PRC Personal Information Protection Law (PIPL)

Introduction

Adopted on 20 Aug, effective from 1 Nov 2021

1st comprehensive law in the personal information protection area

Resemblance to GDPR

8 chapters, 74 articles

- Chapter I General Provisions
- Chapter II personal information processing rules
- Section I General Provisions
- Section II rules for handling sensitive personal information
- Section III special provisions on the handling of personal information by state organs
- Chapter III rules for cross-border provision of personal information
- Chapter IV rights of individuals in personal information processing activities
- Chapter V obligations of personal information processors
- Chapter VI departments performing personal information protection duties
- Chapter VII Legal Liability
- Chapter VIII supplementary provisions

Term	PIPL	GDPR	PISS (Personal Information Security Specification)
Personal information	Personal information refers to all kinds of information related to identified or identifiable natural persons recorded electronically or otherwise, excluding the information after anonymization.	Personal data: any information relating to an identified or identifiable natural person	Personal information: all kinds of information recorded electronically or in other ways that can identify the identity of a specific natural person or reflect the activities of a specific natural person alone or in combination with other information.The information obtained after anonymization of personal information does not belong to personal information.
Sensitive personal information	Sensitive personal information refers to personal information that, once leaked or illegally used, is likely to infringe the human dignity of natural persons or endanger the personal and property safety, including biometrics, religious beliefs, specific identity, medical health, financial accounts, whereabouts and other information, as well as the personal information of minors under the age of 14.	Special categories of personal data: personal 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	Personal sensitive information includes ID number, personal biometric information, bank account, communication records and contents, property information, credit information, whereabouts, accommodation information, health physiological information, transaction information, personal information of children under 14 years old, etc.
Controller	Personal information processor refers to an organization or individual that independently determines the purpose and mode of processing in personal information processing activities.	Controller: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data	Personal information controller: an organization or individual capable of determining the purpose and method of personal information processing.
Processor	no definition	Processor: a natural or legal person, public authority, agency or other body which processes personal data on	no definition

Territorial scope

PIPL

•Processing personal information of natural persons in China

Any of the following circumstances occurs in the processing of personal information of natural persons in China outside China:

（1） For the purpose of providing products or services to domestic natural persons;

（2） Analyze and evaluate the behavior of natural persons in China;

（3） Other circumstances stipulated by laws and administrative regulations.

Set up special agencies or designated representatives in China and submit them to relevant departments

GDPR

Establishment:

the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not

Targeting:

the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union

Principles relating to processing of personal information

Principle	PIPL	GDPR
Lawfulness, fairness and transparency	✓	✓
Purpose limitation	✓ Directly related	✓ Not incompatible
Data minimisation	✓	✓
Accuracy	✓	✓
Storage limitation	✓	✓
Integrity and confidentiality	✓	✓
Accountability	✓	✓

Basis	PIPL	GDPR	PISS
Consent	✓	✓	✓
Contract	It is necessary to conclude and perform the contract to which the individual is a party, or to implement human resources management in accordance with the labor rules and regulations formulated according to law and the collective contract signed according to law	processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract	Necessary for signing and performing the contract according to the requirements of the personal information subject
Legal obligation	✓	✓	✓
Vital interest	It is necessary to deal with public health emergencies or protect the life, health and property safety of natural persons in emergenciesDirectly related	processing is necessary in order to protect the vital interests of the data subject or of another natural person	For the purpose of safeguarding the life, property and other major legitimate rights and interests of the personal information subject or other individuals, but it is difficult to obtain my authorization and consent
Public interest	Necessary for responding to public health emergencies or protecting the life, health and property safety of natural persons in emergencies;Implement news reporting, public opinion supervision and other acts for the public interest, and process personal information within a reasonable range	processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller	Directly related to public safety, public health and major public interests
Legitimate interest	/	processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child	/
Other	To handle, within a reasonable scope, the personal information disclosed by individuals themselves or other legally disclosed personal information in accordance with the provisions of this law;Other circumstances stipulated by laws and administrative regulations.	/	

Right	PIPL	GDPR
Right to information and access	✓	✓
Right to rectification	✓	✓
Right to erasure	（1） The purpose of processing has been achieved, cannot be achieved, or is no longer necessary to achieve the purpose of processing; （2） The personal information processor stops providing products or services, or the retention period has expired;（3） Withdrawal of consent by an individual;（4） The personal information processor handles personal information in violation of laws, administrative regulations or agreements;（5） Other circumstances stipulated by laws and administrative regulations.	(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); (d) the personal data have been unlawfully processed; (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).
Right to restriction of processing	✓	(a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data; (b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; (c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; (d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.
Right to data portability	If an individual requests to transfer his personal information to his designated personal information processor, which meets the conditions stipulated by the national network information department, the personal information processor shall provide a way of transfer.	(a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and (b) the processing is carried out by automated means.
Right to object	✓	The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions.

Cross-border transfer

PIPL

- Through the security assessment organized by the National Network Information Department
- Personal information protection certification by professional institutions in accordance with the provisions of the national network information department
- Enter into a contract with the overseas receiver according to the standard contract formulated by the national network information department

GDPR

- Adequacy decision
- Appropriate safeguards:
  - BCR, SCC, approved code of conduct, approved certification mechanism
- Derogations

Localisation

- Ciio and personal information processing reach the specified amount
- Personal information collected and generated in China is stored in China
- Cross border transfer shall be subject to the security assessment organized by the network information department

Obligations of personal information processor

Internal management system and operating procedures	Personal information classification management	Encryption, de identification and other technical measures	Authority control, regular education and training
Emergency plan for personal information security incidents	Processing personal information up to the specified amount: person in charge of personal information protection	Regular compliance audit	Data disclosure notification

Personal information protection impact assessment

PIPL (PIPIA)

- Handling sensitive personal information;
- Use personal information for automatic decision-making;
- Entrust to process personal information, provide personal information to c information processors, and disclose personal information;
- Providing personal information abroad;
- Other personal information processing activities that have a significant im personal rights and interests.

- Whether the purpose and method of handling are legal, legitimate and necessary;Impact on personal rights and interests and safety risks;Whether the protective measures are legal, effective and appropriate to the degree of risk.The evaluation report and handling records shall be kept for at least 3 years

GDPR (DPIA)

- a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
- processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10;
- a systematic monitoring of a publicly accessible area on a large scale

Thank you!