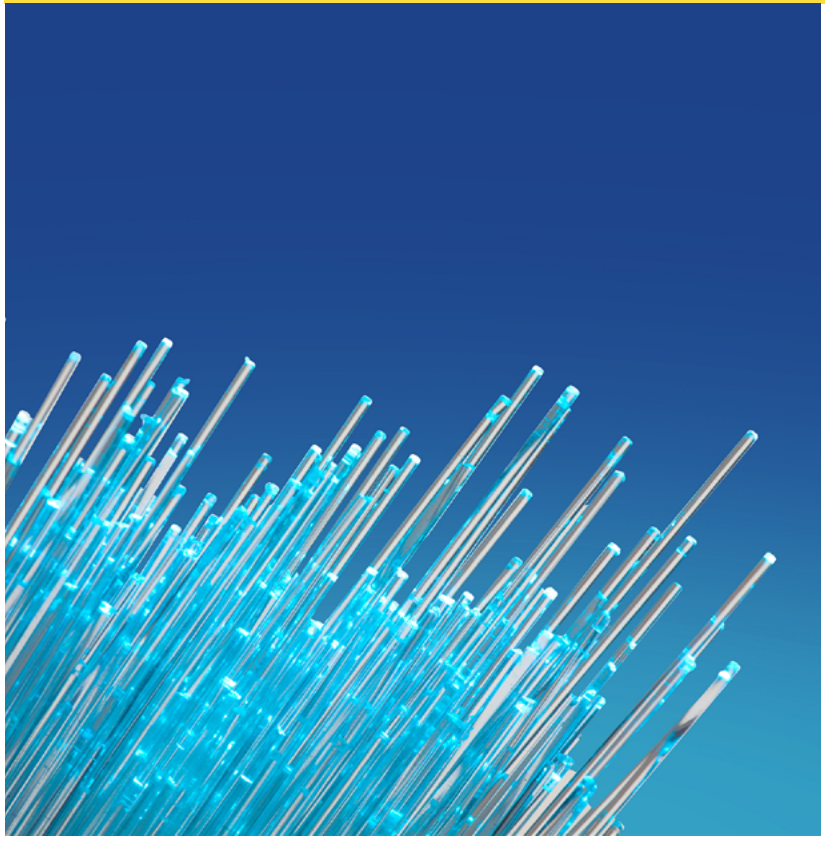
TaylorWessing

Impact of PIPL on Employment Relationships

September 2021
Dr. Guang Li



The Personal Information Protection Law ("PIPL") of the People's Republic of China ("PRC") was adopted at the 30th Session of the Standing Committee of the 13th National People's Congress of the PRC on August 20, 2021. It was promulgated the same day through Presidential Decree No. 91. The PIPL will become effective as of November 1, 2021.

Since in the course of employment employers can independently determine the purpose and method of processing (potential, current and former) employees' personal information (e.g. name, gender, ethnicity, date and place of birth, ID No., address, email account, phone No., general health conditions, educational background, work experience, emergency contacts), employers are personal information processors in terms of PIPL.

Below we summarize some major issues under the PIPL that could have an impact on dealing with employment relationships.

Issues	Rules	Article No.	To-Dos
Extraterritorial application	Under certain circumstances, the PIPL also applies to the processing of individuals' personal information located in the PRC even if such processing is conducted outside the PRC. For instance, (i) where the purpose of such processing is to provide individuals in the PRC with products or services (e.g. certain services provided by the global HR); or (ii) where the activities of individuals in the PRC are analyzed and evaluated (e.g. employee performance evaluation or foreign assignment evaluation through overseas headquarters), the PIPL can apply extraterritorially.	Art. 3 Para. 2	■ To check and verify whether certain personal information processing activities conducted/led by overseas HR or headquarters would fall under the PIPL. ■ If so and appropriate, either to ensure full compliance with the PIPL or have such activities done by HR, entities or service providers within the PRC in compliance with the PIPL.
Basic definitions	"Personal information" refers to all kinds of information related to identified or identifiable individuals that is recorded by electronic or other means, except the anonymized information. "Sensitive personal information" refers to the personal information that is likely to result in damage to the personal dignity of the data subject or damage to his/her personal or property safety once divulged or illegally used, including such information as biometric identification, religious belief, specific identity, medical health, financial account and whereabouts and tracks, as well as the personal information of minors under the age of 14. "Anonymization" refers to the process in which personal information is processed so that it is impossible to identify certain individuals and that it cannot be restored. However, certain personal information such as biometric data can hardly be anonymized. If the anonymized personal information can be technically recovered by the recipient, the PIPL still applies. "Processing of personal information" includes the collection, storage, use, processing, transmission, provision, publication and deletion, etc. of personal information. "Personal information processor" refers to an organization or individual that independently determines the purpose and method of the processing of personal information. However, PIPL does not apply to the processing of personal information by a data subject for his/her own personal or family affairs.	Art. 4, 28, 72 and Art. 73	■ To check and verify what kind of personal information of employees and how they has been and will be processed (e.g. sensitive or not, for what purpose, to what extent, where stored, for how long and in what manner). ■ When anonymizing the personal information, to ensure at least that the anonymized personal information cannot be technically restored by the recipient. ■ In doubt and if appropriate, to consider letting the employees themselves voluntarily release their personal information based on a fully informed basis, which should be well documented.

Issues	Rules	Article No.	To-Dos
Circumstances allowing processing personal information	Only under any of the following circumstances may a personal information processor process personal information: ■ where the consent of the data subject is obtained; ■ where it is necessary for the conclusion or performance of a contract (e.g. an employment contract) to which the data subject (e.g. employee) is a party, or for the implementation of HR management in accordance with the lawfully adopted labor rules and regulations and the lawfully concluded collective contract (no consent of the data subject is required here); ■ where it is necessary for the performance of statutory duties or obligations (e.g. for withholding individual income tax or making social insurance contribution by employers for employees; no consent of the data subject is required here); ■ where it is necessary for the response to a public health emergency or for the protection of the life, health and property safety of an individual (no consent of the data subject is required here); ■ where such acts as news reporting and supervision by public opinions are carried out for the public interest, and the processing of personal information is within a reasonable scope (no consent of the data subject is required here); ■ where it is necessary to process the personal information publicized by the data subject (e.g. personal information publicized in social media) or other personal information that has been lawfully publicized within a reasonable scope unless the data subject expressly refuses such processing (in general no consent of the data subject is required here except where such processing has a significant impact on the data subject's rights and interests); and ■ other circumstances prescribed by laws and administrative regulations (no consent of the data subject is required here).	Art. 13, 18 and 27	■ To check and verify at first whether a specific personal information processing activity requires the employee's consent (general or separate) or not. In the course of employment, employers are entitled to process employees' certain basic personal information without their explicit/further consent for fulfilling their contractual and statutory obligations (e.g. paying salary, withholding individual income tax, making social insurance contribution, arranging sick leaves). ■ To check and verify whether the employment contracts, company rules, employee manuals, collective contracts contain adequate clauses on processing personal information for the implementation of employment contracts and HR management. ■ In emergency, to well document the personal information processing and to let the data subject know about it in a timely manner after the elimination of the emergency. ■ When processing the personal information lawfully publicized, to restrict it to a reasonable extent and well document it. Where such processing of such personal information could significantly affect the employees, to obtain their consent.

Issues	Rules	Article No.	To-Dos
Notification before processing	Prior to the processing of personal information, the personal information processor shall truthfully, accurately and completely inform the data subject of the following matters in an obvious manner and in clear and understandable language: ■ the name and contact information of the personal information processor; ■ the purpose and method of processing personal information, and the type and retention period of the processed personal information; ■ the method and procedure for the data subject to exercise his/her statutory rights; and ■ other matters that shall be informed in accordance with the provisions of laws and administrative regulations.	Art. 17	■ Employers shall adopt comprehensive data processing rules including all content mandatorily required by the PIPL. In this regard, the already collected experience and best practice under foreign data protection laws and regulations such as the GDPR could be referred to. ■ Such rules (including their amendments and updates) shall be made in Chinese and adequately discussed and consulted by the staff as required by the PRC Labor Contract Law. ■ They shall also be made open to the staff for easy access and storage.
Data subject's consent & separate consent	Where the consent of the data subject is legally required, such consent shall be given by the data subject in a voluntary and explicit manner after the data subject has obtained full knowledge. Where the purpose or method of processing personal information or the type of personal information to be processed changes, the consent of the data subject shall be obtained again. The data subject is entitled to withdraw his/her consent. In addition, under any of the following circumstances, the personal information processor must obtain a separate consent from the data subject: ■ providing personal information to a third-party personal information processor (e.g. HR, payroll and professional service providers); ■ publicizing a data subject's personal information (e.g. publicizing employees' personal information in marketing materials or in the course of internal performance evaluation); ■ using a data subject'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;	Art. 14, 15, 21, 23, 25, 26, 27, 28, 29, 39	■ To well document that the employees have full knowledge when voluntarily giving their written consent. ■ When engaging a third party to process employees' personal information, in addition to obtaining the consent from the employees, to ensure the third party's full compliance with PIPL by concluding an agreement in accordance with Art. 21 of the PIPL and to monitoring their continuing compliance through regular and random check.

Issues	Rules	Article No.	To-Dos
Data subject's consent & separate consent ff.	■ processing sensitive personal information (e.g. biometric data, account information, location tracking, health information of employees); ■ where processing of publicized personal information could significantly affect the data subject's rights and interests; and ■ providing personal information to overseas parties (e.g. overseas headquarters, professionals or parties to M&A transactions).	Art. 14, 15, 21, 23, 25, 26, 27, 28, 29, 39	
Cross-border transfer	When providing personal information outside the PRC, at least one of the following four conditions has to be met: ■ passing the security assessment of the Cyberspace Administration of China (**"CAC"**); ■ being certified by a recognized institution for personal information protection in accordance with the requirements of the CAC; ■ concluding a cross-border transfer agreement (a standard template yet to be issued by CAC) with the recipient located outside the PRC and ensuring that the processing meets the protection standards provided under the PIPL; or ■ meeting other conditions prescribed by laws, administrative regulations, or CAC. To provide the personal information to an overseas recipient, the personal information processor shall inform the data subject of such matters as the name of the overseas recipient, contact information, purpose and method of processing, type of personal information and the method and procedure for the data subject to exercise his/her statutory rights against the overseas recipient, and shall obtain the data subject's separate consent. **Without the approval of the competent authorities of the PRC, no personal information processor may provide the personal information stored within the PRC to foreign judicial or law enforcement authorities.**	Art. 38, 39 and 41	■ Before a cross-border transfer of personal information, at least to conclude a cross-border transfer agreement and to seek and well document the data subject's separate consent given on a fully informed basis. ■ To avoid provision of employees' personal information to foreign judicial or law enforcement authorities without the approval of the competent authorities of the PRC (e.g. in the course of internal compliance investigation, legal proceedings conducted overseas). ■ In doubt and if appropriate, to consider letting the employees themselves voluntarily release their personal information to foreign recipients on a fully informed basis, which should be well documented.

Issues	Rules	Article No.	To-Dos
Processor's major obligations	A personal information processor shall take the following measures to ensure the compliance and prevent unauthorized access and divulgence, falsification and loss of personal information: ■ formulating internal management systems and operating procedures; ■ implementing category-based management of personal information; ■ taking corresponding technical security measures such as encryption and de-identification; ■ reasonably determining the authority to process personal information and conducting security education and training for relevant employees on a regular basis; ■ formulating and organizing the implementation of emergency plans for personal information security incidents; and ■ other measures stipulated by laws and administrative regulations. A personal information processor shall regularly conduct compliance audits on its processing of personal information. Under any of the following circumstances, a personal information processor shall conduct an impact assessment on personal information protection beforehand and keep a record of the handling: ■ processing sensitive personal information; ■ using personal information to make automatic decision-making; ■ entrusting others to process personal information, providing other personal information processors with personal information and publicizing personal information; ■ providing personal information to overseas parties; or ■ other personal information processing activities that have significant impact on personal rights and interests. **The report on personal information protection impact assessment and records of handling shall be kept for at least three years.**	Art. 51 - 59	■ To lawfully adopt relevant rules, policies and procedures for processing personal information. ■ To regularly assess, check and update such rules, policies and procedures as well as processing activities in accordance with the continuing development of legislative, judicial and administrative practice. ■ To install a person or a team in charge of data protection and processing. ■ To regularly train managers and staff on data protection. ■ To well document activities in connection with personal information processing and maintain relevant records for internal and external audit.

Issues	Rules	Article No.	To-Dos
Data subject's rights	A data subject is entitled to ■ withdraw his/her consent, ■ consult and copy his/her personal information, ■ ask the personal information processor to correct, supplement, delete his/her personal information, and to clarify its processing rules.	Art. 15, 44 – 50	■ To adopt relevant procedures for employees' exercise of their rights as data subjects. ■ To carefully handle and well document the entire process when employees exercise their rights as data subjects.
Legal Liabilities	Depending on the seriousness, violation of the PIPL can result in: ■ warning, ■ confiscation of illegal gains, ■ fines up to 50 million RMB or 5% of the preceding year's turnover of the company, ■ being ordered to suspend business operations, ■ revocation of business licenses, and ■ being recorded under the social credit system. For individuals violating the PIPL, they might face fines up to 1 million RMB, and be prohibited to act as directors, supervisors, senior executives, and personal information protection officers of the companies within a certain period of time. For overseas parties violating the PIPL, they may be placed on a blacklist by the CAC. The CAC may take measures to restrict or prohibit the provision of personal information to such overseas parties. Where the processing of personal information infringes upon personal information rights and interests and causes damage, the personal information processor concerned carries certain burden of proof. It shall bear liability for damages and other tort liabilities if it cannot prove that it is not at fault. The liability for damages shall be determined based on the losses thus suffered by the data subject or the benefits thus obtained by the personal information processor. If the losses thus suffered by the data subject or the benefits thus obtained by the personal information processor are difficult to be determined, the amount of damages shall be determined by courts in accordance with the actual circumstances.	Art. 42, 66, 67, 69	**"CCC" – CARE, CONTROL & COMPLIANCE!**

TaylorWessing

Your experts

Dr. Guang Li
Salary Partner, Munich
+49 89 21038-0
G.Li@taylorwessing.com

Dr. Michael Tan
Partner, Shanghai
+86 21 6247 7247
m.tan@taylorwessing.com

Heather Jiang
Associate, Shanghai
+86 21 6247 7247
h.jiang@taylorwessing.com

Julian Sun
Associate, Shanghai
+86 21 6247 7247
j.sun@taylorwessing.com

Dr. Axel Frhr. von dem Bussche
Partner, Hamburg
+49 40 36803-0
a.bussche@taylorwessing.com

Thomas Kahl
Partner, Frankfurt
+49 69 97130-0
t.kahl@taylorwessing.com

Dr. Nicolai Wiegand
Partner, Munich
+49 89 21038-0
n.wiegand@taylorwessing.com

Europe > Middle East > Asia

taylorwessing.com