Jurisdiction	People's Republic of China
Date	4 October 2023
Law Firm	ZHONG LUN LAW FIRM
Name and Position of the person in charge	Heng Ding Partner Qijia Liao Associate
Contact Information	dingheng@zhonglun.com liaoqijia@zhonglun.com

Whether there is personal information protection legislation

There are the following comprehensive laws and regulations:

- Personal Information Protection Law of the People's Republic of China ("PIPL")
  - URL: https://www.lawinfochina.com/display.aspx?lib=law&id=36358
  - Enforcement Status: Enacted on November 1, 2021.
  - Subject sector: Data user in public (including local governments) and private sectors.
  - Subject information: All types of information related to identified or identifiable natural persons that are electronically or otherwise recorded (excluding information that has been anonymized).

Information that can be indicators regarding the personal information protection legislation

EU's adequacy decision[1]: N/A

APEC Cross-Border Privacy Rules (CBPR) system: N/A

Business operators' obligations to comply with the eight principles of the OECD Privacy

[1] According to "Measures for the Security Assessment of Outbound Data Transfer" Article 4, the situations in which security assessment obligations must be fulfilled include: (1) critical information infrastructure operators, (2) data processors who provide critical data abroad, (3) data processors who process the personal information of more than 1 million people, (4) data processors who provide personal information of over 100,000 people abroad since January 1 of the previous year, (5) data processors who provide the sensitive personal information of over 10,000 people cumulatively abroad since January 1 of the previous year.

Guidelines or the rights of individuals

The obligations of the relevant agency of business operators or the rights of individuals corresponding to the eight principles of the OECD Privacy Guidelines are as follows:

a) Collection Limitation Principle: It is stipulated in the law described above.
b) Data Quality Principle: It is stipulated in the law described above.
c) Purpose Specification Principle: It is stipulated in the law described above.
d) Use Limitation Principle: It is stipulated in the law described above.
e) Security Safeguard Principle: It is stipulated in the law described above.
f) Openness Principle: It is stipulated in the law described above.
g) Individual Participation Principle: It is stipulated in the law described above.
h) Accountability Principle: It is stipulated in the law described above.

Other systems that may significantly affect the rights and interests of individuals

A system related to the obligation to store personal information within the territory and that may significantly affect the rights and interests of individuals:

- There is a system related to the obligation to store personal information within the territory (including a system that essentially imposes an obligation to store personal information within the territory by restricting the transfer of personal information outside the territory) in PIPL, Cybersecurity Law of the People's Republic of China (中华人民共和国网络安全法)("Cybersecurity Law") and Data Security Law of the People's Republic of China (中华人民共和国数据安全法)("Data Security Law"). The following personal information should be stored within the People's Republic of China.
  a) Personal information processed by state organs.
  b) Personal information collected and generated within the People's Republic of China by critical information infrastructure operators.
  c) Personal information collected and generated within the People's Republic of China by a personal information processor whose processing of personal information has reached the amount stipulated by the national cyber intelligence department.
- Under these laws and regulations, when transferring information outside of the People's Republic of China, the following requirements must be met: (1) if the cross-border data transfer safety evaluation standards are met, the transfer must pass the security evaluation by the national cyber intelligence department; if the safety

evaluation standards are not met, (2) it must undergo personal information protection certification by a specialized organization; or (3) it is a requirement to conclude a personal information cross-border standard contract and submit a notification[2]. In addition, when transferring information outside the territory, if certain requirements are met, it is necessary to comply with other supervisory and management regulations such as cybersecurity reviews[3], export controls[4], and judicial cooperation[5].

- If it is necessary to store personal information within China, there is a risk that the business operator will not be able to adequately respond to disclosure requests from a person. In addition, the obligation to store personal information within the territory under these laws and regulations may not apply to personal information acquired through transfer from a foreign business operator.
- In addition, in some industries, there are stricter regulations regarding cross-border transfers of personal information. For example, in the automobile industry, the "Automotive Data Safety Management Regulations (for Trial Implementation)[6]" (汽

---

[2] According to PIPL Article 38, when a personal information processor needs to provide personal information outside the territory of the People's Republic of China, they must satisfy one of the following conditions: (1) Passing a security assessment organized by the State cybersecurity and informatization department according to Article 40 of this Law; (2) Undergoing personal information protection certification conducted by a specialized body according to provisions by the State cybersecurity and informatization department; (3) 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; or (4) Other conditions provided in laws or administrative regulations or by the State cybersecurity and informatization department.

[3] According to "Cybersecurity Review Measures of China" Article 2, critical information infrastructure operators procuring network products and services and online platform operators conducting data handling activities that influence or may influence national security must be subject to a cybersecurity review according to these measures.

[4] If data awaiting cross-border transfer is included in the list of export-controlled goods, it is possible to transfer it cross-border only after applying to the national export control department and obtaining approval.

[5] PIPL Article 41 provides that "Competent authorities of the People's Republic of China, according to relevant laws and treaties or international agreements that the People's Republic of China has concluded or acceded to, or according to the principle of equality and mutual benefit, are to handle foreign judicial or law enforcement authorities' requests regarding the provision of personal information stored domestically. Without the approval of the competent authorities of the People's Republic of China, personal information handlers may not provide personal information stored within the mainland territory of the People's Republic of China to foreign judicial or law enforcement agencies."

[6] "Several Provisions on the Management of Automobile Data Security (for Trial Implementation)" Article

车数据安全管理若干规定（试行）) restricts the cross-border transfer of important data and stipulates additional obligations regarding annual reporting of automobile data. In the securities industry, the Securities Law of the People's Republic of China[7] restricts the transmission of "documents or materials related to securities business activities" outside China. In the medical industry, the "Measures for the Administration of Population Health Information (for Trial Implementation)[8]", the "National Health and Medical Big Data Standards, Safety and Service Management Measures (for Trial Implementation)[9]", and the "Regulation of the People's Republic of China on the Administration of Human Genetic Resources[10]" stipulates restrictions on cross-border transfers of population health information, health and medical big data and human genetic resource information.

A system that imposes an obligation on business operators to cooperate with government information gathering activities and that may significantly affect the rights and interests of individuals:

---

11 provides that "Important data must be stored within the country in accordance with the law and if it is truly necessary to provide it overseas due to business needs, it must pass a security assessment organized by the national cybersecurity and informatization department in conjunction with relevant departments of the State Council.". Article 13 of the same provides that "Automobile data processors carrying out important data processing activities must report the following annual automobile data security management status to the cybersecurity and informatization departments of the provinces, autonomous regions, and municipalities directly under the Central Government and relevant departments before December 15th of each year. (omitted)"

[7] "Securities Law of China" Article 177 paragraph 2 provides that "Without the consent of the securities regulatory authority under the State Council and the relevant authorities under the State Council, no entity or individual may provide documents or materials related to securities business activities to other countries or regions without authorization."

[8] "Administrative Measures for Population Health Information (for Trial Implementation)" Article 10 provides that "(omitted) Population health information may not be stored in overseas servers, nor may it be hosted or leased in overseas servers."

[9] "National Health and Medical Big Data Standards, Safety and Service Management Measures (for Trial Implementation)" Article 30 provides that "(omitted) Health and medical big data should be stored on safe and trustworthy servers within the country. If it is really necessary to provide it overseas due to business needs, a security assessment and review should be conducted in accordance with relevant laws, regulations and requirements."

[10] "Regulation of the People's Republic of China on the Administration of Human Genetic Resources" Article 7 provides that "Foreign organizations, individuals and the institutions they establish or actually control are not allowed to collect and preserve the country's human genetic resources within the territory of the country, and are not allowed to provide the country's human genetic resources abroad."

I. Cybersecurity Law of the People's Republic of China（中华人民共和国网络安全法）、Cybersecurity Review Measures of the People's Republic of China（中华人民共和国网络安全审查办法）

- Cybersecurity Law requires network operators to provide technical support and cooperation to activities related to the maintenance and protection of national security and criminal investigation by public safety agencies and national security agencies.
- It further requires operators of critical information infrastructure to pass a national security review organized by the national cyber intelligence department in collaboration with relevant departments of the state council when procuring cyber products and services that may affect national security.
- Regarding access to personal information held by private businesses, for example, there are generally no regulations regarding the following points:
    - Restrictions and procedures for enforcement of access
    - Access to the extent necessary to achieve the purpose specified in the law (or a legitimate purpose consistent with that purpose)
    - Approval from an independent authority to conduct the access
    - Restrictions and security management on handling of acquired information
    - Ensuring transparency regarding access practices

II. Data Security Law of the People's Republic of China(中华人民共和国数据安全法)

- Data Security Law requires related organizations or individuals to cooperate with data investigations conducted by public safety agencies and national security agencies as necessary to maintain and protect national security or investigate crimes.
- Regarding access to personal information held by business operators under the Law, for example, there are no regulations regarding the following points:
    - Restrictions on enforcement of access
    - Access to the extent necessary to achieve the purpose specified in the law (or a legitimate purpose consistent with that purpose)
    - Ensuring transparency regarding access practices

III. National Intelligence Law of the People's Republic of China（中华人民共和国国家情报法）

- National Intelligence Law requires related institutions, organizations, and citizens to provide necessary support, assistance, and cooperation for national intelligence activities conducted by national security organs, intelligence departments of public security agencies, and military intelligence departments.

- Regarding access to personal information held by business operators under the Law, for example, there are no regulations regarding the following points:
    - Restrictions and procedures for enforcement of access
    - Access to the extent necessary to achieve the purpose specified in the law (or a legitimate purpose consistent with that purpose)
    - Approval from an independent authority to conduct the access
    - Restrictions and security management on handling of acquired information
    - Ensuring transparency regarding access practices

IV. Personal Information Protection Law of the People's Republic of China（中华人民共和国个人信息保护法）

- PIPL requires related organizations or individuals to provide necessary support and cooperation for investigations, on-site inspection activities, or fact- checking interviews conducted by personal information protection authorities regarding personal information protection.
- Regarding access to personal information held by business operators under the Law, for example, there are no regulations regarding the following points:
    - Restrictions and procedures for enforcement of access
    - Access to the extent necessary to achieve the purpose specified in the law (or a legitimate purpose consistent with that purpose)
    - Approval from an independent authority to conduct the access
    - Restrictions and security management on handling of acquired information
    - Ensuring transparency regarding access practices

V. The Provisions on Administrative Law Enforcement Procedures by Internet Information Departments（网信部门行政执法程序规定）

- The procedures for the government cyber intelligence department to enforce administrative laws such as administrative penalties are clearly specified, including jurisdiction, filing of cases, investigation/evidence collection, public hearings, and determination and delivery of administrative penalties.