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

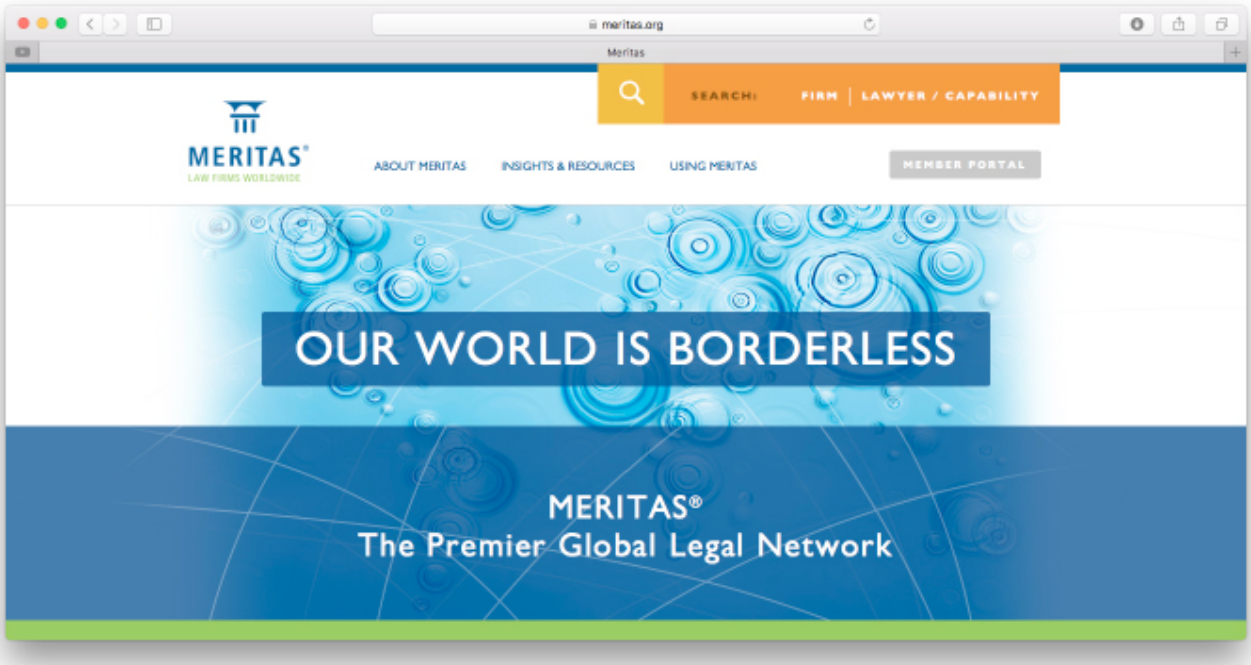
90+ COUNTRIES

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

CHINA

FIRM PROFILE:

汇 衡 律 师 事 务 所
HHP ATTORNEYS-AT-LAW

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

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

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

CONTACT:

YAO RAO
yao.rao@hhp.com.cn

JINGDONG XU
jingdong.xu@hhp.com.cn

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

Introduction

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

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

In China, laws protecting personal information mainly include:

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

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

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

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

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

2. How is "personal information" defined?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

include the following:

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

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

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

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

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

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

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

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

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

(1) **Civil Liability**

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

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

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

(2) **Administrative Liability**

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

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

(3) **Criminal Liability**

Any entity or individual who

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

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

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

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

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

Conclusion

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

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