

Compliance Checklist for China's Personal Information Protection Law

Are you on track for compliance with the Personal Information Protection Law of China?

The long-expected and widely concerned Personal Information Protection Law of China (the "PIPL") was adopted on 20 August 2021 by the Standing Committee of National People's Congress. This landmark data protection regulation will come into effect on November 1, 2021. As a basic law for personal information protection in China, the PIPL clarifies the rules for processing personal information, the obligations of personal information handlers, and the rights of personal information subjects. Notably, the PIPL provides serious punishment for violations of this law, which includes a fine of up to CNY 50 million (approx. USD 7.7 million) or 5% of annual turnover of the previous year.

How can multinational companies prepare for compliance at this stage? We have listed the following the PIPL Checklist to help companies grasp the important points and understand what they are suggested to do next to adapt to these rules more smoothly.

YOUR CHINESE CONTACT



Ken Dai
Partner
Shanghai, China
D +86 139 1611 3437
jianmin.dai@dentons.cn
dentons.com/en/jianmin-dai



Jet Deng
Partner
Beijing, China
D +86 135 2133 7332
zhisong.deng@dentons.cn
dentons.com/en/zhisong-deng

The challenges brought in by the PIPL are wide-reaching and a number of functions within many organizations will be affected by the changes, from marketing to security and, of course, legal and compliance. This checklist also aims to identify, below, the stakeholders which will need to be involved in each set of actions.

- Legal & Compliance
- Procurement
- IT & Information Security
- HR
- Marketing and Customer Relations
- PR & Comms

Category	Action(s) / Deliverable(s)	Article of PIPL
1. Application Scope and Extraterritorial Reach		
(1) Application Scope and Extraterritorial Reach 	Assess whether your organization is processing any personal information in mainland China. <i>Note: “personal information” under the PIPL refers to any kind of information related to an identified or identifiable natural person as electronically or otherwise recorded, excluding information that has been anonymized.</i> <i>Note: “processing” includes activities such as collection, storage, use, processing, transmission, provision, disclosure, and deletion of personal information.</i>	4
	Assess whether your organization is conducting any below activities carried out outside the territory of China but involving processing personal information of individuals located within China: 1. where the purpose of the activity is to provide a product or service to individuals within China; or 2. where the purpose of the activity is to analyze or assess the behavior of individuals within China.	3

2. General Rules for Processing Personal Information

(2) Lawful Basis 	The implementation of personal information processing should have a lawful basis, for example, 1. having obtained the consent from the individual; 2. it is necessary for the conclusion or performance of a contract to which the individual is a contracting party, or it is necessary for carrying out human resources management under an employment policy legally established or a collective contract legally concluded; 3. it is necessary for performing a statutory responsibility or statutory obligation; 4. it is necessary for responding to a public health emergency, or for protecting the life, health or property safety of a natural person in the case of an emergency; 5. the personal information is processed within a reasonable scope to carry out any news reporting, supervision by public opinions or any other activity for public interest purposes; 6. process the personal information, which has already been disclosed by the individual or otherwise legally disclosed, within a reasonable scope.	13
(3) Consent 	Consent should be based on the individual's willing and explicit intent with full information of the processing.	14
	In the event of any change of the purpose or method of processing or the type of personal information to be processed, the consent shall be obtained again.	14
	Provide a convenient method to withdraw consent.	15
	Do not refuse to provide a product or service to individuals on the grounds that they do not consent to processing their personal information or they withdraw their consent unless the processing of personal information is necessary for providing the product or service.	16

(4) Privacy Notice 	Use clear and easily understood language.	17
	Include the name or personal name and contact method of the personal information handler;	17
	Introduce the purpose of personal information processing and the processing methods, the categories of handled personal information, and the retention period;	17
	Provide information on the method and procedure for individuals to make rights requests;	17
	Notify Individuals about any changes of the notice.	17
(5) Provision to Third-party (Data Sharing) 	Notify individuals about the name or personal name of the data recipient, its contact information, the processing purpose and method, and personal information categories.	23
	Separate consent from the individual shall be obtained.	23
	If your organization needs to transfer personal information of any individual due to a merger, division, dissolution or declared bankruptcy, the individual shall be informed of the organizational or personal name and contact information of the receiving party.	22
(6) Automated Decision-making 	Guarantee the transparency of the decision-making and the fairness and justice of the processing result. <i>Note: “Automated decision-making” refers to the use of computer programs to automatically analyze or assess individual behaviors and habits, interests and hobbies, or situations relating to finance, health, or credit status, etc., and engage in decision-making activities.</i>	24
	Do not engage in unreasonable differential treatment of individuals in trading conditions such as trade price, etc.	24
	Provide the option to NOT target an individual’s characteristics or provide the individual with a convenient method to opt-out when using automated decision-making for notifications or commercial marketing.	24
	Provide an opt-out channel if individuals demand to refuse decisions solely made through automated process when the use of automated decision-making produces decisions with a material influence on the rights and interests of the individual.	24

(7) CCTV and Facial Recognition Technology 	Ensure that the installation of image collection or personal identity recognition equipment (e.g. CCTV) in public venues shall be as required to safeguard public security and observe relevant laws.	26
	Set up clear signs of such equipment.	
	Only use the collected personal images and identity recognition data for the purpose of safeguarding public security and not for other purpose except for based on individuals' separate consent.	26
3. Processing Sensitive Personal Information		
(8) Scope of Sensitive Personal Information 	Assess whether your organization is processing any sensitive personal information in China. Note: "sensitive personal information" means personal information that, once leaked or illegally used, may easily cause harm to the dignity of natural persons grave harm to personal or property security, including information on biometric characteristics, religious beliefs, specially-designated status, medical health, financial accounts, individual location tracking, etc., as well as the personal information of minors under the age of 14.	28
(9) Processing Requirements 	Have a specific purpose and sufficient necessity for processing sensitive personal information and take strict protection measures.	28
	Obtain the individual's SEPARATE CONSENT if no other lawful basis can be relied.	29
	Conduct a personal information protection impact assessment (" PIPIA ") in advance and make records.	55
(10) Children's Data 	Assess whether any personal information of minors under the age of 14 is processed.	31
	Obtain the consent of the parent or other guardian of the minor.	31
	Establish specialized personal information processing rules (e.g., Privacy Notice for Minors).	31

4. Data Governance: Personnel

(11) Appointment of “Data Protection Officer” (DPO) 	Appoint personal information protection officers, who is responsible for conducting supervision of personal information processing activities and protection measures, etc.	52
	Disclose the contact of the personal information protection officer (e.g., in the Privacy Notice).	52
	Report the name and contact of the officer to the authority.	52
(12) Appointment of Representative 	For personal information handlers subject to extraterritorial reach of the PIPL, they should establish a dedicated entity or appoint a representative within the borders of China to be responsible for matters related to the personal information you process. Note: “Personal information handler” refers to organizations and individuals that, in personal information processing activities, autonomously determine processing purposes.	53
	Report the name of the relevant entity or the name and contact of the representative to the authority.	53

5. Operation Security

(13) Technical Measures 	Adopt technical measures to ensure the security of personal information processing such as encryption and de-identification.	51
	Prevent unauthorized access as well as data breach, distortion, or loss.	51
(14) Data Retention 	Retain personal information for the shortest period necessary to realize the purpose of the personal information processing.	19
(15) Education and Training 	Conduct education and training on personal information security for employees on a regular basis (e.g., through an online training portal).	51

(16) PIPIA 	Conduct a personal information protection impact assessment (“PIPIA”) in advance and make records of data processing under the following circumstances: 1. processing sensitive personal information; 2. using personal information for automated decision-making; 3. entrusting others to process personal information, providing other handlers with personal information and publicly disclosed personal information; 4. transferring personal information overseas; and 5. conducting other personal information processing activities that have a significant impact on individuals’ rights.	55
	The PIPIA shall cover three main aspects: 1. whether the purpose, manner and other aspects of processing personal information are legitimate, proper and necessary; 2. the impact on individuals’ right and the risk level; and 3. whether the security measures adopted are legitimate, effective and appropriate to the risk level.	56
	The PIPIA reports and processing records shall be retained for at least 3 years.	56
6. Cross-border Transfer		
(17) General Requirements (Notice, Consent and PIPIA) 	Notify the individual about the data importer’s name, contact method, processing purpose, processing methods, and personal information categories, as well as ways or procedures for individuals to exercise the rights.	39
	Obtain the individual’s SEPARATE CONSENT if no other lawful basis can be relied.	
	Conduct a PIPIA in advance, and record the processing situation.	55

(18) Additional Requirements 	In addition to the above general requirements, at least one of the following conditions shall also be met: 1. passing a security assessment organized (only applicable to critical information infrastructure operators (CII) and handlers processing personal information reaching a certain quantity threshold.); 2. undergoing personal information protection certification; or 3. concluding a contract with the data importer in accordance with a standard contract formulated by the state cyberspace administration.	38
	Adopt necessary measures to ensure that the data importer's processing activities reach the standard of personal information protection provided in PIPL.	38
(19) Restrictions on Data Transfer to Foreign Authorities 	Do not provide personal information stored within China to foreign judicial or law enforcement agencies without the approval of the competent Chinese authorities.	41
7. Data Subject Rights and Procedures		
(20) Rights 	Ensure individuals have the following rights: 1. the right to be informed; 2. the right to decision; 3. the right to restriction and objection; 4. the right to access and copy; 5. the right to rectification; 6. the right to deletion; 7. the right to data portability; 8. the right to refuse automated decision-making.	44-49
(21) Response Procedures 	Establish convenient mechanisms to deal with requests from individuals to exercise their rights.	50
	Provide explanation if it is needed to reject individuals' rights request.	

8. Compliant Contracting and Procurement

(22) Engaging a Vendor



Sign a data processing agreement or contractual terms with the entrusted processor to agree on the purpose, period, and method of the contracted processing, the type of personal information to be processed, any protection measure to be taken, and the rights and obligations of both parties, etc.;

Supervise the activities of processing of personal information carried out by the entrusted processor (such as through data compliance audit); and

Conduct a PIPIA in advance and record the processing situation.

21

55

(23) Obligations of vendors



Vendors accepting entrusted processing of personal information shall, according to the provisions of PIPL and relevant laws and administrative regulations, take necessary measures to safeguard the security of the personal information they process, and assist personal information handlers in fulfilling the obligations provided in PIPL.

59

9. Data Breach and Incident Response

(24) Response plan



Formulate and organize the implementation of security incident response plans to ensure compliance.

Prevent unauthorized access as well as personal information leaks, distortion, or loss.

51

(25) Notification to individuals and authority



When a personal information breach, distortion, or loss occurs or might have occurred, the competent authorities and individuals shall be immediately notified. The notification must include:

1. the categories of personal information, the reason and the damages that may be caused of what has or may have been leaked, tampered with or lost;
2. the remedial measures that are taken by the personal information handler and the measures available to an individual to mitigate the damages; and
3. the contact information of the handler.

57

If the measures adopted are able to effectively avoid harm created by information breach, distortion, or loss, individuals may not be notified; however, if the authority considers that the harm may have been caused, it may still require notification to individuals.

57