中倫律師事務所
ZHONG LUN LAW FIRM

Core Issues When Processing Employees' Personal Information（Q&A）

By Peng Cai, Yunlang Hu, Yangyang Su

Key Words:

Multinationals, Human Resource Management, Personal Information Protection

Abstract:

This article answers 10 frequently asked questions about how to process employees' personal information for multinational corporations.

Nowadays, how to ensure compliance with laws when using human resources ("HR") is a hot topic for multinational corporations ("MNCs"). Since the *Personal Information Protection Law of the PRC* ("PIPL") came into effect in 2021, a series of new compliance requirements have been put forward for MNCs processing employees' personal information in the context of HR management, posing fresh challenges for meeting the needs of centralized HR management under the framework of the PRC laws. It's a relief that the recent development of legislation has provided some much-needed answers, and we will look at ten frequently asked questions about processing employees' personal information based on such new development for MNCs to consider.

Q1: How to understand the cross-border processing of employees' personal information?

(1) What kind of information qualifies as employees' personal information?

According to Article 4 of the PIPL, personal information refers to all kinds of information related to identified or identifiable natural persons recorded by electronic or other means, excluding the information processed anonymously. The definition of "personal information" is inclusive and contains rich connotations. According to the

national standard *Information Security Technology Personal Information Security Specifications*, personal information may also include:

i. basic information of an individual (*name, date of birth, gender, nation, nationality, family ties, home address, personal phone number, email address, etc.*);
ii. identification information of an individual (*ID card, passport, etc.*);
iii. biometric information of an individual (*recognizable facial features, etc.*);
iv. information concerning the health and psychological status of an individual (*height, weight, vital capacity, illness, etc.*);
v. information concerning the education and work of an individual (*diploma, degree, educational background, work experience, training records, transcripts, etc.*);
vi. information concerning personal property (*bank account, real estate information, credit information, etc.*);
vii. information concerning online identification symbols, contact information, individual's internet surfing records, information concerning the commonly used devices by individuals, location information, etc.

In practice, by collecting resumes and registration forms when recruiting, corporations often get access to candidates' basic information, contact information, information concerning education and work experience, information concerning personal property, etc.; through pre-employment medical examinations, corporations often collect information concerning the health and psychological status of candidates; and biometric information of employees may also be collected through daily HR management.

Notably, some employees' personal information may fall within the scope of "sensitive personal information". Article 28 of the PIPL defines sensitive personal information as the personal information that is likely to result in damage to the personal dignity of any natural person or damage to his or her personal or property safety once such information is disclosed or illegally used, including such information as **biometric identification, religious belief, specific identity, medical**

health, financial account, whereabouts, movement as well as the personal information of minors under the age of 14. Employees' personal information collected by corporations such as pre-employment medical examination reports, criminal records, religious beliefs, birth information, information on children under the age of 14, ID cards, social security cards or residence documents, credit information, fingerprints, iris recognition information, facial details, whereabouts, bank accounts, and payrolls, probably will fall into the category of "sensitive personal information". The PIPL and relevant laws and regulations set a higher bar for processing sensitive personal information (such as obtaining "separate consent" from personal information subjects).

In summary, to understand the personal information of employees, corporations should understand the connotation and scope of "personal information" defined by PRC laws and regulations, and at the same time, sort out what kind of personal information (sensitive or not) will be processed under each of the specific scenarios when recruiting and managing employees.

(2) How to Understand the "Cross-border Provision of Personal Information" ("CPPI")?

The PIPL does not clearly define what constitutes CPPI. Under the current legislation, CPPI can be dissected from two perspectives :(1) CPPI means processing activities that occur overseas and concern the personal information of natural persons within the Chinese mainland; (2) CPPI means the situations of providing specific personal information generated within the Chinese mainland to overseas recipients. The following scenarios will probably be deemed as CPPI under current PRC laws and regulations:

- providing personal information to entities within the Chinese mainland, but such entities are not subject to or registered under PRC laws.
- accessing and viewing personal information by overseas institutions, organizations, or individuals (with the exception of public information and web

page browsing), despite that such personal information has not been transferred or stored outside the Chinese mainland.

- transferring the internal data of the network operator group to overseas recipients, which involves personal information collected and generated in the course of domestic operations.

The following scenarios may not fall within the scope of CPPI:

i. Exporting personal information that is not collected and generated in the course of domestic operations will not be classified as CPPI, provided that such information has not been altered or processed in any way.
ii. Exporting personal information that is not collected and generated during domestic operations despite being stored and processed within the Chinese mainland. Such export shall not in any fashion concern personal information collected and generated in the course of domestic operations.

Due to rapid changes to laws concerning this sector, the above analysis of CPPI may be subject to adjustment, particularly when the implementation rules of the PIPL are promulgated.

Q2: Whether an overseas importer's remote access to the employees' personal information storage systems (the "System") of domestic exporters constitutes CPPI under PIPL?

Based on the analysis in Q1, we can find that overseas importers' remote access to the System of domestic exporters will be deemed as CPPI and therefore governed by the PIPL. According to Article 4 of the PIPL, the processing of personal information includes the collection, storage, use, processing, transmission, provision, disclosure, deletion of personal information, etc. Even if an overseas importer merely accesses the System, the "access" is very likely to be deemed as the processing ("use") of domestic employees' personal information, thus falling into the scope of CPPI. Whether based on the context of the PIPL or the interpretation of other relevant laws

and regulations, it is likely to be treated as CPPI when overseas importers access the System of domestic exporters through API interfaces or other means.

Q3: How to understand the legal basis for processing personal information as "*necessary for the conclusion or performance of a contract to which the individual concerned is a party, or for the implementation of human resources management in accordance with the labor rules and regulations formulated in accordance with law and collective agreement practices conducted in accordance with law*" in Article 13 of the PIPL?

When processing personal information, a processor must obtain at least one of the seven "legal bases" listed in Article 13 of the PIPL, of which: "(2) [O]r for the implementation of human resources management in accordance with the labor rules and regulations formulated in accordance with the law and the collective agreement practice conducted in accordance with law[.]"(the "Second Legal Basis") Combined with the relevant provisions of the *Labor Contract Law*, this legal basis can be understood from the following two perspectives:

(1) Understanding the necessity to process personal information for the implementation of human resources management in accordance with the labor rules and regulations formulated in accordance with the law: per Article 4 of the *Labor Contract Law*, when an employer formulates, revises, or decides on rules or major matters pertaining to labor remuneration, working hours, rest periods and days off, labor safety and health, insurance and welfare, staff training, labor discipline, and labor quota administration, etc., which directly involves the vital interests of employees, such matters shall be discussed by the employees' congress or all-staff meeting at which employees will make proposals and give their opinions and the employer shall carry out negotiation with the labor union or employee representatives on an equal footing before making a decision. Employers shall announce decisions on rules and major matters which directly involve the vital interests of employees or notify the employees. In another word, to be recognized as effective by PRC laws, employment policies or handbooks shall be enacted through the specific democratic negotiation process,

during which the content of the employment policies or handbooks shall be circulated to the employees, so as to protect their right to be informed, and the final version of the employment policies or handbooks shall include the feedbacks resulting from the full deliberation by the representative employees' congress or the all-staff meeting. To understand "necessary for human resources management", specific items regulated under the employment policies or handbooks should be examined on a case-by-case basis, and corporations should ensure that personal information processing is strictly in accordance with the scope agreed in a particular employment policy or handbook. Exceeding the scope authorized by such policy or handbook will result in forfeiting the Second Legal Basis. For example, when a corporation implements a policy on remuneration through a proper democratic negotiation process, and such policy requires the collection of information such as an employee's name and seniority, such collection should not go beyond the set scope to collect age or gender information, as doing so would compromise the applicability of the Second Legal Basis for personal information processing.

(2) Understanding the necessity to process personal information for human resources management in accordance with the collective agreement practices concluded in accordance with the law: according to Chapter 5, Section 1 of the Labor Contract, the collective agreement usually refers to a contract concluded by a labor union on behalf of the employees with the employer through equal negotiation on matters such as remuneration, working hours, rest periods and leave, labor safety and health, insurance, welfare, etc. A draft collective agreement shall be submitted to the employees' congress or all-staff meeting for discussion and adoption. In practice, collective agreements are often found in certain industries such as construction, mining, and catering. Similarly, to implement human resources management under the collective agreements, it is necessary to pay attention to the personal information required to be processed under the matters specified in the collective agreement (such as labor remuneration, working hours, rest periods and days off, labor safety and health, insurance, and welfare, etc.), and personal information beyond the agreed scope must not be processed.

It should be noted that "consent" is one of the seven legal bases, however, "separate consent" is not listed as an independent legal basis in the PIPL, but as a special form of "consent". Therefore, according to the relevant provisions of Article 13 of the PIPL, if an employer can base personal information processing on the Second Legal Basis, it is not required to obtain "consent" or "separate consent" for processing employees' personal information.

Q4: Where a domestic corporation provides an employee's personal information to an overseas corporation, how should the domestic corporation obtain the employee's separate consent?

Per Article 39 of the PIPL, to provide the personal information of an individual to an overseas importer outside the Chinese mainland, the personal information processor shall inform the individual of matters such as the name and contact information of the overseas importer, purpose and method of information processing, type of personal information and the method and procedure for the individual to exercise the rights stipulated herein against the overseas importer, and shall obtain the individual's separate consent. "Separate consent" can be comprehended from the following perspectives:

(1) Standard to acquire the "separate consent". The standard for obtaining separate consent shall not be set lower than the required standard for obtaining "consent", that is, the personal information processor shall fully inform the individual of the methods, purposes, rules, and so forth for processing the personal information, and such consent shall be given by the individual voluntarily and explicitly under the condition of full knowledge. The personal information processor shall also ensure that individuals can withdraw their "consent" conveniently, and it is necessary to re-acquire an individual's "consent" if the original purpose or method of processing personal information is changed.

(2) Method to acquire the "separate consent". The method for obtaining separate consent shall be "voluntary" in nature. According to Article 4 of *Provisions of the Supreme People's Court on Several Issues concerning the Application of*

Law in the Trial of Civil Cases involving the Processing of Personal Information Using Facial Recognition Technology, consent acquired through methods such as coercion, disguised coercion, threatening not to provide services or products, bundled authorization will not be deemed as the proper ways of acquiring "separate consent".

Based on the above analysis, if a domestic exporter provides employees' personal information to an overseas importer, the domestic exporter should first make sure whether "separate consent" is required. To satisfy the required standard and method of acquiring personal information, and for the sake of good practice, the corporations should also formulate specific SOPs, set up the authorization channels for acquiring consent, and assign special personnel to ensure the proper exercise of rights by the personal information subjects.

Q5: What kind of assessment should a domestic exporter carry out before providing employees' personal information to an overseas importer?

Based on the PIPL, *Measures for Security Assessment of Cross-border Data Transfer (the "Measure"), Safety Certification Specifications for Personal Information Cross-border Processing Activities (the "Rules")* and other regulations, a domestic exporter shall carry out the following assessment work before providing employees' personal information to an overseas importer:

1. *Complete the personal information protection impact assessment.* According to the PIPL, personal information processors shall conduct personal information protection impact assessment before providing personal information to an overseas importer and shall keep a record of such assessment. The personal information protection impact assessment should at least cover the following items:

   i. assessing whether the purpose, method, or any other aspect of personal information processing is lawful, legitimate, necessary, and in compliance with the principle of good faith;

ii. assessing the impact on personal rights and risk of a security breach in CPPI scenarios. It is necessary to assess overseas legal environment in terms of personal information protection, as well as the security mechanism of the recipient and related parties;

iii. assessing whether any security protection measure taken is lawful, effective, and commensurate with the risk level;

iv. retaining the personal information protection impact assessment reports and the processing records for at least three years; and

v. assessing whether the data is at the risk of being leaked, damaged, tampered with, abused, or subject to other risks after being provided to overseas recipients or retransferred, and whether the individuals have a smooth channel to protect their rights and interests concerning their personal information.

2. *Complete the assessment per different CPPI mechanisms.* Article 38 of the PIPL provides three specific mechanisms for CPPI concerning employees, which are (i) completing the security assessment by the national cyberspace authority; (ii) getting a certification of personal information protection; and (iii) entering into a standard contract in the form and substance as provided by China's competent cyberspace authority. In addition to the three, Article 38 also allows mechanisms permitted by other laws or regulations. In general, the applicability and scope of each of the three mechanisms are different, and the assessment work to be completed under each mechanism overlaps but differs from the PIA required by the PIPL (more details will be introduced below). Since regulation regarding the standard contract has not come into effect (currently at the draft for comment stage) and no additional mechanism has been provided by other laws and regulations, this article only provides an introduction to the assessment work involved in security assessment and certification of professional institutions.

(1) *Complete the security assessment.* In accordance with Articles 38 and 40 of the PIPL and Article 4 of the Measures, operators of critical information infrastructure ("CIIO") collect and generate personal information in the

course of operations within the Chinese mainland, and personal information processors who process personal information of no less than one million individuals, accumulatively provide more than 100,000 individuals' personal information or more than 10,000 individuals' sensitive personal information shall pass a security assessment before providing personal information overseas. The security assessment shall combine risk self-assessment and security assessment. More specifically:

- To carry out risk self-assessment, the domestic exporter shall analyze whether the contract, which involves personal information, with the overseas importer has fully stipulated the security protection obligation, and the data export risk self-assessment report shall also be duly retained.
- Prepare and submit required materials, following legal procedures to complete a data export security assessment conducted by the national network information department through the provincial-level Cyberspace Administration of China where the exporter is located and pass the assessment.

It should be noted that CIIO usually refers to a player in critical industries and fields involving public communications and information services, energy, transportation, water conservancy, finance, public services, e-government, and the national defense science and technology. If a corporation intends to provide abroad employees' personal information which belongs to an industry or business type that may fall into the scope of CIIO, it is recommended that such corporation complete a security assessment in advance. At the same time, if a corporation, whether a CIIO or not, intends to provide a large number of employees' personal information or employees' sensitive personal information due to its business nature (such as cross-border labor dispatch services), it should also complete the security assessment required by laws and regulations. Conversely, if the corporation is micro or start-up and does not involve a particular industry or service type, it is not necessarily required to

complete a security assessment when providing employees' personal information across borders.

(2) *Complete personal information protection certification*. Under the Rules, non-CIIOs or entities that do not process employees' personal information or sensitive personal information that exceeds certain volume may choose to obtain personal information protection certification for CPPI scenarios. If an entity chooses to get greenlighted to provide employees' personal information across borders through this mechanism, we recommend that the following assessment work be completed:

i. *Clarifying the responsibilities of the subjects.* If an MNC or a single economic or business entity is formed between a domestic entity and a foreign entity that provides employees' personal information across borders, the domestic entity may apply for certification and bear legal liability. If the domestic entity and the overseas entity belong to different organizations, we recommend that the overseas entity set up a special agent or appoint a representative within the Chinese mainland to complete the certification.

ii. *Assessing whether the statutory principles are complied with during the cross-border provision of employee information.* Where an entity provides employees' personal information across borders, it must assess whether it complies with the following principles:

- *The principles of legality, propriety, necessity, and good faith*. whether the entity has adopted a method that has minimal impact on the rights and interests of employees whose personal information is to be processed;
- *The principle of openness and transparency.* Whether the process of cross-border processing of an employee's information is public and transparent, and whether the employee is promptly informed of the purpose, scope, and method of cross-border provision of personal information;

- *The principle of information quality*. Whether the parties can ensure the accuracy and completeness of personal information in the process of providing employee information across borders;
- *The principle of equal protection.* In the process of cross-border processing of employee information, whether the parties can ensure that the handling of personal information complies with the standards set by relevant laws and regulations of China on the protection of personal information.

iii. *Assessing whether the cross-border provision of employee information meets the basic requirements.* Where an entity provides employees' personal information abroad, it must assess whether it meets the following basic requirements:

- *Legal binding documents*: whether the parties have signed a document with legal binding and enforcement power. The legal documents shall clearly state that the parties involved in cross-border processing of employees' personal information, the purpose, and scope of processing, what measures to take to protect the rights and interests of personal data subjects, and the commitment to abide by unified personal information processing rules and ensure that their level of protection is no lower than the relevant provisions of PRC laws and regulations, and subject to the supervision and legal jurisdiction of certifying bodies;
- *Organizational management.* Whether there is a person responsible for cross-border provision of employees' information, and whether the person in charge is a member of the decision-making body of the entity and has clear responsibilities. Whether each relevant party has established a special protection agency to fulfill the obligation to protect employees' personal information and prevent its leakage, falsification, and loss;

- *Cross-border processing rules.* Whether domestic exporters and overseas importers conducting CPPI have set up and followed unified rules for handling personal information. Whether the content of the unified rules includes the basics (type, sensitivity) of employees' personal information; the purpose, method, and scope of the processing; the start and end of processing time and the processing method after the expiration of employees' personal information if it is stored overseas; whether cross-border processing of employees' personal information needs to be transferred through more than one regions or countries, and if so, which regions and countries; resources and measures taken to protect the rights and interests of employees' information subjects; rules of compensation and handling in case of security incidents;
- *Personal information impact assessment.* The Rules list detailed PIA requirements for this mechanism which differs from the PIA requirement in PIPL. Under this mechanism, we suggest the domestic exporters and the overseas importers assess whether the legal regime of the country or region where the employees' personal information is imported can guarantee effective protection for such information and whether the overseas importer's network environment can provide effective protection for the rights and interests of the employees who own such personal information;
- Notably, regulation for the mechanism of the Standard Contract is expected to be released soon. And by now, the draft regulation requires corporations to conduct PIA distinguishable from the PIA under PIPL before executing a template Standard Contract for CPPI.

Q6: What should the domestic corporation inform the employee of before CPPI?

Before CPPI of employees' personal information, the domestic corporation shall:

i. Inform employees of the purpose, scope, and processing method of CPPI, and ensure that employees understand all the procedures for processing their personal information.

ii. Inform the relevant parties involved in the CPPI of measures being taken to protect the rights and interests of employees' information subjects and the rules for processing personal information to be complied with. Additionally, the entities accountable for the processing in the Chinese mainland should also be specified.

iii. Inform employees of how to exercise their rights as the personal information subjects, as well as how the entities will respond to their requests in this regard; per the request of the employees, corporations should:

- provide legal documents signed with the employees during CPPI;
- put in place an unblocked channel for the employees to exercise their statutory rights as Personal Information Subjects; and
- provide copies of legal documents concerning the rights of the employees.

iv. If a corporation rejects an employee's request, it shall explain the reasons and provide remedies.

v. For the special notification obligation for employees' sensitive personal information, please refer to Question 9.

Q7. What should be stipulated in the contract entered into by and between a domestic exporter and an overseas importer regarding the CPPI of employees' personal information?

Based on *the Standard Contract for Cross-Border Provision of Personal Information (Draft for Comment)*, in principle, the standard contract between a domestic exporter and an overseas importer shall be adjusted and executed based on the template formulated by the Cyberspace Administration of China, and the record-filing, an administrative approval procedure, for the standard contract is also required. In the case that any of the following circumstances occurs, the standard contract should be signed again, and the record-filing should also be submitted once over:

(1) the purpose, scope, type, sensitivity, quantity, method, storage period, storage location, and purpose of CPPI have changed; methods by which overseas importers

applied to process personal information have changed; the storage period of personal information located outside of the Chinese mainland has been extended;

(2) changes to the laws, regulations, or public policies regarding the protection of personal information for a jurisdiction outside the Chinese mainland where the overseas importer resides amount to affect the rights of the personal information subjects;

(3) other circumstances that (adversely) affect the rights of the personal informational subjects.

Notably, all clauses of the standard contract, such as the clause stipulating that PRC laws should be the governing laws should not be contradicted, but only supplemented. Therefore, when using the standard contract, the corporations in fact do not have much room to negotiate on the contract terms.

Q8: As an overseas importer of employees' personal information, how can an overseas corporation protect the statutory rights of employees under the PIPL?

According to Article 39 of the PIPL: "to provide the personal information of an individual to an overseas importer outside the Chinese mainland, the personal information processor shall inform the individual of such matters … for the individual to exercise the rights stipulated herein against the overseas importer." Therefore, as overseas importers of employees' personal information, corporations should focus on protecting employees' statutory rights under the PIPL from the following two aspects:

(1) Clarify the legal rights of the personal information subjects under the PIPL:

Due to the distinctive applicability of the PRC law, overseas corporations are usually unfamiliar with the legal rights of personal information subjects under the PRC legal regime. Therefore, overseas corporations must fully understand such statutory rights. In the CPPI scenarios, statutory rights of the personal information subjects can be summarized as follows:

i. an individual has the right to know and make decisions on the processing of his/her personal information, and the right to restrict or refuse processing of his/her personal information by others;
ii. an individual is entitled to consult, copy, request corrections of, supplement, or delete his/her personal information in the custody of an overseas personal information recipient;
iii. an individual is entitled to request a personal information processor to explain its rules of processing personal information under CPPI scenarios;
iv. an individual has the right to reject the decision made by the personal information processor solely as a result of automatic decision-making;
v. an individual has the right to make complaints or reports to the PRC regulatory authorities responsible for personal information protection.

Judging from the legislative trends, overseas importers also need to be aware of the following two further possible rights:

i. access to relative texts: as the beneficiary of the binding legal documents executed between the domestic exporters and overseas importers, the personal information subjects have the right to request the domestic exporters and overseas importers to provide a copy of the whole or part of the binding legal documents related to the protection of the personal information subjects;
ii. jurisdiction: personal information subjects have the right to initiate judicial proceedings in the courts of their domicile against relevant parties involved in the CPPI scenarios.

In light of the current practice required by the PIPL, overseas importers are recommended to focus on the protection of the first five categories of statutory rights listed above in accordance with the PRC laws and regulations. As for the two further rights, overseas importers are advised to wait and see where the future legislative will take us once implementation details regarding the two rights are promulgated. Corporations should also consider the costs of implementing plans regarding the

protections of the two further rights and confirm with competent authorities if necessary.

(2) Establish a direct and hassle-free channel for accepting and processing employees' requests per the exercise of their legal rights as the personal information subjects:

According to Article 50 of the PIPL, a personal information processor shall establish a direct and hassle-free channel for accepting and processing employees' requests per the exercise of their legal rights as the personal information subjects. If an individual's request for exercising his/her rights is rejected, the reasons must be elaborated in writing. As an overseas importer of the personal information regarding its employees within the Chinese mainland, the corporation shall also establish such a channel based on the clarification of the statutory rights of the personal information subjects.

Per the CPPI scenarios, we recommend the overseas importers execute the specialized privacy policy with employees directly or through the assistance of domestic importers. Within the privacy policy, the information handlers should strive to refine the specific mechanisms ensuring that the personal information subjects exercise their rights properly. If the CPPI scenarios also involve the personal information of job candidates, to ensure good practice, the overseas importers are recommended to require domestic exporters to sign a job candidate privacy policy ahead of the recruitment process to provide comprehensive protection of the candidates' statutory rights.

Q9: What special compliance obligations should domestic corporations pay attention to when providing sensitive personal information of employees to overseas corporations?

(1) Identification of sensitive personal information

To identify what kind of employees' personal information constitutes sensitive personal information, please refer to Q1.

(2) Strictly restricted processing purposes

Article 28 of the PIPL stipulates that personal information processors may only process sensitive personal information if they have a specific purpose and sufficient necessity and take strict protective measures. Under the CPPI scenario, domestic exporters should first evaluate whether the strictly restricted processing purposes are met. If not, they should not carry forward with CPPI regarding employees' sensitive personal information.

(3) Special obligation to inform

Article 30 of the PIPL stipulates that when a personal information processor processes sensitive personal information, it shall also inform individuals of the necessity of processing such sensitive personal information and evaluate the impact of such processing on personal rights and interests. Before CPPI of employees' personal information to overseas importers, domestic exporters shall inform employees of the aforementioned necessity and the impact on employees' rights and interests through agreements or other traceable records which are comprehensible to the employee.

(4) Separate consent obligations under the basis of legality

Based on the above analysis, if the employees' personal information is processed based on the lawful implementation of human resources management in accordance with the legally formulated labor rules and regulations and the legally signed collective agreements, no individual employee's consent is required; if such scenario is not the case, and therefore no such legal basis exists to waive individual consent, whether other applicable legal bases are available should be cautiously analyzed before the employee's personal information is processed.

For MNCs, before its domestic corporation provides employees' personal information across borders to its overseas corporation, it should fully demonstrate the applicability of its legal basis and estimate whether it should obtain the individual consent of the employees in a case-by-case manner. Per Article 73 of the Regulations for the Administration of Network Data Security (Draft) released in 2021, "[']

separate consent [’] means consent to the processing of each item of personal information in specific data processing activities to be conducted by the data processor, not including a one-time consent for multiple items of personal information or to multiple types of processing activities”. Therefore, the core idea of “separate consent” is to require personal information processors to list specific personal information processing activities and ensure that individuals have the right and convenience to make independent judgments on whether to consent to each of such activity. Under the scenario of HR management for MNCs, we suggest that corporations list every item that requires separate consent and has such items confirmed by the employees.

(5) Personal information protection impact assessment obligations

According to Article 55 of the PIPL, in order to process sensitive personal information or personal information in general, processors should conduct a personal information protection impact assessment in advance and record the processing. Before providing sensitive personal information of employees abroad, domestic corporations shall perform the obligation of personal information protection impact assessment by the law and keep written records of such assessment work.

Q10: What penalties will overseas importers face if not fulfilling the obligations to protect the personal information of their employees?

Although geographically located outside of PRC, overseas importers who receive personal information of employees provided by domestic exporters are still governed by the PRC laws. The overseas importers will face the following penalties if not fulfilling their obligation to protect the employees’ personal information:

(1) Civil liability

If the processing of personal information infringes upon the rights and interests of personal information subjects and causes damage, and the personal information processor is unable to prove that such non-compliant processing is not willful or negligent, the processor shall be liable for compensatory damages under tort law. The liability for damages shall be determined according to the loss suffered by the

individual or the benefit received by the personal information processor; if it is difficult to determine the loss suffered by the individual and the benefit received by the personal information processor, the amount of compensation shall be determined according to the actual circumstances.

(2) Administrative penalties

For personal information processors: the PIPL can impose a maximum fine of less than 5% of the previous year's turnover on personal information processors who do not fulfill their legal obligations under the PIPL.

The PIPL stipulates that the directly responsible person in charge and other directly responsible personnel can be fined up to RMB one million, and such personnel should be prohibited from serving as directors, supervisors, senior managers, and personal information protection personnel of relevant entities for a certain period.

(3) Criminal liability

If a personal information processor violates the provisions of the PIPL, the Criminal Law, or other laws and regulations, and the violation amounts to a criminal offense, such personal information processors shall be punished under criminal laws. For crimes such as infringing on citizens' personal information, refusing to fulfill the obligation of information network security management, etc., the maximum imprisonment term can be no more than seven years with certain fines imposed.

Conclusion

It all boils down to that when providing employees' personal information outside of the Chinese mainland, corporations should take a good look at the context of the laws and regulations and legislative purposes, grasp key concepts and deepen their understanding of various statutory obligations. Corporations are also recommended to formulate and implement more effective and customized compliance strategies during their operation and management. We recommend that multinational entities pay attention to the progress of relevant legislation while initiating necessary reform to ensure compliance with the latest progress of relevant laws and regulations.