

# Comparison of Various Compliance Points of Data Protection Laws in Ten Countries/Regions | #1 Scope of Application and Extraterritorial Effectiveness

Author: Jie (Jackie) WONG, Lawyer, Founder of W&W International Legal Team, Kinding Partners, specialising in cyber and internet practice

Date: September , 2021

Note: In the legal context of the PIPL, the “Personal Information Handling” includes, but is not limited to, the collection, storage, use, processing, transmission, provision, disclosure, and deletion of personal information.

## Abstract

The Law of the People's Republic of China on the Personal Information Protection Law (hereinafter referred to as the "PIPL") was enacted on August 20, 2021, and will officially take effect on November 1, 2021. As the **first codified personal information protection law in China, the PIPL** draws on and incorporates the legislative experience of advanced overseas regions, as well as the useful contents of *the Civil Code, Information Security Technology—Personal Information Security Specification, the Network Security Law, the Electronic Commerce Law, and the Data Security Law*, etc., which are related to the PIPL. The PIPL provides comprehensive protection for the rights and interests of personal information subjects in relation to personal information

handling, the cross-border transfer of personal information, the obligations of personal information handlers and their compliance obligations, and other specific aspects.

Overall, the introduction of the PIPL officially announces the birth of the cybersecurity and data compliance troika (*the Cybersecurity Law, the Data Security Law, and the PIPL*) and establishes the rule of law structure and system for personal information protection in China, reflecting China's determination and attitude to attach great importance to the protection and governance of personal information.

WONG focuses on Internet legal services and compliance work, especially in the field of global data and personal information compliance protection, and has been paying special attention to the dynamics and development of overseas data privacy protection legislation.

The purpose of this article is to compare China's PIPL with data protection law of other nine major overseas regions in different dimensions, in order to help overseas Internet companies and personnel that have a lot of contact with personal information to better understand the similarities and differences in data protection in each country/region, as well as the main points of compliance.

Given the limited space, WONG will only briefly list the main comparison dimensions by sections in the form of key points, and look forward to valuable advice and guidance from fellow experts in personal information protection industry.

**This is the first part of the article, which focuses on the interpretation and comparison of scope of application and extraterritorial effectiveness of different data protection laws.**

## Part I: Scope of Application and Extraterritorial Effectiveness

The scope of application of a law refers to the binding force that a law has or grants, as well as the breadth and depth of its application, and generally includes the temporal application effect (the time of commencement and termination), the spatial effect (the territorial scope of the effect), and the effect on persons (for whom it is effective). In the case of data protection laws, the scope of territorial application, the scope of personal application, and the scope of application of the personal information itself will generally be of concern.

### I. Interpretation of the PIPL.

The scope of application of this law is clearly defined in Chapter I, "General Provisions" of the PIPL.

First of all, it is clearly stipulated that "*This Law shall apply to the handling within the territory of the People's Republic of China of the personal information of natural persons.*" It can be seen that China's PIPL adopts the "territorial principle", and clearly states that part of its scope of application is "the activities of handling personal information of natural persons in **China**",

and that **the subject of personal information to which this Law applies is a natural person located in China, regardless of whether the natural person is a Chinese or a foreigner.** For the purposes of PIPL, the two Special Administrative Regions of China, i.e. Hong Kong and Macao, are treated as outside the “territory of the People’s Republic of China”. In other words, even if the subject is a foreigner, when the personal data is generated within the mainland of China, and the personal information is processed by organizations and individuals within the mainland of China, it will fall under the jurisdiction and protection of China's PIPL.

### **Examples**

If a domestic e-commerce app, which mainly provides shopping services for domestic users, collects personal information of a foreign subject located within the mainland of China in the course of its services, the e-commerce app is required to comply with the provisions of China's PIPL when handling the personal information of such foreign subject within the mainland of China. As to whether the handling of personal information of foreign subjects by the e-commerce app will also fall under the scope of **application of the data protection law of the** foreigner's country or other third party countries/regions, or whether the laws of overseas regions have jurisdiction over the personal information handling activities in this scenario, it is necessary to **analyze the**

**scope of application of the data protection law of such overseas regions** (Some concise guidance points will be provided in the comparison table below).

Secondly, China's PIPL makes it clear that it is also extraterritorially applicable, as reflected in the second paragraph of Article 3:

*"This Law shall also apply to the handling outside the territory of the People's Republic of China of the personal information of natural persons located within the territory of the People's Republic of China if the information is processed:*

*(1) for the purpose of providing products or services to natural persons located within China;*

*(2) to analyze or assess the conduct of natural persons located within China;*  
*or*

*(3) under any other circumstance as provided by any law or administrative regulation."*

It can be seen that China's PIPL has borrowed from the GDPR and clarified its **necessary extraterritorial application, providing that the provisions of the PIPL are also applicable when products or services are provided to natural persons within the territory of the mainland of China, or when the analysis or evaluation of natural persons within the territory is performed.**

Back to the previous example, if the e-commerce app deploys a data center in Singapore and processes the foreigner's data in Singapore (outside China), given that the app provides services to natural persons in China and the foreigner is also located within the mainland of China, it still falls within the scope of application of China's PIPL and the data processor needs to comply with the relevant requirements of China's data protection laws and regulations.

In particular, it should be noted that for personal information handlers outside the mainland of China, China's PIPL clearly requires that a **specialized agency or designated representative should be established** in China to handle matters related to personal information protection, and that information about the agency or representative **should be reported to the department** that performs personal information protection duties.

**However, compared to the territorial scope of application of the GDPR, the provisions of China's PIPL contain some subtle differences.**

The GDPR is established by the criteria of "stable arrangement/organizational establishment", and "service objective/in the context of the activities", while the scope of territorial application of China's PIPL is determined by "the place where the act of handling takes place" and "the objective of the service". **The similarity and difference between "stable**

**arrangement/organizational establishment (establishment)" and "handling in the territory" are not the same.** According to the requirements of China's PIPL, as long as the handling of personal information of natural persons takes place within the mainland of China, or with the purpose of providing products or services to natural persons located within the mainland of China, it will be covered by the PIPL, regardless of whether it is necessary to have a stable arrangement or establishment in China.

Of course, the PIPL also specifies the circumstances in which it does not apply, including:

(1) This Law shall not apply when a natural person processes personal information for personal or household affairs; and

(2) Where laws provide for the personal information handling in the process of statistical or archives administration activities organized and implemented by the people's governments at various levels and relevant departments thereof, such provisions shall prevail.

## **II. Comparison of major overseas personal information or data protection laws:**

Comparison Of The Compliance Points Of Data Protection Laws In Ten Countries/Regions				
Part I: Comparison of Scope of Application and Extraterritorial Effectiveness				
Category Country / Region	extraterritorial application	Main provisions (need to be analyzed in the context of business)	Compliance points/special points/remarks	
China PIPL	✓	1. Applicable to the processing of personal information within China. 2. The same applies to the processing of personal information outside of China if it is for the purpose of providing products or services to natural persons within China, or for the analysis or evaluation of the behavior of natural persons within China, or in cases specified by law or regulation.	The processing of in-country data outside of China requires: 1. the establishment of a specialized agency/designated representative 2. reporting to regulatory authorities	
EU GDPR	✓	The GDPR applies to organizations that provide goods and services to the people of EU or collect and analyze data about EU residents, regardless of where the individual or business is located.	The same applies to organizations outside the EU if they provide goods or services to persons in the EU or monitor their conduct.	
California, USA CCPA	✗	The CCPA applies only to companies that conduct business within California and meet one or more of the following conditions each year: 1. have gross revenues more than \$25 million; 2. have revenues from the sale of consumer personal information that represent at least 50% of their gross revenues; or 3. purchase, sell, or share personal information about more than 50,000 consumers.	1. the same applies to companies established outside of California that collect or sell personal information about California consumers while conducting business in California; 2. exclusions: the entire business conduct occurs entirely outside of California (e.g., information about consumers is collected while they are outside of California)	
Brazil LGPD	✓	The LGPD applies to any processing operation, regardless of the country/territory in which it is based or in which the data is located, provided that: 1. the data processing takes place in Brazil; 2. the purpose of the processing activity is to provide goods or services or to process data on individuals located in Brazilian territory; or 3. the processed personal data has been collected in Brazil.	The same applies to the cross-border processing of personal data of Brazilian residents	

<b>India PDPB (Draft)</b>	✓	Applies not only to data collected, disclosed, shared or otherwise processed in India, but also to data processing by data fiduciaries or data processors not located in India, as long as such conduct is 1. related to the business conducted in India or to the activity of providing goods or services to data subjects in India; or 2. related to the data subject's Picturing the activities of the data subject in India.	Similar in substance to the definition of "data controller" in the GDPR, a "data trustee" can be understood as a "data controller"
<b>Korea PIPA</b>	!	From regulatory enforcement, it is generally considered to apply to both Korean companies and companies established outside of Korea but processing data of people living in Korea	The specific provisions on extraterritorial application are not very clear
<b>Japan APPI</b>	✓	APPI applies to all business operators that process personal data in Japan, including not only companies that provide goods and services in Japan, but also companies in Japan and companies with offices outside of Japan.	Certain provisions apply to operators who provide goods or services to a person in Japan and who have acquired personal information relating to a person living in Japan that is handled abroad.
<b>Singapore PDPA</b>	✓	The PDPA applies to all organizations that are not public bodies or that act on behalf of public bodies that engage in activities related to the collection, use and disclosure of personal data in Singapore, whether or not they are formed under or recognized by the laws of Singapore or reside/have a place of business in Singapore.	Combining the principles of territorial jurisdiction and personal jurisdiction
<b>Indonesia PDPA (Draft)</b>	✓	And in the PDPA(Draft), it is stipulated that the PDPA applies to entities in Indonesia and outside Indonesia if it 1. causes legal consequences in Indonesia; and/or 2. affects Indonesian citizens in Indonesia and outside Indonesia.	Further guidance is needed to explain

Hong Kong, China PDPO	✓	1. Hong Kong PDPO and its guidelines and code of conduct apply to the collection, holding, processing or use of personal data by data users. 2. wherever in the world the collection or processing occurs, the personal data will fall within the jurisdiction of the PDPO as long as it is controlled by a data user in Hong Kong.	Also, data users who control the collection, holding, processing or use of personal data, either individually, jointly or jointly with others, are bound by the PDPO.
Illustration Description:			
✓	The country/region has the provisions of extraterritorial application		
✗	No clear regulations, or no corresponding guidelines have been issued		
!	Need for further explanation or clarification		

## Overall

The PIPL draws on the relevant provisions of the GDPR in its scope of application. Looking at the jurisdictional scope of the data protection laws of other countries/regions in the table above, one would easily see that it **has become a legislative trend to expand the extraterritorial effect of the data protection laws of the country/region on a global scale.** In the process of overseas business development, especially when an enterprise is involved in handling personal information of overseas subjects, it should pay special attention to whether its personal information handling behavior will fall under the jurisdiction of the data protection laws of that country or region to further confirm whether and how to comply with the data protection laws of that country or region and the legal provisions related to its business model.

## **About the author**

### **JIE (Jackie) WONG**

Ms. Wong is a certified lawyer and the founder of W&W international legal team, Kinding Partners, and is also the expert of UN World Silk Road Forum, and the council member of Information and Communication Law Research Association of Guangdong Province. Ms. Wong is a Master of International Economic Law and Commercial Law (LL.M) from University of Groningen, the Netherlands, and holding a bachelor degree in domestic law. She is practicing in the field of cyber and internet law, especially Internet products compliance, overseas compliance and global and domestic data protection compliance, and has provided professional legal services to many well-known Internet companies and large and medium-sized foreign enterprises, covering such industry fields as intelligent terminal manufacturing, IOT, Artificial Intelligence, Cloud computing and services, social network platforms, mobile Internet, e-commerce and e-commerce platforms, short video audiovisual live streaming, online games, as well as personal information protection and data security.

Wong has served in Alibaba Entertainment Group and has time-weathered experience in cyberlaw field. With ten years of working experience in IT company and in Chinese as well as foreign law firms, Ms. Wong is able to understand the core demands of clients more accurately, respond to them quickly and provide comprehensive and effective support to clients from basic to strategic level. She is also very good at providing effective compliance solutions and landing support for all kinds of overseas Internet companies to expand into emerging and important markets such as India, Southeast Asia, the Middle East, Africa, Europe and America. And at the same time, she is also the founder and the chief executive of the WeChat public account of Overseas Internet Law Watch“出海互联网法律观察”. She co-authored the "Internet Global Data Compliance Legal Observation Report" and published a number of professional articles in relation to the Internet Law and Data

Compliance, some of which were published in the Wolters Kluwer Professional Database.

Email: [jie.wang@kindinglaw.com](mailto:jie.wang@kindinglaw.com)



# **Comparison of Various Compliance Points of Data Protection Laws in Ten Countries/Regions | #2 Personal Information Handling Rules and Special Considerations**

Author: Jie (Jackie) WONG, Lawyer, Founder of W&W International Legal Team, Kinding Partners, specialising in cyber and internet practice

Date: September, 2021

## **Part II: Personal Information Handling Rules and Special Considerations**

**This is the second part of the article, which focuses on the rules and special considerations for handling personal information of different data protection laws.**

The principles of personal information handling and the specific rules of personal information handling are the most crucial and core contents in the Data Protection Act of every sovereign country. By specifying the lawful base of personal information handling and the corresponding specific rules in the law, it helps the organizations and individuals to better clarify the boundary of rights and obligations when they are involved in the activity of handling personal information. Companies and organizations should pay special

attention to the specific rules required for the handling of personal information.

## **I. Interpretation of the PIPL.**

After the third round of review, PIPL has further refined and perfected the principles and rules on the handling of personal information, setting a clearer red line for companies and organizations when handling personal information.

### **1. Principles of Personal Information Protection**

Articles 5 to 11 of PIPL establish the principles that should be followed in the handling of personal information, emphasizing that the handling of personal information should follow the principles of lawfulness, propriety, necessity and good faith, having a clear and reasonable purpose and be directly related to the purpose of handling, **adopting a way that has the least impact on the rights and interests of individuals**, being limited to the minimum scope of achieving the purpose of handling, disclosing the rules of handling, ensuring the quality of information, and adopting safety protection measures.

In summary, it can be understood as the seven main principles as follows:

### **1.1 Principles of lawfulness, propriety, necessity and good faith**

It means that the handling of personal information shall, on the one hand, have a **base of legality** (analyzed below), **be justified, and shall satisfy the requirement of necessity** (the handling of personal information shall be limited to the extent necessary to achieve the purpose of handling), and, on the other hand, shall comply with the principle of good faith and shall **not** process personal information through **misleading, fraudulent, or coercive** means.

### **1.2 Principles of clarity of purpose and reasonableness**

Compared with the Second Review Draft, the PIPL **has added a new term "using a method with the smallest influence on individual rights and interests"**, which means that the degree of impact on the rights and interests of individuals is regarded as the criterion for judging whether the handling of personal information is clear and reasonable. And PIPL particularly emphasizes that the **scope of information collection shall be directly related to the purpose of handling, and it shall be limited to the minimum extent for achieving the purpose** (the principle of minimum necessity, no excessive collection of personal information).

### **1.3 Principle of openness and transparency**

It means that the handling of personal information, on the one hand, should be publicized on how companies and organizations handle users'<sup>1</sup> personal information; on the other hand, the specific purpose of personal information handling, the handling method and the scope of personal information handling by companies and organizations should be clearly demonstrated through those privacy policies and rules released on the official websites or within the pages of the Apps.

#### **1.4 Principle of Quality**

Compared with the Second Review Draft, the PIPL **added** the requirement of "**ensuring the quality of personal information**", which means that, for realizing the purpose of personal information handling, companies and organizations should ensure the accuracy of the personal information they handle, and timely update it when it is changed.

#### **1.5 Principle of Security protection**

Without the guarantee of data security, there is no strong protection of personal information. Security is a key prerequisite for data protection, and companies and organizations shall be responsible for their personal information handling activities and take the necessary measures to guarantee the security of the personal information they handled.

---

<sup>1</sup> Users hereby means the data subject or the individuals/nature persons where the personal information comes from.

### **1.6 Principle of Prohibition of illegal handling**

The PIPL clearly enumerates eight "prohibited acts" and draws a clear red line for personal information handlers (including the organizations and individuals): no organization or individual shall illegally collect, use, process or transmit the personal information of others, or illegally sell, buy, provide or disclose the personal information of others; or engage in personal information handling activities that harm and endanger national security or the public interests.

### **1.7 Principle of Shared Governance**

Personal information protection is a matter that requires the collaboration and participation of individuals, companies, industry organizations, regulatory authorities and other parties. On the one hand, the government prevents and punishes acts that infringe on the rights and interests of personal information by establishing and improving the personal information protection system; on the other hand, it is also necessary to promote the formation of a good environment for the government, enterprises, relevant industry organizations and the public by strengthening the publicity and education on personal information protection.

## **2. The core rule: "to inform and obtain consent"**

The PIPL clearly defines **"informing and consenting"** as the core rule (the core legality basis) for the protection of personal information within the mainland of China, which, on the one hand, provides an important guarantee for the rights of individuals to be informed and the decision on the handling of their personal information; on the other hand, handling personal information with "Consent" as one of the legal bases **must provide the individual the right to withdraw his or her consent**. This is very similar to the rule set in the GDPR.

Regarding "how to inform the individuals", the PIPL specifies that companies must not only **"fully inform"** the individuals of various matters related to the handling of personal information in a truthful, accurate and complete manner (such various matters are including the identity of the handler, contact information, the purpose of the handling, the manner of handling, the type of information, the retention period, the manner and procedure of exercising the individual's rights, etc.), but also **do it in a prominent and clearly understandable manner**, and to obtain the consent of the individual again in the event of changes in important matters, rather than "obtain consent just in one time".

When it refers to "how consent is obtained", individuals are required to make **voluntary and explicit consent on the premise of "fully informed"**, rather than being coerced, unequal, or ambiguous or unclear.

It is worth mentioning that the PIPL has **added "necessary for the implementation of human resources management" as one of the legal grounds for handling personal information**, however, when using this legal base, it should be noted that it is a legal base with conditional requirements, which requests that "the labor rules and structures shall be lawfully formulated" and "the collective contracts shall be lawfully concluded". And what is meant by "lawfully formulated " and "lawfully concluded", leaves a practical space and compliance space for the companies to discuss when handling their employees' personal information, and it also improves the compliance standards for the companies as well.

### **3. The special rule: "obtain separate consent under some certain circumstances"**

At the same time, the PIPL also **sets up a special rule of requiring separate consent from the individuals under some certain circumstances**, which means that separate consent or written consent shall be obtained to handle personal information while it is provided by the laws or administrative regulations. Such circumstances are listed as follows:

#### **3.1 Handling of sensitive personal information:**

Take an example, when handling sensitive personal information, in addition to informing users of the **specific types of sensitive personal information, the necessity of handling, the impact on individuals, and the adoption of strict protection measures** in the privacy policy, the company should also **inform** its users through methods such as pop-up windows, separate page displays, etc., when that specific scenario is triggered, and it should also obtain a **separate, express and valid consent from** its users, rather than obtaining a "general consent", "blanket consent/bundled authorization", or "default consent".

### **3.2 Handling of children's personal information:**

For example, in scenarios where a company collects personal information from minors under the age of 14, the company **shall also obtain the consent from the minor's parents or other legal guardians.**

### **3.3 Providing personal information to other personal information handlers.**

Cite an example, in the scenario where a company **provides or transfers** personal information to other third-party vendors (other personal information handlers), in addition to inform its users (the PIPL sets out the legal requirements for the content of the informing) and conduct a prior personal

information protection impact assessment, **the company shall also obtain the users' separate consent.**

As for the third-party vendor who is the recipient of the data in the aforementioned case, in addition to handling personal information within the scope of what the transmitting party informs the user, such third-party vendor shall also **re-obtain the consent of its user when** it changes the original purpose and method of handling.

### **3.4 Installing image capture device and personal identification equipment in public places.**

PIPL regulates that the installation of image collection or personal identity recognition equipment in public venues shall occur as required to safeguard public security and observe relevant State regulations, and clear indicating signs shall be installed. This is the new added provision of the PIPL, which is related to the background that a large number of companies abusing Webcams to collect personal information, especially the face recognition information. Additionally, the Supreme People's Court enacted the "Provisions on Several Issues concerning the Application of Law in the Trial of Civil Cases Relating to the Use of Facial Recognition Technologies to Process Personal Information" on August 1, 2021, which is coordinating with the PIPL in such scenario mentioned above.

Therefore , when companies need to install the image capture equipment or personal identity recognition equipment in public venues, they shall pay attention to:

- (1) Limiting the purpose of collection: **it is collected for the necessity of the purpose of maintaining public security;**
- (2) Informing the individuals in a clear method: a **prominent and clear indicating reminders or signs** of “Webcams is collecting your image or identity recognition information” shall be installed in the public venue;
- (3) Limiting the handling of the individuals’ personal image and identifying information: In particular, it is important to note that the collected personal images and personal distinguishing identity characteristic information **can only be used for the purpose of safeguarding public security** and it may not be used for other purposes; except **where the individuals’ separate consent is obtained.**

### **3.5 Disclosure of personal information.**

The PIPL clearly stipulates that, **in principle, no disclosure is allowed, except for obtaining the individual's separate consent.**

It is worth noting that PIPL **also provides for "opt-out" provisions with respect to the** use of publicly available personal information, taking the overseas data protection regulations as reference.

- (1) For personal information that has been disclosed by the individual himself/herself or otherwise lawfully disclosed, the handler of personal information may handle it within a reasonable range, except where the individual expressly refuses.
- (2) For the handling of personal information that has been made public and has a significant impact on the rights and interests of the individual, the handler of personal information shall obtain the consent of the individual.

#### **4. Rules of exemption of informing**

The PIPL not only further refines the content requirements of informing and the form of informing, but also sets up two exemptions for personal information handlers.

- (1) Exemption based on the duty of confidentiality: When there are laws and administrative regulations stipulate that confidentiality shall be maintained or that there is no need to inform, then the name or the contact information of the personal information handler may not be informed.

(2) Exemption based on emergency: If it is impossible to inform the individual in a timely manner in order to protect the natural persons' life, health and the security of his or her property, the personal information handler may not need to inform the individual at the time of the emergency, but it shall inform the individual in time after the emergency is eliminated or after the conclusion of the emergency circumstances.

#### **5. Rules of joint personal information handlers shall bear joint and several liability**

**The concept of joint personal information handlers (those who jointly autonomously decide the handling purposes and handling methods) is formally established in the PIPL and is one of the new added contents.**

Unlike the EU GDPR and previously enacted Chinese personal information regulations and guidance, the PIPL does not conceptually distinguish between controllers and processors. Instead, PIPL sets up joint and several liability for the joint handlers by explicitly stipulating that "in the event of damage caused by infringement of the personal information rights and interests of the individuals where personal information handlers jointly handling personal information, the joint handlers shall bear joint and several liability together in accordance with the law".

**It is necessary to remind the companies that** in the case of joint handling, it should clearly agree on the rights and obligations of each party through the contract with other joint handler(s), clarifying the responsibilities of each party, requiring the other joint handler(s) to jointly meet the requirements of personal information security, and informing the individuals legally at the same time.

**6. Rule of automated decision-making should ensure transparent, fair and justice, and individual reserves the right to make rejections**

This is probably one of the most watched provisions and most heated discussing points of the PIPL, which clarifies the regulation of automated decision-making that should "guarantee the **transparency** of decision-making **and the fairness and justice of the handling results**" and "shall not apply unreasonable differential treatment to individuals in terms of transaction prices and other transaction conditions".

The companies are required to provide individuals with "**non-personalized options**" or "**easy opt-out options**" in the most common circumstances of automated decision making, such as, **information push and commercial marketing**.

In particular, the law explicitly provides the individual with the **right to request a clear explanation and the right to make an express refusal** in cases that the use of automated decision-making produces decisions with a major influence on the rights and interests of the individual.

The provisions mentioned above has attracted the attention of many companies that used personalized recommendation technology, especially the companies conducting precision advertising and marketing. It may trigger out many difficulties in the coming practice of PIPL, nevertheless, from the perspective of the basic compliance of auto-decision making, we suggest that the companies shall pay attention to the points as follows:

- (1) To follow the rule of “inform and consent”, which means that the company shall inform the users through a fully, comprehensively and clearly way, and to obtain a voluntary and specific consent from the users.
- (2) To explain and illustrate the transparency and fairness of the automated decisions which is made by the company itself.
- (3) When automated decisions are used for the purpose of information push, or commercial advertising promotion, the user should be provided with a convenient method to refuse, as well as the option of not targeting the individual’s characteristics.



(4) If the use of automated decision-making produces decisions with a major influence on the rights and interests of the individual, and the individual reserves the right of to ask for the explanation or making refusal, then the company shall guarantee their rights and interests, and additional manual decision-making manner should be taking into consideration.

## II. **Comparison of major overseas personal information protection or data protection laws.**

Given the rules of personal information handling is a relatively complex analytical matter, on the one hand, the data protection laws of different countries will have different regulations, **not only different concepts and classifications for special types of personal information, but also special rules for different special types of personal information**, on the other hand, in the course of a large number of practical operations, it is also necessary to combine specific business scenarios, prerequisites and multiple dimensions for comprehensive consideration. Given the limited space, **we will only briefly compare the definition of sensitive personal information and the requirements for handling and some special points** in the following table. If there are any imperfections, please feel free to let us know.

## Comparison Of The Compliance Points Of Data Protection Laws In Ten Countries/Regions

### Part II : Concept of sensitive personal information and rules for handling it

Country / Region	Category	Special rules for handling sensitive personal information	Key definitions of sensitive information	Rules for processing or special points (needs to be analyzed in the context of the business)
China PIPL			<p>Sensitive personal information is personal information that, once leaked or illegally used, may easily lead to the infringement of a natural person's human dignity or endanger the safety of his or her person or property, including biometric, religious beliefs, specific identity, medical and health, financial accounts, trajectory and other information, as well as the personal information of minors under 14 years of age.</p>	<p>1. It is emphasized that the handling of sensitive personal information <b>shall be subject to the individual's separate consent</b>, and that the processor of personal information may handle sensitive personal information <b>only if it is necessary for a specific purpose and sufficient, and if strict protective measures are taken</b>.</p> <p>2. the individual <b>shall also be informed of the necessity of handling sensitive personal information and the impact on the rights and interests of the individual</b>.</p> <p>3. Special attention should be paid to the fact that in the scenario of personal information of <b>minors under 14 years</b> of age, <b>the consent of the parents or other guardians of the minor shall also be obtained</b>.</p>
EU GDPR			<p>The GDPR special categories of information include: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or <b>trade union membership</b>, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, <b>personal data relating to criminal convictions and offences</b>.</p>	<p><b>Specific circumstances need to be met in order for processing to take place:</b></p> <ol style="list-style-type: none"> <li>1. the explicit consent of the data subject is obtained;</li> <li>2. the processing is necessary for the performance of the data controller's duties, the protection of the rights of the data subject, the core interests of another natural person;</li> <li>3. the legitimate activities of non-profit institutions</li> <li>4. the processing of personal data that have been made public;</li> <li>5. the normal exercise of rights in litigation or administrative or arbitration proceedings;</li> <li>6. activities related to the public interest (medical, public health, scientific or historical research)</li> </ol> <p>The GDPR <b>does not regulate the anonymization of data</b>, but the processing of certain "special" categories of personal data (for example, the disclosure of a person's racial or ethnic origin or personal data relating to his or her health or sexual orientation) will be subject to stricter regulation and will require a special assessment.</p>

California, USA CCPA	!	The CCPA does not have a concept of "sensitive information," but does list sensitive personal information, including ethnic and national origin, religious beliefs, union membership information, personal contact information, identity-related information (e.g., ID card, social security card information), genetic data, biometric information, and health information.	In the definition of personal information section, the CCPA not only revolves around the individual consumer, but also specifically introduces the concept of family and household data
Brazil LGPD	✓	The LGPD's sensitive information includes, among other things, racial or ethnic origin, religious beliefs, <b>political opinions, union or religious affiliation, membership in philosophical or political organizations</b> , health, sex life, genetic or biometric data related to natural persons	The legal basis for processing sensitive personal information under <b>the LGPD is stricter</b> than that for processing personal information in general, with provisions more similar to those of the GDPR, and special categories of personal information may be processed only when: 1. the express consent of the data subject is obtained; 2. in order to comply with legal or regulatory obligations; 3. by a research institution; 4. for the execution of a contract or in connection with a contract 5. for the normal exercise of rights in litigation or administrative or arbitration proceedings; 6. for the protection of life or personal safety; 7. in the interest of health (only for procedures performed by health professionals, health services or health authorities); and 8. to prevent fraud and guarantee the security of the data subject .
India PDPB (Draft)	✓	Adopting an enumeration + generalization approach, the types of sensitive information are listed in more detail than in our personal protection law, including: financial data, health data, <b>official identifiers</b> , sex life, sexual orientation, biometric data, <b>genetic data, transgender or bisexual status, caste or tribe</b> , religious or political beliefs, etc.	1. India also has special requirements for handling sensitive personal information, as reflected in its IT Act and Information Technology Rules, which set out minimum data protection standards for sensitive personal data.  2. Criminal records are not considered sensitive personal information in India at this time.
Korea PIPA	✓	Sensitive information in PIPA includes: <b>ideology</b> , beliefs, <b>membership in trade unions or political parties, political views</b> , health, sexual orientation, genetic information, <b>criminal records</b> , information generated by certain technical means that can be used to identify individuals or races, and information about the physical, physiological and behavioral characteristics of individuals.	1. Korea's PIPA is one of the most stringent data acts, including even ideology in the scope of sensitive information. 2. Also, Korea has more requirements on the processing of sensitive personal information, for example, the consent of the data subject needs to be obtained separately when processing specific identification data (e.g. passport number) and sensitive data, and must also be obtained separately from any other consent.

Japan APPI	✓	Sensitive information in APPI includes, among other things, race, creed, religion, physical or <b>mental disability, medical records, medical and medication records, personal information related to arrests, detentions or criminal proceedings</b> (whether adult or juvenile), or victims of crime.	Japan has relatively special requirements for the handling of sensitive personal information, for example, when transferring sensitive information to a third party, not only is the consent of the principal required (unless an exemption is met), but such consent cannot be given through the use of an opt-out. Japan specifically emphasizes that mental illnesses as well as medical records and medication records are sensitive information, while political opinions are not included in the Act as sensitive information.
Singapore PDPA	!	The PDPA does not explicitly give the scope of sensitive information, but the following types of personal information can be considered as sensitive personal information from past decisions of the regulator, mainly including: medical data, financial data, bankruptcy status, <b>personal information of children, and personal identifiers.</b>	The processing of personal information is required in accordance with the Act's requirements for the processing of "personal information", and children's personal information is considered sensitive in practice and requires the consent of parents and guardians
Indonesia PDPA (Draft)	✓	The PDPA (Draft) specifically addresses sensitive personal data, including data about religion or belief, health, physical and mental condition, sexual life, personal financial data, and other personal data that may pose a risk or harm to the privacy of the data subject.	Although personal sensitive information does not specify children's information, it still falls within the definition of programs that require protection, <b>and prior consent from parents or guardians is required in the Indonesian regulation on the protection of personal data in electronic systems before processing children's information</b>
Hong Kong, China PDPO	!	Unlike the EU GDPR, the Hong Kong PDPO does not define sensitive personal data, and the PDPO does not provide stricter requirements on the categories of sensitive personal data.	However, the Office of the Privacy Commissioner for Personal Data <b>has issued corresponding guidelines</b> on the requirements for the collection, use, retention and erasure of certain types of personal data (including identification numbers, personally identifiable information, consumer credit data and biometric data) <b>with correspondingly stringent requirements.</b>
Illustration Description:			
✓	The country/region has a definition or concept of sensitive personal information		
✗	No clear regulations, or no corresponding guidelines have been issued		
!	Need for further explanation or clarification		

## Overall

The specific rules for the handling of personal information is a very noteworthy part in data protection law of different countries,, and **many data protection laws and regulations in different countries propose special handling rules for some certain types of data** in order to better protect the

rights and the interests of individuals (for example, they will conceptually classify general personal information, sensitive personal information, health information, and biometric information, respectively, as well as provide for different handling rules for those types of information). And such rules also serve as a compass for companies, organizations and individuals in handling personal information, and as a foundation for distinguishing the red line of personal information compliance.

# **Comparison of Various Compliance Points of Data Protection Laws in Ten Countries/Regions | #3 Data localisation requirements**

Author: Jie (Jackie) WONG, Lawyer, Founder of W&W International Legal Team, Kinding Partners, specialising in cyber and internet practice

Date: September , 2021

## **Part III: Data localisation requirements**

**This is the third part of the article, which focuses on the interpretation and comparison of data localisation requirements of different data protection laws.**

Data localisation is one of the ways in which a sovereign country/region restricts the flow of its data outside of its borders by enacting laws or regulations. Data is also known as the “New Oil” in the 21st century and is particularly important in the global Internet Information Era. Therefore, certain countries/regions classified personal information in different dimensions, and regulated data localisation and cross-border transfer restrictions based on different types of personal information.

## I . Interpretation of the PIPL

### 1. The principle of personal information to be stored within the territory is clarified.

PIPL clearly stipulates the principle that the personal information in certain circumstances shall be stored within the mainland of China, and such specific circumstances include:

- (1) Personal information **handled by** State organs.
- (2) Personal information collected and generated by **Critical Information Infrastructure Operators ('CIIOs')** *within the mainland of China*.
- (3) **Even if the handler is not a CIIO, if the amount of personal information collected and generated by the handler within the mainland of China reaches the amount prescribed by the national cyberspace authority,** it shall be stored within the mainland of China.

The PIPL particularly emphasizes that the CIIO and personal information handlers handling personal information reaching the amount specified by the national cyberspace authority **shall store personal information collected and generated within the mainland of China and shall not transfer it outside the mainland of China. If it is indeed necessary to provide personal information outside the mainland of China, it shall pass the security assessment organized by the national cyberspace authority.**

In other words, for the storage, utilization, control and jurisdiction of critical data such as critical information infrastructure, China has put forward a **clear requirement for data localisation**, the basic logic of which is that any Chinese or foreign company collecting and storing personal information related to the critical information infrastructure in China must use the servers which are located within the mainland territory of China.

This is one of the crucial manifestations of China's exercise of "data sovereignty" as a sovereign state, and is also in line with *China's Cybersecurity Law*, which explicitly requires the storage of "personal information and critical data collected and generated by CIIO during their operations within the territory of the People's Republic of China" based on the consideration of safeguarding network data security.

## **2. Brief compliance suggestions to the companies**

From the previous analysis, it is clear that the PIPL does not impose demandingness requirements on data localisation as some sovereign countries (e.g. Russia) do, but rather imposes data localisation requirements and security assessment obligations on **specific subjects**. Companies, especially those involved in international business, need to pay attention to whether they are subject to data localization requirements when handling personal information.

**Step 1: Determine whether the data subject falls into the scope of the mandatory data localization.**

If so, data localisation is required, which means companies shall store personal information collected and generated in China within the mainland of China.

**Step 2: Determine if it is indeed necessary to transfer the information outside the mainland of China.**

In other words, Companies need to consider and confirm the necessity of data transfer in the context of the actual business situation and its operational arrangement.

**Step 3: Determine whether it has passed the security assessment organized by the national cyberspace authority.**

China's data localization requirements do not completely prohibit the cross-border transfer of personal information, and for the personal information that do need to be cross-border transferred, they need to pass a security assessment organized by the national cyberspace authority before being transferred.

According to the requirements of the 2019 " *Measures on Security Assessments for the Export of Personal Information and Important Data (Draft for Comments)*" released by Cyberspace Administration of China (CAC), in the circumstance of personal information cross-border transfer, only the conducting of internal security assessments by the company is not sufficient. Moreover, the company shall conduct the security assessments organized by the provincial national cyberspace authority where they are located,. The focus of the security assessment includes:

- (1) Assessing whether the cross-border transfer of personal information is in compliance with laws, regulations and policies.
- (2) Whether the contract signed by the transferring party and the receiving party can adequately protect the legitimate rights and interests of the subject of personal information.
- (3) Whether the contract is being effectively enforced.
- (4) Whether the transferring party and the receiving party have a history of harming the legitimate rights and interests of the subject of personal information, and whether there has been a major network security incident.
- (5) Whether the transferring party obtained personal information legally and legitimately.

## **II . Comparison of major overseas personal information or data protection laws**

## Comparison Of The Compliance Points Of Data Protection Laws In Ten Countries/Regions

### Part III: Comparison of data localization requirements

Country / Region	Category	Availability of regulatory guidelines	Mandatory requirement for data localization	The main provisions of the country/region's data protection law	Compliance points/special points/remarks
China PIPL		✓	✓	The following cases, personal information required to be stored in the territory: (1)Personal information handled by State organs. (2)Personal information collected and generated by Critical Information Infrastructure Operators ('CIIOs') within the mainland of China. (3)Even if the handler is not a CIIO, if the amount of personal information collected and generated by the handler within the mainland of China reaches the amount prescribed by the national cyberspace authority, it shall be stored within the mainland of China.	China's current data protection law has high requirements for data localization, and it is necessary to pay attention to the specific definition requirements for the three cases that need to be stored within the mainland of China, as well as the security assessment requirements before export
EU GDPR		✓	!	No data localization requirements unless cross-border data transfer requirements are not met	Cross-border transfer requirements are high, and there are white list, BCR, SCCs and other provisions of the constraints, more complex, need to be combined with the specific business situation to analyze and match
California, USA CCPA		✗	✗	There is no mandatory requirement for data localization	However, some public procurement contracts may include domestic data storage as a requirement.
Brazil LGPD		✗	!	There is no mandatory requirement for data localization, but there are separate requirements in specific sectoral laws such as the financial sector and the public sector.	Attention should be paid on the requirements for data localization of special data categories
India PDPB (Draft)		✗	!	1. For general personal data, there are no localization or data transfer restrictions in India. 2. For critical personal data, it can only be processed within India, although exceptions are provided, such as for emergencies or for national security interests of the central government. 3. For sensitive personal data, it must be stored within India, but copies can be transferred outside India as required for cross-border transfers	India has data localization/processing restrictions for critical personal data and sensitive personal data, and different restrictions on original information storage and copy storage for different types of information.

Korea PIPA	✗	!	There is no mandatory requirement for data localization, but there are additional requirements in specific sectoral laws such as the healthcare industry.	The need to focus on the requirements for data localization of special data categories
Japan APPI	✓	!	There is no mandatory requirement for data localization, but there are additional requirements in special sectoral laws such as the pharmaceutical sector.	Attention should be paid on the requirements for data localization of special data categories
Singapore PDPA	✓	✗	Among the general personal information protection requirements, Singapore does not have mandatory requirements for data localization	However, Singapore has relatively strict restrictions on cross-border transfers
Indonesia PDPA (Draft)	✗	!	Only public electronic system operators are required to locate their electronic systems and data locally in Indonesia.	Unless otherwise specified, private electronic system operators may locate their electronic systems and data within or outside Indonesia
Hong Kong, China PDPO	✓	✗	According to Hong Kong PDPO, there is no requirement for data localization.	Attention should be paid on the changes in the 33 regulations
Illustration Description:				
✓	There are corresponding requirements			
✗	No clear regulations, or no corresponding guidelines have been issued			
!	Need for further explanation or clarification			

**For the above-mentioned types of data required to be localized, they can be broadly classified into three types:**

(1) Data protection laws that do not explicitly require data localisation, but may provide strict restrictions when making cross-border transfers, including the EU, Singapore, etc..

(2) Types of data are classified and different data localization requirements are provided for different data types. India, for example,

is divided into critical personal data, sensitive personal data and general personal data. Critical personal data must be stored in India, but exceptions are provided; for sensitive personal data, it must be stored within the territory of India, but the copies of it can be transferred outside India in accordance with cross-border transfer requirements.

(3) The data subjects are divided into several types, and different data localisation requirements are imposed for the data subjects in certain types. For example, Indonesia requires that only the public electronic system operators shall store their electronic systems and its data within the territory of Indonesia.

## **Overall**

Data localization is increasingly becoming a global challenge as national regulators, and they recognize the need for certain types of data to be stored within borders and the need for stricter controls on cross-border data transfers. For companies involved in overseas business, it is suggested that they may pay special attention to the data localisation requirements of the target countries that they are planning to enter into, and consider the location and solution of server deployment in conjunction with the overall business development plan and business operation cost, so as to better meet the data compliance requirements of the target country while improving the efficiency of the

internal operation of the company.

# **Comparison of Various Compliance Points of Data Protection Laws in Ten Countries/Regions | #4 Rules and requirements for cross-border data transfer**

Author: Jie (Jackie) WONG, Lawyer, Founder of W&W International Legal Team, Kinding Partners, specialising in cyber and internet practice

Date: September , 2021

## **Part IV: Rules and requirements for cross-border data transfer**

**This is the fourth part of the article, which focuses on the interpretation and comparison of rules and requirements for cross-border data transfer of different data protection laws.**

In the era of digital economy, data is a fundamental strategic resource that countries are competing for. Countries are constantly enacting rules and policies on cross-border data transfer to strengthen their control over data resources in order to occupy a favorable position in the global digital economy development environment. At the same time, the flow of data is the only way to generate economic dividends, and how to balance the cross-border data flow to bring great promotion for transnational cooperation while also better

safeguarding states sovereignty in terms of privacy, corporate commercial interests and national security, which brings new challenges to the policy makers.

## **I . Interpretation of the PIPL**

### **1. Pre-requisites for cross-border data transfer**

The PIPL formalizes the system of rules for the cross-border flow of personal information in China, stipulates that personal information shall be stored within the territory as the principle, and establishes the rules for transferring personal information outside the territory only under certain legal conditions.

It can be seen that China **has adopted the approach of ex ante regulation on the cross-border transfer of personal information**, and it is based on the fact that the cross-border flow of personal information will affect the security of personal privacy, corporate interests and even national security, as well as the irreversible nature of the cross-border flow of data.

Article 38 of the PIPL clearly states that if a personal information handler really needs to provide personal information outside the People's Republic of China for business and other reasons, it should **have at least one of the following** conditions:

- (1) Passing a security assessment organized by the national cyberspace authority according to Article 40 of this Law;*
- (2) Undergoing personal information protection certification conducted by a specialized body according to provisions by the national cyberspace authority;*
- (3) Concluding a contract with the overseas receiving party in accordance with a standard contract formulated by the national cyberspace authority, agreeing upon the rights and responsibilities of both sides;*
- (4) Other conditions provided in laws or administrative regulations or by the national cyberspace authority.*

*Where treaties or international agreements that the People's Republic of China has concluded or acceded to contain provisions such as conditions on providing personal data outside the territory of the People's Republic of China, it is permitted to act according to those provisions.*

Firstly, from the analysis of the original meaning of the Article 38 of the PIPL, at least one of the conditions shall be met with by the handler, however, in practice, it would be better if the other conditions can also be met with.

Secondly, it should be noted that, passing the security assessment or undergoing the personal information protection certification, is not a matter

of self-assessment or self-certification by enterprises, instead, both of them shall be carried out under the arrangement and organization of the national cyberspace authority. And for the details of measures for security assessment is provided within the *"Measures for Security Assessment for Cross-border Transfer of Personal Information (Draft for Comments)"* issued by the Cyberspace Administration of China (CAC) in 2019, however, such rules related to security assessment are still in the stage of seeking public opinions, therefore, there is no other further mandatory regulations and policy guidelines related to such issues that have been effected yet.

Therefore, although there is no specific enacted standard contract designated by the national cyberspace authority yet, a more feasible way for multinational enterprises to transfer personal information across borders is to adopt the approach of "signing contract with the overseas recipient", by requiring the provider and the recipient to sign a comprehensive contract to agree on the rights and obligations of both parties in the handling of personal information.

## **2. Basic requirements for cross-border provision of personal information**

**Cross-border transfer is a kind of handling activities personal information,** therefore, in the case of meeting the "pre-requisites", companies are still required to follow the PIPL's basic requirements when they prefer to provide

personal information to other foreign countries out of the territory of the mainland of China, and such basic requirements are mainly including:

(1) **Informing** the data subject of the identity and contact information of the recipient outside the country, the purpose of handling personal information, the manner of handling, the type of personal information, the corresponding rights of the data subject, and the retention period (and should be the minimum time necessary to achieve the purpose of handling, etc.).

(2) Obtaining **separate consent from the data subject**;

(3) Conducting a prior **personal information protection impact assessment (DPIA/PIA)**;

(4) Taking the necessary measures to ensure that the activities of offshore recipients in handling personal information are able to **meet with the personal information protection standards** required by the PIPL.

(5) Ensuring that the overseas recipient **does not fall into the blacklist of the national cyberspace authority**.

### **3. Reciprocity requirements for cross-border provision of personal information**

The PIPL established the "principle of reciprocity" for cross-border transfer of information, that is, if the country or region of the recipient takes

discriminatory **prohibitions, restrictions or other similar** measures against China in the protection of personal information, as **China can take reciprocal prohibitions, restrictions or other similar measures against that country or region according to the actual situation**. In such a case, when personal information is provided to such countries or regions by companies, then there will be some certain restrictions, , which need to be analyzed case-by-case.

#### **4. Special requirements for cross-border provision of personal information**

**A. When providing personal information outside the territory of the mainland of China, special attention shall also be paid to the type and the quantity of the personal information being transferred.**

For CIIOs, as well as personal information handlers that handle personal information reaching the quantities specified by the national cyberspace authority, they shall:

- ◆ **Storing** personal information collected and generated within the territory of the mainland of China.
- ◆ Passing a security assessment organized by the national cyberspace authority while it is truly necessary to transfer the personal information abroad; where laws or administrative regulations and provisions of the national cyberspace authority permit that security assessment not be conducted, those provisions are to be followed.

**The definition of "critical information infrastructure"**, which is mentioned in the *"Regulations on the Security Protection of Critical Information Infrastructure"* that have been taken into effect recently, and it mainly refers to public communications and information services, energy, transportation, water conservancy, finance, public services, e-government, national defense science and technology industry and other important industries and fields, as well as other crucial network facilities and information system that, once damaged, function loss, or data leaked, may seriously jeopardize national security, the people's livelihood, and public interests.

**Regarding the definition of "personal information reaching the quantities prescribed by the national cyberspace authority"**, it can be referred to the *"Measures on Network Security Censorship (Revised Draft for Comments)"* enacted by the CAC in July, 2021, as well as the *"Measures for Evaluating the Security of Transferring Personal Information and Important Data Overseas (Draft for Comments)"* enacted by the CAC in 2017.

#### **B. Provisions of assistance in offshore judicial enforcement**

The PIPL sets a very high threshold in assistance in offshore judicial enforcement, clearly stipulating that personal information stored in China shall **not be provided to foreign judicial or law enforcement agencies without the approval of national competent authorities**. It can be seen that China also emphasizes and adopts the principle of ex ante regulation in this case, even if

various security assessments are conducted, consent of data subjects is obtained, and personal information protection certification is conducted, it cannot be a pre-requisites for providing personal information to foreign judicial or law enforcement agencies, and the only way to flow out of the mainland of China is to obtain explicit approval from the governing national authorities.

## **II . Comparison of major overseas personal information or data protection laws**

## Comparison Of The Compliance Points Of Data Protection Laws In Ten Countries/Regions

### Part IV: Comparison of data cross-border transfer rules restrictions and requirements

Country / Region	Category	Availability of regulatory guidelines	Restrictions	Exemptions	The main provisions of the country/region's data protection law	Compliance points/special points/remarks
China PIPL		✓	✓	✓	<p>Personal information and important data generated and collected in the territory, in principle, should be stored in the territory.</p> <p>if a personal information handler really needs to provide personal information outside the People's Republic of China for business and other reasons, it should have at least one of the following conditions:</p> <p>(1) Passing a security assessment organized by the national cyberspace authority according to Article 40 of this Law;</p> <p>(2) Undergoing personal information protection certification conducted by a specialized body according to provisions by the national cyberspace authority;</p> <p>(3) Concluding a contract with the overseas receiving party in accordance with a standard contract formulated by the national cyberspace authority, agreeing upon the rights and responsibilities of both sides;</p>	<p>Cross-border transfer requires compliance with the statutory duty to inform, including informing the individual of:</p> <ol style="list-style-type: none"> <li>1. the identity and contact information of the foreign recipient ;</li> <li>2. the purpose of handling and the manner of handling;</li> <li>3. the type of personal information</li> <li>4. the manner in which the individual can exercise his /her rights under the PIPL to the foreign recipient, and other matters.</li> </ol> <p>And the individual's separate consent is required to be obtained.</p>
EU GDPR		✓	✓	✓	<p>Cases where the transfer of personal data outside the EEA is permitted:</p> <ol style="list-style-type: none"> <li>1. where the recipient is located in an area that the EC considers to provide an adequate level of protection for personal data;</li> <li>2. where appropriate safeguards are in place, such as standard contractual clauses approved by the EC or binding corporate rules approved by the DPA;</li> <li>3. in other reasonable circumstances, such as where the data subject has expressly agreed that the transfer is necessary for the performance of a contract, is necessary for the realization of the data subject's interests, necessary to achieve the public interest, necessary to establish, exercise or defend a claim of a legal nature, necessary to protect the vital interests of the data subject or others, and other circumstances.</li> </ol>	<p>In addition to the generic cross-border transfer scenarios described above, the GDPR also supports data transfers for international legal cooperation in accordance with national legal instruments.</p>

California, USA CCPA	✗	✗	✗	The CCPA has no regulations regarding cross-border transfer of data.	Unlike most other countries, data transfers are considered part of selling personal information in CCPA, and consumers have the right to refuse to have their data shared with third parties (based on the right to know, the right of access and the right to refuse)
Brazil LGPD	✗	✓	✓	The LGPD provides for seven circumstances in which international transfers of personal information are permitted, and cross-border transfers can only be made under these several legal circumstances, and there are specific and detailed requirements for different circumstances.	The LGPD is very comprehensive in terms of the circumstances in which individuals can transfer data across borders, and basically covers all the circumstances in which transfers are permitted in other countries.
India PDPB (Draft)	✗	✓	✗	The transfer of copies of sensitive personal data outside of India is permitted provided that: 1. the data subject has given his or her explicit consent; 2. it is done under a DPA-approved contract or intra-group program; 3. the government considers a country or class of entities within a country to provide adequate protection; and 4. the DPA has explicitly authorized the transfer.	Other exceptions to cross-border transfer exist, such as certain exemptions for preventing, investigating or prosecuting crimes, enforcing legal rights and obtaining legal advice.
Korea PIPA	✗	✓	✓	The consent notification for cross-border transfer is specified in PIPA. In general, the cross-border transfer of data requires notification of: 1. the recipient of the data 2. the purpose of the transfer 3. what data is being transferred 4. the duration of use and retention  On top of this, the following must be notified and consent obtained from the data subject: (1) the country to which the data is transferred; (2) the date, time and manner of transfer; (3) the name and contractual information of the recipient; and (4) the purpose.	PIPA emphasizes the notification of data subjects and the content of the notification. Violations of cross-border transfer requirements may result in fines of up to 3% of the relevant revenue (or up to \$300,000 if the amount is difficult to calculate). There are also special provisions for offshore deployment of servers, which need to be dealt with specifically in the context of business realities.

Japan APPI	✓	✓	✓	<p>Data may be transferred from Japan to a third country only if:</p> <ol style="list-style-type: none"> <li>1. the data subject has consented to the transfer</li> <li>2. the transfer is to a country on an approved white list (31 European countries)</li> <li>3. the transfer is to a member of a code of conduct program that has received certain qualifications or has been approved by the relevant supervisory authority;</li> <li>4. the data recipient has achieved sufficient advance protection measures to meet the requirements of the PPC. For example, data transfer agreements or internal rules are in place that are equivalent to the obligations set out in the APPI.</li> </ol>	Japan and many European countries have data transfer whitelist, so the feasibility and convenience of cross-border transfer is better
Singapore PDPA	✓	✓	✓	<p>The PDPA sets out the institution's transfer limitation responsibilities. Data transfer outbound requires the institution to meet the following requirements:</p> <ol style="list-style-type: none"> <li>1. take appropriate measures to meet the transfer limitation responsibilities and data protection principles set forth under the PDPA</li> <li>2. take appropriate measures to ensure and meet the data recipient's obligation to provide data protection capabilities no less than those required by the PDPA; and</li> <li>3. obtain the consent of the data subject.</li> </ol>	This part of the "obligation" is mainly reflected in the form of "laws, contracts, binding corporate rules and other binding instruments". In addition, the amendments effective in 2020 include two new certifications that meet the "obligation" requirement by default.
Indonesia PDPA (Draft)	✗	✓	✓	<p>According to Article 49 of the PDPA (Draft), data transfer is permitted if:</p> <ol style="list-style-type: none"> <li>1. a data transfer contract exists between the personal data operator and the offshore data recipient;</li> <li>2. an international bilateral agreement exists.</li> </ol>	Article 27(1) of the Indonesian Law on Electronic Information and Transactions and Article 21(a) of Kominfo Regulation No. 20 prohibit the transfer of personal data without the consent of the data subject.
Hong Kong, China PDPO	✓	✓	!	<p>Personal data may be transferred in Hong Kong to a third party (outside Hong Kong):</p> <ol style="list-style-type: none"> <li>1. to a recipient belonging to a class of transferees notified to the data subject in accordance with the duty to inform; or</li> <li>2. with the data subject's consent;</li> <li>3. subject to the "data subject consent" exception</li> </ol> <p>Article 33 of the PDPO is not yet in force</p>	For personal data transfers outside of Hong Kong (to mainland China or elsewhere), while there are no specific restrictions for the time being, there is a need to keep an eye on the future changes and effectiveness of the Section 33 regulations.
Illustration Description:					
✓	There are corresponding requirements				
✗	No clear regulations, or no corresponding guidelines have been issued				
!	Need for further explanation or clarification				

## Overall

In terms of cross-border data flows, the regulatory pathways are mainly brought about by the U.S. and the EU.

The U.S. advocates the "free flow of data" in terms of data inflow, emphasizing the advantages of U.S. technology and data resources to promote the development of the digital economy; in terms of data outflow, it restricts the data of high-tech, dual-use technology out of the country through export control means.

The EU has opted for a cross-border data management model that is "Loose within the EU , strict outside the EU". It promotes the free flow of data within the territory of EU by adopting the "framework for the free flow of non-personal data in the European Union ", and at the same time, it also strengthens the control of data outflow by establishing the legal framework for data protection in the EU by enacting the "General Data Protection Regulation". Additionally, the protection of EU personal data has been strengthened through its long-arm jurisdiction.

# **Comparison of Various Compliance Points of Data Protection Laws in Ten Countries/Regions | #5 Rights of data subjects in personal data handling activities**

Author: Jie (Jackie) WONG, Lawyer, Founder of W&W International Legal Team, Kinding Partners, specialising in cyber and internet practice

Date: September , 2021

## **Part V: Rights of data subjects in personal data handling activities**

**This is the fifth part of the article, which focuses on the interpretation and comparison of the rights of data subjects in personal information handling activities of different data protection laws.**

Every individual has his or her own right to protect personal information or data relating to him/her. And the handling of a personal information must be carried out for a specific purpose and on the legal bases such as the consent of the data subject, and the handling process of the personal information should be in a fair, equal and voluntary way. **Such personal information rights of data subjects may be divided into different types, including the right to maintain the dignity of the data subject,** such as the right to access the data

collected from him/her (**right to inform, right to access**), and the right to rectify it (**right to rectification**); the right to negatively control the use of data, such as the **right to delete/right to be forgotten, right to restrict handling/right to refuse**, etc.; and the right to actively process and control the data , such as **the right to transfer/the right to data portability**.

It is very important and crucial to grant data subjects the rights in personal information handling activities through the effective law, which not only means that every individual has the right to protect their personal information, **but also reflects that enterprises shall handle and use the personal information of these data subjects in a fair, legal and compliant manner, and respect the personal information rights of each individual.**

## **I . Interpretation of the PIPL**

The PIPL, while learning from the overseas advanced data protection laws, it also having its own characteristics, granting the personal information rights for the data subjects in eight aspects, and in particular, it has made further improvement on the accessible ways for data subjects to exercise their personal rights, as well as on the protection of the rights of the deceased, so that the overall framework of personal information protection in China is much more well-established.

### **1. Right to Inform**

The most fundamental right for the data subject, is the right to be fully informed and understand how personal information is collected, used and processed, and this is also in line with the legal requirements of the PIPL, which requiring companies to fulfill their obligation to inform data subjects and obtain the voluntary and explicit consent from data subject.

When handling personal information, the enterprise shall make the data subject clearly understand the various contents and rules concerning the handling of personal information by explicit personal information protection policy, including but not limited to the companies' identity, contact information and other basic information, the specific type of and the scope of personal information collected, the collection method of personal information, the storage period, the handling rules of data export, the purpose of handling of personal information, method and scope of personal information, etc.

## 2. Right to decide

The right of the data subject to make independent decisions regarding his/her personal information is the core of data subject right protection. Data subjects reserve the right to decide whether to accept the collection, use, and processing of his/her personal information by the personal information handler or not. Companies should provide adequate safeguards for the data subject's right to decide when handling personal information, for example, by actively checking the consent agreement, and by distinguishing between necessary

and additional business functions to provide the data subject with the ability to choose whether to accept the service or not.

### **3. Right to restrict**

The right to restrict personal information handling is an extension of the **right to decide**, for example, the data subject has the right to request the collection of the personal information by the enterprise or organization shall be limited to the smallest scope for realizing the handling purpose, and require the enterprise or organization not to collect excessive personal information; and the data subject also has the right to request the enterprise or organization to use personal information only within the limited scope that has been informed and agreed upon, and if the scope exceeds the consensual scope or exceeds the reasonable and lawful scope, it is necessary to inform and obtain consent again.

### **4. Right to object**

The right to refuse of the data subject can also be understood as an **extended manifestation of the right to decide**, for example, the data subject can refuse to provide personal information for certain business functions where providing personal information is not necessary. CAC issued the *"Provisions on the Scope of Necessary Personal Information for Common Types of Mobile Internet Applications"* in March 2021 to carry out clear requirements, stipulating that Mobile Internet Application (App) operators shall not refuse

**users to use the App's basic functional services if the users do not agree to collect non-essential personal information.** The PIPL, in the personal information handling rules, also further guarantees the possibility of the right to object for the data subjects by requiring the personal information handlers shall not refuse to provide products or services on the grounds that individuals do not consent to the handling of their personal information or individuals withdraw their consent (except when the handling of personal information is necessary for the provision of products or services).

## **5. Rights to access and data portability**

The **data subject has the right to view, access and copy the personal information collected and processed,** but exemptions are provided, for example, in cases where companies or organizations are required by law to keep personal information confidential or are not required to inform when handling it.

**The PIPL also specifically added the right to data portability, a right that was not reflected in the previous first or second drafts.** This right explicitly requires that when a data subject requests the transfer of his/her personal information to another personal information handler designated by him/her, the personal information handler shall provide the means and the possibility for the transfer if the conditions specified by the PIPL are also met.

Data portability also brings a lot of problems and controversies in practice, which we may discuss in another article, but not here for now.

## **6. Right to rectification and supplement**

Personal information will also have a dynamic change, and it is important to give the data subject the right to rectify and supplement it, because inaccurate and incomplete personal information will not only affect individuals in their lives and work, but also bring other risks for enterprises when handling personal information (especially when it comes to sensitive areas and situations such as credit, finance, and medical care). Therefore, **when data subjects request rectifications, supplement or other objections to their personal information, enterprises, organizations and other handlers should respond and process in a timely manner, verify the accuracy of personal information, and correct and add to incorrect and incomplete information in a timely manner.**

## **7. Right to delete**

The right to delete personal information is an important manifestation of the protection of the rights of the data subject, which may also be called differently in other countries or regions, such as the right to erasure and the right to be forgotten (there will be specific and subtle differences).

Compared with the previous draft, the PIPL adds **"the purpose of handling cannot be achieved"** to the reasons for delete, and also provides for the remedy guarantee of the right to delete for the personal information handler, which means, when the data subject requests to exercise the right to delete, and the retention period required by other laws and regulations has not yet expired, or if technical difficulties exist, the handler of personal information shall stop handling personal information, except for storing and taking the necessary security measures. The stop for handling personal information is regarded as the remedy to the data subject when the enterprise or organization is unable to satisfy the right to delete.

At the same time, it is important to note that, **in principle, in some special cases, the personal information handler shall delete personal information actively.** If the personal information handler does not take the initiative to delete the information, then the PIPL provides the individual the right to request the personal information handler to do so. Therefore, as a personal information handler, it shall pay attention to the circumstances as follows:

- (1) The purpose of the handling has been achieved, cannot be achieved, or is no longer necessary to achieve the purpose of the handling.
- (2) Personal information handlers cease to provide products or services, or the retention period has expired.
- (3) Individual withdraw his/her consent.

(4) Personal information handlers violate laws, administrative regulations or violate the agreement to handle personal information.

(5) Other circumstances specified in laws and administrative regulations.

## **8. Right of Explanation**

As mentioned earlier, companies should clearly inform users of the rules for **handling personal information** and related contents, which is an effective protection for the rights of data subjects. Therefore, the PIPL grants **data subjects the right to request companies to explain the rules for handling their personal information**, and when individuals make such a request, handlers of personal information should give feedback and response to it in a timely manner.

## **9. Inheritance rights of near relatives regarding personal information of the deceased**

**This is one of the highlights of the PIPL's new content.** From a global perspective, the law for the protection of personal information and privacy protection of the deceased, many countries are still in the process of exploration, some countries have clear legislative provisions, such as the United States HIPPA for the deceased in the privacy protection of medical aspects.

The PIPL also provides a certain degree of protection for the personal information of the deceased, in the case of death of a natural person, when the near relatives of the deceased is for their own legal and legitimate interests, then they may exercise the rights to access, rectify, delete and other related rights to the personal information of the deceased, except **if the deceased has made other arrangements by agreement during his/her lifetime.**

It can be seen that the **statutory basis for the rights of the deceased data subjects exercised by the near relatives of the deceased is clear, including lawfulness, legitimacy, or compliance with the arrangements made by the deceased during his/her lifetime.** At the same time, the rights that can be exercised by the near relatives and other heirs of the deceased are specific and clear as well, which is including the right to access, the right to rectify and the right to delete.

#### **10. Ways of exercising individual rights**

Without an effective way to realize the rights of individuals, the rights of the above-mentioned data subjects will remain only on paper.

**Therefore, the PIPL, especially at the end of this chapter, adds and clearly requires that enterprises, organizations and other personal information handlers should establish convenient, truly accessible and user-friendly ways to exercise the rights of data subjects, including the channels to report, and the feasible complaint and dispute settlement mechanism.**

At the same time, enterprises, organizations and other personal information handlers are explicitly required **to clearly state their specific reasons for refusing requests from individuals to exercise their rights. In the event that a personal information handler** refuses to exercise the request of data subject, then the **individual reserves the right to file a lawsuit to the court in order to obtain effective judicial remedy.**

## **II . Comparison of major overseas personal information or data protection laws**

Comparison Of The Compliance Points Of Data Protection Laws In Ten Countries/Regions								
Part V: Comparison of data subject rights								
Country / Region	Right to Inform	Right to Access	Right to Rectification	Right to Erasure	Restriction of Processing	Right to Object/Opt-out	Data Portability	Automated Decision-making
China PIPL	✓	✓	✓	✓	✓	✓	✓	<p>!</p> <p>Personal information processors using personal information for automated decision-making shall ensure transparency in decision-making and fair and equitable results, and shall not apply unreasonable differential treatment to individuals in terms of transaction prices and other transaction conditions.</p>
EU GDPR	✓	✓	✓	✓	✓	✓	✓	✓
California, USA CCPA	✓	✓	✗	✓	✗	✓	✓	✗
Brazil LGPD	✓	✓	✓	✓	✓	<p>!</p> <p>The right to object is not explicitly provided for, but sections 8, 15, 16 and 18 of the LGPD provide for the right to withdraw consent to processing.</p>	✓	✓
India PDPB (Draft)	✓	✓	✓	✓	<p>However, section 20 of the PDPB(Draft) provides for a right to restrict further disclosure of the forgotten and this right may only be exercised by order of an adjudicating officer designated under section 62 of the Act.</p>	<p>Sections 7 and 11 of the PDPB(Draft) set out the conditions for consent and withdrawal of consent</p>	✓	✗
Korea PIPA	✓	✓	✓	✓	✓	✓	✗	✗
Japan APPI	✓	✓	✓	✓	✗	✓	✗	✗

Singapore PDPA	✓	✓	✓	! However, the retention of such personal data must cease if it is no longer necessary for legal or business purposes in accordance with the retention limitation obligation	✗ ✗	✓	✗	✗
Indonesia PDPA (Draft)	✓	✓	✓	✓	✓	✓	✓	✓
Hong Kong, China PDPO	✓	✓	✓	✗	✗	! However, 6A of the PDPO provides the right to request the cessation of processing related to direct marketing	✗	✗
Illustration Description:								
✓	There are corresponding requirements							
✗	No clear regulations, or no corresponding guidelines have been issued							
!	May have proviso section or need for further explanation or clarification							

## Overall

The data protection laws of various countries are still relatively adequate in protecting the rights of data subjects, especially in the protection of the core basic rights such as the right to Inform, the right to access, the right to rectification, and the right to delete. With the continuous iteration and development of data protection laws, the rights of data subjects will receive more effective and perfect legal protection in the future.

# **Comparison of Various Compliance Points of Data Protection Laws in Ten Countries/Regions | #6 Data protection impact assessment (DPIA/PIA) requirements**

Author: Jie (Jackie) WONG, Lawyer, Founder of W&W International Legal Team, Kinding Partners, specialising in cyber and internet practice

Date: September , 2021

## **Part VI: Data protection impact assessment (DPIA/PIA) requirements**

This is the sixth part of the article, which focuses on the interpretation and comparison of rules and data protection impact assessment (DPIA/PIA) requirements of different data protection laws.

This article is the **sixth part** of the series "**Comparison of Top Ten Compliance Points of Data Protection Laws in Ten Countries/Regions**", which focuses on the interpretation, comparison and analysis of the **requirements of data protection impact assessment (DPIA/PIA)**.

Data Protection Impact Assessment ('DPIA') is a provision from the GDPR that requires data controllers to carry out a DPIA for operations that may pose

a high risk to the rights and freedoms of natural persons. The DPIA, also known as Privacy Impact Assessment ('PIA') in some countries or regions, refers to the obligation of the data controller to conduct a DPIA before starting data handling activities and/or in some specific circumstances. In order to help companies identify and systematically analyze the risks involved in the data handling process, data controllers are obliged to conduct impact assessments on different dimensions of the data handling behavior and assess the different risks that may cause damage to the legitimate rights and interests of data subjects.

Given the limited space, this article will only provide a basic comparison of the situations that require a DPIA/PIA, and will not discuss how to conduct a DPIA/PIA for the time being; we may analyze how to conduct a DPIA in other articles.

## **I . Interpretation of the PIPL**

Before the enactment of the PIPL, China already has relevant laws and national standards and guidelines and other documents that stipulated the issue on "personal information security impact assessment", such as the "Cybersecurity Law" requires that "*Personal information and important data collected and produced by critical information infrastructure operators during their activities within the territory of the People's Republic of China, shall be*

*stored within the territory; where due to business requirements it is indeed necessary to provide such information and data to the overseas parties, a security assessment shall be conducted according to the measures jointly formulated by the national cyberspace administration and the relevant departments of the State Council "*; for another example, the *Data Security Law* provides that "handlers of important data" shall "conduct regular risk assessments of their data handling activities in accordance with the provisions of the law, and report the assessments to the relevant competent authorities as well". The State Administration of Market Supervision and Administration, and the National Standardization Administration also enacted the "Information Security Technology - Personal Information Security Impact Assessment Guide ('GB/T39335-2020')" to provide assessment rules and reference content on how to conduct DPIA, in order to provide more effective practical reference tools and standards for enterprises.

Although the aforementioned provision of personal information security impact assessment had been enacted before the PIPL, for most non-CIIOs and non-critical data handlers, the need for DPIAs is not mandatory, so many companies may not have made it as an internal compliance mechanism. However ,**the PIPL has explicitly regulated DPIA as a mandatory legal requirement in certain specific circumstances, which has put forward more**

**stringent requirements for the construction of the internal compliance system of enterprises.**

The PIPL does not stipulate the necessity for a DPIA on general scenarios, instead, it focuses on specific handling activities as a reference point for determining whether a DPIA/PIA is required. **The circumstances in which personal information handlers shall conduct a DPIA prior to data handling activities (ex ante risk assessment) include:**

- (1) Handling sensitive personal information;
- (2) Using personal information to make automated decision;
- (3) Entrusting personal information handling;
- (4) Providing personal information to other personal information handlers;
- (5) Disclosing personal information;
- (6) Providing personal information abroad;; and
- (7) Other personal information handling activities that have a significant impact on the rights and interests of individuals.

Regardless of whether it is a CIIO, an important data handler, or any other personal information handler, as long as it falls under the definition of "personal information handler" in the context of the PIPL, then, such enterprises or organizations may distinguish whether it shall conduct a DPIA/PIA based on the statutory circumstances described above.

At the same time, the PIPL also makes clear what contents within the DPIA/PIA **shall be included**:

- (1) Whether or not the personal information handling purpose, handling method, etc., are lawful, legitimate, and necessary;
- (2) The influence on individuals' rights and interests, and the security risks;
- (3) Whether protective measures undertaken are legal, effective, and suitable to the degree of risk.

In addition, the PIPL has also set specific retention periods for companies in terms of the requirements for corporate record-keeping systems through clear legal provisions, i.e., personal information handlers **shall keep records of personal information protection impact reports and handling for at least three years**.

## **II . Comparison of major overseas personal information or data protection laws**

## Comparison Of The Compliance Points Of Data Protection Laws In Ten Countries/Regions

### Part VI: Comparison of Data Impact Assessment (PIA/DPIA)

Country / Region	Category	Availability of assessment guidelines	Mandatory requirements	Whether assessment is recommended	Scenarios requiring assessment	Exceptions
China PIPL		Provides for a personal information protection protection impact assessment system	✓	✓	Assessments are required in the following scenarios: 1. Handling sensitive personal information; 2. Using personal information to make automated decision; 3. Commissioning of personal information processes; 4. Offerring of personal information to other handlers; 5. Disclosing of personal information; 6. Offerring of personal information to foreign countries; and 7. Other personal information handling activities that have a significant impact on the rights and interests of individuals.	N/A

EU GDPR	✓	✓	✓	<p>An evaluation is required in the following scenarios:</p> <ol style="list-style-type: none"> <li>1. systematic and comprehensive evaluation of personal factors related to natural persons, such evaluation being based on automated processing (including user profiling) and whose decisions have a legal or similarly significant impact on natural persons</li> <li>2. processing specific types of data as defined in Article 9(1) in a large-scale processing manner;</li> <li>3. processing personal data whose conviction is related to a violation of the law</li> </ol>	N/A
California, USA CCPA	✗	✗	CCPA does not recommend, mandate, or enforce DPIA	✗	✗
Brazil LGPD	✗	✗	No DPIA recommendations have been issued	<p>When the processing is based on its legitimate interests, the Brazilian Data Protection Agency may require the controller to conduct a DPIA and to observe commercial and industrial confidentiality.</p>	N/A
India PDPB (Draft)	Provides for a personal information protection protection impact assessment system	✓	No DPIA recommendations have been issued	<p>An assessment is required in the following scenarios.</p> <ol style="list-style-type: none"> <li>1. if the critical data trustee intends to perform any processing involving new technologies, large-scale analysis, use of sensitive personal data (e.g., genetic or biometric data), or any other processing with significant risk, a DPI must be performed prior to the processing.</li> <li>2. In addition, the DPA may specify mandatory situations or processing exercises.</li> </ol>	N/A

Korea PIPA	No DPIA guidelines have been issued, but the Korea Communications Commission has provided guidance on biometrics and biometric technology proposals	✓	No PIA recommendations have been issued	An assessment is required in the following scenarios: 1. when a situation arises where the personal information of a data subject may be violated by the application of standard personal information documents specified in a presidential decree, the head of a public agency is required to conduct a PIA. 2. when the personal information of a data subject may be breached as a result of processing activities, the agency or organization defined as a Korean public agency is required to conduct a PIA	✓
Japan APPI	✓	✓	✓	An assessment is required in the following scenarios: 1. when the administrative agency intends to keep a file of specific personal information 2. when important changes are to be made to specific personal information files	✓
Singapore PDPA	✓	✗	✓	An assessment is required in the following scenarios: 1. when the organization is relying on the individual's "Notification is considered as consent" for the collection of personal information; and 2. when personal data is collected, used or disclosed for the legitimate interests of the organization or others	N/A
Indonesia PDPA (Draft)	✗	✗	Current legislation does not require DPIA/PIA	N/A	N/A

Hong Kong, China PDPO	✓	✗	✓	The PDPC recommends that an assessment be made in the following circumstances: 1. the processing (either by the data user itself or by an agent designated by the data user) or creation of large amounts of personal data 2. the implementation of privacy-invasive technologies that may affect a large number of individuals; or 3. significant changes in organizational practices that may result in an expansion in the volume and scope of personal data collected, processed or shared.	N/A
Illustration Description:					
✓	The country/region has requirements in terms of DPIA/PIA				
✗	No clear regulations, or no corresponding guidelines have been issued				
N/A	Not applicable				

## Overall

When companies are involved in handling sensitive and important data, it is still very necessary to conduct DPIA as an essential internal compliance system. Even though DPIA/PIA cannot eliminate all data compliance risks for enterprises, it can help enterprises minimize the risks associated with data compliance to a greater extent, as well as help enterprises determine the corresponding data risk level and make a judgment on whether to accept such risks. From the perspective of GDPR, DPIA is one of the key manifestations to fulfill the accountability obligations of GDPR; from the perspective of the PIPL,

it is a mandatory requirement for enterprises to conduct prior risk assessment in some legal situations.

By implementing and better completing a DPIA, enterprises can not only reduce the occurrence of various potential data risks, but also help them to self-prove that they are in compliance with the provisions and requirements of the applicable data protection laws of the country/region where they do business, in addition, the enterprises can adopt effective compliance strategies and safeguards based on the results of the DPIA as well.

# **Comparison of Various Compliance Points of Data Protection Laws in Ten Countries/Regions | #7 Data Breach Notification Requirements**

Author: Jie (Jackie) WONG, Lawyer, Founder of W&W International Legal Team,  
Kinding Partners, specialising in cyber and internet practice

Date: September , 2021

## **Part VII: Data Breach Notification Requirements**

**This is the seventh part of the article, which focuses on the interpretation and comparison of data breach notification requirements in the event of a security incident of different data protection laws.**

Data breach is no trivial matter, it always happens inevitably in the process of daily business operation, and once the data breach and other different types of security events occur, it will cause varying degrees of harm and impact on data subjects. The causes of data breach are diverse and complex, such as system vulnerabilities of network operators, failure to update technical measures, intentional attacks by hackers, illegal operations or intentional leaks by internal managers, etc., which are difficult to eliminate and restraint completely. Therefore, data protection laws in different regions and countries

have established a "data breach notification system" in their legislation to strengthen the management of data breaches and effectively protect the rights and interests of data subjects by taking timely and effective measures and controlling the expansion of the scope of damage. The data breach notification refers to the obligation of the personal information controller and processor to notify and report the breach to different subjects in the event of a data breach.

## **I . Interpretation of the PIPL**

Articles 33 and 34 of the GDPR set out the requirements for data controllers to notify supervisory authorities and affected data subjects in the event of a data breach, making it mandatory that data controllers shall report data breaches to supervisory authorities within 72 hours of discovering the data breach, unless the data breach is unlikely to pose a risk to the rights and freedoms of natural persons. If the data breach is likely to lead a higher risk, the data controller shall also immediately notify the data subject of the data breach.

The PIPL, based on the reference to overseas data protection legislation, has also adopted specific legal requirements for data breach notification.

### **1. The circumstances that require enforcement of the data breach notification obligation is clarified.**

The PIPL requires personal information handlers to comply with data breach notification obligations in the event of or in the event of a potential (1) breach of personal information; (2) manipulation of personal information; and (3) loss of personal information.

From the current regulations, the situations that trigger a data breach notification are in two major types.

Firstly, whenever personal information is breached, regardless of whether it is sensitive personal information or general personal information, the data breach notification may need to be activated.

Secondly, specific scenarios that trigger the notification are clarified, which is including encountering information breach, manipulation, or loss. The PIPL does not specify the quantities of personal information that has been breached, and as the criterion for determining whether to initiate the data breach notification mechanism, it is clear that the PIPL does not rely on the "quantities" to determine whether the data breach notification should be triggered, but rather on whether the "information breach, manipulation, or loss" has occur or not, and whether such event is "harmful to the data subject".

## **2. The subject of fulfilling the data breach notification obligation is clarified.**

Similar to the GDPR, in the context of the PIPL, the obligation of data breach notification is imposed on "personal information handlers", which

means, companies, organizations and individuals who have the right and autonomy to determine the purpose and manner of data handling will be obliged to comply with the obligation of data breach notification.

### **3. Subject that needs to be notified of the data breach is specified.**

With reference to overseas experience in data legislation, the PIPL also classifies the subjects to be notified into two categories of subjects.

- (1) Data regulator: the department that performs personal information protection duties; and
- (2) The data subject itself: the individual.

However, instead of using the number and scale of data breach incidents as the basis for judging whether to notify the data regulator, as in the case of some overseas data laws, the PIPL clearly stipulates that whenever personal information breach, manipulation, or loss occurs or is likely to occur, the personal information handler shall notify the departments fulfilling personal information protection duties and responsibilities. In the view of the fact that China is still in a state of multi-headed supervision in the regulation of personal information, it is still expected that the coming judicial interpretations and policy guidelines will provide the data regulator more guidance on the requirements and scope of notification.

The PIPL also provides certain exemptions as to whether a data subject is required to be notified or not. If the personal information handler is able to take prompt and immediate measures to effectively prevent the harm caused by information breach, manipulation or loss, the personal information handler may not need to notify the data subject. However, it should be noted that the PIPL imposes strict conditions on the "opt-out" exemption, which requires both that the personal information handler "immediately" take measures and that such measures are "effective in avoiding" harm to the data subject.

Also, there is a restriction on the "opt-out" exemption, which means, if the department responsible for the protection of personal information believes that a data breach may cause harm, the corresponding data regulator has the right to require the handler of personal information to notify the individual.

#### **4. What should be included in the data breach notification is clarify.**

After confirming whether to initiate a data breach notification, it is also a key part of the notification system as to what specific content should be included in the notification. The PIPL has also made clear that the notice shall include:

- (1) The type/categories, of information where breach, manipulation or loss of personal information that occurred or might have occurred.

- (2) The causes for the leak, manipulation, or loss that occurred or might have occurred.
- (3) The possible harm caused by this event.
- (4) Remedial measures taken by personal information handlers.
- (5) Measures that the individuals can take to mitigate the harm.
- (6) Contact information for personal information handlers

#### **5. Time limit requirements for notification.**

The data protection laws in some of the much more developed regions clearly stipulate the form of notification, the time limit and the procedure for notification of data breach. At present, the PIPL in China does not have the requirement of "within 72 hours" or "within two working days" for the time limit of notification, but it indeed requires to take "immediate remedial measures" and to "notify the relevant subjects in a timely manner". The specific requirements on the form, time and procedure for data breach notification are required further clarification by the coming up judicial interpretations, guidelines and standards, which will provide more specific practical instructions to the companies with more specific practical instructions.

## **II . Comparison of major overseas personal information or data protection laws**



## Comparison Of The Compliance Points Of Data Protection Laws In Ten Countries/Regions

### Part VII: Comparison of Data Breach Notification Requirements

Country / Region	Category	Whether notification is required	Whether data regulators need to be notified	Whether data subjects need to be notified	Whether there are specific notification requirements	Time limits	Exemption
China PIPL		✓	✓	✓	1. the occurrence or potential occurrence of personal information breach, falsification, loss of information types, causes and possible harm caused 2. the remedial measures taken by the personal information handler and the measures the individual can take to mitigate the harm 3. the contact information of the personal information handler	No clear time requirement, but need to be immediate	1. where measures can effectively avoid harm caused by information breach, tampering or loss, the personal information handlers may not notify the individual. 2. However, if the data regulator believes that harm may be caused, it has the right to request the personal information processor to notify the individual.
EU GDPR		✓	Trigger conditions must be met	Trigger conditions must be met	The GDPR has specific requirements regarding the content and form of notifications, and the requirements for notifications to regulators will differ from those for data subjects.	Notification to the regulator must be "without undue delay and, where practicable, within 72 hours of becoming aware of the breach"	1. Notification to the regulator: Notification may be waived if the breach is "unlikely to pose a risk to the rights and freedoms of natural persons". 2. Notification to data subjects: Exemption from notification in cases where Article 34(3) of the GDPR is satisfied
California, USA CCPA		✓	✓	✓	✓	The most appropriate time to do so, without undue delay	✓
Brazil LGPD		✓	Notification is required when the data subject is exposed to a risk or related damage	Notification is required when the data subject is exposed to risk or related damage	✓	Defined by the Brazilian data regulatory, but notification is recommended within 2 business days	Not specified, but can be defined by the Brazilian data regulatory
India PDPB (Draft)		✓	Trigger conditions must be met	✗	✓	As early as possible and within a reasonable time	Information technology law distinguishes between matters that require mandatory reporting and those that can be reported optionally
Korea PIPA		✓	Trigger conditions must be met	✓	✓	PIPA requires notification to be "without delay", which is interpreted as within 5 days according to the KPPB's guidelines	N/A

Japan APPI	APPI itself does not provide any data breach notification requirements, but the data breach guidelines issued by the Japan Personal Information Data Council have corresponding requirements	✓	Notification is recommended	Different categories of personal information are distinguished, and the type, content, and requirements for notifying different types of personal information are different	There are no specific requirements for timing, but it is generally required that notification be made immediately or without delay	There are different exemptions for different types of personal information
Singapore PDPA	✓	✓ Trigger conditions must be met	✓ Trigger conditions must be met	The PDPA has specific requirements regarding the content and form of notifications, and the requirements for notifications to regulators may differ from those for notifications to data subjects	The PDPC must be notified as soon as possible, but in any event no later than 3 days after the date of the enterprise's assessment of the data breach	✓
Indonesia PDPA (Draft)	✓	There is no need to notify any government agency in the event of a data breach. However, if PDPA comes into force, personal data controllers will be required to notify in writing.	✓	✓	Notification of a data breach must be sent to the data subject within 14 days of the electronic system operator becoming aware of the breach.  Under the PDPA(Draft), notification of a data breach must be sent by the personal data controller within a specified period of time.	✗
Hong Kong, China PDPO	There is no explicit requirement for notification, but it is recommended that consideration be given to notifying affected data subjects and related parties	Depending on the severity of the data breach	Depending on the severity of the data breach	N/A	Notify as soon as practicable after discovery of a leak	N/A
Illustration Description:						
✓	There are corresponding requirements					
✗	No clear regulations, or no corresponding guidelines have been issued					
N/A	Not applicable					

## **Overall**

Data breach is one of the most important threats to network security, and it is necessary to build up an effective notification management system and to take remedial measures in the case of data breach. Countries are gradually adopting legislation to clarify the provisions of data breach notification, including the circumstances triggering the notification, the subject of fulfilling the obligation of the notification, the subject to be notified, the content of notification, the form and procedure of notification, the time requirement of notification and the penalty system for violating the data breach notification obligation, which such requirements have been stipulated much more specific and detailed. Therefore, the enterprises and organizations should pay great attention to how to implement and enforce the data breach notification requirements in order to avoid serious harmful results due to failure to fulfill the obligation of notification or inadequate fulfillment.

# **Comparison of Various Compliance Points of Data Protection Laws in Ten Countries/Regions | #8 Requirements For The Appointment Of A Data Protection Officer**

Author: Jie (Jackie) WONG, Lawyer, Founder of W&W International Legal Team, Kinding Partners, specialising in cyber and internet practice  
Date: September , 2021

## **Part VIII: Requirements For The Appointment Of A Data Protection Officer**

**This is the eighth part of the article, which focuses on the interpretation and comparison of the requirements for the appointment of a Data Protection Officer of different data protection laws.**

A Data Protection Officer ('DPO'), as a functional role explicitly required by the GDPR to assume responsibility for corporate data protection compliance, is primarily a designated professional who helps to comply with the applicable data protection laws. The GDPR specifies the circumstances and conditions under which a Data Protection Officer must be designated.

A related role is that of the EU Representative, which is essentially a representative appointed by an organization located outside the EU to fulfill obligations under the GDPR, where applicable. The two positions and roles are different and need to be distinguished.

Internally, the Data Protection Officer, as an important role in the organization's governance structure, is responsible for all kinds of compliance work related to personal information; externally, the Data Compliance Officer needs to assist in various matters related to personal information protection and is a stakeholder in the data protection responsibility framework.

## **I . Interpretation of the PIPL**

In the context of the PIPL, the personal information protection officer is a professional who is responsible for the overall coordination and implementation of the 'compliance work on personal information protection, and he is also directly responsible for the security of personal information, and the personal information protection officer is a role that requires supervision of personal information handling activities and the protection measures taken.

The PIPL stipulate the specific circumstances in which a personal information protection officer shall be designated. In conjunction with the *"Information security technology - Personal information security specification"*

(GB/T 35273 -2020), which came into effect on October 1, 2020, we will briefly analyze the provisions of personal information protection officer in the PIPL as follows:

### **1. Cases requiring the establishment of a personal information protection officer**

According to the PIPL, when the handling of personal information **reaches the quantity specified by the national cyberspace authority**, the handler of personal information **shall designate a personal information protection officer**.

As previously mentioned in the fourth article of this paper, regarding the definition of "personal information reaching the quantities prescribed by the national cyberspace authority", it can be referred to the " Measures on Network Security Censorship (Revised Draft for Comments)" enacted by the CAC in July, 2021, as well as the "Measures for Evaluating the Security of Transferring Personal Information and Important Data Overseas (Draft for Comments)" enacted by the CAC in 2017.

And in GB/T 35273-2020, there are also specific provisions on responding to the establishment of a personal information protection officer. According to the requirements in the GB/T 35273-2020, a **full-time** personal information

protection officer **and a personal information protection department shall be set up when an enterprise meets with one of the following conditions:**

- (1) The main business **involves** personal information handling, and the size of the workforce is **greater than 200 people;**
- (2) Handling personal information of **more than one million people**, or is estimated to process personal information of **more than one million people within a 12-month period;** or
- (3) Handling **sensitive personal information of more than 100,000** people.

## **2. The main responsibilities of the personal information protection officer**

The PIPL has expressed the main responsibilities of the personal information protection officer in a macro manner, that is, he/she is responsible for "supervising the activities of handling personal information and the protection measures taken, etc.", reflecting the desire **that the dynamic compliance actions of the personal information protection officer will promote the implementation and enforcement of the static personal information protection requirement and then provide continuous monitoring on it.**

**At the same time, there are clear legal requirements for the identity of the personal information protection officer:**

**(1) Public Identity.**

The contact information of the personal information protection officer shall be explicitly required to be **disclosed** by the personal information handler (commonly through the privacy policy, privacy statement clause, company official website, etc.); and

**(2) Report to regulatory authorities**

The personal information handler is explicitly required to report the name and contact information of the personal information protection officer to the department that performs personal information protection duties.

In GB/T 35273-2020, in addition to the duty of supervision, we also discover more specific requirements on the duties of the personal information protection officer, and adopt a broad expression of "including but not limited to", in order to better meet the subsequent development of personal information protection changes in legislation and enforcement. The main responsibilities of the personal information protection officer and personal information protection department are summarized as follows:

**(1) Coordination.**

Overall coordination of the implementation of the organization's internal personal information security work, taking direct responsibility for personal information security.

**(2) Plan development and implementation.**

Organizing the development of personal information protection work plan and supervising its implementation.

**(3) Policy and Structures Creation and Maintenance.**

Draft, issue, implement, and regularly update personal information protection policies and related procedures.

**(4) Permission Management.**

Establish, maintain and update a list of the personal information the organization handles (including the type, quantity, source, recipient of personal information) and the policy for access authorization.

**(5) DPIA.**

Conducting impact assessments of personal information security, proposing countermeasures for personal information protection, and supervising the rectification of security risks.

**(6) Training.**

Organizing training on personal information security.

**(7) Pre-testing.**

Testing products or services before the release of products or services to avoid unknown personal information collection, use, sharing and other handling activities.

**(8) Handling complaints.**

Publishing complaints, reporting methods and other information and timely receipt of complaints and reports.

**(9) Compliance Audit.**

Conducting security audits.

**(10) Supervision and Communication.**

Maintaining communication with supervision and management to inform or report on personal information protection and incident handling, etc.

**3. Requirements on the qualification and role positioning of the personal information protection officer**

There are no special provisions on the qualification requirements of the personal information protection officer in PIPL, however, in practice, only the professionals who are specializing in personal information protection, having a professional legal background, dealing with data security protection work with comprehensively understanding, are qualified to be as a personal information protection officer.

In GB/T 35273-2020, on the other hand, the personal protection officer and the personal information protection department are required in terms of qualification and role positioning.

**(1) Professional background requirements:**

Personnel with relevant management experience and expertise in personal information protection.

**(2) Reporting to management directly:**

Participate in important decisions regarding personal information handling activities, and report directly to the main person in charge of the organization.

**(3) Guaranteeing the independent performance of duties:**

Providing the personal protection officer with the necessary resources to guarantee their independence in performing their duties.

It should be noted that similar to the "EU representative" mentioned in the EU GDPR, there are similar provisions in the PIPL, which need to be distinguished from the role of "personal protection officer". According to the PIPL, for overseas personal information handlers to which the PIPL applies, a special organization shall be established in China or a representative shall be appointed in China to handle matters related to personal information protection. At the same time, such overseas personal information handlers are required to report the name and contact information about the specialized agency or the designated representative within the mainland of China to the

department that performs the personal information protection duties. For overseas personal information handlers that may fall under the jurisdiction of the PIPL, attention should be taken to prepare for the establishment of a domestic agency or designated representative in China and conducting the corresponding reporting work.

Designating and appointing a DPO is a strong guarantee for companies to do a good job of personal information compliance protection, and it is also an indispensable key part for companies to effectively implement a series of data protection systems.

From the perspective of personal information compliance, on the one hand, it is necessary to appoint a qualified personal information officer to help companies better comply with the requirements of personal information protection regulations; on the other hand, to improve the company's ability to reduce personal information risks by establishing a personal information protection department, for example, by establishing a data protection committee to coordinate the work of various departments in the protection of personal information and data security protection, and to provide timely and rapid feedback and response in the event of a security incident. At the same time, personal information handlers also need to pay attention to ensuring the independence and independence of DPO through a system to ensure that he or

she can perform his or her personal information protection duties independently and professionally and make comprehensive, accurate and reasonable decisions.

## **II . Comparison of major overseas personal information or data protection laws**

## Comparison Of The Compliance Points Of Data Protection Laws In Ten Countries/Regions

### Part VIII: Comparison of requirements for the appointment of Data Protection Officer

Country / Region	Category	Whether the appointment is required	Appointment scenarios or other exceptions	Whether professional qualifications are required	Whether data regulators need to be notified
China PIPL		Recommended for appointment, while, in the case of compliance with the provisions of the law is necessary to make the appointment	1. where the handling of personal information reaches the amount specified by the national network information department, the person responsible for the protection of personal information shall be appointed. 2. where the handling of personal information of children is involved, the network operator shall appoint a person responsible for the protection of personal information of children	✓	The name of the relevant organization or the name and contact information of the representative needs to be reported to the department that performs personal information protection duties
EU GDPR		✓	1. where data processing activities are carried out by public authorities or institutions (except for courts exercising jurisdictional functions) 2. where the core activities of data processing involve regular large-scale systematic monitoring of data subjects (including all forms of online tracking, analysis and forecasting, etc.) 3. where special categories of personal data (such as sensitive data on ethnicity, religion, political opinions, sexual orientation, etc.) or large-scale processing of personal data related to criminal offences.  If a data controller meets the criteria for mandatory designation, its processors are not necessarily required to designate a DPO.	✓	The data controller or data processor must notify the data supervisory authority of the contact details of the DPO
California, USA CCPA		The CCPA does not require the appointment of a DPO, but recommends having	N/A	N/A	N/A
Brazil LGPD		✓	N/A	N/A	N/A
India PDPB (Draft)		For processing sensitive personal data, companies must appoint a "grievance officer" to resolve complaints and disputes related to this matter	If the Indian data regulator determines that you are a "material data fiduciary", you must appoint a DPO and the DPO must be located in India	✓	✗

Korea PIPA	✓	N/A	Data controllers who are not public bodies must appoint the persons specified in PIPA as DPO, such as representatives of companies or heads of departments responsible for the processing of personal information	N/A
Japan APPI	According to APPI, there is no requirement to appoint a DPO, but industry guidelines recommend the appointment of a DPO	N/A	✓	N/A
Singapore PDPA	✓	N/A	✓	Not required to notify, but encouraged to notify
Indonesia PDPA (Draft)	The current law does not require the appointment of a DPO	However, according to the draft requirements, data controllers and data processors are obliged to appoint DPOs in certain cases where 1. the processing of personal data is performed by data controllers and/or data processors performing public services 2. the core activities of the data controller are of a nature, scope and/or purpose that requires regular and systematic monitoring of large-scale personal data; and 3. the core activities of the data controller include the processing of specific personal data and/or personal data related to criminal acts on a large scale.	✓	N/A
Hong Kong, China PDPO	There is no requirement to appoint a DPO under the PDPO, but there are recommendations for appointment in the guidelines	N/A	✓	✗
Illustration Description:				
✓	There are corresponding requirements			
✗	No clear regulations, or no corresponding guidelines have been issued			
N/A	Not applicable			

## **Overall**

In addition to the EU, an increasing number of countries/regions are adopting legislation requiring companies under their jurisdiction to establish a data protection officer. Although the names, functions, application and conditions is different, they are all designed to help and ensure the companies are able to comply with the provisions and requirements of the applicable data protection laws during the process of handling personal information and the relevant data.

# **Comparison of Various Compliance Points of Data Protection Laws in Ten Countries/Regions | #9 The main obligations of the personal information handler**

Author: Jie (Jackie) WONG, Lawyer, Founder of W&W International Legal Team, Kinding Partners, specialising in cyber and internet practice

Date: September , 2021

## **Part IX: The main obligations of the personal information handler**

**This is the ninth part of the article, which focuses on the interpretation and comparison of the main obligations of the personal information handler of different data protection laws.**

The main obligation of personal information handler, from the enterprise's point of view, can be briefly understood as the need for the organization to establish and develop various internal and external personal information protection and management structures, as well as the security and technical safeguards to better comply with the provisions of data protection laws when handling personal information, in accordance with the requirements of the

applicable data protection laws, which is a particularly important part of the data compliance work of each enterprise.

## **I . Interpretation of the PIPL**

### **1. Developing internal management systems and operating procedures**

The PIPL requires companies to establish internal structures and operating procedures for the protection and management of personal information. The system of personal information compliance can be large and complex, or small but complete.

Therefore, companies should combine their own business development, especially the specific situation of personal information handling activities involved in the process of business development, and embed the basic requirements of personal information protection into business processes in order to develop a set of internal management system suitable for the company's unique business scenarios, and further clarify and implement the personal information in the lifecycle through the implementation of feasible operational procedures, so as to achieve the purpose of effectively safeguarding personal information security through system and management.

### **2. Establishing a management system for grading and classifying personal information**

From the perspective of ensuring the security of personal information, the PIPL requires companies to manage personal information in a graded and classified manner, which is one of the technical solutions for companies to prevent and manage the risk of personal information security.

*Network Security Law* requires network operators to take measures such as data classification, important data backup and encryption; the *Data Security Law* also confirms that China achieves data protection by establishing a data classification and grading system.

Therefore, enterprises should develop a grade and classification catalog of personal information, technical standards of the collected personal information, and corresponding safety management measures for the collected personal information, by taking different business scenarios and the type of data into account.

### **3. Establishing data security system and adopt security technical measures**

From the perspective of technical security, the PIPL requires enterprises to take appropriate encryption, de-identification and other security technical measures. In the *GT 35273-2020*, it also requires enterprises to adopt requirements for security measures such as encryption when transmitting and

storing sensitive personal information; as well as a proposal to require enterprises to de-identify personal information immediately after collection.

Therefore, on the one hand, enterprises need to take different levels of encryption measures according to the type, sensitivity and other characteristics of the personal information they handle, especially when it comes to the handling of sensitive information, they should use password management technology that meets with the national standards; on the other hand, when it comes to the circumstance of displaying personal information through the interface, or other situations that require external transfer or disclosure, enterprises should take technical measures to de-identify and anonymize personal information according to the nature of personal information, so as to effectively reduce the risk of personal information breach. At the same time, enterprises should pay attention to the separate storage of different types of sensitive information, for example, enterprises are required to store information that can be used to restore the identification of individuals separately from the de-identified information; personal biometric information should be stored separately from personal identity information, etc.

#### **4. Establishing personal information authority management structures , safety education and training system**

In the process of personal information protection work of enterprises, how to effectively manage internal personnel, especially those who handle and access users' personal information in large quantities, is a very important part of compliance work. The PIPL requires companies to reasonably determine the operating authority of internal personnel for personal information handling by setting up a permission management system, and to provide regular safety education and personal information compliance training to employees.

Therefore, companies should establish a reasonable and effective personal information authority management system for the control of personal information, especially sensitive personal information (such as personal information access, viewing, modification, deletion, copying, destruction and other operational behaviors). Some examples are as following:

- (1) Determining the trigger conditions for authorized operations based on the necessity of the business procedure;
- (2) Establishing a minimum authorized access control policy for the personnel with authorized access to personal information (so that they can only access minimized personal information necessitated by their duties);
- (3) Setting up internal approval processes for important operations regarding personal information, such as copy and downloading;

- (4) Conducting background checks and sign confidentiality agreements for practitioners who have significant access to sensitive personal information; and
- (5) Conducting regular safety education and personal information compliance training for employees within the company, especially those involved in personal information handling positions, to help them to be familiar with the principles of handling personal information protection and the manner to handle users' personal information legally and compliantly.

**5. Developing and implement emergency response mechanisms for personal information security incidents**

The PIPL stipulates that the enterprises shall develop, organize and implement contingency plans for personal information security incidents, and after a security incident, enterprises shall take the following measures according to the contingency plans:

- (1) Keeping records of personal information security incidents.
- (2) Assessing the potential impact of a personal information security incident.

- (3) Taking timely, needful and effective measures to effectively control and stop the possible impact of personal information security incidents in a timely manner.
- (4) Reporting personal information security incidents to regulatory authorities in a timely manner according to the "*National Network Security Incident Emergency Response Plan*" and other relevant provisions.

In daily business operations, enterprises should also pay attention to personal information security incidents and emergency plans for rehearsal, to ensure that in the event of similar events can be timely response and treatment.

In addition, the PIPL stipulates that when a personal information breach occurs, companies shall fulfill their personal information breach notification and remediation obligations. For more information on this point, please refer to Part VII of this article.

## **6. Appointing of DPO**

For more information on this point, please refer to Part VIII of this article.

## **7. Conducting regular compliance audits**

The PIPL imposes a requirement to conduct regular compliance audits on personal information handling activities and compliance protection. Therefore, for the purpose of ensuring continuous compliance of personal information handling activities, companies should establish a regular compliance audit system and focus on effective compliance audits of personal information handling activities, personal information protection policies, management systems and operating procedures for personal information protection, technical security measures, and other components.

#### **8. Conducting ex ante risk assessment and establishing data impact assessment system**

For more information on this point, please refer to Part VI of this article.

#### **9. "Gatekeeper Rule"**

The PIPL imposes special compliance obligations on "important Internet companies that provide basic Internet platform services, have a large number of users, and have complex business operations". This is mainly because platform-based enterprises involved with many types of personal information handlers, and concerning the handling of a large number of users' personal information, therefore, the PIPL provides the legal obligation to such important Internet platform enterprises and regulates them to manage the products or

service providers within the platform. This is commonly known as the "gatekeeper rule".

Therefore, for head Internet platform enterprises involving the handling of a large amount of personal information of users, special attention should be paid to:

- (1) Establishing a complete compliance system and structure for personal information protection and set up an independent body to supervise the protection of personal information, and the independent body should be composed of external independent persons such as independent directors, external consultants, independent law firm professionals, and external experts.
- (2) In accordance with the principles of openness, fairness and justice, reasonable platform rules should be formulated to clarify the "standards of handling personal information" and "obligations to protect personal information" of the product or service providers in the platform. For example, service providers in the platform are required to have independent privacy policies and provide adequate security technology protection measures.
- (3) If a product or service provider in the platform is found to be in serious violation of laws and regulations to handle personal information, it

shall take necessary punitive measures and stop providing services to it.

- (4) Regularly publishing social responsibility reports on personal information protection and to accept social supervision.

#### **10. Other measures provided by laws and administrative regulations**

Finally, the PIPL adopts the miscellaneous clause to clarify to enterprises that they also need to comply with the provisions of other relevant laws and administrative regulations in addition to the PIPL, in order to cope with various new situations and requirements that may arise in the process of building a legal system for personal information compliance in the future.

### **II . Comparison of major overseas personal information or data protection laws**

Given the fact that in the data protection laws of different countries/regions, the legal obligations that personal information handlers need to comply with are very specific and detailed, and there may be special provisions for special cases or scenarios, and some countries/regions' data protection laws distinguish the roles, responsibilities and obligations of personal information from controllers and processors. Considering the complexity of this issue and the length of this article, we will only briefly list

some of the basic obligations that companies should pay attention to in the handling of personal information in comparison table below.

Comparison Of The Compliance Points Of Data Protection Laws In Ten Countries/Regions		
Part IX:The main obligations of the personal information handler		
Category Country / Region	Brief list of basic obligations (Need to analyze the business situation)	Compliance Points/Special Points/Remarks
China PIPL	1. management system and operating procedures 2. classification management 3. security technical measures such as encryption and de-identification 4. determination of authority and internal control mechanism 5. education and training 6. establishment of emergency response basis 7. determination of responsible organization and person in charge of personal information protection 8. compliance audit 9. ex ante risk assessment 10. gatekeeper rule	1. the basic system is proposed to build a personal information protection standard system, certification and marking system, risk assessment, de-identified processing and other basic systems. 2. organizations that meet certain conditions are required to establish a full-time personal information protection officer and a personal information protection work organization to be responsible for personal information security.

<b>EU GDPR</b>	<p>The main obligations imposed by the GDPR on controllers and processors of personal data are well established and can be used as a reference template for companies in their own compliance at home or abroad, mainly in:</p> <ol style="list-style-type: none"> <li>1. data processing notification obligations;</li> <li>2. recording data processing activities;</li> <li>3. conducting DPIA;</li> <li>4. appointing a DPO;</li> <li>5. implementing technical security measures</li> <li>6. data breach notification;</li> <li>7. special categories of personal data protection requirements;</li> <li>8. contractual requirements between controllers and processors, etc.</li> </ol>	<p>Particular attention is paid to the need to notify both the data regulator and the affected data subject of the data breach notification; and the need to consider the risks that may be posed by processing activities when taking security measures, and to set out specific security measures required.</p>
<b>California, USA CCPA</b>	<p>The CCPA's special obligations are, among other things, as follows (only partially listed):</p> <ol style="list-style-type: none"> <li>1. "Do not sell my personal information" link on the front page of the website</li> <li>2. not sell their personal information for at least 12 months after the consumer has requested not to sell it</li> <li>3. give consumer rights in the privacy policy or special CCPA page</li> <li>4. companies must implement reasonable security measures to detect fraudulent authentication activities and to prevent unauthorized access to or deletion of consumers' personal information</li> </ol>	<p>When a consumer requests that his /her personal information not be sold, use his/her personal information only for the purpose of satisfying that unsold demand</p>
<b>Brazil LGPD</b>	<p>The main obligations imposed by the LGPD on controllers and processors of personal information are relatively well-defined, mainly in terms of obligations to record data processing activities, implement technical and administrative security measures, notification obligations in the event of a data security incident, privacy protection impact assessment, appointment of a data protection officer, etc.</p>	<p>The processor of personal information is also responsible for damages caused by violations of the LGPD during the processing of data</p>
<b>India PDPB (Draft)</b>	<p>Special attention needs to be paid to the requirements set by the PDPB(Draft) on the obligations of data trustees, mainly in terms of providing a privacy policy (with specific requirements on the content of the privacy policy), documenting data processing activities, implementing security safeguards, reporting data breaches to regulatory authorities, and establishing a grievance mechanism.</p>	<p>When certain conditions or circumstances are met by the trustee of important data, corresponding responsibilities and obligations are attached, including, for example, conducting a data protection impact assessment, appointing a data protection officer, conducting annual data audits, etc.</p>

<b>Korea PIPA</b>	<p>The concept of data handler or personal information controller under Korean PIPA is similar to the concept of data controller under GDPR. The obligations of data processors under the Korean PIPA are also well established and strict, mainly in terms of recording data processing activities, implementing technical and administrative security measures, establishing a management system for personal information, maintaining access logs, notification obligations in the event of data security incidents, privacy protection impact assessment, appointment of data protection officers, protection requirements for children's data and other special categories of data, etc.</p>	<p>PIPA sets additional obligations for the processing of special categories of personal data (e.g., sensitive personal information, criminal records, etc.), such as the need to obtain the data subject's consent for the processing of specific identifying information or sensitive personal information, respectively.</p>
<b>Japan APPI</b>	<p>Japan APPI's obligations to information controllers are mainly reflected in the requirement for data controllers to control and supervise third parties (including data processors), including but not limited to: enforcing agreements between data controllers and service providers; providing security measures to service providers; and instructing and investigating service providers around data processing practices</p>	<p>Specific compliance points vary by processor status and scenario, requiring case-by-case analysis.</p>
<b>Singapore PDPA</b>	<p>The obligations of the Singapore PDPA to data controllers are reflected in the appointment of a data protection officer, the obligation to notify in the event of a data security incident, and the implementation of technical security measures.</p>	<p>Under the PDPA, organizations must appoint a Data Protection Officer to be responsible for and ensure that the organization is compliant with the PDPA in its personal information processing activities.</p>
<b>Indonesia PDPA (Draft)</b>	<p>The obligations required by Indonesia's PDPA(Draft) and laws and regulations related to the protection of personal information are numerous, mainly in terms of:</p> <ol style="list-style-type: none"> <li>1. maintaining the confidentiality of personal data collected, processed and analyzed by the company;</li> <li>2. implementing technical and administrative security measures to protect personal information and documents containing such information from theft or unlawful use;</li> <li>3. privacy protection impact assessment;</li> <li>4. notification in the event of a data security incident</li> <li>5. the use of personal information only in accordance with the needs of the user, etc</li> </ol>	<p>It is important to note that Indonesian Kominfo 20 imposes obligations on electronic system providers, such as certifying electronic systems managed by companies, ensuring that personal data stored in electronic systems is encrypted, etc.</p>

<p><b>Hong Kong, China PDPO</b></p>	<p>The Hong Kong PDPO advocates that organizations implement a privacy management program (PMP) to protect personal data as part of their corporate governance responsibilities, and the "Best Practice Guide" (PMP Guide) issued by the PCPD recommends that organizations protect personal information by providing an organizational commitment to personal information protection; by establishing Personal information protection system, effective control of personal information processing activities, and continuous evaluation and revision of personal information processing activities.</p>	<p>The PMP guidelines encourage organizations to appoint a Data Protection Officer to oversee their compliance with the PDPO and the implementation of the PMP.</p>
-------------------------------------	---	---

## Overall

The data protection laws of most countries/regions will provide relatively sufficient and comprehensive provisions on the basic legal obligations of personal information handlers, as well as provide corresponding special provisions according to their own special national conditions. For companies going abroad, a full understanding of the PIPL laws of the applicable countries regarding the basic obligations and responsibilities of personal information handlers is the key to mastering compliance points in personal information handling activities.