China PIPL Readiness Record

Aug 3, 2023

The Lucid China PIPL Readiness Record is a quick tool to ascertain your business's readiness to comply with the China Personal Information Processing Law.

About the PIPL:

The China Personal Information Protection Law (PIPL) is a comprehensive data protection legislation, aimed at safeguarding the personal information of Chinese citizens. Enacted on November 1, 2021, the PIPL reflects China's growing concern over data privacy issues, and shares many similarities with the EU GDPR.

The PIPL establishes a comprehensive framework for the collection, use, and processing of personal information by both domestic and foreign entities operating within China's borders. Failure to comply with the PIPL can result in substantial fines and penalties, emphasizing the Chinese government's commitment to ensuring data privacy for its citizens..

Lucid Privacy's PIPL Readiness Record is designed to identify key areas where operational changes may be required, and to assist your organization in prioritizing efforts along the path to PIPL compliance. The assessment can be completed at any stage during your organization's compliance efforts, and can be revisited periodically to assess the progress of operational changes.

About the questions in the Readiness Record:

This survey lays out the essential questions that need to be answered and the operational/legal areas that will need to be covered to satisfy PIPL obligations.. This document forms the basis of a 'self-certification' against the PIPL requirements.

Please address the following questions as comprehensively as possible so that we can carry out an assessment of your business activities against PIPL obligations.

GLOSSARY	
"Personal Information"	"Personal Data"
"Sensitive Personal Information"	"Sensitive personal information refers to the personal information that can easily lead to the infringement of the personal dignity or natural persons or the harm of personal or property safety once leaked or illegally used, including such information as biometrics, religious belief, specific identities, medical health, financial accounts, and whereabouts, and the personal information of minors under the age of 14."
"PI Handling"	"Data Processing"
"PI Handler" OR "Personal Information Processor"	"Data Controller"

"PIPIA" - "Personal Information Protection Impact Assessment"	"DPIA" or in some contexts "TIA"
"Entrusted Persons"	"Data Processors"
"Cross-Border Transfers"	"International Transfers"
"Personal Information Protection Officer"	"DPO"
QUESTIONS	**RESPONSES**
Company:	
Brief description of the business activities: For example, whether the focus is B2B or B2C, and what the sources of revenue are.	
Your name and contact details:	
Date prepared:	
Jurisdiction[1]	
Do you have China-based entities/establishments that process personal data?	*If YES, please provide details of the entity and its geographic location:*
Do you offer goods/services to persons within China?	
Do you monitor the behavior of individuals within China?	
What kinds of individuals are concerned?	*Select all that apply:* • Customers • Children • Employees • Job Applicants • Patients • Prospects • Vendors • Website Visitor • Other *If OTHER, please explain.*

[1] Article 3, Article 53

Have you appointed an 'authorized representative' in China?	
Nature of the data	
Do the data practices involve the collection, use or disclosure of "personal data"? This includes any information that allows an individual to be singled out from other members of a group, even if their name, email address or other personally identifiable information is unknown. It can also include things like: • Cookies • IP addresses • MAC, MAID, UDIDs • Interests, demographics, psychographics • Transactional information • Behavioral information • Inferred information	*If YES, please identify the main types of personal data collected, used or disclosed:*
Do the data practices involve the collection, use or disclosure of "sensitive personal data"? Sensitive personal data includes information relating to: • Biometrics • religious belief • specific identities • medical health • financial accounts • whereabouts (location data) • minors under the age of 14	*If YES, please provide details:*
Governance[2]	
Do internal policies clearly set out the organizational structure for managing privacy?	

[2] Article 51, Article 52, Article 54

Describe privacy management and governance arrangements.	*Describe privacy committee arrangements, how privacy issues and risks are communicated to senior executives etc.*
Provide details of your Personal Information Protection Officer (PIPO)	
Are PIPO details communicated in Privacy Notice?	
Provide details of your privacy audit programme:	
Policy and Procedure[3]	
List all relevant organizational policies: eg data protection policy, information security policy, retention policy, breach policy etc.	
Training and Awareness[4]	
Provide details of your privacy training programme:	
Individual Rights[5]	
Provide details of your individual rights management processes:	*Do staff receive training about how to recognise requests and where to send them?* *Is a specific person/s or team responsible for managing and responding to requests?* *Do you maintain a record of your organization's request responses, and any disclosed or withheld information?* *Do you produce regular reports on performance and case quality assessments to make sure that requests are handled appropriately?* *Are all requests processed in a 'timely manner'?*
Do you have procedures in place to honor requests to **access** personal information?	*YES/NO*
Do you have procedures in place to honor requests to **restrict** personal information processing?	*YES/NO*
Do you have procedures in place to honor requests to **object to** personal information processing?	*YES/NO*

[3] Article 51
[4] Article 51
[5] Article 24, 44, 45, 46, 47, 50

Do you have procedures in place to honor requests to **delete** personal information?	*YES/NO*
Do you have procedures in place to honor requests to **rectify** personal information?	*YES/NO*
Do you have procedures in place to honor requests to **port** personal information?	*YES/NO*
Do you have procedures in place to honor rights relating to **deceased persons?**	*YES/NO*
Do you have procedures in place to honor rights relating to **automated decision making?**	*YES/NO*
Do you have procedures in place to respond to privacy-related complaints?	*YES/NO*
Transparency[6]	
Does the Privacy Notice include all information required by the PIPL?	• *The name or personal name and contact method of the personal information handler;* • *The purpose of personal information handling and the handling methods, the categories of handled personal information, and the retention period;* • *Methods and procedures for individuals to exercise the rights provided in this Law;* • *Details of sensitive personal information handling.* • *Details of Cross Border data transfers.* • *Details of data sharing with other Handlers (Data Controllers).*
Do individuals receive privacy information when their data is collected?	
Do you have in place a procedure to notify individuals if there is a change in the way information is being processed?	

[6] Article 17, 23, 30, 39, 44, 48

Risk and PIPIA[7]	
Do you have PIPIA risk assessments in place for all activities that require?	*1. Handling sensitive personal information;* *2. Using personal information to conduct automated decision-making;* *3. Entrusting personal information handling, providing personal information to other personal information handlers, or disclosing personal information;* *4. Providing personal information abroad;* *5. Other personal information handling activities with a major influence on individuals.*
Do PIPIAs conform to PIPL requirements?	*The content of the PIPIA shall include:* *1. Whether or not the personal information handling purpose, handling method, etc., are lawful, legitimate, and necessary;* *2. The influence on individuals' rights and interests, and the security risks;* *3. Whether protective measures undertaken are legal, effective, and suitable to the degree of risk.*
Data Sharing and Processors[8]	
Are agreements (DPAs) in place with all 'entrusted persons' (Data Processors)?	
Are agreements in place with all Joint Controllers?	
Cross Border Transfers[9]	
Have you mapped cross border transfers of data outside of China?	
Do all cross border data transfers satisfy at least one of the measures to safeguard data export?	• *Passing a security assessment organized by the State cybersecurity and informatization department according to Article 40* • *Undergoing personal information protection certification conducted by a specialized body according to provisions by the State cybersecurity and informatization department* • *Concluding a contract with the foreign receiving side in accordance with a standard contract formulated by the State cyberspace and informatization department, agreeing upon the rights and responsibilities of both sides* • *Other conditions provided in laws or administrative*

[7] Article 55, 56
[8] Article 20, 21, 22, 23, 59
[9] Article 38, 39, 40, 41

	regulations or by the State cybersecurity and informatization department.
Are Transfer PIPIAs in place for all transfers?	*A PIPIA is a type of Transfer Impact Assessment, specific to exports of data from China.* *We have prepared a template PIPIA that you can use to draft PIPIAs.*
Data Retention[10]	
Do you have in place a retention schedule for all personal information?	
Are retention periods implemented throughout the organization?	
Data Breach[11]	
Do you have in place a procedure to notify Chinese regulatory authorities if necessary?	*Where a personal information leak, distortion, or loss occurs or might have occurred, personal information handlers shall immediately adopt remedial measures, and notify the departments fulfilling personal information protection duties and responsibilities and the individuals. The notification shall include the following items:* *1. The information categories, causes, and possible harm caused by the leak, distortion, or loss that occurred or might have occurred;* *2. The remedial measures taken by the personal information handler and measures individuals can adopt to mitigate harm;* *3. Contact method of the personal information handler.* *Where personal information handlers adopt measures that are able to effectively avoid harm created by information leaks, distortion, or loss, personal information handlers are permitted to not notify individuals; however, where departments fulfilling personal information protection protection duties and responsibilities believe harm may have been created, they may require personal information handlers to notify individuals.*
Do you have in place a procedure setting out how you will tell affected individuals about a breach if necessary?	
Do you have a response plan in place	

[10] Article 19
[11] Article 51, 57

for addressing any security incidents and personal data breaches that occur?	
PI Handling Rules[12]	
Do you process personal information using one of the lawful bases for processing?	*Personal information handlers may only handle personal information where they conform to one of the following circumstances:* *1. Obtaining individuals' consent;* *2. Where necessary to conclude or fulfill a contract in which the individual is an interested party, or where necessary to conduct human resources management according to lawfully formulated labor rules and structures and lawfully concluded collective contracts;* *3. Where necessary to fulfill statutory duties and responsibilities or statutory obligations;* *4. Where necessary to respond to sudden public health incidents or protect natural persons' lives and health, or the security of their property, under emergency conditions;* *5. Handling personal information within a reasonable scope to implement news reporting, public opinion supervision, and other such activities for the public interest;* *6. When handling personal information disclosed by persons themselves or otherwise already lawfully disclosed, within a reasonable scope in accordance with the provisions of this Law.* *7. Other circumstances provided in laws and administrative regulations.*
Do you obtain consent to process sensitive personal information?	
Do you obtain parental consent to process information relating to minors (under-14)?	
Do you display privacy information/signage near all CCTV installations?	

[12] Article 13, 26, 29, 31