

大成 DENTONS

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

Title	Partner
Office	Shanghai, China
Email	jianmin.dai@dentons.cn
Mobile	+86 139 1611 3437
Website	dentons.com/en/jianmin-dai








Jet Deng

Title	Partner
Office	Beijing, China
Email	zhisong.deng@dentons.cn
Mobile	+86 135 2133 7332
Website	dentons.com/en/zhisong-deng

	<p>employment policy legally established or a collective contract legally concluded;</p> <p>(3) it is necessary for performing a statutory responsibility or statutory obligation;</p> <p>(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;</p> <p>(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;</p> <p>(6) process the personal information, which has already been disclosed by the individual or otherwise legally disclosed, within a reasonable scope.</p>	
<p>(3) Consent</p> <p>● ● ● ● ● ●</p>	<p><input type="checkbox"/> Consent should be based on the individual's willing and explicit intent with full information of the processing.</p> <p><input type="checkbox"/> 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.</p> <p><input type="checkbox"/> Provide a convenient method to withdraw consent.</p> <p><input type="checkbox"/> 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.</p>	<p>14</p> <p>14</p> <p>15</p> <p>16</p>
<p>(4) Privacy Notice</p> <p>● ● ● ● ● ●</p>	<p><input type="checkbox"/> Use clear and easily understood language.</p> <p><input type="checkbox"/> Include the name or personal name and contact method of the personal information handler;</p> <p><input type="checkbox"/> Introduce the purpose of personal information processing and the processing methods, the categories of handled personal information, and the retention period;</p> <p><input type="checkbox"/> Provide information on the method and procedure for individuals to make rights requests;</p> <p><input type="checkbox"/> Notify Individuals about any changes of the notice.</p>	<p>17</p> <p>17</p> <p>17</p> <p>17</p> <p>17</p>
<p>(5) Provision to Third-party (Data Sharing)</p>	<p><input type="checkbox"/> Notify individuals about the name or personal name of the data recipient, its contact information, the processing purpose and method, and personal information categories.</p> <p><input type="checkbox"/> Separate consent from the individual shall be obtained.</p>	<p>23</p>

<p>● ● ● ● ●</p>	<p><input type="checkbox"/> 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.</p>	<p>23 22</p>
<p>(6) Automated Decision-making</p> <p>● ● ● ●</p>	<p><input type="checkbox"/> Guarantee the transparency of the decision-making and the fairness and justice of the processing result.</p> <p>- <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></p> <p><input type="checkbox"/> Do not engage in unreasonable differential treatment of individuals in trading conditions such as trade price, etc.</p> <p><input type="checkbox"/> 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.</p> <p><input type="checkbox"/> 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.</p>	<p>24 24 24 24</p>
<p>(7) CCTV and Facial Recognition Technology</p> <p>● ● ●</p>	<p><input type="checkbox"/> 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.</p> <p><input type="checkbox"/> Set up clear signs of such equipment.</p> <p><input type="checkbox"/> 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.</p>	<p>26 26</p>
<p>3. Processing Sensitive Personal Information</p>		
<p>(8) Scope of Sensitive Personal Information</p> <p>● ● ● ● ● ●</p>	<p><input type="checkbox"/> Assess whether your organization is processing any sensitive personal information in China.</p> <p>- <i>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</i></p>	<p>28</p>

	<i>information of minors under the age of 14.</i>	
(9) Processing Requirements 	<input type="checkbox"/> Have a specific purpose and sufficient necessity for processing sensitive personal information and take strict protection measures.	28
	<input type="checkbox"/> Obtain the individual's SEPARATE CONSENT if no other lawful basis can be relied.	29
	(10) <input type="checkbox"/> Conduct a personal information protection impact assessment (“PIPIA”) in advance and make records.	55
(11) Children’s Data 	<input type="checkbox"/> Assess whether any personal information of minors under the age of 14 is processed.	31
	<input type="checkbox"/> Obtain the consent of the parent or other guardian of the minor.	31
	<input type="checkbox"/> Establish specialized personal information processing rules (e.g., Privacy Notice for Minors).	31
4. Data Governance: Personnel		
(12) Appointment of “Data Protection Officer” (DPO) 	<input type="checkbox"/> Appoint personal information protection officers, who is responsible for conducting supervision of personal information processing activities and protection measures, etc.	52
	<input type="checkbox"/> Disclose the contact of the personal information protection officer (e.g., in the Privacy Notice).	52
	(13) <input type="checkbox"/> Report the name and contact of the officer to the authority.	52
(14) Appointment of Representative 	<input type="checkbox"/> 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.	53
	(15) - <i>Note: “Personal information handler” refers to organizations and individuals that, in personal information processing activities, autonomously determine processing purposes.</i>	53
	<input type="checkbox"/> Report the name of the relevant entity or the name and contact of the representative to the authority.	
5. Operation Security		
(16) Technical Measures 	<input type="checkbox"/> Adopt technical measures to ensure the security of personal information processing such as encryption and de-identification.	51
	<input type="checkbox"/> Prevent unauthorized access as well as data breach, distortion, or loss.	

<p>(20)General Requirements (Notice, Consent and PIPIA)</p> <p>● ● ● ● ● ●</p>	<p><input type="checkbox"/> 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.</p> <p><input type="checkbox"/> Obtain the individual's SEPARATE CONSENT if no other lawful basis can be relied.</p> <p><input type="checkbox"/> Conduct a PIPIA in advance, and record the processing situation.</p>	<p>39</p> <p>55</p>
<p>(21)Additional Requirements</p> <p>● ● ● ● ● ●</p>	<p><input type="checkbox"/> In addition to the above general requirements, at least one of the following conditions shall also be met:</p> <p>(1) passing a security assessment organized (only applicable to critical information infrastructure operators (CIIO) and handlers processing personal information reaching a certain quantity threshold.);</p> <p>(2) undergoing personal information protection certification; or</p> <p>(3) concluding a contract with the data importer in accordance with a standard contract formulated by the state cyberspace administration.</p> <p><input type="checkbox"/> Adopt necessary measures to ensure that the data importer's processing activities reach the standard of personal information protection provided in PIPL.</p>	<p>38</p> <p>38</p>
<p>(22)Restrictions on Data Transfer to Foreign Authorities</p> <p>● ● ● ● ● ●</p>	<p><input type="checkbox"/> Do not provide personal information stored within China to foreign judicial or law enforcement agencies without the approval of the competent Chinese authorities.</p>	<p>41</p>
<p>7. Data Subject Rights and Procedures</p>		
<p>(23)Rights</p> <p>● ● ● ● ● ●</p>	<p><input type="checkbox"/> Ensure individuals have the following rights:</p> <p>(1) the right to be informed;</p> <p>(2) the right to decision;</p>	<p>44-49</p>

	<p>(3) the right to restriction and objection;</p> <p>(4) the right to access and copy;</p> <p>(5) the right to rectification;</p> <p>(6) the right to deletion;</p> <p>(7) the right to data portability;</p> <p>(8) the right to refuse automated decision-making.</p>	
<p>(24)Response Procedures</p> <p></p>	<p><input type="checkbox"/> Establish convenient mechanisms to deal with requests from individuals to exercise their rights.</p> <p><input type="checkbox"/> Provide explanation if it is needed to reject individuals' rights request.</p>	50
<p>8. Compliant Contracting and Procurement</p>		
<p>(25)Engaging a Vendor</p> <p></p>	<p><input type="checkbox"/> 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.;</p> <p><input type="checkbox"/> Supervise the activities of processing of personal information carried out by the entrusted processor (such as through data compliance audit); and</p> <p><input type="checkbox"/> Conduct a PIPIA in advance and record the processing situation.</p>	21
<p>(26)Obligations of vendors</p> <p></p>	<p><input type="checkbox"/> 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.</p>	55
<p>9. Data Breach and Incident Response</p>		
<p>(27)Response plan</p>	<p><input type="checkbox"/> Formulate and organize the implementation of security incident response plans to ensure compliance.</p>	59

<p>● ● ● ●</p>	<p><input type="checkbox"/> Prevent unauthorized access as well as personal information leaks, distortion, or loss.</p>	
<p>(28)Notification to individuals and authority</p> <p>● ●</p>	<p><input type="checkbox"/> 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:</p> <p>(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;</p> <p>(2) the remedial measures that are taken by the personal information handler and the measures available to an individual to mitigate the damages; and</p> <p>(3) the contact information of the handler.</p> <p><input type="checkbox"/> 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.</p>	<p>57</p> <p>57</p>