HR compliance management: Measuring the impact of the upcoming Personal Information Protection Law of the People's Republic of China

September 2021
Issue 23

In brief

The *Personal Information Protection Law of the People's Republic of China* (the "PIPL") will become effective as of November 1, 2021.

In relation to HR management, the PIPL, adopted 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, imposes new obligations on enterprises. In order to ensure compliance with the law, we recommend that companies undertake a prompt assessment of the new provisions and make appropriate adjustments to their practices.

We set out below the key compliance issues under the PIPL in relation to HR management, and provide advice on real-world scenarios and actions by leveraging our extensive experience and expertise in HR compliance practice.

In detail

1. Is the PIPL applicable to your enterprise?

The answer is yes.

The law regulates the use of personal information. Almost every step of HR management involves the processing of personal information of employees. Each and every enterprise, therefore, as an employer, is a typical "processor" of personal information and should comply with the provisions of the PIPL. We have set out some examples of "processing" in question 3 below.

In addition, the PIPL has extraterritorial effects and may apply to an enterprise incorporated outside the PRC. To be specific, the analysis and assessment of the activities of data subjects, regardless of whether they are a Chinese citizen or a foreign worker, by an offshore parent or investor is governed by the PIPL. Therefore, domestic employers should also include their offshore affiliates in the scope of their compliance management framework in order to protect the personal information of their employees.

2. Which personal information is subject to PIPL protection?

The general personal information and sensitive personal information of a natural person are protected by the PIPL.

Taking recruitment and employment procedures as an example, an employer needs to collect the basic personal information of its employees, including the name, date of birth, ID card number, residential address, telephone number, educational background, work experience, bank account details, etc., all of which constitute

"personal information" as defined under the PIPL, i.e. "all types of information related to identified or identifiable natural persons recorded electronically or otherwise, excluding anonymised information."

In addition, an employer will commonly handle sensitive personal information relating to its employees. Examples of such sensitive personal information include, among others, health check reports required as part of the on-boarding process of employees, information about the underaged children of employees for the purposes of benefits management, medical records of employees for the purposes of sick leave management, fingerprint or facial recognition information of the employees for attendance check management, location tracking of employees for remote work management and epidemic prevention and control, etc. All the foregoing information is expressly defined under the PIPL as sensitive personal information.

3. What is the "processing" of personal information?

The "processing" of personal information under the PIPL means the performance of a series of acts and behaviours including the collection, storage, use, processing, transmission, provision, disclosure and deletion, etc. of personal information.

To facilitate understanding, we briefly summarise below some typical "processing" scenarios that may occur in HR management:

- **Collection** – direct or indirect acquisition of personal information, such as receiving candidates' CVs directly or through a head-hunter, or requiring the employees to fill out employment registration forms, etc.;
- **Storage** – storing personal information as required by law or for reasonable purposes, such as the retention of a candidate's background check results or the retention of personal file (a.k.a. P File) or salary information of employees;
- **Use** – applying, using, analysing and/or assessing the personal information, such as adding an employee's personal information to the employer's HR management system;
- **Processing** – compiling personal information according to a specific data format, such as to create an employee register or to calculate annual leave compensation or sick leave salaries, etc.;
- **Transmission** – transferring personal information within the company or to a third party within China or offshore, such as sharing personal information among different departments or to an offshore parent for human resource analysis and management;
- **Provision** – providing personal information to a third party, such as to the company's external advisors and service providers for the provision of professional individual income tax advice or payroll services; or providing the personal information of the employees or their family members to insurance companies in order to purchase commercial insurance for them;
- **Disclosure** – disclosing personal information to the public, such as disclosing employee CVs and work experience on the company's official website, marketing materials, etc.;
- **Deletion** – removing or deleting employees' personal information, such as disposing hard copies of their CVs and deleting the employees' electronic files from the company's online system or applications, etc.

4. How to ensure compliance?

The PIPL stipulates that employers must have a legal basis for processing an employee's personal information. The general rule is that individual consent must be obtained in order to legally process personal information. However, the PIPL provides six exceptions to the general rule which allows employers to legally process personal information without individual consent. The exceptions include processing an employee's personal information "where it is necessary for the conclusion or performance of a contract to which the individual concerned is a party" or "for carrying out human resources management in accordance with internal rules and policies or collective agreement, which are legally formulated under China law".

It is worth noting that the exception for "the implementation of human resources management" was included in the final version of the law but did not appear in prior drafts. From a practical perspective, this newly added exemption greatly reduces the time cost and management burden of obtaining consent from individual employees for the processing of personal information. However, employers should still be aware of the limitations of their right to process such personal information and ensure the fulfilment of all relevant compliance requirements by taking the following steps:

- insert consent provisions in the employment contract or collective agreement to ensure each employee has granted consent to the processing of their personal information;
- in respect of the processing of sensitive personal information, obtain specific and separate consent from the relevant employee;
- restrict the processing of employees' personal information only to the extent "necessary for human resources management";
- formulate internal rules and regulations by adopting employee consultation procedures and clearly define the rules and SOP of personal information management;
- categorise personal information appropriately and take all necessary security measures, such as encryption, de-identification, etc.;

- grant access permission/authorisation only to the necessary personnel within the enterprise for processing of personal information, conduct periodic security education and training for relevant staff; and
- develop contingency plans for personal information security incidents.

In practice, determining whether the use or processing of personal information without employee consent is "necessary for carrying out human resources management" has become a hot legal and management issue. In the period before more PIPL implementation rules are promulgated, we suggest that employers undertake a detailed steps review of their HR management, identifying policies and procedures that are missing, conducting an analysis of key steps that fall into the gap between PIPL and GDPR, assessing the particular challenges to which they may be exposed and drafting an improvement plan and incident contingency plan in advance.

5. How to process sensitive personal information?

An employer may process an employee's personal information in multiple steps during the entire HR management life cycle. For example, in the context of the Covid-19 epidemic, increasing numbers of employers have adopted flexible and remote working policies, resulting in employees being required to use office management software to record their day-to-day work assignments, whereabouts and primary work locations as a way to manage workflow and office attendance. As a result, employers will have access to a huge quantity of their employees' sensitive personal information.

The PIPL has set out additional requirements for processing sensitive personal information, including:

- **More specific purpose and sufficient necessity** – processing must only for a specific purpose with sufficient and justifiable reasons;
- **More stringent protection** – stricter protection measures must be taken; and
- **More open and transparent procedures** – subject to separate "inform-consent" procedures.

In terms of daily HR practice, employers are advised to categorise and review their existing internal management processes and related HR documentation and include the "inform-consent" step specifically for sensitive personal information as and when appropriate and necessary.

In processing sensitive personal information, employers should conduct an impact assessment regarding personal information protection beforehand and maintain appropriate records of such actions for at least three years. The records should contain the following detail: whether the purpose and method of processing personal information is lawful, legitimate and necessary; the impact on personal rights and interests and security risks; and whether the protection measures taken are lawful, effective and commensurate with the degree of risk.

6. How should cross-border personal information be processed?

The PIPL applies to the offshore processing of the personal information of natural persons located within the PRC under certain circumstances, including: (1) where the purpose is to provide natural persons within China with products or services; (2) where the activities and behaviours of natural persons within China are analysed and evaluated; and (3) other circumstances as prescribed by laws and administrative regulations.

In the HR context, there are two key circumstances in which personal information may flow cross-border: (1) where the personal information of domestic employees is stored on an offshore server and/or managed by the HR department of the offshore parent company; and (2) the personal information of overseas natural persons and their family members are provided to an onshore entity and/or delegated to an authorised domestic vendor for handling certain professional services. Both of the foregoing circumstances are subject to the PIPL. To be specific:

Transfer of personal information of PRC employees offshore

PRC companies which are part of a multinational group will frequently need to share employee information with their offshore parent company in order to accommodate the overall HR management requirements of the group. Such flow of information is important for offshore headquartered companies for talent management and to centralise HR costs. Such sharing of employee information will involve the cross-border transmission of personal information through the group HR management system or via day-to-day emails and attachments.

As mentioned in above, the PIPL requires employers to satisfy certain statutory conditions before effecting any cross-border transmission of personal information, such as obtaining approval from the relevant competent authority and executing standard contracts with overseas recipients, etc. In addition, notice must be given to the data subject of any cross-border transfer of their personal information. Such notice should contain sufficient detail of the information being transferred, as well as the reason for the offshore processing. The data subject should give their consent to such cross-border transmission.

Processing information of overseas staff in the PRC

Global mobility is a good example of a situation in which the cross-border transfer of employee's personal information will occur. The secondment of expatriates by overseas entities to work in China may involve direct processing of personal information of the secondees and their family members by its own China entity, or involve various third-party vendors to handle such information for tax, legal, commercial insurance, payroll, HR consulting services, etc.

In some cases, the overseas company may not have set up an independent HR team in China, or the China HR team is not authorised to participate in the information processing of foreign secondees and their family members due to business considerations. In that case, the overseas entities shall not only take into account the requirements for compliance with data protection and security laws in their own jurisdiction, but also proactively satisfy the compliance requirements under the PIPL.

In the context of cross-border data transmission generally, there is a lot of discussion as to whether an employer's day-to-day practices will require any prior assessment or authentication by the overseas entities for cross-border data transfer. We suggest that HR departments take the following steps: (1) carry out a comprehensive assessment of data security and compliance requirements for cross-border data transfers by collaborating with other departments within the company, paying particular attention to aspects such as data flow, information systems, fundamental data security protection capabilities and completeness of data security management systems; and (2) in order to ensure that each of the domestic and offshore entities is in compliance with all applicable local and offshore data security and personal information protection requirements, develop a compliance framework based on the specific scenarios of the cross-border processing of personal information of the employees.

7. What HR management challenges may be encountered?

As discussed above, employers need to follow the new requirements set out under the PIPL before processing an employee's personal information. Similarly, employees have been granted new rights under the PIPL in their capacity as data subjects, including the right to be informed, right to decide, right to restrict, right to refuse, right of access, right of data portability, correction and deletion, and the right to keep his/her personal information intact and accurate. As a result of these rights, we expect that employers will face multiple challenges to their HR compliance management once the PIPL becomes effective.

In order to manage their risks, employers should consider addressing the following questions in the context of their HR management cycle:

Recruitment

- How to make sure that CVs of job candidates are collected in a lawful manner?
- How to obtain the consent from candidates for the processing of their personal information prior to employment?
- If an employee is recruited via internal referral, how to properly make sure that the CV provided by the employment agency has been authorised by the referee?
- How to deal with CVs of candidates who are not ultimately recruited?
- If an employee is recruited through a third-party platform, how to define the respective rights and responsibilities between the employer and such third party?
- How to monitor and guarantee the level of compliance of a third party to reduce legal and reputational risks?

Pre-employment/Employment

- Is there any additional separate consent required from an employee if the employer wants to obtain a health check report from him/her?
- Is there any additional separate consent required from a candidate or an employee prior to conducting a background check?
- How to properly keep the employment materials submitted by a candidate/an employee, such as graduation certificate, ID card, qualification credentials, etc.?
- How to properly advise an employee of the necessity and means of processing his/her personal information during the term of his/her employment contract?

During employment

- What should an employer do to guarantee compliance if a real-time location tracking system or fingerprint/facial recognition attendance system is used?
- Can an employee refuse to use a real-time location tracking system or fingerprint/facial recognition attendance system?
- If the employee refuses to use such attendance system, how can the employer respond?
- In addition to sick leave certificates, can the employer require the employee to submit any other medical document as supporting material for sick leave approval?
- Does the employee have the right to refuse to submit any such relevant medical document?
- How can the employer make sure that all managerial staff having access to an employee's personal information act diligently?

- How should the employer respond to a data breach relating to the employee's personal information?
- How should the employer make sure that the employee's personal information is processed in a compliant manner when conducting investigations into violations?
- How should the employer properly manage personal information of expatriates received from its offshore affiliates? Is it necessary to clarify the right of use and limitations of each involved entity?
- Will the secondment of expatriates by offshore affiliates to China trigger any compliance requirements under the PIPL? How should the employer handle compliance?

Leaving/Post-leaving

- After the employee leaves, when should the employer delete his/her personal information?
- In what timeframe should the personal information be kept and removed?
- Does the employer have to cooperate with the departing employee if he/she requests for background checks or reference letters for the new employer? If so, how should the employer cooperate?

8. Compliance advice

As there is now less than one month until the official implementation of the PIPL, we suggest that employers take immediate action to assess the impact of the PIPL on the different steps of their HR management cycle, and develop the necessary action plan to comply with the new requirements. Below is a brief summary of the steps that should be taken by employers:

(1) Fully assess the current status of collection and management of employees' personal information, and identify the key steps in the HR management cycle that involves the processing of such information;
(2) Understand the typical scenarios in which employee's personal information is transferred cross-border (including inward and outward transfer);
(3) Review the existing rules and regulations and identify any gaps or weaknesses in compliance;
(4) Review all instances of collaboration between the company and third-party HR service providers and identify all situations in which personal information is processed by each party;
(5) Develop a data security compliance action plan based on the company's existing management practices;
(6) Update the company's privacy notices, relevant rules and regulations and HR contract templates to ensure compliance with the new requirements;
(7) Conduct training for all personal information processors within the company to educate them on the new legal requirements and management requirements.

We recommend that employers have the following compliance documents in place as best practice going forward in order to protect personal information:

- different versions of employee notice and consents to the processing of personal information, customised for different scenarios;
- privacy protection policies;
- rules and procedures for personal information processing;
- personal information protection and management policies;
- emergency plans for personal information security incidents; and
- internal training materials.

In addition, we recommend that HR departments collaborate with their company's data security compliance departments, such as legal, compliance, cybersecurity IT teams, to ensure consistency between the company's overall policies and their effective application in different human resources scenarios.

As the first law in China dedicated to the protection of personal information, the importance of the PIPL cannot be emphasised enough. HR and legal departments should pay close attention to the detail of the law, as well as future clarifications and interpretations.

In order to support our clients, we will keep a close eye on all subsequent regulations affiliated with the PIPL implementation, which may include provisions providing practical guidance. Further, we will monitor the expected judicial interpretations of the PIPL by the Supreme Court, as well as from local judicial authorities and relevant case precedents. We will continue to publish articles on this subject from time to time. If you wish to have an in-depth understanding of the PIPL or compliance advice, please feel free to contact us.

Let's talk

For a deeper discussion of how this impacts your business, please contact:

Rui Bai Law Firm

Vivienne Jin
Senior Counsel (Partner Equivalent), Employment
+86 (10) 8540 4646
vivienne.jin@ruibailaw.com

Ivy Zhang
Senior Attorney, Employment
+86 (10) 8540 4667
ivy.ja.zhang@ruibailaw.com

Barbara Li
Head of Corporate (Partner Equivalent)
TMT and Data Practice Lead
+86 (10) 8540 4686
barbara.xb.li@ruibailaw.com

Xin Bai Law Firm

Bin Qin
Head of Employment, Partner
+86 (21) 5368 4168
bin.b.qi@xinbailaw.com

Tiang & Partners

Martyn Huckerby
Head of Competition Law, Asia-Pacific (Partner Equivalent)
+852 2833 4918
martyn.p.huckerby@tiangandpartners.com

PwC China

Jacky Chu
China Global Mobility Services Leader
+86 (21) 2323 5509
jacky.chu@cn.pwc.com

In the context of this News Flash, China, Mainland China or the PRC refers to the People's Republic of China but excludes Hong Kong Special Administrative Region, Macao Special Administrative Region and Taiwan Region.

This China Tax and Business News Flash is issued by the **PwC's National Tax Policy Services** in Mainland China and Hong Kong, which comprises of a team of experienced professionals dedicated to monitoring, studying and analysing the existing and evolving policies in taxation and other business regulations in Mainland China, Hong Kong, Singapore and Taiwan. They support the PwC's partners and staff in their provision of quality professional services to businesses and maintain thought-leadership by sharing knowledge with the relevant tax and other regulatory authorities, academies, business communities, professionals and other interested parties.

For more information, please contact:

Long Ma
+86 (10) 6533 3103
long.ma@cn.pwc.com

Please visit PwC's websites at http://www.pwccn.com (China Home) or http://www.pwchk.com (Hong Kong Home) for practical insights and professional solutions to current and emerging business issues.

www.pwccn.com
www.ruibailaw.com
www.xinbailaw.com
www.tiangandpartners.com

pwc

瑞栢律师事务所
Rui Bai Law Firm

信栢律师事务所
Xin Bai Law Firm

Tiang & Partners
程偉賓律師事務所