君泽君律师事务所
JunZeJun Law Offices

# JunZeJun New Law Express

**Context**

# I. A Reading of *Personal Information Protection Law*

## ❖ Regulation Overview

The *Personal Information Protection Law of the People's Republic of China* (herein refer to "the PIPL"), after the third review and being requested for public comments twice, was passed at the 30th Session of the Standing Committee of the 13th National People's Congress of the People's Republic of China on August 20, 2021, and formally carried out since November 1, 2021. As a basic law in the field of personal information protection, its promulgation solves the problem that laws and regulations on personal information are scattered and unsystematic. Together with the Data Security Law, the Cyber Security Law and the Cryptography Law, the PIPL constructs the legislative framework for data governance in China.

## ❖ A Reading of the Key Contents

The PIPL consists of 74 articles in eight chapters, including the General Provisions, Rules for Processing Personal Information, Rules for Cross-Border Provision of Personal Information, Rights of Individuals in Activities of Processing Personal Information, Obligations of Personal Information Processors, Authorities Performing Duties of Personal Information Protection, Legal Liability, etc., and it fully stipulates the protection of personal information and establishes the basic institutional framework in the field of personal information protection in China. Its main features are as follows:

1. Clarifying the applicable scope of law and its extraterritorial effect. The PIPL stipulates that the processing of personal information of natural persons within the territory of PRC shall be subject to the PIPL; meanwhile, if an analysis or evaluation on activities of domestic natural persons for the purpose of providing products or services to domestic customers, even if the processing of such information occurs outside the PRC, it shall also be subject to the PIPL.

2. The PIPL clarifies the core concepts and expands the scope of sensitive information. The definition of personal information in the PIPL adopts the standards of "identified or identifiable" and "relating

to", and excludes the information that has been anonymized. Meanwhile, the personal information of minors under the age of 14 is included in the scope of sensitive personal information by reference to the relevant provisions of *the Personal Information Security Specification*.

3. Improving the rules for processing of personal information. It is emphasized in the PIPL that personal information shall be processed in a lawful and proper way, for a clear and reasonable purpose, with a limit to the minimum range for processing purposes, with principles of processing openly, ensuring information accuracy, taking security protection measures, etc., and the above principles shall be applied throughout the whole process and each step of personal information processing.

4. Improving the requirements for cross-border transmission of personal information. The PIPL is made clear that for key information infrastructure operators and processors whose capacity of personal information processing reaches that prescribed by the national cyberspace administration, if it is necessary to provide personal information overseas, they shall pass the security assessment organized by the national cyberspace administration; for other circumstances under which cross-border provision of personal information is required, certification by professional institutions and other requirement is needed.

5. Clarifying the rights of individuals in the processing of personal information. The PIPL grants the individuals the relevant rights related to protection of personal information, such as the right to know and the right to decide on the processing of his/her personal information, the right to restrict or refuse others to process his/her personal information, the right to access and copy his/her personal information, and the right to request the transfer of personal information to the designated personal information processor and to require for correcting, supplementing and deleting his/her personal information;

6. Clarifying the obligations of personal information processors. The PIPL stipulates the obligations of personal information processors for security protection, compliance audit, an impact assessment on personal information protection, security incident notification, etc., and put forward higher requirements for personal information processors.

7. Legal Liability for violation of the PIPL. The PIPL imposes three legal liabilities on illegal processing of personal information, or processing of personal information without fulfilling the legal

obligations to protect personal information: 1) the authorities performing duties of protecting personal information shall order those who violate the PIPL to make corrections, give warnings, confiscate its illegal gains, and order them to suspend or terminate the provision of services for applications of illegally processing personal information; 2) a fine of not more than CNY1,000,000 for those who refuse to make corrections; 3) a fine of not less than CNY10,000 but not more than CNY100,000 shall be imposed on the person directly in charge and other directly liable persons.

Besides, for those who violate the PIPL seriously, they are faced with stricter legal liabilities to bear: firstly, the authorities performing duties of protecting personal information at or above the provincial level shall order the violating parties to make corrections, confiscate the illegal gains, and impose a fine of not more than CNY50,000,000 or not more than 5% of their turnover of the previous year; additionally, the authorities may order them to suspend relevant business or suspend business for rectification, and inform the relevant competent authorities to revoke their business permits or business license. Secondly, a fine of not less than 100,000 yuan but not more than 1 million yuan shall be imposed on the person directly in charge and other directly liable persons, and a decision may be made to prohibit the said persons from acting as directors, supervisors, senior executives and persons-in-charge of personal information protection of relevant enterprises within a certain period of time.

- **Influence on Foreign Investment**

The implementation of the PIPL will have a significant impact on multinational companies in various industries. From the perspective of compliance management, enterprises shall establish and improve the personal information protection system and personal information processing rules, etc., preparations shall be made in terms of the cross-border transfer of information, information security assessment, evidence tracing and other important aspects, so as to take precautions, predict in advance and to avoid compliance risks in a timely manner.

Especially the foreign enterprises in China, an employer shall, in accordance with the legal requirements of “notification and consent”, improve the authorization documents for personal

information processing at the time of establishing an employment relationship, and adhere to the principle of "appropriateness, necessity and proportion", to ensure the cross-border information security as much as possible when processing employee information overseas, and to reduce the impact of cross-border personal information processing on employees.

# II. Modification of *the Criminal Law Amendment (XI)* to the Crime of Infringement of Trade Secrets

## ❖ Regulation Overview

Since intellectual property protection strategy is a vital strategy for development of a country, China pays more attention on intellection property right protection. In addition, with an increasing number of fresh formidable challenges in judicial practice in cases of infringement of trade secrets, the corresponding laws are revised from time to time in order to keeping with the pace.

Bringing in line with international rules, *Anti-Unfair Competition Law* partially has modified the part of trade secrets, appropriately reduced the burden of proof of plaintiffs, and effectively strengthened the protection of trade secrets. Article 123 of *the Civil Code* clearly defines trade secrets as one of the types of intellectual property rights, which directly solves the disputes of attributes of trade secrets. To coordinate with other laws, *the Criminal Law Amendment (XI)* has made significant changes to the crime of infringing trade secrets, and increased the criminal punishment for infringing trade secrets.

## ❖ A Reading of the Key Contents

1. Clarified behaviors of the crime of infringing trade secrets

In this *Amendment*, definition of behaviors of the crime of infringing trade secrets was changed from "obtaining by theft, bribery, fraud, coercion, or other improper means" to "obtaining by theft, bribery, fraud, coercion, **electronic intrusion** or other improper means". It added "electronic intrusion" as a mean of infringing trade secrets, and changed the expression of "inducement" into more standard expressions which are "bribery" and "fraud".

The aforesaid re-definition of behaviors of the crime of infringing trade secrets not only meets the needs of the development of the times brought by internet technology blooming, but also directly

responses to the act to obtain trade secrets by taking use of the internet system which is very common these days. In the past, when it comes to the behavior of hacking into the computer system of the obligee, stealing or deleting trade secrets, in judicial practice such a behavior was basically deemed as a criminal offence of illegally invading the computer information system, illegally obtaining data from the computer information system, or destroying the computer information system. However, after this amendment, according to the principle that the special law is superior to the general law, that behavior shall constitute the crime of infringing trade secrets.

2. Expanded the scope of those who shall bear confidentiality obligation

In the previous law, the confidentiality obligation of trade secrets was only limited to contractual obligations, while this amendment expanded the scope of those who shall bear confidentiality obligation, which is not only limited to contractual obligations. Those who are obliged under statutory confidentiality obligation and who are assumed by the public to undertake confidentiality obligation, have been covered in the revised amendment. For example, business personnel such as enterprise consultants and agents, people with professional identity who engage in litigation, non-litigation business or perform supervision and management duties, and someone who may know business secrets due to business activities are all included. This expansion provides a solution to a new situation that constantly appears in judicial practice.

3. Added commercial espionage crime

Added a sub-clause in Article 219 of the Criminal Law, namely, “the crime of stealing, spying, buying or illegally providing trade secrets for foreign countries”, known as commercial espionage crime. Two statutory punishments are set for this crime, of which the first statutory punishment does not require “serious circumstances”, which means that the above acts shall constitute the crime as long as the acts are conducted. By lowering the standard of committed such crimes, it reflects China’s zero-tolerance attitude towards it.

## ❖ Advice to Enterprises

*The Criminal Law Amendment (XI)* has strengthened the crackdown on the crime of infringing trade secrets, raised the statutory penalty, and effectively protected the interests of the company.

As for the company, it should establish a complete trade secret protection compliance system, sign confidentiality agreements with employees to effectively prevent employees from infringing business secrets, and take specific confidentiality measures for all kinds of business secrets on the basis of clearly defining the scope of business secrets through internal verification and evaluation.

At the meanwhile, this Amendment makes special provisions on "commercial espionage", which not only meets requirement under the current intellectual property protection system, but also establishes a progressive relation with the crime of infringing trade secrets. It fills up the lack of regulations for the crime of stealing, spying, buying, illegally providing state secrets, providing information to overseas organizations and individuals, improves China's criminal legislation system of trade secrets, and protects the safety of international competition and cooperation of Chinese enterprises.

君泽君律师事务所
JunZeJun Law Offices

# Contact Us

# 联系我们


Zhengyang Wang, Senior Partner

LANDLINE：021-61060889-8072

EMAIL：wangzhengyang@junzejun.com

MOBILE：13816677991

ADDRESS：4002, Tower 1, Lujiazui Century Financial Plaza, No.729 South Yanggao Road,

Shanghai 200127, P.R.C.