PIPL Readiness

Compliance Guide

Ext.prc.001.02 | 06.06.2025

Table Of Contents

PIPL – China's Personal Information Protection Law

- On August 20, 2021, China's first comprehensive Personal Information Protection Law ("PIPL") was passed into law. **The PIPL will become effective on November 1, 2021**

- **The Cybersecurity Law, the Data Security Law, and the PIPL of China are the three pillars of China's data protection framework**, which govern cybersecurity, data security, and personal information protection, respectively. Understanding and complying with all three laws are vital for organizations to process data of individuals in China.

- **PIPL, focuses on "personal information,"** serving as China's first comprehensive personal data privacy law, similar to the EU's General Data Protection Regulation ("GDPR").

- PIPL specifies the scope of personal information; clarifies the legal bases for processing personal information; lays down the obligations and responsibilities imposed on processors; and imposes stringent requirements on data localization, safeguarding the interest of China in the case of cross-border transfer of personal information.

PIPL - Definitions

Personal Information Processor:
Similar to the GDPR's definition of "data controller," PIPL uses the term, "Personal Information Processor" as the "organization or individual that independently determines the purposes and means for processing of personal information" (Article 73).

Entrusted Party:
PIPL uses "Entrusted Party" to refer to the entity that processes personal information on behalf of the Personal Information Processor, comparable to GDPR's definition of "data processor" (Article 21).

Personal Information:
Similar to the GDPR, PIPL defines personal information as any "information related to identified or identifiable natural persons recorded by electronic or other means" (Article 4). Also, like the GDPR, anonymized information is not considered personal information under the PIPL.

Processing of Personal Information:
Similarly broad in scope as under EU and US privacy laws, encompassing "the collection, storage, use, processing, transmission, provision, publication, and erasure of personal information."

PIPL – Chapters and Articles

- General Provisions
- *purpose and definitions*

Article 1 – 12 — 1

- Rules on Processing of Personal Information
- *lawful collection and processing of PII*

Article 13 – 37 — 2

- Rules on Cross-Border Provision of Personal Information
- *preconditions and controls for transferring PII abroad*

Article 38 – 43 — 3

- Rights of Individuals in processing of Personal Information
- *Individuals' rights over their own PII and to give or withdraw consent over the use of their PII*

Article 44 – 49 — 4

- Obligations of Personal Information Processors
- *A set of requirements for PII processors to protect the data collected*

Article 50 – 55 — 5

- Authorities Fulfilling Personal Information Protection Duties and Responsibilities
- *Responsibilities of CAC and related departments.*

Article 56 – 61 — 6

- Legal Liability
- *Penalties and fines for violation of the regulatory requirements stated in this law*

Article 62 – 67 — 7

- Supplementary Provisions
- *Definitions and official enactment date*

Article 68 – 70 — 8

PIPL - Key Highlights and Interpretations

Category	Article No. and Consent	Measures adopted by ZINFI
Obtain Consent of Individuals for Data Handling	Article 24: Notifications to, and explicit consent from the data subjects when third parties are involved in the PII Processing.	All matters related to PII processing activities, including the identity and contact details of data recipients are provided to data subjects. Consent is obtained prior to any PII processing.
Organizational Governance	Article 50: PII processors to adopt security measures to prevent unauthorized access and protect the PII from data leakage, theft, distortion of deletion.	We adopt security measures to protect the PII collected (e.g. applying data encryption, providing security training and education to employees).
	Article 51 & 52: PII processors (both in or outside of China) to appoint responsible persons for supervision of PII processing and protection activities.	We appoint responsible person(s) for supervising the data activities on PII and security measures adopted for protecting PII,
Rights of Individuals	Article 44, 45, 46 & 48: Data subjects' rights access or correct the PII, and to know, decide or request for the explanation of the processing of their PII.	Individuals can decide whether we can process their PII and to what extent, or to make changes, or delete the PII collected.
Cross Border Data Transfer (CBDT)	Article 39: Notifications to, and explicit consent from the data subjects when their PII needs to be transferred outside of People's Republic of China.	We notify the individual on the CBDT arrangement, ways to exercise their rights, and obtain consent.
	Article 40: When CIIOs and PII processors process PII exceeding the amount set by CAC, they should pass a security assessment if they need to provide PII to any party outside the People's Republic of China.	If we meet data volume threshold (as determined by CAC) we have policies and provisions to undergo security assessments before cross-border data transfer can take place.

PIPL Requirements and ZINFI

Data Subject Rights

Options provided by ZINFI to Data Subjects - Edit, Remove, Restrict the use of their data, or withdraw consent given previously.

Data Processing Agreements

ZINFI has data processing agreements in place for engaging entrusted parties.

Privacy Governance and Security Controls

ZINFI has established internal personal information management program based on administrative measures (policies, operating rules, and technical controls). security controlsto be applied when storing and processing the PII.

Data Localization

ZINFI supports storing of personal information within China, when the amount of PII exceed the threshold set by the Cybersecurity Administration of China (CAC).

Data Breach Incidence Management

ZINFI has defined policies to immediately take remedial measures, and inform the department designated with the duty of personal information protection and individuals concerned.

- PIPL is applicable to ZINFI when we process PII of individuals in China.
- Business contact details such as name, business email, business phone numbers, etc. are primarily processed and housed at ZINFI.
- ZINFI does not sell personal information.
- ZINFI as a foreign Personal Information Processor has a designated representative in China for personal information protection.

PIPL - Compliance Road Map

1. **Discover**
   Identify what personal data you have and where it resides
2. **Control**
   Manage how personal data is used and accessed
3. **Protect**
   Establish security controls to prevent, detect and respond to vulnerabilities and data breaches
4. **Report**
   Act on data subject requests, consents and required documentation
5. **Review**
   Analyze your data and systems, stay compliant and reduce risk

PIPL Ready

- **Rights of Individuals**
  Policies to fulfill individual rights
- **Consent**
  Review consent-related permissions
- **Database Impacts**
  Storage of personal data and consent forms
- **Transparency**
  Compliance of private notices
- **Data Privacy Impact Assessments**
  Data usage and processes
- **Data Security**
  Security and data protection
- **Data Breaches**
  Breach policies and procedures in place
- **Data Governance**
  Data processing and protection office
- **Contracts**
  Review of data collection & processing contracts

Controls and Security

ZINFI's Seven-Factor PIPL Commitment

- Data Protection Office
- Data Security
- Consent Management & Policies
- Data Accuracy
- Data Processing
- Breach Procedures
- Training

Operational Security

- Intrusion Detection
- Reducing Insider Risk
- Safe Employee Devices & Credentials
- Safe Software Development

User Identity & Storage

- Authentication
- Login Abuse Protection
- Encryption

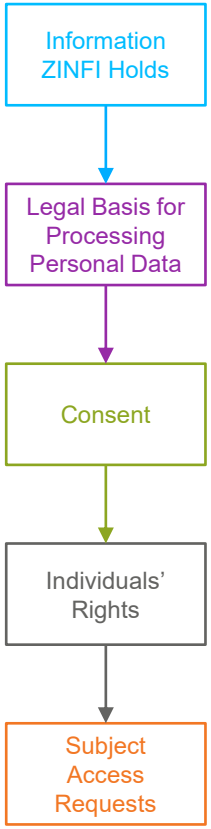
Internet Communication

- Network Security
- DoS Protection
- User Authentication

Service Deployment

- Access Management of End User Data
- Encryption of Inter-Service Communication
- Inter-Service Access Management
- Service Identity, Integrity, Isolation

Consent Management



Consent Management

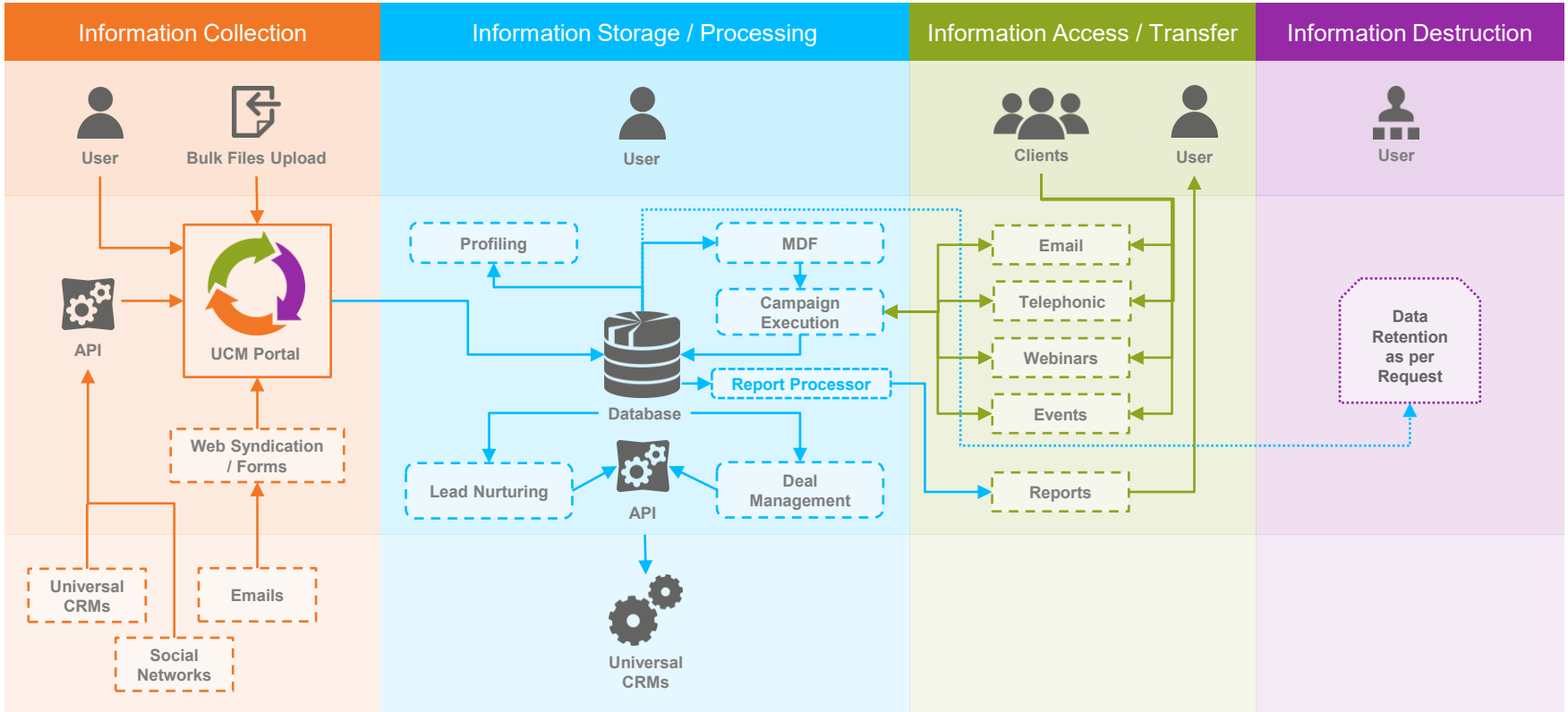
ZINFI establishes:

- Not only simple consent-obtaining procedures, but also demonstrates that the data subject has consented to processing of his/her data; records stored for fingertip access.
- Consent requests in the context of a written declaration are presented in an intelligible and easily accessible form, using clear and plain language. "Do Not Sell My Personal Information" Policy is presented transparently..
- Requests for consent conforms to the use of the service for which it is collected. The following are clearly defined and mailed to CA clients, prior to processing:
    - Why we collect the specific information
    - What we do with it
    - How long we keep it
    - How we destroy/retain it
    - How individuals can access the information you hold on them
    - Right to be forgotten information: data subject's right to withdraw consent at any time; the process for withdrawing consent should be just as easy as that for giving consent

Implementing Procedures

- Privacy policies defined and revised for PIPL and undertaken by organization
- Marketing data protection policy (rulebook on filtering and sending customer offers)
- HR employee data protection policy (consent management of employees/associates for internal processing activities)
- Disagreement to consent policy (withdrawal management)
- Data retention policy/agreement
- Cookie usage and acceptance policy (defines data subject tracking consent, if any)

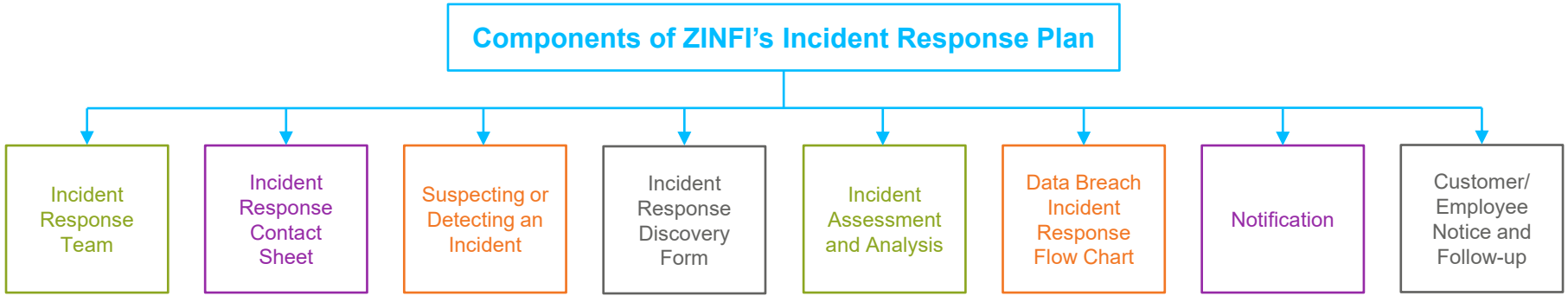
System Data Flow



Data Breach Incidence Handling

Maintenance of data breach incident response plan

1. Aims to reduce the exposure of organizations, customers/ employees and partners that arises from a data theft or data loss incident
2. Specifically includes policies and procedures to:
   - Assess the nature and scope of an incident, and identify what customer information systems and types of customer/employee information have been accessed or misused
   - Contain and control the incident to prevent further unauthorized access to, or misuse of, customer information, while preserving records and other evidence
   - Notify appropriate entities (data subjects, legal departments, etc.) about breach
   - Maintain or restore business continuity



Training

The PIPL compliance parameters requires workforce privacy awareness training.

There are three types of training that are conducted by ZINFI:

- **General workforce privacy awareness training** – basic privacy awareness for the entire workforce.
- **Training about PIPL** – training that introduces select employee groups to PIPL (i.e., employees who need to know more about how PIPL works).
- **Role-based training** – training for specific roles in organizations, such as managing products and services for privacy or vendor management. Some individuals will require more specialized training about new responsibilities they will have under PIPL. We offer courses for specific, role-based privacy training.

Training deliverables:

Overview	Principles	Rights	Responsibilities
• What is data protection? • Who does PIPL apply to? • What does PIPL apply to? • Non-compliance and fines • Knowledge check	• Principles of PIPL • Lawfulness • Accountability • Policies • Data privacy	• Individual rights • Data subjects and rights • B2B/B2C rights • Reporting rights • Obligations of data controllers and processors	• PIPL compliance dos and don'ts • Breach notification • Roles of data security • Conclusion • Assessment

Conformance

Conducting Conformance Assessments and Registering:

Determine key metrics to measure privacy program
- Define conformation "success" for privacy program
- Determine metrics to assess privacy program and how they will be collected

→

Description of Data Flows
- Type of data
- Use of data
- Recorded in a flowchart
- Preparation of information asset register

→

Identifying Privacy Risks
- Apply the data protection principles
- Individual risks
- Compliance risks
- Preparation of risk register

→

Identification of Privacy Solutions
- Accept
- Reduce
- Eliminate
- Review Privacy Policies
- Maintain privacy inbox and respond to consumer requests

→

Registering outcomes
- Document status of each risk
- Identify risk objects
- Prepare final report
- Publish final report

PIPL implications to ZINFI from data life cycle perspective:

Data Subject Notification → Right to Use & Disclose → Data Collection → Data Usage → Data Sharing / Transfer → Data Disposal / Retention

ZINFI Technologies, Inc.
6200 Stoneridge Mall Road, Suite 300
Pleasanton, CA 94588

sales@zinfitech.com