Data Protection), Chapter 3 (Rights of the personal data owner), Chapter 5 (Complaint), Chapter 6 (Civil Liability), Chapter 7 (Penalty), Article 95 and Article 96 will come into force and effect on 28 May 2020. The PDPA aims at restricting the collection, use, transfer and disclosure of personal data by personal data controllers and personal data processors.

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

The major personal data protection legislation in Thailand is the PDPA. Previously, the constitution of the Kingdom of Thailand guarantees the right to privacy; however, there is no specific law governing personal data protection. In practice, the applicable laws are the Penal Code, which can only be enforced against certain persons with respect to certain types of private data i.e. a medical practitioner, lawyer, and the Civil and Commercial Code, which establishes causes of action for damages against infringers (Tort) and certain provisions of the financial laws that require the financial operator to keep and protect its customer information. Therefore, the PDPA serves as the first and main specific law governing data protection in Thailand.

2. How is personal information defined?

Under the PDPA,

"Person" means an individual person.

"Personal data" means information which can identify a person, whether directly or indirectly, excluding information of a deceased person.

"Personal data controller" means a natural or juristic person who has an authority to make decisions on the collection, use, or disclosure of personal data.

"Personal data processor" means a natural or juristic person who collects, uses, or discloses personal data directly or on behalf of the personal data controller.

According to the above definitions, information of a juristic person is not protected by the PDPA but the Trade Secret Act B.E. 2545 (2002) must be taken into the account in that regard.

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

The PDPA protects personal data during their whole life cycle from their collection to destruction. It obliges data users to comply with six data protection principles which are discussed in the answers to Questions 4 and 5 below. Any person, including the private sector and government departments, who controls the collection, usage, disclosure, holding, processing or use of the personal data must comply with the principles.

Both public and private organizations have to be responsible for any collection of personal data for use or disclosure. The PDPA defines duties and responsibilities for protecting and managing the personal data carefully in order to prevent violation of the rights of the data owner. If not followed, the offending organization will be subject to civil liabilities, penalties and administrative penalties.

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

Personal data must be collected in a lawful manner by obtaining consent from the data owner before acquiring, collecting, using and disclosing Personal data. The consent must be separated, clearly visible by the data owner and made in the form or content which is accessible and understandable. Also, it must at least contain the purposes of the data collection, the types of personal data to be collected, the time period for which it will be kept, the types of relevant third parties to whom the personal data will be disclosed, information regarding the data controller and their contact information as well as the rights of the personal data owner under the PDPA.

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. A data user must obtain consent from the data owner unless the data falls within the category of data or situation which the law allows to be collected without the data owner's consent. 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 subjects before using or disclosing personal data for that purpose. 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?

The Personal Data Protection Committee may prescribe a list about the protection for the delivery and transfer of personal data to another country.

Yes, subject to 1) the standard of personal information protection in the destination country; 2) any exceptions under the applicable law e.g. to comply with contractual obligations, applicable laws or court orders; or 3) the data owner's consent to release the information granted upon his awareness of the insufficiecy of protection standard. In this regard, the Personal Data Protection Committee will subsequently announce the standard of personal data release to another country.

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:

- To request his/her personal data be destroyed.
- To withdraw consent at any time.
- To access, suspend the use of their personal data and request a copy of such data.
- To update, delete or revise his/her personal data.
- To transfer his/her personal data.
- To object at any time:
  - If the collection of personal data has a consent exception.
  - For any collection of personal data for use or disclosure in the objectives of direct marketing.
  - The collection of personal data for disclosure in the objectives of science, history or statistical research except if it necessary for the public.

In case of withdrawal of consent to retain personal information by a third party, the data owner shall have to withdraw consent through the data controller who will subsequently withdraw its consent from such third party.

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 also protected by the PDPA.

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

A Personal Data Protection Committee has been established to enforce the PDPA and publish guidance to help organizations act in compliance with the laws.

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

The PDPA establishes punishments for non-compliance in 3 categories:

- The Personal data controllers and the Personal data processors who violate provisions of the PDPA and cause injury to data subjects are liable for paying civil compensation and punitive damages (based on a court order).
- Imprisonment of up to one year and/or fines up to THB 1 million.
- Administrative fines up to THB 5 million (based on the severity of the offence).

11. Is there any recent notable development(s) in Thailand or cases which you think is likely to affect data privacy/data protection in the future? E.g. 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 except for provisions under Chapter 2 (Personal Data Protection), Chapter 3 (Rights of the personal data owner), Chapter 5 (Complaint), Chapter 6 (Civil Liability), Chapter 7 (Penalty), Article 95 and Article 96 of the PDPA which will come into force and effect on 28 May 2020.

Conclusion

For data owners, the PDPA lays down clear-cut definitions as to who will have the rights over their own personal data, as well as, protective measures designed to prevent misuse of this data, and mandatory actions for leakage and loss of personal data. In essence, the Act is setting an internationally-accepted standard for the handling of personal data in Thailand. On the other hand, all companies who collect data of any person especially banks, insurers, telecommunication companies, markeing companies, and e-commerce businesses have to pay close attention to the remaining provisions in the PDPA which will come into force and effect on May 27, 2020.

MERITAS®
LAW FIRMS WORLDWIDE

VIETNAM

FIRM PROFILE: Russin & Vecchi

Russin & Vecchi is one of the first foreign law firms in Vietnam. We serve large multinationals and the middle market. A large part of our Vietnam practice is performed for foreign companies as they begin, continue or expand their operations in Vietnam. We handle ongoing matters in a wide range of corporate issues, advise and assist clients to structure investments, and to deal with issues arising during the course of the operation of their business. We play key roles in many cross-border transactions, structuring transactions, advising on regulatory framework, drafting transaction agreements, conducting due diligence investigations, interacting with regulators and undertaking regulatory procedures, coordinating transaction closings, and advising on different legal aspects of post-investment integration.

Our practice covers a wide range of industries and sectors: manufacturing, banking, healthcare, real estate, energy, technology, and commercial services. We also have in-depth practice areas in tax, employment, intellectual property, FCPA/AML compliance, and dispute resolution.

Our firm is well recognized among top law firms in Vietnam, with solid rankings in professional directories in Asia.

CONTACT:

SESTO VECCHI
sevecchi@russinvecchi.com.vn

NHUT NGUYEN
nhmnhut@russinvecchi.com.vn

+84-28-3824 3026
www.russinvecchi.com

Introduction

In Vietnam, personal data protection is a constitutional right. The right is often reflected in other pieces of legislation as well. While a general framework for data protection in Vietnam exists, the rules and regulations are often drafted in broad language and are open to interpretation.

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

The general framework for data protection of Vietnam was introduced in the Law on Network Information Security No. 86/2015/QH13 adopted by the National Assembly on November 19, 2015 ("LNIS"). Rules governing the collection, storage, processing, use, disclosure, and publication of personal data are also set out in Vietnam's Civil Code 2015 and in various sectoral laws, ranging from electronic transactions, from cinematographic to journalism, and cybersecurity.

2. How is personal information defined?

The LNIS defines personal information as any information which relates to the identification of a natural person. This includes any information that relates to a data subject's:

- Personal life, name, date of birth, address, telephone number, identification number, or email address.
- Personal or family secrets.
- Personal communications, including, but not limited to, written correspondence and the content of telephone calls.

This definition can be interpreted to also cover information related to deceased persons and biometric data, including but not limited to the fingerprints, irises and DNA sequences of any specific individual.

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

The LNIS sets out the following key principles relating to protection of personal information:

- Individuals are responsible for the protection of their own personal information when using any service;
- Data processors (see definition in Question 5) are responsible for the protection of the information they process;
- The protection of personal information must be conducted appropriately in accordance to the LNIS and the applicable sectoral law; and
- Information security must be maintained regularly, continuously, promptly and effectively.

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

The LNIS explicitly prohibits unauthorized collection, use, publishing, sale of, or any other business activities relating to the personal information of any data subject. Beyond that, the LNIS additionally requires data processors to inform data subjects of the scope and purposes of the collection and usage of personal information. In addition, the law requires that data processors must obtain the consent of data subjects before processing, including but not limited to collecting the personal data of any such data subject.

Vietnamese law defines persons of 16 years of age or younger to be minors. To collect the personal data of a minor aged 7 or younger, the consent of the minor's mother, father or guardian is required. To collect the personal data of a minor between the ages of 8 to 16, the consent of the minor's mother, father or guardian, and of the minor are required. These requirements apply equally to the processing, use and disclosure of personal data of a minor.

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

The LNIS defines processing of personal data as engaging in one or more of the following activities: collecting, editing, using, storing, providing to any third party, transferring, sharing or the publishing of personal data.

Before processing the personal data of a data subject, the LNIS requires the data processor to:

- Obtain the consent of the data subject;

The law does not specify any requirements on the form of consent. Because the nature and level of consent required is ambiguous, consent should be recorded electronically and should not be implied.

- Publish its policy regarding the processing and protection of personal data;

There are no specific requirements on the form or the content of the privacy policy.

- Provide an adequate level of protection for the personal data, following the technical standards for protection of personal data.

The law does not define "an adequate level of protection" or "technical standards." Data processors should implement internationally recognized (or higher) standards to protect the personal data of users, such as those set by the EU General Data Protection Regulations (GDPR).

Additionally, the law provides an exhaustive list of exceptions where a data processor may collect, use, and process the personal data of a data subject without consent. The list includes circumstances in which the processing is used to:

- Comply with obligations provided in the law;
- Execute, adjust, or perform contracts for the use of data, goods, or services over a network environment; or
- Calculate premiums, fees for the use of data, goods, or services over a network environment.

Certain types of personal data, such as bank account balances and medical records, are considered state secrets and enjoy additional protections. The Government determines and issues a list of information it deems to be state secrets for each sector.

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

There are no restrictions on transferring personal data outside of Vietnam, unless such data relate to banking information. However, with respect to the personal data of Vietnamese data subjects, the data processor and any secondary processors outside of Vietnam must comply with the obligations discussed in Question 4 and Question 5.

Vietnamese law is rather strict on the transfer of banking customer information to foreign individuals or organizations. The general rule is that banking customer information (such as a customer's bank statements) is treated as "State Confidential Information" (a sub-category of state secrets as mentioned in Question 5) and may be provided to foreign individuals or organizations only with approval from the State Bank of Vietnam.

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 law gives data subjects two basic rights in connection with their personal information. First, the law allows a data subject to require a company to disclose any personal information that the company has collected which belongs to the data subject. Second, a data subject has the right to request a data processor to update, modify or delete any personal information the data processor has collected concerning the data subject or to stop transferring the same to any third party.

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?

Vietnamese law 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 5.

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

Implementation and enforcement of personal information protection laws in Vietnam fall under the powers and responsibilities of the Authority of Information Security of the Ministry of Information and Communications.

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

Non-compliance with the data protection laws can be subject to both administrative penalties and criminal penalties. Depending on the violation and the severity of the consequences thereof, administrative penalties range from 10 million Vietnamese Dong (VND) to 50 million VND; criminal penalties can range from a warning to non-custodial reform (probation or supervised release), to imprisonment. Additionally, violation of the data protection laws can result in violation of other sectoral laws, which may lead to additional penalties.

11. Is there any recent notable development(s) in Vietnam or cases which you think is likely to affect data privacy/data protection in the future? E.g. 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 Vietnamese Government does not have any plans to pass any new legislation to protect personal information.

On January 1, 2019, the Cybersecurity Law of Vietnam came into effect and it is perceived to have a negative impact on the processing of personal data in Vietnam. The Cybersecurity Law provides two requirements (1) mandatory local storage of data in servers within Vietnam, and (2) mandatory establishment of a local entity in Vietnam, applicable to any domestic and offshore enterprises, which (i) provide services on the internet or on a telecommunications network or provide other value-added services on the internet to customers in Vietnam, and (ii) collect, exploit, analyze and process personal data, customer information or any information created by customers in Vietnam. Strict interpretation of this provision would require all data processors to establish a physical presence in Vietnam and store its data in Vietnam. However, there is no clear indicator as to how the Cybersecurity Law will be implemented. In fact, a detailed procedure for enforcement and a system of administrative sanctions against violations of the Cybersecurity Law are still lacking. The Government is in the process of establishing these procedures and systems.

Conclusion

The Law on Network Information Security and related legislation provide a basic framework for the collection, use and disclosure of personal information. While the legislation may appear basic on its face, and open for interpretation, the law provides reasonable protections for individuals, which is crucial in an era where information can easily be disseminated and abused. Additionally, in the context of the ratification of major FTAs (including the EVFTA and the CTTPP), concerns regarding privacy and protection of personal information are growing, which may be the necessary push for the Vietnamese Government to adopt additional guidance or to revise its legal framework to be compatible with other major players in the global market, including the EU.

MERITAS®
LAW FIRMS WORLDWIDE

AUSTRALIA

FIRM PROFILE:

SWAAB

We are a Sydney based full service Commercial and Family law firm. Established in 1981, 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 a 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.

Areas of law include: Corporate, Commercial, Construction, Employment, Estate planning, Family, Franchising, Intellectual property & technology, Litigation and insolvency, Property, planning & projects and Strata 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 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 contract between controllers and processors.

Australia privacy law does not have an express equivalent of those provisions of 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 to 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.

1. 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 under the Privacy Act 1988 (Cth) is "personal information" means 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 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 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.

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 Q9.

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:

- Examining proposed legislation which would allow interference with privacy or may have any adverse effects on peoples privacy
- Researching and monitoring developments in data processing and computer technology to ensure that adverse effects on people's privacy are minimised promoting an understanding and acceptance of the Australian Privacy Principles and their objects
- Preparing and publicising guidelines for agencies and organisations to follow to avoid breaches of privacy
- Encouraging industries to develop programs to handle personal information consistent with the Australian Privacy Principles.

11. Is there any recent notable development(s) in Australia or cases which you think is likely to affect data privacy/data protection in the future? E.g. 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:

- How personal information is collected, stored, used and disclosed, and from whom;
- The types of personal information in question;
- How the information may be used and disclosed (and by and to whom);
- The mechanisms available to the collector to provide opt-ins and opt-outs;
- The range of contracts entered into by the collector which have personal information management implications; and
- The extent to which Australian collections involve ex-Australian dealings or customers or data flows.

As with 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:

- Informed awareness;
- Measures which protect personal information from misuse, interference, loss, unauthorised access, modification or disclosure;
- The giving of access to and rights to correct personal information; and
- 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, Insolvency, Employment, Trusts, Estates and Relationship Property.

Established in 1921, we are very well regarded in the market with a number of practice areas and partners ranked by international publications or recognised nationally 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, financing, 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

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 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:

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

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

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.

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

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

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.

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.

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.

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

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

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.

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 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 aware of NZ$90,000 plus costs in favour of Mr Dotcom.

11. Is there any recent notable development(s) in New Zealand or cases which you think is likely to affect data privacy/data protection in the future? E.g. 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. The Bill has passed the Select Committee stage and is currently working its way through Parliament.

Much of the Bill remains the same as the existing law, with updates and clarification to the wording. There are however some key amendments being:

1. Mandatory reporting to the Privacy Commissioner and affected individuals of privacy breaches that have caused or are likely to cause, serious 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. The Bill also clarifies that when a New Zealand agency engages an overseas service provider, it will have to comply with New Zealand privacy laws.

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. The Privacy Commissioner may publish the fact that a compliance notice has been issued including the identity of the agency involved (with exceptions).

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.

While the Bill will bring New Zealand more into line with the European Union General Data Protection Regulations (GDPR) the Bill does not go as far as the GDPR. For example the Bill does not provide rights of erasure for individuals (also known as the "right to be forgotten").

The Bill is expected to become law on 1 March 2020.

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

EUROPE

PROFILE:

The Meritas European Data Protection Group is a collaborative, member-lead group, which brings together Data Protection and Privacy lawyers from across the Meritas European network. By working together, group members are able to resolve their client's domestic and international data protection legal needs; share insights on international regulatory developments and enhance the practice of data protection law.

Meritas member firms provide legal services on a wide range of domestic and international data protection and data privacy issues, including:

- Preparing data protection policies, procedures and agreements
- Conducting data protection assessments and audits
- Advising on the transfer of personal data across borders
- Managing the privacy issues related to employment and the management of personnel
- Managing the privacy issues related to marketing activities and the use of clients' data
- Ensuring compliance with data protection regulations, including adaptation to the EU GDPR.
- Advising on big data and data science projects
- Providing consultation and training to Data Protection Officers

Please contact any member of the group for assistance with your data protection needs in specific countries and across Europe.

AUSTRIA
Barbara Spanberger
Siemer-Siegl-Fureder & Partner
spanberger@ssfp-law.at
www.ssfp-law.at

BELGIUM
Bastiaan Bruyndonckx
Lydian
bastiaan.bruyndonckx@lydian.be
www.lydian.be

BULGARIA
Desislava Krusteva
Dimitrov, Petrov & Co. Law Firm
desislava.krusteva@dpc.bg
www.dpc.bg

DENMARK
Morten Bordrup
Brinkmann Kronborg Henriksen
mb@bkhlaw.dk
www.bkhlaw.dk

ENGLAND & WALES
Robert Lands
Howard Kennedy
robert.lands@howardkennedy.com
www.howardkennedy.com

ESTONIA
Rauno Kinkar
LEXTAL
rauno.kinkar@lextal.ee
www.lextal.ee

FINLAND
Markus Myhrberg
Lexia
markus.myhrberg@lexia.fi
www.lexia.fi

FRANCE
Elise Dufour
Bignon Lebray
edufour@bignonlebray.com
www.bignonlebray.com

GERMANY
Hans Helwig
Arnecke Sibeth Dabelstein
h.helwig@asd-law.com
www.asd-law.com

IRELAND
Emma Richmond
Whitney Moore Solicitors
emma.richmond@whitneymoore.ie
www.whitneymoore.ie

ITALY
Mario Valentini
Pirola Pennuto Zei & Associati
mario.valentini@studiopirola.com
www.pirolapennutozei.it

LUXEMBOURG
Hervé Wolff
LG Avocats
hw@lgavocats.lu
www.lgavocats.lu

POLAND
Bartosz Marcinkowski
Domański Zakrzewski Palinka
bartosz.marcinkowski@dzp.pl
www.dzp.pl

PORTUGAL
Margarida Roda Santos
FCB Sociedade de Advogados
mrs@fcblegal.com
www.fcblegal.com

SLOVAKIA
Miroslava Benediková
BEATOW PARTNERS
miroslava.benedikova@beatow.com
www.beatow.com

SWITZERLAND
Claudia Keller
Wenger & Vieli
c.keller@wengervieli.ch
www.wengervieli.ch

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 Euro 20million. Protection of personal data must now be taken seriously.

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.

Below is a general outline based on 11 questions we are asked regularly about the new regulation. Also provided are references to major changes to how the GDPR is implemented in different countries across Europe and examples of cases in which fines and penalties have been levied against companies not complying with 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 (EU General Data Protection Regulation – GDPR).

The 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) Extended rights for data subjects - including the right to be forgotten and data portability;

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

(6) Increased compliance obligations upon controllers and processors;

(7) Obligation upon controllers to be able to demonstrate compliance.

2. How is personal information defined?

Art. 4 (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.

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. 5: personal data shall be:

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

(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;

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

(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;

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

Recital 39 with respect to the storage time stipulates 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.

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;

(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 and 14 GDPR: the data subject should be informed at the time of the collection of the data or, where personal data have not been obtained from the data subject, within a reasonable period after obtaining the personal data, but at the latest within one month:

(1) The identity of the data controller and contact of the data protection officer, where applicable;

(2) The purpose for which the data is collected;

(3) Where applicable, the legitimate interests pursued by the controller;

(4) Where applicable, the existence of automated decision-making, including profiling;

(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;

(9) Where personal data have not been obtained from the data subject, from which source the personal data originate, and if applicable, whether it came from publicly accessible sources.

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

In addition to the elements listed under answer to Q4, the processing, use and disclosure of personal information shall in addition respect:

(1) Accountability;

(2) The obligation to implement data protection by default and by design;

(3) The obligation to carry out data protection impact assessments, where applicable;

(4) The obligation to keep records of processing;

(5) The obligation to appoint a data protection officer, where applicable.

The disclosure of personal data is admissible provided a legal ground exists, i.e. consent of the data subject or the necessity to comply with a legal/regulatory obligation.

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

Art. 44 to 50 GDPR. The transfer outside the EU/EEA is not possible, unless 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: Andorra, Argentina, Canada (only commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and USA (if the recipient belongs to the Privacy Shield). Adequacy talks are ongoing with South Korea.

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.

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?

Chapter III, Articles 12 to 23 of the GDPR describe the rights of the data subject to:

(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.

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).

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

The European Data Protection Board (EDPB) 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

Email: edpb@edpb.europa.eu

Website: www.edpb.europa.eu

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

Art. 83 GDPR provides penalties up to EUR 10 or 20 million or 2% to 4% of the global turnover (GDPR) depending on the offence. Individuals have also right to civil damages and may institute class actions for damages.

11. Is there any recent notable development(s) in Europe or cases which you think is likely to affect data privacy/data protection in the future? E.g. 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.

The ePrivacy Regulation was due to come into force on 25 May 2018 alongside GDPR, however, continued deliberation and lobbying of some of its finer detail have delayed its enactment. It is unlikely that the regulation will be passed before the end of 2019 and could be delayed further into 2020.

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.

SPECIFIC EUROPEAN COUNTRY COMMENTARY

Following the adoption of the GDPR, local data protection laws in different European counties have been revised or amended to reflect the new regulations. The following provides details on some of the key differences between the GDPR and local data protection laws and examples of recent fines or penalties levied against companies for non-compliance.

AUSTRIA

Through the introduction of the GDPR, in Austria the Data Protection Act was amended with effect from May 25th, 2018. This refers now generally to the GDPR, but there are still some peculiarities in the Austrian Data Protection Act.

In particular § 1 (which is a constitutional provision) was not changed, whereby also legal persons further enjoy a certain level of data protection and may, among other things, exercise the rights of the data subjects.

The DSG also contains provisions regarding image processing (private as well as public), such as video surveillance, and regulations regarding data processing by security police bodies.

Beside own penal regulations, if not Art. 83 GDPR is applicable, the DSG provides the possibility of an imprisonment of up to one year if someone carries out unauthorised data processing for profit or with malice intention.

There were also significant changes in the area of research and through the amendment of the Research Organisation Act, keyword: Broad Consent.

Fines and Penalties
There have already been some criminal convictions, including for unlawful video surveillance. A criminal case against an allergy day clinic is currently of interest, in the course of whose official examination proceedings around 14 violations of the DSGVO/DSG were found.

BELGIUM

In Belgium, two important acts were adopted pursuant to the GDPR.

Firstly, the law of 3 December 2017 on the establishment of the Data Protection Authority implements the requirements of the GDPR with respect to national supervisory authorities and establishes the Belgian Data Protection Authority.

Secondly, on 5 September 2018, the Act of 30 July 2018 regarding the protection of individuals with respect to the processing of personal data entered into force. This Act addresses the national substantive aspects of the GDPR, introduces several specifications and derogations such as determining the age of consent for children in an online context (13), imposing additional security measures in relation to sensitive data (listing who has access to the data and certain confidentiality obligations) and determining specific legal grounds for the processing of criminal conviction and offence data. In addition, the Act includes various restrictions on data subjects' rights and also provides for criminal sanctions.

Fines and Penalties
So far, the Belgian Data Protection Authority has been very modest in its sanctions. Only in May 2019, the Data Protection Authority imposed its first administrative sanction since the GDPR came into force. This administrative fine amounted to EUR 2,000 and concerned the misuse of personal data by a politician for election purposes.

BULGARIA

Bulgaria adopted changes in the Bulgarian Personal Data Protection Act (PDPA) with an amendment act from 26 February 2019. With the changes, the provisions of both GDPR and Directive 2016/680 were reflected in the national legislation.

In Bulgaria, a special supervisory authority was established for monitoring the processing of personal data by courts acting in their judicial capacity and by the prosecution and investigative authorities when acting as bodies of the judiciary for the purposes listed in Art. 1 of Directive 2016/680. This authority is the Inspectorate to the Supreme Judicial Council.

In addition, the PDPA introduces some local specific rules on the processing of employees' data, monitoring of employees, copies of ID documents, use of national identification numbers, processing of data concerning deceased persons and others.

Fines and Penalties

According to the Annual Report of the Commission for Personal Data Protection for 2018, the Commission received the most complaints and signals against data controllers and processors in the following sectors: telecommunications, video surveillance, banks and credit institutions, electronic media, education. Most fines were imposed on telecom companies, utility operators and banks.

The total amount of the sanctions for 2018 is about EUR 130,000. One case concerns a central heating company which was fined for using the data of a person who has never been their client in legal proceedings, which were supposed to be led against another person with the same name.

The biggest fine for 2019 until July was imposed on a telecom operator who was fined more than EUR 27,000 for using a client's data in the process of changing his subscription plan after a false request was made for the change by another person. The telecom company had numerous previous infringements.

DENMARK

Art. 87 in the GDPR gives the member states the possibility to determine specific conditions for the processing of national identification numbers. In Denmark, this number, the "CPR-number", is considered as a special category of personal data, as the number is used as a part of precautionary measures in banks, hospitals etc. According to the Danish Data Protection Act, the CPR-number can be processed by public authorities for the purpose of identification of records, and by private actors if, for example, the processing is laid down by law, the data subject has given its consent, or if the processing has scientific research purposes.

Further, the Danish Data Protection Agency (in Danish: "Datatilsynet") is not allowed to impose administrative fines as set out in the GDPR. As main rule, the fines must instead be imposed by national courts – based on a recommendation from the DPA – as a criminal sanction.

Fines and Penalties

Recently, the DPA has recommended a taxi company for a fine in the amount of EUR 160,000 for failure to delete 9 million customer phone numbers. Also, a furniture design company is facing a EUR 200,000 fine for failing to delete names, addresses, phone numbers and the buying behavior regarding 385,000 customers.

ENGLAND & WALES

The UK Data Protection Act 2018 (UK DPA) introduces derogations to GDPR (such as lowering the digital majority to 13), implements the EU Law Enforcement Directive and deals with processing not covered by EU law. It introduces a requirement for an "appropriate document" when relying on certain exemptions, creates a suite of criminal offences and a new immigration exception (which is being challenged through the Courts).

We also have the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 which prepare the UK for Brexit and align "consent" under the older Privacy and Electronic Communications Regs to GDPR standards.

Fines and Penalties

The ICO recently announced that from 25 May 2018 to 1 May 2019 it received over 41,000 reports of data protection concerns from the public. However, it got off to a slow start when issuing GDPR-level fines. That changed in July 2019 when over a period of 24 hours the ICO announced the intention to fine Marriott International £99.2million and British Airways a record-breaking £183milion for breaches. With the British Airways fine reportedly only 1.5% of its global annual turnover, we expect to see many more fines (and potentially many greater fines) over the coming years.

ESTONIA

Following adoption of the GDPR, the Estonian Data Protection Act (PDPA) finally came into force on 15 January 2019. Now that the PDPA has come into force, the internal regulations in Estonia do not conflict with the GDPR and adequately adopt the regulation.

Fines and Penalties

Given the late adoption of the PDPA, there have been no fines or penalties of any meaningful scope made by the Estonia Data Protection Inspectorate (EDPI) under the GDPR.

NB: The legal system of Estonia does not allow for administrative fines as set out in the GDPR. The rules on administrative fines deriving from the GDPR are applied in such a manner that in Estonia the fine is imposed by the supervisory authority in the framework of a misdemeanour procedure.

Additionally, under § 60 of the PDPA, but only upon failure to comply with a precept of the EDPI, the EDPI may also impose a penalty payment (not a fine; upper range also 20 000 000 or 4% of undertaking turnover).

FINLAND

The GDPR harmonised a significant part of national data protection legislation in Finland. In consequence of the GDPR, the former Personal Data Act (523/1999) was repealed, and the GDPR is nationally supplemented by the new Data Protection Act (1050/2018) which came into force at the beginning of January 2019. The Data Protection Act is applied in parallel with the GDPR, specifies and supplements the GDPR, and regulates certain special situations related to the processing of personal data.

In addition, employment privacy related issues are governed with the Act on the Protection of Privacy in Working Life (759/2004) which was amended due to the GDPR, and the amendment came into force at the beginning of April 2019. There are also several special and sectoral legislations in Finland concerning the processing of personal data in certain situations such as processing credit and payment default data, patient and health data as well as cookie related data.

Fines and Penalties

The number of cases referred to the Finnish supervisory authority has increased significantly as it registered 9,617 cases in 2018, compared to 3,957 in the previous year. The Data Protection Ombudsman has issued several warnings regarding infringements of the GDPR. However, no fines have been imposed yet.

FRANCE

Since June 1, 2019, the newly-worded law of January 6, 1978, known as law "Loi Informatique et Libertés", has been in force. It includes, in particular, the provisions on "national leeway" authorized by the General Data Protection Regulation (GDPR) that the legislator has chosen to use and the measures transposed into French law by the Police-Justice Directive.

The new wording specifies the different regimes applicable depending on the nature of the processing concerned: RGPD processing, police-justice processing, national defense or state security processing, etc. It also contains common provisions applicable to any treatment.

As a reminder, the "Loi Informatique et Libertés" is not intended to reproduce in full the provisions of the GDPR, even if it refers to it expressly in certain cases. As for the processing under the GDPR, a good understanding of the legal framework therefore requires a combined reading of both the GDPR and the law of January 6, 1978.

Fines and Penalties

For the CNIL, this first year of application of the GDPR has been described as "exceptional", with 2,044 notifications of data breaches (compared to 600 previously) and complaints increased from 3,797 in the first 4 months to more than 11,900 after one year.

But, the most significant event was Google's conviction of a record financial penalty of EUR 50 million for a series of GDPR breaches, including a breach of transparency and information obligations and for failure to provide a legal basis for advertising personalization processing.

GERMANY

Germany has implemented the GDPR by way of a comprehensive renewal of its Federal Data Protection Act (BDSG) with effect on May 25, 2018. To date no legislative changes have been made.

However, the Federal Data Protection Commissioner and the Commissioners of the federal states have published guidelines for interpretation of the GDPR.

At the same time, we see first judgments by courts and their interpretation of the GDPR or BDSG, which are not necessarily in line with the guidelines of the Commissioners. The right of access according to Art. 15 GDPR may serve as an example. According to the Commissioners joint opinion, an employee may not ask for hard copies of all emails that contain personal data, whereby a District Employment Court ruled that the employer has to present hard copies of all respective emails have to be handed to the employer.

Fines and Penalties
Within the first "GDPR-year" a total of roughly EUR 450,000 of fines have been imposed for violation of the GDPR. The top three fines amounted to EUR 80,000 and EUR 20,000 for the insufficient protection of personal health data and publically accessible customer data. A start-up internet bank had to pay EUR 50,000, when it became public that it had blacklisted former customers. More than the fines it is interesting that the GDPR apparently raises the awareness of the public.

So far consumers have filed more than 37,000 complaints for alleged violations of the GDPR, an average of more than 3,000 per month.

IRELAND

The Data Protection Act 2018 (the 'Act') was signed into law in Ireland on 24 May 2018. The Act implements the GDPR into national law and transposes the law enforcement Directive EU 2016/680. The Act is intended to amend existing data protection legislation in line with the GDPR where applicable, and to give effect to the GDPR where Member State flexibility is permitted. The Act is intended to be read in conjunction with the GDPR.

The Act confirms enhanced measures for the protection of children's data and specifies the "digital age of consent" for children in Ireland at 16. Section 30 of the Act makes it an offence to process children's data for direct marketing, profiling or micro-targeting, although this section has not been commenced.

Fines and Penalties
The Data Protection Commission has not as yet issued any fines or penalties under the new GDPR regime. The Data Protection Commission has however instigated up to 19 statutory inquiries into international tech companies such as Facebook and Google, who have their EMEA headquarters in Ireland. It is anticipated that fines will be issued, and other penalties or further enforcement action will be taken, shortly.

ITALY

On 9 August 2018, legislative decree 101/2018 allowed for the existing Italian Data Protection Code to be revised and renewed to take into account provisions of EU GDPR (EU Regulation 2016/679).

There are several interesting elements in the revised Italian Data Protection Code, including the possibility for a minor aged 14 to give consent to data treatment. It was also decided to save the provisions of the Italian Data Protection Authority as well as its authorizations, which will be the subject of subsequent review.

On 29 July 2019, the Italian Data Protection Authority adopted a measure concerning the obligations which must be met with regards the treatment of certain categories of personal data such as those related to health, political opinions, ethnicity, sexual orientation.

As far as the criminal sanctions for unlawful data processing are concerned, the current Italian Data Protection code states imprisonment from a minimum of six months to a maximum of one and a half years and in the most serious cases, from one to three years.

Fines and Penalties
No fines and penalties have been, to date, levied by the Italian Data Protection Authority against companies for failing to comply with the GDPR. There are, however, some proceedings currently pending before the Italian Data Protection Authority, which could carry administrative and criminal penalties.

LUXEMBOURG

The Law of 1 August 2018 organising the National Commission on Data Protection (the "CNPD") and implementing the GDPR provides for specific rules in various areas.

In particular, the processing of personal data in the employment context for monitoring purposes is subject to specific safeguards. The controller must inform the works council or, if no works council exists, the Inspectorate of Labour and Mines, of any processing for monitoring purposes in the employment context, prior to the implementation of such processing. The works council or, as the case may be, the employees, can request the CNPD to provide its opinion on the compliance of the monitoring activities within fifteen days of being notified of the processing by the controller.

When processing sensitive personal data for archiving purposes, scientific or historical research purposes or statistical purposes which allow for the exemption of data subjects' rights, Luxembourg law provides for certain additional safeguards, intended to protect the data subjects' rights and freedoms

Additionally, specific derogations exist with respect to the processing of personal data for the purposes of journalistic, academic, artistic or literary expression in order to balance the provisions of the GDPR with fundamental rights.

Fines and Penalties
The CNPD has yet to impose fines for breaches of the GDPR. To date, the CNPD has only published statistics on data breaches notified between 25 May 2018 and 31 December 2018. It shows that there has been 172 breach notifications, and 57% of these data breaches were accidental acts due to internal human errors.

POLAND

The difference in the application of the GDPR in Poland is linked to Polish regulations on data protection, in particular the Act on Personal Data Protection of 10 May 2018 and labour law regulations.

Poland has taken advantage of Article 84 of the GDPR and introduced criminal liability for unlawful processing of personal data. Moreover, the President of the Personal Data Protection Office may limit personal data processing if there is a risk that the processing will breach personal data protection regulations and further processing may have serious consequences. Labour law specifies which personal data may be processed and for how long.

Fines and Penalties
Within the last 12 months, approximately 100 audits were carried out which led to two financial penalties being imposed on controllers. The first fine was approximately EUR 220,000 (PLN 1 million). The main reason for the decision was failure to provide a privacy notice mentioned in Article 14 of the GDPR. The second fine was approximately EUR 12,790 (PLN 55 thousands) and was imposed due to disclosure of a personal identification number (PESEL) on the website of the soccer association.

PORTUGAL

As at 7 August 2019, Portugal is in the final stages of having a GDPR implementation law which has already been approved by the Parliament and sanctioned by the President and it is only pending on publication in the Official Gazette.

Its major key differences with respect to the GDPR are the fact that the penalties are graduated in two levels: (i) extremely severe and (ii) severe and they are applicable based on the size of the infringing company in accordance with Recommendation no. 2003/361/EC, of the European Commission, dated of 6 May 2003 and based on the fact that the infringer may be an individual person, therefore:

Extremely severe penalties' fines range from:

- EUR 5,000 to EUR 20,000,000 or 4% of the turnover for large companies
- EUR 2,000 to EUR 2,000,000 or 4% of the turnover for SMEs
- EUR 1,000 to EUR 500,000 for individual persons

Severe penalties' fines range from:

- EUR 2,500 to EUR 10,000,000 or 2% of the turnover for large companies
- EUR 2,000 to EUR 1,000,000 or 2% of the turnover for SMEs
- EUR 500 to EUR 250,000 for individual persons

Fines and Penalties

The Portuguese data protection authority (CNPD) levied an aggregate fine of EUR 400,000 against a public hospital for not controlling efficiently the access to patients' data and also due to incapability to show the capacity to ensure data integrity and resilience. In fact, 985 different doctors had access to clinical data and the hospital has only 296 doctors.

This fine has been challenged in court. No outcome yet.

SLOVAKIA

In response to the introduction of the GDPR, Slovakia adopted a completely new local data protection legislation – Act No. 18/2018 Coll. on Personal Data Protection (PDPA), which came into effect on May 25, 2018. To date no further substantial legislative changes have been made.

The PDPA mostly sets forth the rules for processing of personal data outside the material scope of GDPR (such rules generally mirror the relevant rules set out by GDPR). It also transposes the Police Directive into Slovak law. Finally, it implements certain authorizations for local variations granted by GDPR (e.g., it authorizes employers to publish certain basic job-related data of their employees without employees' consent).

Since the GDPR's entry into application, the Slovak Personal Data Protection Office has issued a couple opinions on application of certain GDPR rules (e.g., opinion on obligations of controllers operating e-shops). In line with Art. 35 {4) GDPR, the Office has issued a list of the kind of processing operations requiring a data protection impact assessment.

Fines and Penalties

So far, the Office has only imposed a few minor fines for GDPR non-compliance. Further fines are expected to be imposed, as there are several proceedings with respect to non-compliance with GDPR currently pending before the Office.

SWITZERLAND

Switzerland being neither an EU member state nor part of the EEA (other than Norway, Liechtenstein and Iceland) is under no obligation to implement the GDPR into its local legislation.

Currently there are a fair number of differences between the data protection requirements under the GDPR and under the Swiss Data Protection Act. For one, Swiss legislation not only protects data of natural but also of legal persons. Also, the requirements with respect to accountability (DPIAs, obligations to document processing activities, data breach notifications) are less extensive or non-existent. The Swiss legislation is currently being revised and the revised draft of the Data Protection Act introduces rights of data subjects and obligations of data controllers and processors similar to that of the GDPR. The revised draft is being debated in the Swiss Parliament late 2019/early 2020 and the outcome of the debate is still open.

Fines and Penalties

The current Swiss legislation does not foresee any specific fines or penalties but rather it is up to the individual data subject to initiate civil or criminal proceedings. There are a number of cases pending where Swiss companies are being investigated for a violation of the GDPR due to its extraterritorial scope but no details as to possible fines/penalties are yet available.

MERITAS®
LAW FIRMS WORLDWIDE

USA

FIRM PROFILE:

MEYER UNKOVIC SCOTT
ATTORNEYS AT LAW

Meyer, Unkovic & Scott LLP, 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, immigration issues, 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 LLP 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 a 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): The 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 its 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 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 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 there any recent notable development(s) in the USA or cases which you think is likely to affect data privacy/data protection in the future? E.g. 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.

The following firms can provide assistance with your data protection needs in the United States.

CALIFORNIA
Procopio
San Deigo, CA
www.procopio.com

FLORIDA
Smith Hulsey & Busey
Jacksonville, FL
www.smithhulsey.com

Lowndes, Drosdick, Doster,
Kantor & Reed, P.A.
Orlando, FL
www.lowndes-law.com

GEORGIA
Parker, Hudson, Rainer
& Dobbs LLP
Atlanta, GA
www.phrd.com

IOWA
Nyemaster Goode
Des Moines, IA
www.nyemaster.com

ILLINOIS
Goldberg Kohn
Chicago, IL
www.goldbergkohn.com

INDIANA
Kahn, Dees, Donovan &
Kahn, LLP
Evansville, IN
www.KDDK.com

Krieg DeVault LLP
Indianapolis, IN
www.kriegdevault.com

MARYLAND
Tydings & Rosenberg LLP
Baltimore, MD
www.tydingslaw.com

MICHIGAN
Miller Johnson
Grand Rapids, MI
www.millerjohnson.com

NORTH CAROLINA
Johnston, Allison & Hord, P.A.
Charlotte, NC
www.jahlaw.com

Wyrick Robbins Yates &
Ponton LLP
Raleigh, NC
www.wyrick.com

NEW JERSEY
Norris McLaughlin, P.A.
Bridgewater, NJ
www.norrismclaughlin.com

NEW YORK
Carter Ledyard & Milburn LLP
New York, NY
www.clm.com

PENNSYLVANIA
Stradley Ronon Stevens &
Young LLP
Philadelphia, PA
www.stradley.com

Meyer, Unkovic & Scott LLP
Pittsburgh, PA
www.muslaw.com

TENNESSEE
Chambliss, Bahner &
Stophel, P.C.
Chattanooga, TN
www.chamblisslaw.com

TEXAS
Langley & Banack, Incorporated
San Antonio, TX
www.langleybanack.com

WISCONSIN
Boardman & Clark LLP
Madison, WI
www.boardmanclark.com

WEST VIRGINIA
Kay Casto & Chaney PLLC
Morgantown, WV
www.kaycasto.com

***Each firm is an active member of the Meritas Privacy and Data Security Group.**

MERITAS®
LAW FIRMS WORLDWIDE

USA
CALIFORNIA

FIRM PROFILE:

Procopio®

Procopio is a full-service business and litigation law firm with more than 170 attorneys in San Diego, Silicon Valley, Las Vegas, and Phoenix serving clients around the world, from small to mid-sized companies to large multinationals. The firm supports small to mid-sized companies and large multinationals at every stage of the business life cycle. Our global reach across Latin America, Asia and Europe further expands our international partnerships and cross border capabilities.

At Procopio, achieving greater diversity and inclusion within the firm and in the legal profession is a vital part of its practice and culture. Procopio is ranked in the Top Ten for Diversity among AmLaw 200 firms and a Best Law Firm for Minority Attorneys as rated by Law360.

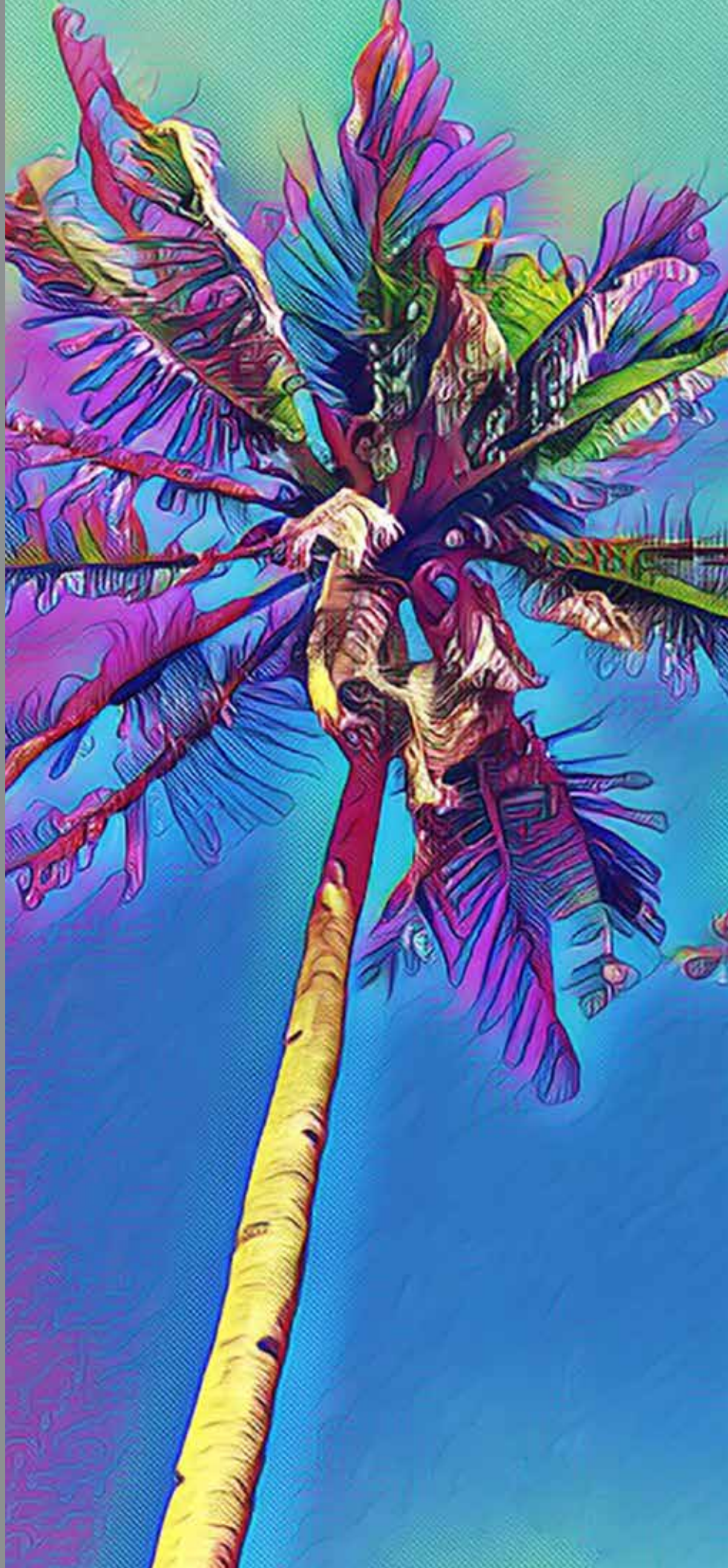
Procopio's Privacy and Cybersecurity practice attorneys provide legal counsel on all aspects of data management, work with clients to ensure compliance with international, federal and state regulations, and manage litigation providing defense against privacy and data security class action suits. Learn more at Procopio.com.

CONTACT:

S. TODD NEAL
todd.neal@procopio.com

DENNIS DOUCETTE
dennis.doucette@procopio.com

+1-619-238-1900
www.procopio.com



Because of the size of the state of California and the active involvement of the California legislature, this chapter will highlight how California is dealing with the issue of data privacy protection.

Introduction

When it goes into effect on January 1, 2020, the California Consumer Privacy Act (California Civil Code § 1798.100 to § 1798.199) (the "CCPA") will be the most comprehensive privacy legislation in the United States with new compliance requirements and liabilities. While the law was drafted with threshold requirements for application, it will have significant reach given California's undeniably large global economic impact. Additionally, while California's law is the first comprehensive data privacy law at the state level, it likely will not be the last. Other states are currently considering comprehensive data privacy laws and there are also discussions around possible federal legislation.

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

As described in further detail below, the CCPA grants California residents a number of new rights with respect to the collection of their personal information, including, among other things, the right to be forgotten (deletion of information), the right to opt-out of the sale of their personal information, and the right to know what information is collected by a business about them. The CCPA applies generally to for-profit businesses and sets threshold requirements for its application. It will apply to businesses collecting personal information on California residents if they exceed one of the following thresholds:

- Annual gross revenues of $25 million;
- Annually buys, sells, receives or shares for commercial purposes the personal information of 50,000 or more consumers, households or devices; or
- Derive 50 percent or more of its annual revenues from selling consumers' personal information.

Parent companies and subsidiaries sharing the same branding will also need to comply even if they themselves do not exceed the applicable thresholds.

2. How is personal information defined?

Under the CCPA, only a "consumer" can exercise their rights. The term "consumer" is broadly defined to include any natural person who is a California resident. A consumer's "personal information" is also broadly defined and includes information that directly or indirectly identifies, describes, or can reasonably be linked to a particular consumer, device, or household. As the law exists currently, personal information includes, but is not limited to, the following:

- Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers;
- Characteristics of protected classifications under California or federal law;
- Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies;
- Biometric information;
- Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement;
- Geolocation data;
- Audio, electronic, visual, thermal, olfactory, or similar information;
- Professional or employment-related information;
- Education information;
- Inferences drawn from any of the information collected to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

Specifically excluded from the definition of "personal information" is any information publicly available, meaning any information that is lawfully made available from state, federal or local government records. "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge.

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

The key principles relating to personal information protection under the CCPA follow that of the United States more broadly, including creating and following a California-specific privacy policy for the collection

and use of information from consumers and using reasonable safeguards for the protection of personal information. The CCPA also provides for a private right action where the business has suffered a breach compromising personal information. The security provision within the CCPA refers to a business's "duty to implement and maintain reasonable security procedures and practices." Reasonable security is not defined in the statute but it does include a proportionality element stating it is the duty of the business to maintain reasonable security procedures and practices "appropriate to the nature of the information."

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

The CCPA grants California residents a number of new rights and as a result, covered businesses have several compliance requirements. At or before the time of collection, businesses have an obligation to make affirmative disclosures to consumers via privacy policy or notice. Businesses that sell information, as defined by the statute have additional disclosure obligations, including disclosing to consumers the categories of personal information sold or disclosed for a business purpose in the last 12 months, or if information has not been sold or disclosed for a business purpose in the preceding 12 months, that fact must be disclosed.

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

Generally, the processing, use and disclosure of personal information is not prohibited under the CCPA. Consumers, however, have the right to request a business and its service providers delete their personal information, subject to important exceptions. Businesses need not delete information if it is necessary to, among other things, complete the transaction for which it was collected, provide a good or service requested by the consumer, perform a contract between the business and consumer, detect security incidents, identify and repair errors that impair existing intended functionality, protect against certain fraudulent or illegal activities, ensure the exercise of free speech by the consumer, or comply with a legal obligation. The CCPA also provides consumers a right to opt-out of the sale of their personal information by a business.

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

The CCPA does not explicitly place restrictions on personal information being transferred to foreign jurisdictions. Instead, the CCPA incentivizes businesses to have written contracts in place with vendors restricting the use, retention or disclosure of personal information for any purpose except performing the services specified in the contract.

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 noted above, the CCPA gives California consumers new rights over their information. The new rights include the right to request from a business:

- The categories and specific pieces of personal information collected;
- The categories of sources from which the personal information is collected;
- The business or commercial purpose for collecting or selling the personal information;
- The categories of third parties with whom the business shares personal information; and
- Deletion of personal information about the consumer that the business has collected, subject to some important exceptions.

The information must be delivered free of charge to the consumer, in a format that is portable, and typically must be delivered within 45 days.

Where a business is selling personal information as defined by the statute, the consumer has the right to opt-out of the sale of their personal information. A clear and conspicuous link on the business's internet homepage, titled "Do Not Sell My Personal Information," must be made available and the link must enable consumers to opt-out of the sale of their 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?

As initially passed, the CCPA protected all California residents with respect to any information that related to them, including in their role as employees. In 2019, the California legislature passed an amendment excluding from the CCPA any information an employer business collects from an employee consumer in the employment context. Notably, the amendment includes a sunset provision after one year, which means there will likely be additional legislation or amendments proposed regarding employee privacy in 2020. Despite that the amendment excludes employee data from many of the CCPA's requirements, employers are still required to inform employees what types of information they are collecting and the reasons for collecting it.

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

Enforcement authority for the CCPA rests with the California Attorney General. There is also a limited private right of action for unauthorized access, theft, or disclosure of nonencrypted or nonredacted personal information on account of the business failing to implement reasonable security practices and procedures appropriate to the particular type of personal information.

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

If after receiving notice of a violation from the California Attorney General the business is unable to cure the violation within 30 days, the California Attorney General can seek civil penalties up to either $2,500 per violation or $7,500 per intentional violation. In an action brought by a consumer for data breach liability under the CCPA, statutory damages between $100 to $750 per California resident and per incident, or actual damages, whichever is greater, are available.

11. Is there any recent notable development(s) in California or cases which you think is likely to affect data privacy/data protection in the future? E.g. 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?

Data privacy legislation in California, like the United States more broadly, is very much in flux. With regard to the CCPA specifically, the California Attorney General has been tasked with issuing regulations (standards for enforcing the law) on or before July 1, 2020 pursuant to the first amendment passed by the California legislature. It is anticipated the regulations will provide some clarity around several of the requirements under the law. Additionally, as industry continues to weigh in, it is likely there will be further amendments to the law in 2020 and beyond. As a result, for the foreseeable future, there will continue to be significant developments relating to the CCPA and privacy law more generally in California.

Conclusion

The California constitution guarantees every Californian an "inalienable right" to privacy. With that in mind, California has pressed forward with adopting new laws aimed at protecting privacy at every level and often considers itself the leader in privacy legislation in the United States. Given the prominence of tech companies, the large number of residents, and the large economic footprint of the state, businesses can expect California will continue its effort to insert itself into the national and international conversation about privacy.

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