A GLOBAL ROADMAP TO PERSONAL DATA PROTECTION

Asia Pacific, Europe & USA

First Edition

MERITAS®
LAW FIRMS WORLDWIDE

A GLOBAL ROADMAP TO PERSONAL DATA PROTECTION

Asia Pacific, Europe & USA

Dennis Unkovic, Editor

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

Meyer, Unkovic & Scott LLP
www.muslaw.com

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

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

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

ABOUT MERITAS®

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

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

7,500+ EXPERIENCED LAWYERS

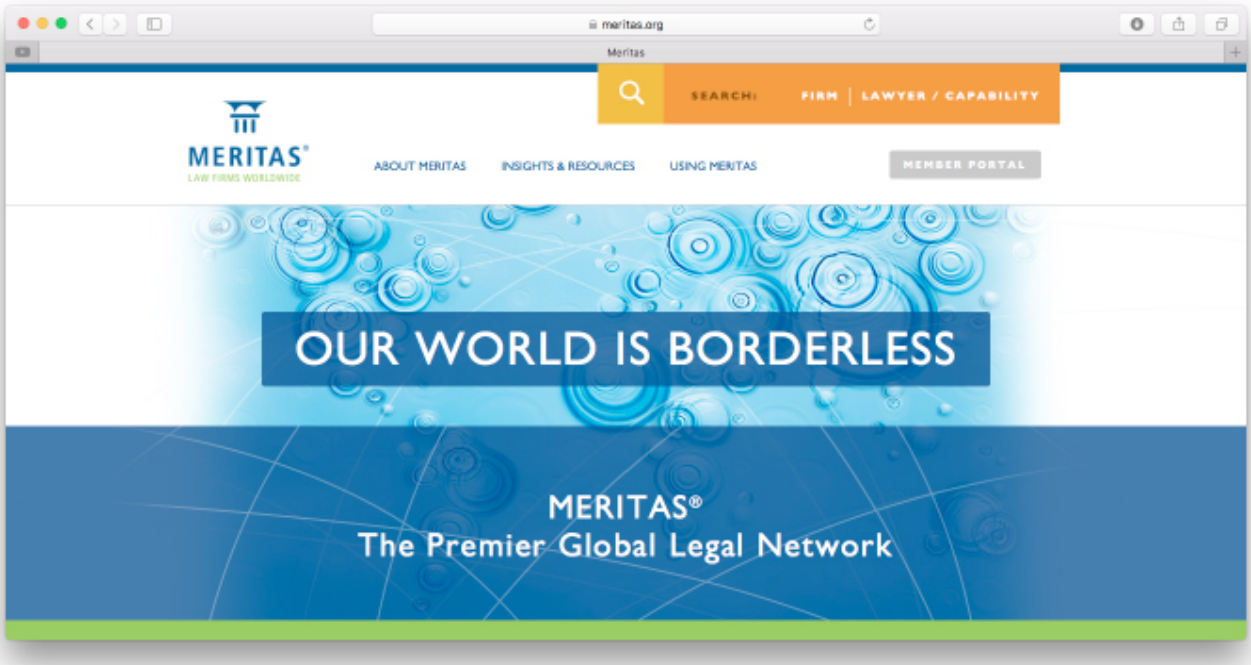
90+ COUNTRIES

180+ LAW FIRMS

240+ GLOBAL MARKETS

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

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



For more information visit:

MERITAS®
LAW FIRMS WORLDWIDE

www.meritas.org

MERITAS®
LAW FIRMS WORLDWIDE

HONG KONG

FIRM PROFILE:

Gallant

何 耀 棣 律 師 事 務 所

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

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

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

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

CONTACT:

PHILIP WONG
philipwong@gallantho.com

BRENDA LEE
brendalee@gallantho.com

+852 2526 3336
www.gallantho.com

Introduction

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

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

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

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

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

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

2. How is personal information defined?

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

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

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

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

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

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

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

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

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

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

Individuals have the right to:

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

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

(3) Request the erasure of incorrect data;

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

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

(6) Claim compensation in civil

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

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

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

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

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

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

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

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

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

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

Conclusion

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

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

Author: Walter Lee

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