

China's Personal Information Protection Law ("PIPL") FAQs

Last updated: September 2026

1. WHAT IS THE DATA PROTECTION APPLICABLE IN CHINA?

The Personal Information Protection Law ("PIPL") is China's comprehensive data protection law with a focus on protecting personal information. The PIPL shares similar concept and principles with the European Union's General Data Protection Regulation ("GDPR") and consolidates the previous patchwork of legislation, rules and measures on data privacy, by establishing a comprehensive framework that complements the existing laws such as the China Cybersecurity Law and Data Security Law. It also expands the requirements for processing and transferring personal information, introducing controls over cross border transfer of personal information, and introducing various personal information rights of individuals.

The PIPL was adopted by the Standing Committee of the National People's Congress on 20 August 2021 by China's National People's Congress and comes into force on 1 November 2021.

2. WHAT IS THE TERRITORIAL SCOPE OF THE PIPL?

The PIPL applies to the processing of personal information **within the territory of the People's Republic of China**, regardless of whether the processor is a Chinese or foreign entity or individual. The PIPL will also be applicable to the processing of personal information outside China where the processing relates to individual located in China and is carry out for one of the purposes below:

- a) Providing product and services to individual within China;
- b) analyze or assess the behavior of individuals in China including profiling, behavioral analytics or targeted advertising; or
- c) as provided for in laws or other regulations.
- d) Please note that the PIPL does not apply the processing of personal information in Hong Kong, Taiwan and Macao.

3. WHAT DOES IT MEAN TO PROCESS PERSONAL INFORMATION?

Under the PIPL, "personal information" means any information related to identified or identifiable natural persons, recorded electronically or by other means. This includes information that does not identify a natural person but may be "related" to an identified person.

Personal information "handling" (which has the equivalent meaning of "processing" in other data protection legislation) is also very broadly defined, meaning the collection, storage, use, processing, transmission, provision, disclosure and deletion of personal information.

4. WHAT IS A PERSONAL INFORMATION HANDLER? DATA PROCESSOR?

The PIPL uses the terminology of "personal information handlers" (which is akin to the GDPR's definition of a "data controller"), which means any organisation or individual that independently makes decisions about the purposes and methods of personal information handling in personal information handling activities.

Persons that are entrusted to process personal information (which is akin to the GDPR's definition of a "data processor") are required to take measures to safeguard the security of personal information they process and assist handlers in fulfilling their obligations under the PIPL.

Where we provide products and services to our customers and process personal information of individuals for and on behalf of our customers, we are entrusted as a processor for customer content. Where we act as a personal information handler such as when we process personal information of our employees, we will inform the individual directly and take appropriate steps under the PIPL.

5. WHAT RIGHTS DO INDIVIDUALS HAVE UNDER THE PIPL AND HOW WILL AUTODESK SUPPORT THESE RIGHTS?

Similar to the GDPR, where we act as personal information handler, we recognize that the PIPL aims to provide individuals with certain rights over their personal information, these rights include:

- Right to be informed
- Right to correct, update, deletion and erasure
- Right to restrict processing and/or limit use of personal information
- Right to opt out or object processing personal information
- Right to withdraw consent
- Right to require handlers to provide an explanation of automated decision-making or to object to decisions made solely through automated decision-making means.

Under the PIPL, no organization or individual is allowed to illegally collect, use, process or transmit others' personal information, nor is it permitted to illegally trade, provide or disclose others' personal information.

As a global company, Autodesk supports the rights mentioned above. Individuals can exercise their rights by privacy notice linked below.

In addition to the above, the PIPL also provides for rights of the deceased – where a natural person dies, the PIPL permits their close relatives to, for their own lawful and legitimate interests, exercise the right to access, correct, and delete the relevant personal information of the deceased, unless otherwise arranged before the death of the deceased.

6. DOES THE PIPL REQUIRE PERSONAL INFORMATION TO STAY IN CHINA?

The PIPL (in line with the separate Cyber Security Law ("CSL")) requires organizations designated as operators of critical information infrastructure ("CII") that manages key network facilities or information systems such as in areas of energy, public communications, transportation, water resources, finance, public services, e-government, and national defense, whose damage or data leakage could harm national security, the economy, or public welfare, as well as personal information handlers who handle personal information whose volume has reached the threshold specified by the State cyberspace department, to store personal information within the territory of mainland China, unless otherwise approved by the

Cyberspace Administration of China (“CAC”). However, as Autodesk has not been designated as an operator of critical information infrastructure by the relevant authorities in China, we understand that these requirements under the CSL do not apply to Autodesk.

Apart from the above, General prerequisites for transferring personal information abroad:

- The transfer must be for “business or other needs.”
- The data handler must:
 - Notify the individual (the name and contact information of the overseas recipient, the purpose and method of handling, the type of personal information and the manner in and the procedures by which the individuals exercise the rights under this Law to the overseas recipient);
 - Obtain the individual’s consent;
 - Implement appropriate data protection and security measures.
- Depending on the circumstances data handler may need to complete one of the following:
 - Security assessment
 - Standard contract
 - PI protection certification - Undergo a review by a third party designated by Government authorities.
- Additional approvals may be required for transfers to foreign judicial or law enforcement authorities.

Where we act as a personal information handler and in the event one of the above is applicable to us, we will inform the individual directly and take appropriate steps under the PIPL.

7. DOES PIPL CREATE SPECIAL RULES FOR MINORS?

The PIPL deems the personal information of minors under the age of 14 to be sensitive personal information. Personal information handlers are required to obtain the consent of the minors' parents or other guardians and develop special rules for the handling of such personal information. You can find more information on our educational products and our updated Children’s Privacy Statement for China linked [here](#).

8. HOW WILL AUTODESK DEMONSTRATE COMPLIANCE WITH THE PIPL?

We are committed to practicing transparency in how we handle personal information. We conduct internal assessments and refer to local counsel to maintain our obligations under the PIPL. We maintain ISO certifications for the operational environment of certain cloud products and have undergone SOC 2 compliance audits for selected cloud products. For additional information, please visit our Trust Center. You can find our Privacy Statement for [China here](#).