COUNTRY COMPARATIVE GUIDES 2024

The Legal 500 Country Comparative Guides

Hot Topic | Employment and Labour Law

Employees' Personal Information Management Under Prc Personal Information Protection Law

Contributor

King & Wood Mallesons

Linda Liang

Partner | linda.liang@cn.kwm.com

Piao Liu

Associate | liupiao@cn.kwm.com

Chutian Wang

Associate | wangchutian@cn.kwm.com

EMPLOYEES' PERSONAL INFORMATION MANAGEMENT UNDER PRC PERSONAL INFORMATION PROTECTION LAW

A. Introduction

With the rapid development of technology and the digital economy, data protection has been attached with more and more importance and we have seen a number of legislative developments in this space in China in recent years. As the first law targeted at regulating the area of personal information protection in the People's Republic of China ("**PRC**"), the *PRC Personal Protection Law* ("**PIPL**") came into effect on 1 November 2021. PIPL, together with the *PRC Cyber Security Law* (effective on 1 June 2017), and the *PRC Data Security Law* (effective on 1 September 2021), collectively constitute the three fundamental and framework laws regulating cybersecurity and data security protection in PRC.

After the PIPL came into force for more than a year, it has come into play in various scenarios involving personal information processing, including employment-related scenarios where employers deal with the personal information of employees in the entire lifecycle of employee management. In addition, there have also been supporting rules and regulations coming out, providing more detailed guidance on personal information processing. In this article, we will introduce the main contents of PIPL and its key implications to the area of employment, together with the newly issued supporting rules.

B. Main contents of the PIPL

PIPL sets up comprehensive and systematic rules on the processing and protection of personal information. Below please find a summary of the main contents.

1. What is Personal Information

According to the PIPL, "Personal information" ("**PI**") refers to all kinds of information related to identified or identifiable natural persons that are electronically or otherwise recorded, excluding information that has been anonymized. In the employment-related scenarios, employee's PI includes but is not limited to his or her name, date of birth, identification number, residential addresses, phone numbers, email addresses, etc.

The PIPL also defines certain personal information as "sensitive personal information" ("**Sensitive PI**"), of which processing is subject to stricter regulations. Sensitive PI refers to the personal information, if being leaked or used illegally, may easily cause harm to the dignity of natural persons, or serious damage to the safety of individuals and properties, including information relating to biometric identification, religious beliefs, specific identities, healthcare, financial account, individual location tracking, etc., and personal information of minors under the age of 14.

2. What is Processing and what are the principles of PI processing

The processing of PI includes but is not limited to collection, storage, use, handling, transmission, provision, disclosure, and deletion of PI. The key principles of processing PI set by the PIPL are as follows:-

- Lawful, Transparent, Accurate, and Secured: PI shall be processed in accordance with the principles of legality, legitimacy, necessity, good faith, openness, and transparency. In addition, the quality and security of PI shall be guaranteed during the processing;
- With Specified Purpose: PI shall be processed for a specified and reasonable purpose. The processing shall be directly relevant to the processing purpose and in a manner that has the minimum impact on personal rights and interests;
- Minimized Collection: The collection of PI shall be limited to the minimum scope necessary for achieving the processing purpose and shall not be excessive;
- With Limited Retention Period: The retention period of PI shall be the shortest time necessary for achieving the processing purpose, except as otherwise provided by any law or administrative regulation.

3. Rules of PI processing

The PIPL sets out specific requirements in terms of legal grounds for PI processing (individuals' consents as the principal legal ground), rules for processing Sensitive PI, consent requirements, sharing PI with third parties, PI outbound transfer, PI retention, etc. We will explore the specific requirements and implications in the employment-related scenarios in the Section C "Management and Protection of Employees' PI" below.

4. Legal Liabilities

PI processors who violate the PIPL regarding their PI processing will be subject to the following legal liabilities:-

- Civil liabilities: Presumption of Fault & Public Interest Lawsuit

Individuals can file lawsuits against PI processors according to the *PRC Civil Code* claiming infringement on PI. As provided by the PIPL, the burden of proof for such cases is on the PI processor to prove that it is not at fault. Otherwise, the PI processor shall be liable for damages and other civil liabilities.

In addition to civil lawsuits filed by individuals, where PI processors violate the requirements under the PIPL during PI processing and infringe the rights and interests of multiple individuals, the People's Procuratorate, consumer organizations prescribed by the laws, and organizations determined by the state cyberspace authorities may file lawsuits.

- Administrative Liabilities: Huge amount of fines for violations & liabilities for responsible person

Competent PI protection authorities can also issue orders for rectification, warnings, and confiscate unlawful income against PI processors for violations of PIPL. In the case of failure to rectification, fines can be imposed on PI processors (up to RMB 1,000,000) and the person in charge who is directly

responsible and other personnel who bear direct responsibility (from RMB 10,000 to RMB 100,000).

For serious violations, in addition to rectification and confiscation of unlawful income, a fine of up to RMB 50,000,000 or 5% of the turnover for the previous year can be imposed. In addition, the person in charge who is directly responsible and other personnel who bear direct responsibility shall be liable to a fine between RMB 10,000 and RMB 100,000.

- Criminal Liabilities: the PIPL refers to *PRC Criminal Law* for relevant behaviors constituting crimes. According to *PRC Criminal Law*, fines and/or up to 7 years of imprisonment can be imposed for illegally acquiring, selling or providing PI to third parties.

5. Rights of PI Subjects

The PIPL provides PI subjects with a number of rights, including the right to access and copy their PI; rectify their PI; have their PI erased; withdraw their consent to PI processing; restrict the processing of their PI; object to the processing of their PI; and object to the use of automated individual decision-making.

6. Others

The PIPL also provides the following aspects of regulations: 1) specific requirements for state organs and critical information infrastructure operators ("**CIIO**") processing PI, and PI processors that process PI beyond a specific amount threshold (not crystal clear but may refer to the standard listed in the newly issued *Measures for the Standard Contract for Outbound Transfer of Personal Information*, please refer to Section C, point 4 below for details); 2) obligations of PI processors to establish a comprehensive PI protection mechanism including but not limited to formulating internal management policies and operation process, classifying PI, adopting security technical measures, etc.; 3) requirements for local storage and establishing special institutions or designating representatives within PRC under certain circumstances, etc.

C. Management and Protection of Employees' PI

1. Legal Grounds for Processing Employees' PI

a) Legal grounds for processing PI

According to the PIPL, PI can only be processed based on one of the following seven lawful grounds:

- The individual's consent has been obtained;
- The processing is necessary for the conclusion or performance of a contract to which the individual is a contracting party or for conducting human resource management under the employment rules and regulations legally established and collective contracts legally concluded;
- The processing is necessary to fulfil statutory functions or statutory obligations;
- The processing is necessary to respond to public health emergencies or protect the life, health or property safety of natural persons under emergency circumstances;
- PI is processed within a reasonable scope to conduct news reporting, public opinion-based supervision, or other activities in the public interest;

- The PI that has been disclosed by the individuals themselves or other PI that has been legally disclosed and is processed within a reasonable scope in accordance with the PIPL; or
- Under any other circumstance as provided by any law or administrative regulations.

2) Is employees' consents a "must" for processing their PI?

Among the above grounds for lawful processing PI, the grounds most related to employment are the first two grounds: "consent" and "necessary for conducting human resource management". As "necessary for conducting human resource management" alone is a legal ground for processing PI, if the PI is necessary for conducting human resource management, such PI can be processed without the employees' consent.

However, the PIPL does not stipulate specific standard for determining what constitutes "necessary for conducting human resource management". To date, it also lacks clear standard for reference in practice. For example, some employers may understand that employees' fingerprints are necessary for daily check-in for the purpose of attendance management and thus are "necessary for conducting human resource management". By contrast, others may argue that there are other alternative ways for achieving this purpose, and therefore it is not "necessary".

Considering that there are uncertainties in determining whether it is "necessary for conducting human resource management", at the current stage, it is suggested that it is better for the employers to try to obtain consents from the employees for PI needed in the first place. The employers can adjust the scope of PI necessary to obtain consents from the employees accordingly if detailed rules and/or standards in practice later come out in the future.

3) What is a sufficient "consent"

In order to meet the standards of "consent" as required by the PIPL, the consent shall be voluntarily and explicitly given by the individual on a fully informed basis. The PI processor shall truthfully, accurately and completely inform individuals of the following matters ("**Items to Inform**") in a conspicuous way and in clear and easily understood languages:

- The name and contact information of the PI processor
- Purposes and methods of processing the PI, categories of PI to be processed, and the retention periods
- Methods and procedures for individuals to exercise the rights provided by PIPL; and
- Other matters that should be notified as provided by laws and administrative regulations.

The PIPL also requires "separate consent", which is a form of consent with higher requirements, under the following circumstances:

- Providing PI to third parties;
- Disclosing PI to the public;
- Processing Sensitive PI;
- Installing personal images and identification information collecting devices in public places for purposes other than public security; and
- Outbound transferring PI.

The specific requirement and form of Separate Consent is not specified by the PIPL. Based on the current understanding and practice, in order to constitute a Separate Consent, the specific item involving PI processing should be listed as a separate item requesting the individual's specific consent explicitly to this item, instead of being hidden in a package of items pending for obtaining individual's consent altogether.

In light of the above, it is suggested that a consent letter be signed by the employee, specifying the contents listed above as required by the PIPL to obtain employees' consents, including separately listed the items requiring separate consent.

For example, if the employer needs to process employees' Sensitive PI, it is suggested to be explicitly listed in the consent letter that "the employee agrees that his/her Sensitive PI (a definition or list can be included) will be collected and processed by the employer for specific purposes (to be specified)".

2. Processing Employees' Sensitive PI

Employers may process abovementioned Sensitive PI of employees during the employment process, such as when employers use fingerprints or face identity information for daily check-in, collecting employers' health-related information for insurance purposes, etc.

According to the PIPL, the following requirements shall be met for processing Sensitive PI:

- The process shall be with specific purposes and sufficient necessity and strict protection measures shall be taken;
- Apart from the Items to Inform, Inform individuals of the necessity of the processing Sensitive PI and the impacts on individuals' rights and interests;
- Obtain separate consent; and
- Conduct Personal Information Protection Impact Assessment ("**PIPIA**").

3. Sharing Employees' PI to Third Parties

The PIPL sets further requirements for sharing PI to third parties. The most relevant employment-related scenarios include engaging third parties in background checks, recruitment, payroll services, and labor dispatch, etc.

The PIPL differentiates third parties into "joint PI processor" and "entrusted PI processor" based on whether the third-party PI processor independently determine the processing purpose and processing method. For entrusted PI processor, it only processes the PI in accordance with the processing purpose and processing method determined by the entrusting PI processor.

When entrusting a third party to process PI on behalf of the employer, an agreement shall be entered into between the employer and the entrusted party to specify the purposes, duration and means of processing, categories of PI and protection measures, as well as rights and obligations of both parties, etc.

For sharing employees' PI to third party processors, apart from the Items to Inform, the employer shall also inform the employees of the recipient's name, contact information, purposes and methods of

processing, categories of PI, and obtain the employee's separate consent.

4. Outbound Transferring Employees' PI

Outbound transfer of employees' PI is not rare in practice, especially for multinational employers sharing employees' PI within the global management system. Considering the special nature of outbound transfer, the PIPL sets detailed requirements in this regard including:

- Any one of the following three requirements ("**Outbound Transfer Approach**") shall be met: 1) security assessment organized by National Cyberspace Department ("**Approach 1**"); 2) certification by a specialized agency for protection of personal information in accordance with the provisions of the National Cyberspace Department ("**Approach 2**"); or 3) entering into the standard contract formulated by the National Cyberspace Department with the overseas recipient ("**Approach 3**");
- Apart from the Items to Inform, inform the employee the name of the overseas recipient, contact information, purpose and method of processing, type of PI and the method and procedure for the individual to exercise the rights stipulated in PIPL against the overseas recipient;
- Obtain the data subject's separate consent; and
- Conduct PIPIA.

For the Outbound Transfer Approach listed in the first bullet point above, on February 24, 2023, PRC Cyberspace Administration issued the *Measures for the Standard Contract for Outbound Transfer of Personal Information* ("**Standard Contract Measures**"), with the template of standard contract for outbound transfer of PI ("**Standard Contract**") as its annex (which will come into effect on June 1, 2023). The Standard Contract Measures, together with the *Measures for Data Outbound Transfer Security Assessment* (effective on 1 September 2022) and *Implementing Rules on Personal Information Protection Certification* (effective on 4 November 2022), collectively provide more detailed guidance on each of the Outbound Transfer Approach.

In practice, many employers will consider adopting Approach 3 (entering into standard contract). According to the Standard Contract Measures, for a PI processor to apply Approach 3 in outbound transfer, the following conditions shall be met by the PI processor simultaneously:

- It is not a CIIO (where Approach 1 shall be adopted according to Article 40 of the PIPL);
- It has processed the PI of less than one million individuals; and
- It has provided the PI of less than 100,000 individuals on a cumulative basis to overseas recipients since January 1 of the previous year; and
- It has provided the Sensitive PI of less than 10,000 individuals since January 1 of the previous year.

In addition, the PI processors shall enter into Standard Contract in strict accordance with the template (may agree upon other terms while should not conflict with the terms of the template), and shall file the Standard Contract (together with the PIPIA report) with the provincial cyberspace authority within 10 working days from the effective date of the Standard Contract.

5. Retaining Employees' PI

According to the PIPL, the retention period of PI shall be the shortest time necessary for achieving the processing purpose though the specific length of the retention period is not specified. It is suggested that employers decide the retention period according to the type of PI and the specific stage in the employment lifecycle.

- Before Employment

For candidates during the recruitment process, considering that the purpose of collecting their PI shall be to assess their eligibility, only the PI related to such purpose shall be collected and such PI shall be deleted if the candidate is not selected. Some employers may retain relevant information of such candidates even if they are not selected, as standby for future recruitment. According to the PIPL, it is suggested to obtain consents from the candidates. In addition, under such circumstances, it is suggested to cease any processing of PI other than storing and taking necessary security protection measures for such information.

- During Employment

For management purposes, PI of employees can be retained throughout the whole process of employment subject to other processing requirements as stipulated by the PIPL.

- Termination

Under PRC employment laws, the employer shall preserve the employment contracts for not less than two years for reference purposes after termination of the employment relationship. The employer shall also preserve records relating to salary payment, including the payment amount, date, receiver's name, and signature for not less than two years.

Other than the abovementioned PI, although main purposes of retaining employees' PI have been achieved upon the termination of employment, there are certain scenarios where it may also be reasonable for the employers to retain some type of employee's PI. For example, employers may need to retain relevant PI for purposes such as cooperating with prospective new employers of the ex-employees in conducting background checks, reviewing the employee's rejoining, for possible labor disputes arises in the future, etc.

Considering that the PIPL sets stronger protection for sensitive PI, it is suggested that employers delete Sensitive PI of ex-employees such as fingerprints and face identity information (as check-in is no longer needed). For other PI of ex-employees, it is suggested that the employers only keep PI based on legal grounds (better to obtain consent from the employees), and set a reasonable period for such retention.

D. Conclusion

With the PIPL and its supporting rules and regulations coming into force, employers have been facing more requirements and challenges in processing employees' PI and carrying out daily work. Employers are suggested to upgrade relevant HR operations and follow the best practices where possible to ensure its processing of employees' PI is compliant with the PIPL.

It is also expected to see developed practices related to employees' PI protection together with further

detailed interpretation and guidance from relevant authorities as time goes on, and employers shall be able to gradually find a better balance between the management of employees and the protection of employees' PI.

Author 1 Name: Linda Liang

Job Title: Partner

Tel: +86 010 5878 5161

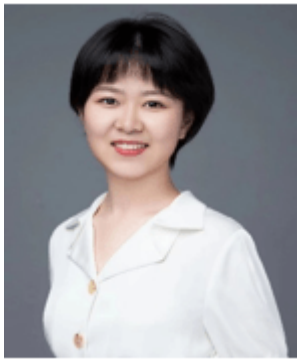
Email: linda.liang@cn.kwm.com

Author 2 Name: Piao Liu

Job Title: Associate

Tel: +86 010 5878 5698

Email: liupiao@cn.kwm.com



Author 3 Name: Chutian Wang

Job Title: Associate

Tel: +86 010 5661 2451

Email: wangchutian@cn.kwm.com

Contributors

Linda Liang
Partner
linda.liang@cn.kwm.com

Piao Liu
Associate
liupiao@cn.kwm.com

Chutian Wang
Associate
wangchutian@cn.kwm.com