DATA PRIVACY LAWS AND REGULATIONS

What laws apply to the collection and use of individuals' personal information?

Data privacy laws have become more prominent in recent years. As the amount of personal information available online has grown substantially, there has been an enhanced focus on the processing of personal data, as well as the enforcement of such laws.

Employers are subject to a patchwork of laws relating to employee privacy. The following regulations form the backbone of the People's Republic of China (PRC) Data Protection laws:

The Personal Information Protection Law (PIPL) promulgated on August 20, 2021 and effective November 1, 2021 is the most comprehensive law regulating personal information. It imposes new obligations on the collection, use, processing, disclosure, and international transfer of personal information. PIPL defines personal information as all kinds of information related to an identified or identifiable natural person, recorded electronically or by other means, excluding anonymized information (Art. 4).

PIPL defines "sensitive personal information" as personal information that, once leaked or used illegally, can easily lead to the infringement of the personal dignity of natural persons or the harm of personal and property safety, including biometrics, religious beliefs, legally protected characteristics, medical health, financial accounts, geolocation information, as well as personal information of minors under the age of fourteen (Art. 28).

Employers should be aware that "basic information directly related to the labor contract" collected pursuant to requirements under the PRC Labor Contract Law would be subject to the PIPL. "Basic information" has yet to be officially defined, but in practice it generally includes employee's name, gender, ethnicity, date and place of birth, identification number, address, email address, general health conditions, educational background, work experience, emergency contacts, and immediate family members.

Network Security Graded Protection of Information Security Technology (信息安全技术 网络安全等级保护测评要求) (GB/T 28448-2019); **Security Design and Technology Requirements for Network Security Graded Protection of Information Security Technology** (信息安全技术 网络安全等级保护安全设计技术要求) (GB/T 25070-2019). These national standards were promulgated by the State Bureau of Market Administration and Supervision and the National Information Security Standardization Technical Committee on May 13, 2019. These standards and requirements set the graded security level of networks and required protection measures for each level based on the Cybersecurity Law. Note that these are neither laws nor regulations and are not legally binding.

National Standard of Information Technology – Personal Information Security Specification (个人信息安全规范, GB/T 35273-2020) (the "2020 Specification"), recently updated by the National Information Security Standardization Technical Committee, and effective October 1, 2020. This Standard sets the guidelines businesses should follow relating to personal data. Note that the Specification is not law or regulation.

Technology Requirement for Personal Information Protection of Smart Mobile Terminal, promulgated by the National Information Security Standardization Technical Committee, effective on May 1, 2018. This Requirement sets the personal information protection guideline and technology requirements of mobile terminals. Note that the Requirement is not law or regulation.

National Standards of Network Security Graded Protection:
The **Draft Measures on Security Assessment of Cross-border Data Transfer** was made available for public comment on October 29, 2021. It provides the assessment process for personal information to be transferred abroad. The **Draft Network Data Security Management Regulations** was made available for public comment on November 14, 2021, and sets protection measures for personal data and important data based on a categorized and hierarchical system. Note that these are currently in draft form and are not legally binding.

The **Data Security Law (DSL)**, was promulgated in June 10, 2021, and effective on September 1, 2021. The primary purpose of the DSL is to regulate data processing activities, safeguard data security, promote data development and usage, protect the legitimate rights and interests of individuals and entities, and safeguard state sovereignty, state security, and development interests. The most significant element of the law (Art. 21) is the establishment, by relevant government agencies, of a data classification and hierarchical protection system that categorizes data into different levels of protection according to the importance of the data in economic and social development, national security, and public interest and requires key protection for important data.

The jurisdictional scope of the rules does not include Hong Kong, Macau and Taiwan. The PIPL applies to entities outside PRC that provide products or services to China residents, and process China residents' personal information for "analyzing or assessing" their activities.

China does not have a single central data protection authority charged with enforcing privacy laws. The major regulators involved with possible issues regarding privacy laws include the:

- **Ministry of Industry and Information Technology (MIIT)** – regulates personal data collected and used in telecom and internet sectors
- **Ministry of Public Security (MOS)** – regulates internet security management and violations of personal information management
- **Office of the Central Cyberspace Affairs Committee (OCCAC)** and **Cyberspace Administration of China (CAC)** – regulates internet content monitor
- **National Health and Family Planning Commission (NHFPC)** – regulates medical records and population health information
- **State Post Bureau (SPB)** – regulates personal data collected and used in mailing and courier services
- **State Administration for Industry and Commerce (SAIC)** – regulates consumer personal information, except in areas or sectors where a specific authority has been given responsibility
- **State Bureau of Market Administration and Supervision (SAMR)** – regulates business activities of enterprises in Chinese market
- **National Information Security Standardization Technical Committee (NISSTC)** – sets the national standards of data security management

Last updated November 2021.