CLIENT ALERT

Employee Personal Information Protection in China – Are You Up to Speed?

Aug.25.2021

On August 20, 2021, China's national legislature passed the Personal Information Protection Law ("PIPL"), which will become effective on November 1, 2021. As China's first comprehensive system for protecting personal information, the PIPL is an extension of the personal information and privacy rights enshrined in China's Civil Code, and also a crucial element of a set of recent laws in China that seek to strengthen data security and privacy. Among other things, the PIPL sets out general rules for processing and cross-border transfer of personal information. A number of provisions, notably various obligations imposed on data processors, restrictions on cross-border transfer, and hefty fines, will have significant impact on multinational corporations' HR activities, including recruitment, performance monitoring, cross-border transfers, compliance investigations, termination of employment relationships, and background checks.

This alert will highlight specifically how the PIPL will apply to workplace scenarios in China and provide suggestions to help ensure data privacy compliance for multinational corporations' China labor and employment operations.

Employee Consent and Exceptions to Consent

Under Article 4 of the PIPL, "personal information" is defined broadly as information related to natural persons recorded electronically or by other means that has been used or can be used to identify such natural persons, excluding information that has been anonymized. Specific types of personal information have been noted for additional protection under Article 28 of the PIPL as "sensitive personal information". Sensitive personal information is defined under the law as personal information that is likely to result in damage to the personal dignity, physical wellbeing or property of any natural person, and includes, among others, information such as biometric identification, religious belief, special identity, medical health, financial account, physical location tracking and whereabouts, and personal information of those under the age of 14.

For an employer, in addition to the above sensitive personal information, the broad definition of personal information under the PIPL means that "basic information directly related to the labor contract" collected pursuant to requirements under the PRC Labor Contract Law will be subject to the PIPL. Although neither PIPL nor the PRC Labor Contract Law has clarified the scope of such "basic information", in practice, it generally includes an 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.

While employee consent is already a common approach (and explicitly provided for in the PIPL) for processing employee personal information in China, the legal basis for processing under Article 13 of PIPL is not limited to consent. Specifically, under Article 13 of PIPL, an employer is permitted to process personal information without consent from the employee when it is necessary for execution or performance a labor contract, for HR management according to the labor rules and regulations, and for response to a public health emergency such as the COVID-19 pandemic.

Additionally, under the following circumstances, the employer must obtain "separate consent" from an employee. Separate consent is not defined, but the language in the PIPL suggests that express consent for each specific purpose is required whenever the circumstance arises:

i. to provide personal information to a third-party personal information processor (Article 23); in the employment context this includes human resource service suppliers, background investigation agencies, insurance companies, etc.;
ii. to publicize an employee's personal information (Article 25), for example, in marketing or recruiting materials;
iii. to use an employee's personal image and personal identification information collected by image capturing and personal identification equipment installed in the public workplace (e.g., CCTV system in the workplace, facial recognition or iris identification access control system) for purposes other than maintaining public security (Article 26);
iv. to process sensitive personal information (Articles 28 and 29), which notably in the employment context may include biometric identification system for entry onto premises or access to IT equipment, location tracking on company issued devices, health information related to medical insurance or periodic health checks; and
v. to provide employees' personal information to overseas parties (e.g., overseas parent company/affiliates and global investigation agencies) (Article 39), which in the employment context can occur, for example, during internal audits and investigations, global mobility and employment transfers, sharing of online HR databases, M&A transactions, and global outsourcing.

Under the PIPL, an employee can only give consent in a clear and voluntary declaration of intent, under the premise of full knowledge. If the purpose or method of processing personal information has changed, the employer must seek such employee's consent again. For personal information that must be processed with consent, the employee has the right to withdraw such consent. However, the data processing made before the employee withdraws his/her consent will not be affected.

Cross-Border Transfer of Employees' Personal Information

Under Article 39 of the PIPL, when transferring documents and files with personal information of a Chinese employee to overseas parties, employers must seek a separate consent first from such Chinese employee and inform him/her of the name of the overseas recipient, contact information, purpose and method of processing, type of personal information to be transferred and procedures for the employee to exercise his/her rights stipulated under PIPL against the overseas recipient.

In addition to the separate consent, an employer providing employees' personal information outside China must meet one of the four conditions under at least one of the following conditions under Article 38 of PIPL:

i. Passing the security assessment of the Cyberspace Administration of China ("CAC") if the company is defined as a critical information infrastructure[1][1] operator or reaches the volume of personal information being processed as prescribed by CAC (such companies must store the personal information within the territory of China);
ii. Being certified by a recognized institution for personal information protection in accordance with the requirements of the CAC;
iii. Executing a cross-border transfer agreement (a standard template to be issued by CAC) with the recipient located outside China and ensuring that the processing meets the protection standards provided under PIPL; or
iv. Meeting other conditions prescribed by laws, administrative regulations, or CAC.

Notably under Article 41 of the PIPL, employers are not permitted to provide any personal information of employees stored within territory of China to any foreign judicial authorities or legal enforcement agencies unless approved by competent authorities in China.

The above requirements for cross-border transfers of employees' personal information will have significant impact on day-to-day human resources operations for multinational corporations. For example, it is not unusual for a multinational company operating in China to have a regional HR representative, not located in China, overseeing HR matters. Employers will need to consider specific strategies to enable those regional HR roles to continue their regular functions and take the necessary steps (such as obtaining separate consents from employees and executing cross-border data transfer agreements) to ensure compliance with the cross-border transfer of personal information requirements under the PIPL. The restrictions under Article 41 also add a new consideration for companies conducting audits and investigations on their employees in China, especially if such audits and investigations can lead to the involvement of legal enforcement agencies and/or judicial authorities.

Obligations of Employers and Enhanced Legal Liabilities for Violation

The PIPL does not provide any differentiation between personal information (or sensitive personal information for that matter) obtained from employees and other natural persons such as customers, vendors, employment candidates, or consultants. As such, general obligations on data processors under Articles 51 and 54 that include establishing internal administrative policies and operating procedures, implementing classified and hierarchical administration of personal information, taking technical security measures such as encryption and de-identification, making reasonable determination regarding permission for data processing, setting up contingency plans, providing regular security education and training for employees, and conducting regular audits of personal information processing activities, are also be relevant when processing employees' personal information. Although the PIPL does not explicitly indicate the minimum or maximum time limit for keeping personal information, Article 47 does require deletion of the personal information once the purpose of processing such personal information has been achieved or such purpose is no longer necessary. This requirement is also applicable to personal information collected from employees.

Similarly, Article 55 of the PIPL applies to employees' personal information. Under that provision, companies are required to conduct a risk assessment in advance and keep records, when processing sensitive personal information of employees, when making automated decisions using employees' or candidates' personal information, when entrusting a third party to process employees' or candidates' personal information or providing a third party with employees' and candidates' personal information and disclosing personal information, and when making cross-border transfers of employees' personal information. During such risk assessment, an employer will need to consider:

i. Whether the purpose and method of processing personal information are legitimate, justifiable and necessary;
ii. The impact on personal rights and interests, and the level of risks;
iii. Whether the security protection measures taken are legitimate, effective, and appropriate to the level of risks.

An employer is required to keep the risk assessment report and processing record for at least three years.

Violation of the PIPL can result in fines up to 50 million RMB or 5% of the preceding year's turnover of the company (which might be far more than 50 million RMB). According to Article 66 of PIPL, based on the seriousness of violation, competent authorities can also order suspension of business operations and revoke business licenses. Moreover, such a violation may be

recorded under the social credit system (a complex set of economic and social reputation rankings in China applicable to both individuals and companies) which will have significant negative impact, as the social credit record is crucial for license applications and approval procedures with authorities including China customs, foreign exchange, tax, and company registry. For individuals violating PIPL, they might be facing fines ranging between 100,000 RMB and 1 million RMB, and also be prohibited to act as directors, supervisors, senior executives, and persons-in-charge of personal information protection of the companies within a certain period of time.

Specifically, under Article 42, any overseas entities, organizations or individuals violating personal information rights and interests of Chinese citizens, or endangering national security or the public interest of China, may be placed on a blacklist by the CAC, and the CAC may take measures to restrict or prohibit the provision of personal information to such overseas entities or individuals.

Recommended Practices

Multinational companies are recommended generally to review current global and China data privacy policies to ensure compliance with the PIPL. Specifically, from the employment perspective, employers with operations in China should consider taking the following actions:

- Conduct a review of the flow of HR information from employees in China, including where personal information is stored and may be accessed, for the purpose of identifying any risks under the PIPL.
- Review any existing data privacy notices and consents from employees in China and assess whether those existing consents are sufficiently comprehensive in light of the requirements of the PIPL, especially if overseas transfer of employees' personal information is involved; if necessary, revise the data privacy policies and notice and consent templates, and obtain additional consents.
- In addition to any general data privacy training that may be provided to all staff, provide specific training on issues that may arise in relation to employees' personal information under the PIPL including any record-keeping requirements to managers and HR professionals in China to ensure compliance.
- When engaging third-party human resource suppliers to collect personal information of candidates or conduct background checks, request such suppliers to present their data protection policy and certify that they have obtained consent from individuals to process their personal information; if additional information is needed from a candidate that is beyond the scope of consent (especially for those not considered as abovementioned "basic information" but is essential for the position), seek additional written consent from such candidates.
- Consider additional strict protection measures for processing sensitive personal information (such sensitive personal information will very often be from employees) and only process sensitive personal information when there is a specific purpose and sufficient necessity; inform the employee of such necessity and possible impact on the employee's personal rights and interests.

Employers with operations in China will want to act now to secure a good understanding of their privacy practices in China and put into place processes and procedure to comply with the PIPL when it becomes effective on November 1, if not before. In addition, employers will need to track carefully how this law will be implemented and enforced and make potential adjustments to the policies they put into place. In developing and adjusting policies, employers will want to be attuned to the law, the spirit of the law and conditions on the ground in China.

Crowell & Moring will continue to follow the PIPL and compliance activities from our offices in China and the U.S.

---

[1] See article 2 of *Critical Information Infrastructure Security Protection Regulation*《关键信息基础设施安全保护条例》to be effective on September 1, 2021: key information infrastructure is referring to critical network infrastructures or information systems for public communications and information services, energy, transportation, water conservancy, finance, public service, electronic government affairs, national defense technology and industry, and other important industries and fields, whose destruction, loss of function or data leaks may cause severe damage to national security, to the national economy and Chinese citizens' livelihood, and to the public interest.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Nicole Janigian Simonian
Partner – Los Angeles, Shanghai
Phone: +1 213.310.7998
Email: nsimonian@crowell.com

Robert Holleyman
Partner and C&M International President & CEO – Washington, D.C.
Phone: +1 202.624.2505
Email: rholleyman@crowell.com

Jackson C. Pai
Counsel – Los Angeles
Phone: +1 213.310.7989
Email: jpai@crowell.com

Zhongdong Zhang
Senior Counsel – Shanghai
Phone: +86.21.8030.1688
Email: zzhang@crowellmoring.asia

Yi Huang
Counsel – Shanghai
Phone: +86.21.8030.1688
Email: yhuang@crowellmoring.asia

Aurora Zhang
Associate – Shanghai
Phone: +86.21.8030.1688
Email: azhang@crowellmoring.asia