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

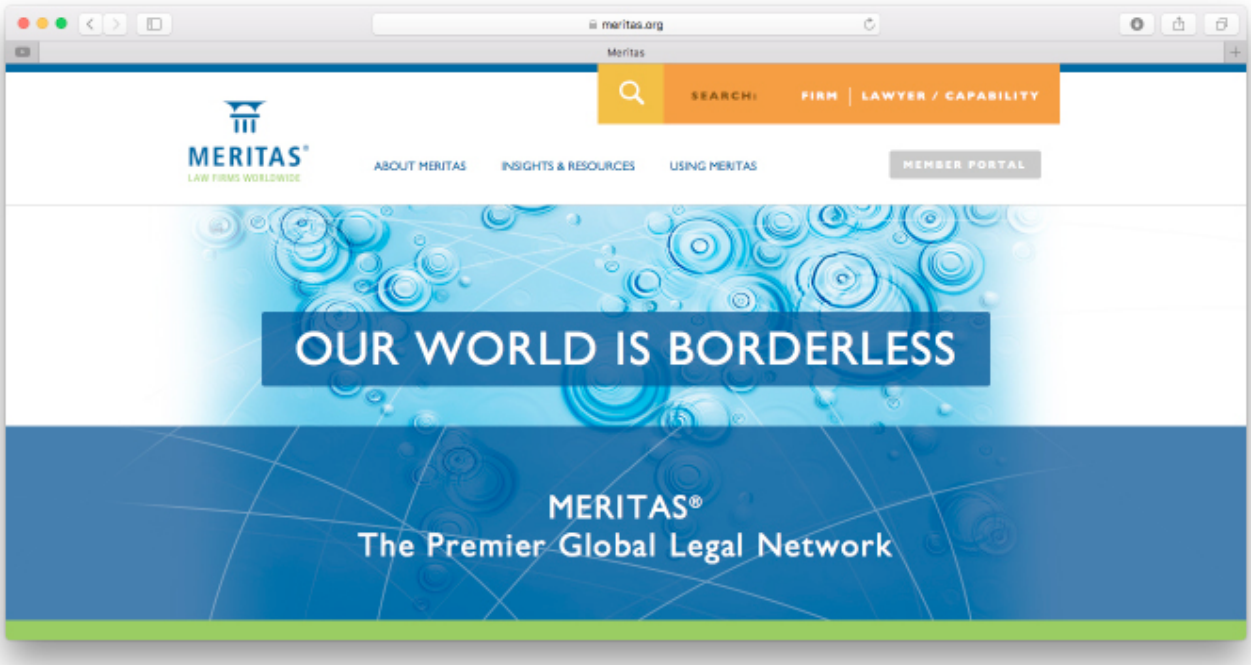
90+ COUNTRIES

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

Introduction

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

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

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

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

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

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

2. How is personal information defined?

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

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

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

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

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

The key principles related to Taiwan personal information protection are:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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