PILLAR LEGAL

Implementing China's Personal Information Protection Law

CHINA REGULATION WATCH[1]
January 12, 2022

By: Greg Pilarowski | Zhu Ziwei | Alexandra Ashbrook

1. Introduction

On August 20, 2021, the Standing Committee of the National People's Congress (全国人大常务委员会) (the "Standing Committee") issued the Personal Information Protection Law of the People's Republic of China (个人信息保护法) ("PIPL"), which became effective on November 1, 2021. The final version of PIPL followed two prior draft versions that the Standing Committee released for public comment on October 21, 2020, and April 30, 2021.

PIPL is the first comprehensive data privacy law of the People's Republic of China ("China"). The law materially alters the landscape of personal information protection legislation in China, and outlines the requirements for nearly every aspect of personal information processing activities. As noted in our previous China Regulation Watch,[2] PIPL, the Cyber Security Law,[3] and the Data Security Law[4] provide the current legislative foundation for China's data sector. A great deal of supporting regulations, rules, measures and guidelines have since been issued or are still on their way to supplement the current framework. We list many of such supporting documents for reference in Exhibit A below.

Although PIPL consolidates previously issued personal information protection rules into a single unified law, it does not designate a specific government authority to perform personal information protection duties. Instead, the Cyberspace Administration of China (网信办) ("CAC"), the Ministry of Industry and Information Technology (工业和信息化部) ("MIIT"), the Ministry of Public Security (公安部) ("MPS"), and the State Administration for Market Regulation (国家市场监督管理总局) ("SAMR") are expected to cooperate to carry out PIPL's regulatory duties.

[1] This China Regulation Watch is provided by Pillar Legal, P.C. (the "Firm") as a service to clients and other readers. The information contained in this publication should not be construed as legal advice, and use of this memorandum does not create an attorney - client relationship between the reader and the Firm. In addition, the information has not been updated since the date first set forth above and may be required to be updated or customized for particular facts and circumstances. This China Regulation Watch may be considered "Attorney Advertising" under applicable law. Questions regarding the matters discussed in this publication may be directed to the Firm at the following contact details: +1-925-930-3932 (San Francisco Bay Area office), +86-21-5876-0206 (Shanghai office), email: info@pillarlegalpc.com. Firm website: www.pillarlegalpc.com. © 2022 Pillar Legal, P.C.

[2] See "China's Evolving Personal Information Protection Rules".

[3] Cyber Security Law (网络安全法), issued by the Standing Committee of the National People's Congress (全国人大常务委员会) on November 7, 2016, and effective on June 1, 2017.

[4] Data Security Law (数据安全法), issued by the Standing Committee of the National People's Congress on June 10, 2021, and effective on September 1, 2021.

This article provides an overview of PIPL and select currently effective and draft regulations that support the implementation of PIPL. This article also provides various examples of how leading China technology companies are complying with aspects of PIPL, such as the separate consent requirements, and information on the status of various elements of PIPL that are not yet fully implemented, such as the cross-border data transfer requirements. We also provide an updated comparison table that compares the key provisions of PIPL with the European Union's General Data Protection Rules ("GDPR") and California Consumer Privacy Act ("CCPA") and California Privacy Rights Act ("CPRA", and together with CCPA, the "California Privacy Acts") in Exhibit B below.

2. Extraterritorial Effect

PIPL regulates personal information processing activities[5] conducted within the territory of China, in addition to processing activities outside China that relate to providing services to, or analyzing behaviors of, individuals located in China.[6] PIPL also requires personal information processors[7] outside of China to establish an institution or appoint an agent in China to handle personal information protection matters within the country.[8] Similar requirements can be found in GDPR, which requires data controllers or data processors who process or control data on a large scale[9] within the European Union to appoint a representative established in the European Union.[10]

3. Definition of Personal Information

PIPL defines personal information as any kind of information recorded electronically or in other forms that is related to an identified or identifiable natural person,[11] excluding information that has been anonymized.[12] In practice, it may be difficult to determine whether certain types of information should be regarded as personal information. The proposed Guidelines for Data Classification and Grading (数据分类分级指引)[13] issued in September 2021 provide some practical guidance on identifying personal information. The guidelines indicate that there are two approaches to identify personal information: (1) "from information to

[5] Personal information processing activities include the collection, storage, use, processing, transmission, provision, disclosure and deletion of personal information. See Article 4 of PIPL.

[6] See Article 3 of PIPL.

[7] A personal information processor under PIPL plays a similar role as data controller under GDPR. Pursuant to Article 73 of PIPL, personal information processor refers to any organization or individual that independently determines the purpose and method of processing activities.

[8] See Article 53 of PIPL.

[9] GDPR does not define "large scale", but various commentators argue that "large scale" refers to having over 10,000 records or user accounts.

[10] See Article 27 of GDPR.

[11] PIPL doesn't specify the meaning of identified or identifiable

[12] See Article 4 of PIPL.

[13] See Section 5 of Guidelines for Data Classification and Grading (数据分类分级指引) issued by the National Information Security Standardization Technical Committee (全国信息安全标准化技术委员会) for public comment in September 2021.

individual," and (2) "from individual to information."

Under the "from information to individual" approach, any information that can identify a specific natural person, independently or in combination with other information, should be regarded as personal information. Information such as name, national identity number, email address, mobile phone number, and bank account number can independently identify a specific natural person, and thus are classified as personal information. Similarly, information like gender, birth date, profession, marital status, and education background is also classified as personal information, because this information can be used in combination with other information to identify a specific natural person.[14] Under the "from individual to information" approach, a natural person's inherent characteristics such as nationality, personal biometric information, and any information generated during such natural person's activities such as personal location information, personal communication information, web browsing records is also classified as personal information.[15]

Anonymization vs. De-identification

Is "de-identified" or "pseudonymized"[16] personal information considered "anonymized" for purposes of a PIPL exemption? PIPL distinguishes de-identified information from fully anonymized information, and thus de-identified information is still subject to PIPL.[17] Under PIPL, properly anonymized information can no longer be restored to its original state and connected with a natural person; therefore anonymized personal information is no longer considered personal information. Conversely, de-identified personal information can still identify a specific individual with the help of additional information. Therefore, processing of personal information after de-identification is subject to all PIPL requirements.

Sensitive Personal Information

The Personal Information Security Specification (个人信息安全规范) first defined the term "sensitive personal information," and PIPL largely follows this previously established

[14] The "from information to individual" explanation appears to clarify the meaning of the "information related to an identifiable natural person" portion of the definition of personal information under PIPL. This prong of the PIPL definition is similar to the definition of an identifiable natural person under GDPR. Pursuant to Article 4(1) of GDPR, an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

[15] The "from individual to information" explanation appears to clarify the meaning of the "information related to an identified natural person" portion of the definition of personal information under PIPL.

[16] Pseudonymization under GDPR means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

[17] Pursuant to Article 73 of PIPL, "de-identification" refers to the process in which any personal information is processed to the extent that it cannot identify a specific natural person without the help of additional information; "anonymization" refers to the process in which any personal information is processed to the extent that it cannot identify a specific natural person and cannot be restored to its original state.

approach.[18] Under PIPL, sensitive personal information refers to personal information that, once leaked or illegally used, will easily lead to infringement of human dignity or harm to the personal safety or property of a natural person. The regulation further expressly identifies certain types of sensitive personal information, including biometric recognition, religious beliefs, specific identity, medical and health information, financial account information, personal location tracking and other information of a natural person, as well as any personal information of a minor under the age of 14 (a "Minor").

In addition to the general processing requirements as further discussed in Section 4 below, additional security measures and processes are required to collect or process sensitive personal information:

- The personal information processor must inform the individual of the necessity of processing sensitive personal information and the impact that the processing activities may exert on the individual's rights and interests;
- When processing the personal information of a Minor, the personal information processor must obtain a separate consent[19] from the individual or the guardian of the Minor before processing;
- The personal information processor must conduct a personal information protection impact assessment[20] before processing sensitive personal information;
- The personal information processor must establish a special privacy policy for processing personal information of Minors.

4. General Processing Principles and Requirements

When processing personal information under PIPL, a personal information processor must comply with a range of general principles and requirements, key select provisions of which are listed below. Failure to comply with such principles and requirements may result in liability under PIPL.

Lawful Basis

Under PIPL, a processor may lawfully process personal information with the explicit consent of the individual. Personal information also may lawfully be processed without obtaining prior consent under any of the following enumerated circumstances:

- Where it is necessary for the conclusion or performance of a contract to which the individual is a party;
- Where it is necessary for human resources management, and personal information is

[18] Information Security Technology – Personal Information Security Specification (信息安全技术 - 个人信息安全规范), issued by the National Standardization Administration and the State Administration for Market Regulation on March 6, 2020, and effective on October 1, 2020.

[19] Please find more information about separate consent in Section 4 below.

[20] Please find more information about personal information protection impact assessment in Section 4 below.

processed pursuant to a legally established employment policy, or a legally concluded collective contract;

- Where it is necessary for performance of a statutory duty or obligation;
- Where it is necessary for responding to a public health emergency, or for protecting the life, health or property of a natural person in case of an emergency;
- Where the personal information is processed within a reasonable scope for public interest purposes, such as for news reporting or for public opinion supervision; or
- Where the personal information, which has already been disclosed by the individual or otherwise legally disclosed, is processed within a reasonable scope.[21]

Separate Consent

To provide more protection for personal information rights, PIPL created a "separate consent" requirement, which if fully implemented will increase compliance burdens for personal information processors. A personal information processor is required to obtain separate consent from an individual before:

- Providing personal information to another personal information processor;[22]
- Processing sensitive personal information;[23]
- Providing personal information to an overseas recipient;[24]
- Publicly disclosing personal information;[25] or
- Using personal information collected from an image capturing device or personal identification device in a public place for a purpose other than maintaining public security.[26]

What constitutes a separate consent in practice is a hot topic that has been widely discussed in China. The plain meaning of the words suggests that a separate consent should be obtained in a different manner than a general click through consent for a privacy policy. This separate consent mechanism is designed to provide the individual with full and clear knowledge about how their personal information or sensitive personal information will be used in certain scenarios. Additionally, the separate consent mechanism would give the individual an opportunity to opt out of certain sensitive processing activities, prohibiting processors from obscuring these details in a long privacy policy and obtaining the necessary authorization through a general consent.

Several months after PIPL has become effective, however, China's leading internet companies have not yet adopted a separate consent mechanism. In our review of privacy policies

[21] See Article 13 of PIPL.
[22] See Article 23 of PIPL.
[23] See Article 29 of PIPL.
[24] See Article 39 of PIPL.
[25] See Article 25 of PIPL.
[26] See Article 26 of PIPL.

and new account creation processes for several commonly used applications in China,[27] the developer did not provide a specific notification or separate consent solicitation for the collection of sensitive personal information or for providing personal information to another personal information processor. Instead, the disclosure related to these matters is simply highlighted or bolded in the privacy policy. It is unclear if this practice complies with the requirements of PIPL.

Minimization Principle

The principle of "data minimization" was first introduced in China under the Cyber Security Law.[28] PIPL adopts this principle and restricts the personal information a processor may permissibly collect to the minimum scope necessary for achieving the purpose of the processing.[29] PIPL also expressly prohibits a personal information processor from refusing to provide services to individuals who do not give consent to processing personal information beyond what the processor requires to provide the services.[30] In other words, personal information processors are only allowed to collect personal information that is necessary for providing the functions or services associated with the processor's services or products. An individual must have the ability to reject any processing of their personal information outside of this minimum scope.

The phenomenon of excessive collection and processing of personal information has been a significant problem in China's mobile application marketplace. In the years preceding PIPL, several rounds of administrative actions were carried out to remove from various app stores a number of mobile applications that excessively collect and process personal information. Such administrative actions were undertaken in accordance with the Methods for Identifying Unlawful Acts of Apps to Collect and Use Personal Information (App 违法违规收集使用个人信息行为认定方法) issued jointly by CAC, MIIT, MPS and SAMR on November 28, 2019.[31]

Clear and Explicit Notice

Before processing personal information of an individual, a personal information processor must inform the individual of the processing activities in a conspicuous way, usually through a privacy policy. The notice must be in clear and easy-to-understand language, and must be truthful, accurate, and complete. A personal information processor's disclosure notice or privacy policy must be publicly available and easy to access and store. If a personal information

[27] We tested WeChat, Bilibili, Weibo, Taobao, NetEase Music, please find their respective privacy policy by clicking the hyperlink here.

[28] Pursuant to Article 41 of the Cyber Security Law, network operator shall not collect personal information irrelevant to their services.

[29] See Article 6 of PIPL.

[30] See Article 16 of PIPL.

[31] In the first three quarters of 2021, MIIT conducted 10 reviews, reported 1,494 illegal apps in total, and removed 408 apps that failed to comply with the data minimization principal. See "MIIT: 408 illegal apps off the shelves in the first three quarters (工信部: 前三季度下架 408 款违规 APP)" posted by Guangzhou Daily on October 19, 2021.

processor changes any processing activities, the personal information processor must first inform the individual users and obtain renewed consents.

Many privacy policies in China and elsewhere are now longer than ever. Personal information processors must explain technical matters in the privacy policy, which is not always easy to do in "easy-to-understand language." Various technology companies in China are updating their privacy policies, trying to find an appropriate balance between a clear policy and a detailed policy.[32]

On November 1, 2021, MIIT issued a notice about improving information and communication services (工业和信息化部关于开展信息通信服务感知提升行动的通知) (the "MIIT Notice"), which proposed additional requirements to optimize privacy policies, including:

- Establishing a list of personal information collected from individuals, which should include the type of information collected, along with the purpose and the scenario for processing such personal information;
- Establishing a list of third parties with whom personal information is shared, which should include the type of personal information shared, the purpose and the scenario for sharing such personal information, and the way by which such personal information is shared;
- Providing a summary of the privacy policy; and
- Providing a list of device permissions accessed by the personal information processor, such as photo album, address book and location, and informing users of the purpose for requesting such device permissions and the way to restrict or change such device permissions.

MIIT also released a list of companies, which include many of China's top tech companies such as Tencent, Alibaba, Baidu, NetEase, Bytedance and Ximalaya, that MIIT required to comply with the MIIT Notice by the end of year 2021. Our review of several updated privacy policies from these companies did indicate that they are more readable and user-friendly.[33]

On November 14, 2021, CAC issued the draft Administrative Regulations on Internet Data Security (网络数据安全管理条例) for public comments, which incorporated the privacy policy requirements from the MIIT Notice into official regulations.[34]

Retention Period

Personal information collected from individuals cannot be held indefinitely by the

[32] NetEase Music updated its privacy policy on August 25, 2021, and then again on November 3, 2021. Taobao updated its privacy policy on September 27, 2021, and then again on November 1, 2021.
[33] See the Weibo privacy policy updated on November 29, 2021, and the Ximalaya privacy policy updated on December 28, 2021.
[34] See Article 20 of the draft Administrative Regulations on Internet Data Security (网络数据安全管理条例).

personal information processor. PIPL requires personal information processors to retain personal information for the minimum period necessary for achieving the processing purpose (i.e., providing services or products to the individual) unless otherwise required by applicable law or regulation.[35]

There are several circumstances where personal information is required to be kept for a longer, predetermined period. For instance, the E-Commerce Law of China requires operators of e-commerce platforms to keep commodity and service information and transaction information for at least three years.[36]

Security Measures

Personal information processors must also take appropriate security measures to protect personal information from any unauthorized access, leakage, tampering or loss, including by:

- Implementing internal management and operational procedures;
- Managing personal information based on classification;
- Implementing appropriate technical security measures, like encryption and de-identification;
- Determining the authorization levels of employees that are involved in processing activities, and conducting security trainings for such employees on a regular basis; and
- Implementing emergency plans for personal information security incidents.[37]

Personal Information Protection Impact Assessment

A personal information protection impact assessment ("PIPIA") is a process designed to help identify, analyze and mitigate the risks associated with certain personal information processing activities. PIPL requires personal information processors to conduct a PIPIA before:

- Processing sensitive personal information;
- Using personal information in automated decision-making;
- Entrusting a third party to process personal information;
- Providing personal information to another personal information processor;
- Publicly disclosing personal information;
- Providing personal information to an overseas recipient; and
- Any other processing activity that will have a material impact on an individual's rights and interests.[38]

[35] See Article 19 of PIPL.

[36] See Article 31 of E-Commerce Law of the People's Republic of China, which was issued on August 31, 2018, and became effective on January 1, 2019.

[37] See Article 51 of PIPL.

[38] See Article 55 of PIPL.

A PIPIA shall cover the following topics:

- Whether the purpose, method or other aspects of the processing activities are lawful, legitimate and necessary;
- The impact and level of risk with respect to an individual's rights and interests; and
- Whether any security protection measure taken is lawful, effective and commensurate with the level of risk.[39]

Conducting a PIPIA is, however, still relatively new in China. Since PIPIA is similar to the data protection impact assessments ("DPIA") provided for under GDPR, many companies may look to practices in Europe when conducting their first PIPIA. In addition, the National Standardization Administration (国家标准化管理委员会) and SAMR issued Guidance for Personal Information Security Impact Assessment (个人信息安全影响评估指南) on November 19, 2020, which also serves as a helpful reference material when conducting a PIPIA.

5. Processing Activities Involving a Third Party

PIPL contemplates several situations where a third party is involved in processing activities: joint processing, entrusting a third party to process personal information, a change of the personal information processor due to a company restructuring, and providing personal information to another personal information processor.

Entrusted Party

When entrusting a third-party to process personal information, the "entrusted party" is not considered a personal information processor, because the entrusted party does not independently determine the purpose and method of processing activities.[40] The entrusted party must only process personal information within the purpose and method agreed by the personal information processor, and must process such personal information under the supervision of the personal information processor. The relationship between the personal information processor and the entrusted party under PIPL is similar to the relationship between a data controller and a data processor under GDPR.

Typically, the personal information processor and the entrusted party enter a data processing agreement to determine the processing purpose, method, service term, the type of personal information processed, the security measures employed, as well as the rights and obligations of both parties. In addition, the entrusted party is prohibited from subcontracting the agreed processing activities to any other party without the consent of personal information processor. When the data processing agreement terminates (or is cancelled or void), the entrusted

[39] See Article 56 of PIPL.

[40] Pursuant to Article 73 of PIPL, personal information processor refers to any organization or individual that independently determines the purpose and method of processing activities.

party must delete or return all the personal information to personal information processor.[41]

Given the limited processing authorities that an entrusted party has, the obligations of the entrusted party under PIPL are also quite limited. Pursuant to Article 59 of PIPL, the entrusted party mainly handles the security measures taken for the processing activities and assists the personal information processor in ensuring compliance with the obligations of PIPL.

Another Personal Information Processor

In certain situations, a personal information processor may share personal information with another personal information processor. PIPL addresses the concepts of joint processing, a change of personal information processor, and provision of personal information to another personal information processor.

Joint processing means two or more personal information processors jointly determine the purpose and method of processing activities. Joint personal information processors must agree on their respective rights and obligations for the processing activities. Joint personal information processors are jointly and severally liable for any violation of PIPL, and individuals are entitled to exercise their rights under PIPL with respect to and against each of the joint personal information processors.[42]

The successor of a prior personal information processor due to a company restructuring, such as a merger, division, dissolution, or bankruptcy, must inform individuals of the successor's name and contact information. The successor must follow the processing purpose and method of the prior personal information processor. If the successor seeks to change the purpose or method, the successor first must obtain a new consent from individuals.[43]

Providing personal information to another personal information processor is slightly more complicated than the prior two situations. It not only requires the disclosure of the new personal information processor's processing activities, but also requires the first processor to obtain a separate consent from the individual. In addition, the first processor must conduct a PIPIA before providing personal information to the other processor.[44]

6. Cross-Border Provision of Personal Information

Under PIPL, the cross-border provision of personal information is subject to evolving requirements that are more strict than those provided for under GDPR. Under PIPL, the cross-

[41] See Article 21 of PIPL.
[42] See Article 20 of PIPL.
[43] See Article 22 of PIPL.
[44] See Article 23 of PIPL.

border provision of personal information includes sharing or transferring personal information to an overseas recipient, as well as entrusting an overseas recipient to process personal information.[45]

Before providing personal information to an overseas recipient, a personal information processor must:

- Pass a security assessment conducted by CAC;
- Obtain a personal information protection certification from a professional agency pursuant to regulations provided by CAC; or
- Enter into a standard contract with the overseas recipient in the form stipulated by CAC, which specifies the rights and obligations of both parties.[46]

For critical information infrastructure operators,[47] or personal information processors whose processing of personal information reaches the threshold amount designated by CAC,[48] a CAC security assessment is compulsory.[49] However, none of the three approaches are available yet for personal information processors that provide personal information to overseas recipients. The CAC security assessment process and the professional agency certification mechanism are not yet established, and the CAC form standard contract has not yet been published. On October 29, 2021, however, CAC issued draft Measures for Security Assessment for Cross-border Data Transfer (数据出境安全评估办法) for public comments, which essentially align with the previously released draft Measures for Security Assessment for Cross-border Data Transfer of Personal Information (个人信息出境安全评估办法)[50] (discussed in our prior China Regulation

[45] In the context of processing activities involving third parties within the territory of China, PIPL distinguishes between entrusting a third party to process personal information and the provision (share, transfer) of personal information to a third party. In the context of cross-border provision of personal information, however, PIPL has been interpreted to refer to both entrusting an overseas third party to process personal information and the provision (share, transfer) of personal information to an overseas third party who may independently decide the purpose and method of processing activities.
A frequent question is whether accessing personal information from overseas is regarded as cross-border provision of personal information. We believe that China's data privacy authorities would regard this situation as the cross-border provision of personal information, since the cross-border rules are designed to prevent personal information from being shared with overseas recipients that are beyond the reach of China's regulators. Therefore, as long as such access of personal information may result in infringement of individual's personal information rights and interests, the cross-border rules should apply.

[46] See Article 38 of PIPL

[47] Critical information infrastructure ("CII") refers to the key network facilities and information systems in important industries, which may seriously endanger the national security, national economy, people's livelihood and public welfare once they are subject to any destruction, loss of function or data leakage. Such industries include public telecommunication and information services, energy, transport, water conservancy, finance, public service, e-government and science and technology industries for national defense. See Article 2 of Regulations on the Security Protection of Critical Information Infrastructure (关键信息基础设施安全保护条例) issued by the State Council on July 30, 2021, and effective on September 1, 2021.

[48] The threshold ***might*** refer to (i) personal information processors who process personal information of more than one million individuals, or (ii) personal information processors who accumulatively provide personal information of more than 100,000 individuals to overseas recipients, or (iii) personal information processors who accumulatively provide sensitive personal information of more than 10,000 individuals to overseas recipients, pursuant to Article 4 of the proposed Measures for the Security Assessment for Cross-Border Data Transfer of Personal Information (数据出境安全评估办法（征求意见稿）) issued by CAC on October 29, 2021.

[49] See Article 40 of PIPL.

[50] The draft Measures for Security Assessment for Cross-border Data Transfer of Personal Information (个人信息出境安全评估办法) was issued by CAC for public comments on June 13, 2019. The current Measures for Security Assessment for Cross-border Data Transfer (数据出境安全评估办法) is its substitute.

Watch)[51] with respect to the general procedures for security assessments, the security assessment report requirements, the cross-border data agreement requirements and the assessment criteria to be considered by CAC.

Similar to when a processor provides personal information to another personal information processor within China, when a processor provides personal information to an overseas recipient, the processor must disclose the details of any overseas recipient's processing activities, obtain the individual's separate consent, and conduct a PIPIA.[52]

7. Individuals' Personal Information Rights

PIPL provides for a variety of personal information rights, which are similar in many respects to the rights of a data subjects provided for under GDPR.

Right to Know, Decide, Restrict or Deny

Individuals have the right to request that a personal information processor explain the personal information processing rules.[53] Subject to the minimization principle, individuals also have the right to deny or restrict processing activities based on the functions of services and products provided by a personal information processor.[54]

Right to Access or Copy

Individuals have the right to access or make copies of their personal information. If an individual requests the transfer of their personal information to another personal information processor, the current personal information processor should provide assistance.[55]

Right to Correct or Complete

If the personal information collected is incorrect or incomplete, individuals can request a personal information processor to correct the personal information, to complete personal information, or provide a way for individuals to correct or complete the personal information.[56]

Right to Delete

Individuals have the right to request a personal information processor delete all the

[51] See Section 8 of "China's Evolving Personal Information Protection Rules".
[52] See Article 39 and 55 of PIPL.
[53] See Article 48 of PIPL.
[54] See Article 16 and 44 of PIPL.
[55] See Article 45 of PIPL.
[56] See Article 46 of PIPL.

personal information relating to the individual in the personal information processor's possession. However, in the event that such personal information is required to be retained for a longer period pursuant to applicable law or regulation, a personal information processor should not conduct any processing activities on such personal information other than storage and implementation of security necessary measures.[57]

Right to Withdraw Consent

An individual can withdraw a consent previously given in connection with using a processor's products, services, or certain functions of the products or services, when the individual no longer use such products, services or functions. The personal information processor may not process an individual's personal information after consent is withdrawn; however, the processing activities already undertaken will not be affected.[58]

Response Period

When an individual requests to exercise his or her personal information rights, the personal information processor must respond within 15 business days,[59] which is shorter than the 30 days required under GDPR. If a personal information processor fails to timely respond to an individual's request, the individual may bring a lawsuit against such personal information processor for infringing his or her personal information rights.

Enabling individuals to exercise their personal information rights is one of the most important obligations of a personal information processor. Many recently updated China-based privacy policies provide detailed instructions of the ways and methods for individuals to exercise their personal information rights. Moreover, the mechanisms for exercising personal information rights are increasingly simple and easy to use.[60]

8. Remedies and Legal Liabilities

Under PIPL, there are two primary approaches to remedy a personal information processor's violation of the law. One is the civil lawsuit approach, mentioned in Section 7 (Individual's Personal Information Rights) above, which essentially treats personal information rights similarly to privacy rights under China's Civil Code.[61] The other remedy is the administrative approach enumerated by PIPL, pursuant to which any organization or individual

[57] See Article 47 of PIPL.
[58] See Article 15 of PIPL.
[59] See Section 6 of the Methods for Identifying Unlawful Acts of Apps to Collect and Use Personal Information (App 违法违规收集使用个人信息行为认定方法) issued jointly by CAC, MIIT, MPS and SAMR on November 28, 2019.
[60] See Section 4 of privacy policy of Taobao.
[61] See Article 1037 of the Civil Code, issued by the National People's Congress on May 28, 2020, and effective on January 1, 2021.

can file a complaint or report against any illegal processing activity with the authority that performs personal information protection duties.[62]

The legal liabilities under PIPL are quite severe. Fines imposed on a personal information processor can be up to fifty million Renminbi or five percent of an organization's annual revenue. For an individual, fines for noncompliance may be up to one million Renminbi. However, as most PIPL requirements are still new, and the authorities have yet to promulgate the means by which some rules will be implemented, it is likely that the authorities will initially require processors to rectify noncompliant practices or temporarily suspend services rather than immediately imposing severe fines.[63]

[62] See Article 65 of PIPL.

[63] See "MIIT Circular: Rectification Required Within the Time Limit (工信部通报：限期整改)" posted at Sina.com on November 5, 2021.

EXHIBIT A

CHINA DATA RULES

	Laws and Regulations	Issue Department	Issuance Date (YYYY-MM-DD)	Effective Date (YYYY-MM-DD)	Level of Authority
1.	Cyber Security Law (网络安全法)	The Standing Committee	2016-11-7	2017-6-1	Law
2.	Data Security Law (数据安全法)	The Standing Committee	2021-6-10	2021-9-1	Law
3.	Personal Information Protection Law (个人信息保护法)	The Standing Committee	2021-8-21	2021-11-1	Law
4.	Regulations on Security Protection of Critical Information Infrastructure (关键信息基础设施安全保护条例)	The State Council (国务院)	2021-7-30	2021-9-1	Administrative Regulations
5.	Provisions on the Online Protection of Children's Personal Information (儿童个人信息网络保护规定)	CAC	2019-8-22	2019-10-1	Department Regulations[64]
6.	Measures for Cybersecurity Review (网络安全审查办法)	CAC, the Ministry of State Security (国家安全部), and other government authorities[65]	2021-12-28	2022-2-15	Department Regulations
7.	Several Provisions on Vehicle Data Security Management (for Trial Implementation) (汽车数据安全管理若干规定（试行）)	CAC, NDRC, MIIT, MPS, the Ministry of Transport (交通部)	2021-8-16	2021-10-1	Department Regulations
8.	Provisions on Administration of Algorithm Recommendation of Internet Information Services (互联网信息服务算法推荐管理规	CAC	2021-12-31	2022-3-1	Department Regulations

[64] Department regulations (部门规章) are rules issued by national level government departments. Department regulations are binding, but with a lower legal effect than laws.

[65] Other government authorities include the National Development and Reform Commission (国家发展和改革委员会), the Ministry of Industry and Information Technology (工业和信息化部), the Ministry of Public Security (公安部), the Ministry of Finance (财政部), the Ministry of Commerce (商务部), the People's Bank of China (中国人民银行), the State Administration for Market Regulation (国家市场监督管理总局), the National Radio and Television Administration (国家广播电视总局), the National Administration of State Secrets Protection (国家保密局) and the State Cryptography Administration (国家密码管理局).

	定)				
9.	Regulations on Administration of Internet Data Security (网络数据安全管理条例)	CAC	2021-11-14	Draft	Department Regulations
10.	Measures for the Security Assessment for Cross-Border Data Transfer of Personal Information (数据出境安全评估办法)	CAC	2021-10-29	Draft	Department Regulations
11.	Methods for Identifying Unlawful Acts of Apps to Collect and Use Personal Information (App 违法违规收集使用个人信息行为认定方法)	CAC (网信办), MIIT (工信部), Ministry of Public Security (公安部), State Administration for Market Regulation (国家市场监督管理总局)	2019-11-28	2019-11-28	Normative Document[66]
12.	Information Security Technology – Personal Information Security Specification (信息安全技术 - 个人信息安全规范)	National Standardization Administration (国家标准化管理委员会), State Administration for Market Regulation (国家市场监督管理总局)	2020-3-6	2020-10-1	National Standard[67]
13.	Information Security Technology – Basic Specification for Collecting Personal Information in Mobile Internet Applications (信息安全技术 - 移动互联网应用程序 (App) 收集个人信息基本规范)	National Standardization Administration (国家标准化管理委员会), State Administration for Market Regulation (国家市场监督管理总局)	2020-1-15	Draft	National Standard
14.	Information Security Technology – Self Assessment Instruction for Personal Information Collection and Use of Mobile Internet Application (信息安全技术-移动互联网应用程序收集使用个人信息自评估指南)	National Information Security Standardization Technical Committee (全国信息安全标准化技术委员会)	2020-7	2020-7	National Standard
15.	Network Security Standard Practice Guide - Guidelines for Data Classification and Grading (网络安全标准实践指南 – 数据分类分级指引)	National Information Security Standardization Technical Committee (全国信息安全标准化技术委员会)	2021-9	Draft	National Standard

[66] Normative documents (规范性文件) can be issued by government departments at various levels. These documents are binding, but with lower legal authority than department regulations.
[67] National standards are not binding rules, but they do provide practical instructions.

EXHIBIT B

COMPARISON TABLE: CHINA EUROPE AND CALIFORNIA

	China	**Europe**	**California**[68]
Protects	Personal information rights and interests of any “**natural person**”.	“**Data subjects**” who are in the European Union that can be identified by reference to an identifier such as a name, an identification number, location data, online identifiers, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.	“**Consumers**” who are California residents that are either: • In California for other than a temporary or transitory purpose; or • Domiciled in California but currently outside the state for a temporary or transitory purpose. **"Households”**, i.e., a group, however identified, of consumers who cohabitate with one another at the same residential address and share use of common device(s) or service(s).
	PIPL Article 2	**GDPR** Article 3	**Cal. Civ. Code** § 1798.140(i) **Cal. Civ. Code** § 1798.140(q) **11 C.C.R.** § 999.301(k)
Regulates	“**Personal information processors**” that: • Process personal information in China; or • Process personal information of any natural person located in China **from overseas**, with the purpose of (i) providing product or	“**Controllers**” located both inside and outside of the European Union who are natural or legal people, public authorities, agencies, or bodies which determines the purpose and means	“**Businesses**” that: • Have annual gross revenues in excess of US$25,000,000; • Annually buy, sell, or share the information of 100,000 or more consumers or households; or

[68] This column of the Comparison Table represents the California Privacy Acts, including the 2018 Act as amended by the 2020 Act.

	service to natural person located in China; or (ii) analyzing the behavior of natural person located in China. **"Activities of processing personal information"** including the collection, storage, use, processing, transmission, provision, disclosure, and deletion of personal information.	of processing of personal data of data subjects. "**Processors**" located both inside and outside of the European Union who are natural or legal people, public authorities, agencies, or bodies which process personal data of data subjects on behalf of a controller.	• Derive 50% or more of annual revenues from selling or sharing consumers' personal information.
	PIPL Article 3 **PIPL** Article 4	**GDPR** Article 24 **GDPR** Article 28	**Cal Civ. Code** § 1798.140(d)
Types of Data	"**Personal information**" meaning any kind of information related to an identified or identifiable natural person as electronically or otherwise recorded, excluding information that has been anonymized. "**Anonymization**" refers to the process in which any personal information is processed to the extent that it cannot identify a specific natural person and cannot be restored to its original state. "**Sensitive personal information**" refers to personal information that, once leaked or illegally used, will easily lead to infringement of personality rights or harm personal or property safety of a natural person, including biometric recognition,	"**Personal data**" that relates to an identified or identifiable data subject. "**Pseudonymized data**" that is processed in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information when the business also: • Keeps any additional information separately; and • Implements technical and organizational measures to ensure personal data is not attributed to an identified	"**Personal information**" that identifies, relates to, describes, or is capable of being linked to or associated with a particular consumer or household. Non-exhaustive examples include: • Commercial information • Internet or electronic network activity information • Audio, electronic, visual, thermal, olfactory, or similar information • Professional or employment-related information • Education information • Inferences drawn from information "**Deidentified**" information refers to information that cannot reasonably be

	religious belief, specific identity, medical and health, financial account, personal location tracking and other information of a natural person, as well as any personal information of a minor under the age of 14.	or identifiable data subject. "**Special categories of data**" revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, 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.	used to infer information about, or otherwise be linked to, a particular consumer. "**Sensitive personal information**", a subcategory of personal information that includes but is not limited to: • Identifiers such as name, postal address, online identifier, IP address, email address, social security number, and other similar identifiers • Characteristics of protected classifications under California or federal law • Biometric information • Precise geolocation
	PIPL Article 4 **PIPL** Article 73 **PIPL** Article 28	**GDPR** Article 3 **GDPR** Article 9	**Cal. Civ. Code** § 1798.140(o) **Cal. Civ. Code** § 1798.140(m) **Cal. Civ. Code** § 1798.140(ae)
Required Notices	Prior to processing activities, personal information processors must inform the individual of: • The processor's name and contact information; • The processing purpose, method, information type, retention period; and	Controllers must **provide information** to the data subject, in situations where personal data is collected from the data subject or a third-party.	"**Privacy policy**" made available to consumers describing the business' practices regarding the collection, use, disclosure, and sale of personal information, and the rights of consumers regarding their own personal information. "**Notice at collection**" given by a business to a consumer at or before the point at

	- The procedure of exercise individual's rights under PIPL. Any change to the above-mentioned matters must be conveyed to the individual. Prior to the **processing sensitive personal information**, processors must also inform the individual of the **necessity** and the **impact on the individual's rights and interests.**		which the business collects personal information. "**Notice of right to opt-out**" given by a business informing consumers of their right to opt-out of the **sale or sharing** of their personal information and/or sensitive personal information, including in an interactive form accessible via a clear and conspicuous link titled "**Do Not Sell or Share My Personal Information**" on the business's website or mobile application. "**Notice of right to limit use and disclosure of sensitive personal information**" given by a business informing consumers of their right to limit the use and disclosure of sensitive personal information, including in an interactive form accessible via a clear and conspicuous link titled "**Limit the use of My Sensitive Personal Information**" on the business's website or mobile application. **"Notice of financial incentive"** given by a business explaining each financial incentive or price or service difference related to providing personal information.
			11 C.C.R. §§ 999.308 **11 C.C.R.** §§ 999.305

	PIPL Article 17 **PIPL** Article 30	**GDPR** Articles 13 – 14	**11 C.C.R.** §§ 999.306 **11 C.C.R.** §§ 999.307 **Cal. Civ. Code** § 1798.120 **Cal. Civ. Code** § 1798.121
Minors	Processing of personal information of **minors below 14 years of age** must be consented to by the minor's parent or guardian. Personal information processors must establish **special rules** for processing personal information of minors under the age of 14.	Processing of personal data of **minors below 16 years of age** must be consented to by the minor's parent or guardian.	Businesses with personal information of **minors under 13 years of age** must establish, document, and comply with a reasonable method for determining and receiving affirmative authorization from the minor's parent or guardian to opt-in to the sale or sharing of their personal information. Businesses with personal information of **minors at least 13 and less than 16 years of age** shall establish, document, and comply with a reasonable process for allowing such minors to opt-in to the sale or sharing of their personal information.
	PIPL Article 31	**GDPR** Article 8	**11 C.C.R.** §§ 999.330 **11 C.C.R.** §§ 999.331 – 999.332
Third Parties	When **providing** personal information **to another personal information processor**, the first personal information processors shall: • Provide the individual with detailed information of the receiving party and the processing activities involved; • Obtain specific consent from the individual; and	Once personal data is **transferred or shared**, the receiving party will become a data controller, and therefore will be required to comply with all the requirements applicable to a controller under GDPR. "**Engaging a processor to process**" data on behalf of a	**Third party contracts** that involve **selling, sharing, or disclosing personal information** are required to include terms and provisions compliant with procedure under the Privacy Acts. Required contract terms must include provisions that: • State that the business sells or discloses the personal information only for limited and specified purposes;

	- Conduct a personal information protection impact assessment. When **engaging a third party** to process personal information, personal information processors shall: - Reach an agreement with the third party on the purpose, period, and method of the processing, the type of personal information to be processed, any protection measure to be taken, and the rights and obligations of both parties, and - Supervise third party's processing activities.	controller must be governed by a data processing agreement between the controller and the processor, which sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. The obligations of a processor that must be set forth in a data processing agreement include: - Process the personal data on instructions from the controller; - Ensure that persons authorized to process the personal data are under an appropriate statutory obligation of confidentiality; - Take all measures required for data security; - Assist the controller to respond to requests for exercising the data subject's rights; and - Delete or returning all the personal data to the controller after the processing service ends.	- Obligate the third party to comply with California's Privacy Acts and require them to provide the same level of privacy protection the Privacy Acts require; - Grant the business rights to take reasonable and appropriate steps to help ensure that the third party uses the personal information in a manner consistent with California's Privacy Acts; - Require the third party notify the business if it determines that it can no longer meet its privacy obligations; and - Grant the business the right to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information.
	PIPL Article 23 **PIPL** Article 55 **PIPL** Article 21	**GDPR** Article 28	**Cal. Civ. Code** § 1798.100(d)

Cross-Border Transfers	Before providing personal information **to an overseas recipient**, a personal information processor must fulfill at least one of the following conditions: • Pass the security assessment conducted by Cyberspace Administration of China ("CAC"); • Undertake personal information protection certification conducted by professional agencies; • Sign a contract with the overseas recipients in accordance with the standard contract provided by CAC. Additionally, personal information processors shall: • Provide individuals with detailed information of the overseas recipient, the processing activities involved, and the procedure of exercising individual's rights under PIPL; • Obtain specific consent from the individual; and • Conduct a personal information protection impact assessment. Personal information processors whose processing of personal information reaches the **threshold amount** prescribed	In cases of transfer of personal data **within the EU**, the GDPR does not impose any additional requirements. In the case of transfer of personal data **outside of the EU**, the GDPR requires the recipient's country to be covered by an **adequacy decision** by the EU commission or the transfer to be subject to **appropriate safeguards**. If a controller or processer is established outside the EU, they shall designate a representative established in the EU for the purpose of ensuring compliance with GDPR.	No prohibitions on cross-border transfers of personal information.

	by CAC, must pass the **security assessment** conducted by CAC before providing personal information to an overseas recipient. An overseas personal information processor who **provides a product or service** to a natural person located in China or **analyzes the behavior** of natural person located in China, shall: • Establish a special agency or appoint a representative in China to be responsible for personal information protection-related affairs; and • Submit the name and contact information of its agency or representative to relevant government authorities.		
	PIPL Article 38 **PIPL** Article 39 **PIPL** Article 55 **PIPL** Article 40 **PIPL** Article 53	**GDPR** Article 44 **GDPR** Article 45 **GDPR** Article 46 **GDPR** Article 27	
Automated Decision Making and Profiling	For push-based information and business marketing provided to individual based on automated decision-making technology, personal information processors must provide the individuals with:	Data subjects have the right to not be **subject to a decision based solely on automated processing**, including profiling, which produces legal or other significant effects.	California consumers will be able to **opt-out of automated decision-making technology**, and to access the logic involved in the decision-making process and a description of the process's likely outcome.

	• An **option** not targeting the personal characteristics of the individual; or • An **easy way to refuse** to receive such information generated by automated decision-making. No unreasonable **differential treatment** of individuals in terms of **transaction prices** or other **transaction terms** should be implemented when using automated decision-making technology.		
	PIPL Article 24	**GDPR** Article 22(1)	**Cal. Civ. Code** § 1798.185(a)(16)
Right(s) to…	**China**	**Europe**	**California**
Know	The right to receive detailed information of the personal information processor, the processing activities, the procedure for the individual to exercise rights under PIPL, and any change to the processing rules. The right to know any provision of personal information to a **third party** or an **overseas recipient**.	The right to **receive detailed information** about a Controller's data collection and protection activities, including the legal basis for processing, and how to exercise data rights under the GDPR. The right to know what data is **shared with third parties.**	The right to know **what personal information is sold and shared** and to whom.
	PIPL Article 17 **PIPL** Article 23 **PIPL** Article 39	**GDPR** Article 13 **GDPR** Article 14	**Cal. Civ. Code** § 1798.115
	The **right to access** or **make copies** of their personal information.	The "**right of access**" to obtain confirmation from the controller	The right to **access personal information** and to know what personal information is

Access		as to whether the data subject’s personal data is being processed, as well as the data subject’s right to obtain access to the personal data in a readable format.	being collected or has been collected about the consumer or household and to whom the personal information has been disclosed.
	PIPL Article 45	**GDPR** Article 15	**Cal. Civ. Code** § 1798.110
Correct	The **right to request** personal information processors to **correct or complete** their personal information.	The “**right to rectification**” by the data subject to obtain from the controller the rectification of inaccurate personal data.	The right to **correction** of personal information that is not accurate.
	PIPL Article 46	**GDPR** Article 16	**Cal. Civ. Code** § 1798.106(a)
Delete	The **right to request** personal information processors to **delete** personal information by withdrawing consent.	The “**right of erasure**” to obtain from the controller the erasure of personal data concerning the data subject without delay, subject to certain conditions.	The right to **request to delete** personal information about the consumer or household that the business has collected from the consumer.
	PIPL Article 47	**GDPR** Article 17	**Cal. Civ. Code** § 1798.105
Restrict Processing	The **right to restrict or deny** personal information processors from the processing of their personal information.	The “**right to restrict processing**” of personal data so that the controller can only continue to process the data subject’s personal data with the data subject’s consent, subject to certain conditions. The “**right to object**” by the data subject to particular types of processing.	In accordance with the ability to limit the use and disclosure of sensitive personal information (see above), the right to restrict **sensitive personal information** to only the purpose for which the consumer disclosed the information.

	PIPL Article 44	**GDPR** Article 19 **GDPR** Article 21	**Cal. Civ. Code** § 1798.135(2)
Data Portability	Personal information processors must provide a way to transfer personal information to another personal information processor as designated by the individual.	The "**right to data portability**" whereby the data subject may request to transmit the data subject's personal data provided to a controller to another controller without hindrance.	Businesses must disclose and deliver information to a consumer free of charge within 45 days of receiving a verifiable consumer request from the consumer in a **readily useable format** that allows the consumer to transmit the information **from one entity to another entity without hindrance**.
	PIPL Article 45	**GDPR** Article 20	**Cal. Civ. Code** § 1798.130(a)(2)
No Retaliation/ Against Discrimination	Personal information processors **cannot refuse to provide service** to individuals that do not consent to the processing of their personal information, unless such personal information is necessary for providing the service.	Data subjects must be **protected from discriminatory consequences** derived from the processing of their personal data.	Businesses **cannot discriminate** against consumers for exercising their privacy rights under California law.
	PIPL Article 16	**GDPR** Article 5 **GDPR** Article 22	**Cal. Civ. Code** § 1798.125(a)(1)
Complain	The right to **file a complaint or report** about any illegal activity of processing of personal information **with an authority performing personal information protection duties**.	The "**right to lodge a complaint with a supervisory authority**" by the data subject	Implied right to lodge a **sworn complaint** with the CPP Agency.
	PIPL Article 65	**GDPR** Article 77	**Cal. Civ. Code** § 1798.199.45
Request Verification	No specific request verification procedures.	No specific request verification procedures. Controllers must use all reasonable measures to verify the identity of a data subject who requests access.	Businesses must establish, document, and comply with, a reasonable method for verifying that the person making a request is the consumer about whom the business has collected information.

		GDPR Recital 64	**11 C.C.R.** §999.323
	China	**Europe**	**California**
Internal Requirements	Personal information processors shall conduct "**compliance reviews**" for their processing activities on a regular basis. Personal information processors shall conduct a **"personal information protection impact assessment"** when: - Processing sensitive personal information; - Using personal information in automated decision-making; - Providing or disclosing of personal information to third party; or - Providing personal information to overseas recipient. Personal information protection impact assessment reports and relevant processing records shall be **retained for at least 3 years**. Personal information processor whose processing of personal information **reaches the threshold amount** prescribed by CAC shall appoint a **"personal information protection officer",** and such officer's name and contact information shall be disclosed to the	Controllers must maintain records of all processing activities under their responsibility. Processors must maintain a record of all categories of processing activities carried out on behalf of a controller. Controllers and processors must conduct a **"data protection impact assessment"** where a type of processing uses new technologies and is likely to result in a high risk to data subjects. Controllers and processors must appoint a "**data protection officer**" in cases where: - The processing is carried out by a public authority or body; - The core activities of the controller or processor consist of processing operations which require regular and systematic monitoring of data subjects on a large scale; or	All businesses handling personal information must: - Inform individuals responsible for handling consumer inquiries about the requirements under California's Privacy Acts and how to direct consumers to exercise their rights; and - Maintain records of consumer requests made pursuant to California's Privacy Acts and how the business responded for at least 24 months. A business whose processing of consumers' personal information presents a significant risk to consumers' privacy or security must conduct a **cybersecurity audit** and submit a **risk assessment** to the CPP Agency with respect to their processing of the personal information. A business that reasonably should know that it buys, receives for commercial purposes, sells, or shares for commercial purposes the personal information of 10,000,000 or more consumers in a calendar year must:

	public and submitted to the authorities in charge of personal information protection. If a network operator collects or processes the data of minors below the age of 14, it must appoint a **“specific person”** in charge of the minors’ personal information protection.	- The core activities of the controller or processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offenses.	- Compile metrics for the previous calendar year as listed in 11 C.C.R. § 999.317(g)(1); - Disclose such metrics by July 1 of every calendar year; and - Establish, document, and comply with a training policy for all individuals responsible for handling consumer requests and privacy law compliance.
	PIPL Article 54 **PIPL** Article 55 **PIPL** Article 56 **PIPL** Article 52 **Minor Personal Information Protection Provisions** Article 8	**GDPR** Article 30 **GDPR** Article 35 **GDPR** Article 37	**11 C.C.R.** § 999.317 **Cal. Civ. Code** 1798.185(15)
Security Requirements	Network operators shall take **technical measures and other necessary measures** to ensure the security of personal information collected and to prevent information leakage, damage, and loss. Personal information processor shall implement the following measures where appropriate to ensure the security of personal information: - Making plans for internal administration and operation; - Classifying personal information; - Taking appropriate technical security measures such as encryption and de-identification;	Controllers and processors must implement **appropriate technical and organizational measures** to ensure a level of security appropriate to risk, including as appropriate: - Pseudonymization and encryption of personal data; - The ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services; - The ability to restore the availability and access to personal data in a timely manner in the event of a	Businesses must implement **reasonable security procedures and practices** appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure.

	• Determining authority of employees in charge, and training employees on a regular basis; and • Making emergency plans for personal information security incidents.	physical or technical accident; and • A process for regularly testing the effectiveness of technical and organizational measures for ensuring processing security. Controllers and processors may demonstrate compliance with security requirements by adhering to an **approved code of conduct** or an **approved certification mechanism.**	
	Cyber Security Law Article 42 **PIPL** Article 51	**GDPR** Article 32 **GDPR** Article 40 **GDPR** Article 42	**Cal. Civ. Code** §1798.100(e) **Cal. Civ. Code** § 1798.150
Data Breaches	For any leakage of, tampering with, or loss of personal information that occurs or may occur, a personal information processor shall take timely remedial measures, and notify the authorities in charge of personal information protection and any individual concerned.	Controllers and processors must notify the supervisory authority. When the data breach is likely to result in a high risk to the rights and freedoms of the data subject, the controller must communicate information about the breach to the data subjects.	A business must notify any California resident whose unencrypted and unredacted personal information was acquired by an unauthorized person. Any entity required to issue a security breach notification to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification to the Attorney General. **Cal. Civ. Code** § 1798.29(a), (e)

	PIPL Article 57	**GDPR** Articles 33 – 34	**Cal. Civ. Code** § 1798.82(a), (f)
Valuing Data	PIPL does not require the calculation of personal data values.	The GDPR does not require controllers or processors to calculate the value of personal data.	Businesses offering financial incentives or price or service differences in exchange for the sale or sharing of consumer personal information must use and document a reasonable and good faith method for calculating the value of the consumer's data.
			Cal. Civ. Code § 1798.125 **11 C.C.R.** § 999.337
Legal Liability	Violators will be ordered to **make a correction**, given a **warning**, ordered to **suspend or terminate** its services, and any illegal gains shall be **confiscated**, for a violation of PIPL. If the required correction is not made, a **fine** of up to **RMB1,000,000** will be imposed on the violator; and a fine between **RMB10,000 and RMB100,000** will be imposed on the person in charger or directly liable for the violation. If the violation is of a grave nature: • The violator will be ordered to make correction, confiscated of illegal gains, and fined up to **RMB 50,000,000 or 5% of last year's annual revenue**; and may also be ordered to **suspend any related**	Infringement of GDPR that causes material or non-material damage to a data subject entitles the data subject to compensation for the damages suffered from the controller and/or processor. Supervisory authorities may also impose **administrative fines** dependent upon the circumstances of each individual case. Fines for lesser violations are subject to fines up to **10,000, 000 EUR** or up to **2% of total worldwide annual turnover** for the preceding financial year, whichever is higher.	A consumer whose nonencrypted and nonredacted personal information, or whose email address in combination with a password or security question and answer, is subject to a data breach may institute civil action to recover damages between **US$100 and US$750** per consumer per incident, or **actual damages**, whichever is greater. Any entity that violates California's Privacy Acts is subject to an injunction and liable for **a civil penalty** of not more than **US$2,500** for each violation and **US$7,500** for each intentional violation and each violation involving the personal information of minors.

	business for rectification, or have its business permit or business license cancelled; and • Its person in charge or directly liable for the violation will be fined between **RMB100,000 and RMB1,000,000**, and also be **banned** for a certain period from serving as a director, supervisor, senior officer or personal information protection officer of certain enterprises. Any violation under PIPL will be recorded into **credit files** and **disclosed to the public**. Where any damages are caused due to an infringement of personal information rights and interests, the personal information processor **shall bear tort liability**.	Fines for larger violations may reach as high as **20,000,000 EUR** or up to **4% of total worldwide annual turnover** for the preceding financial year, whichever is higher.	
	PIPL Article 66 **PIPL** Article 67 **PIPL** Article 69	**GDPR** Article 82 **GDPR** Article 83	**Cal. Civ. Code** §1798.150 **Cal. Civ. Code** § 1798.155