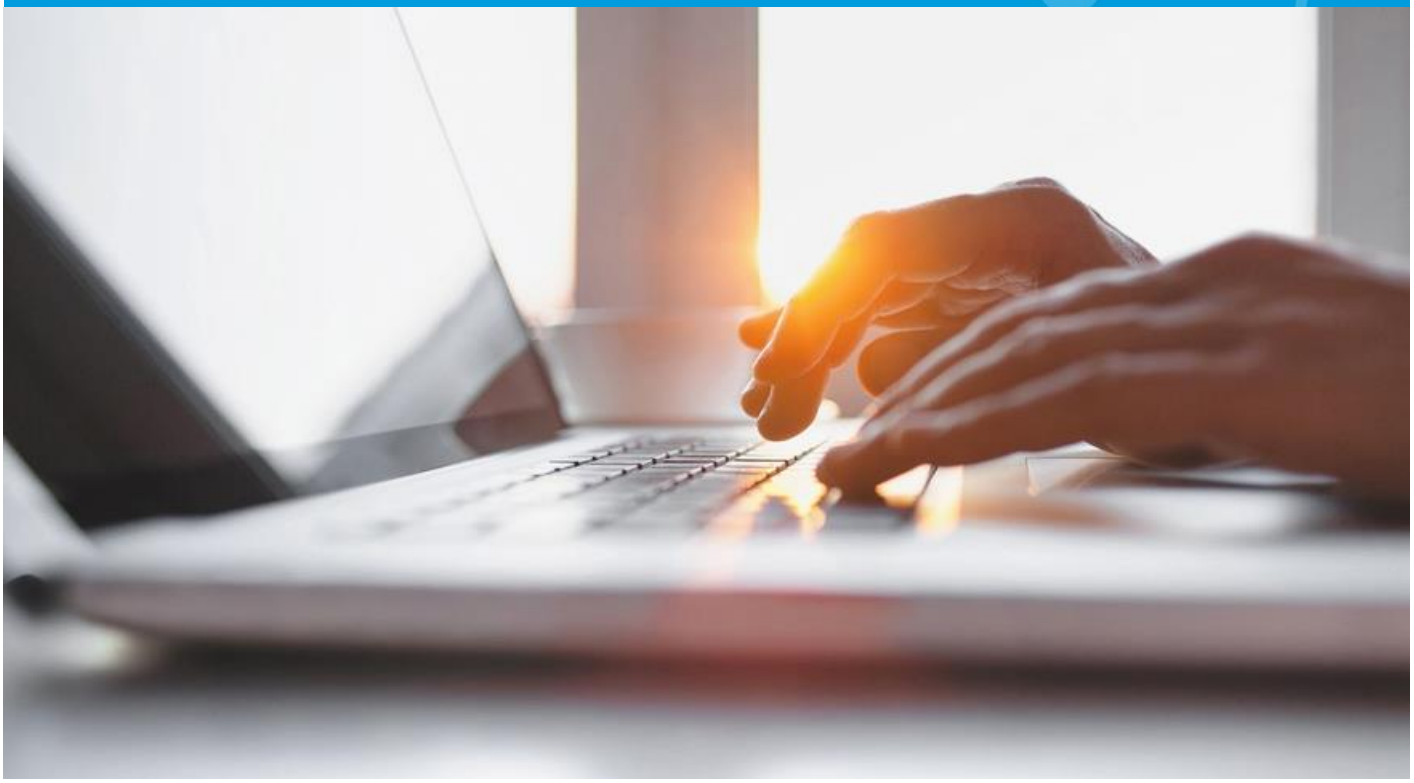
STEPHENSON HARWOOD
WEI TU (CHINA)
罗夏信-伟途 联营

July 2022

Businesses operating in Hong Kong that provide services to individuals in Mainland China: Personal data issues to consider



Introduction

The Personal Information Protection Law (the "**PIPL**"), which took effect on 1 November 2021, is Mainland China's (the "**PRC**") first piece of legislation that relates entirely to data protection and privacy. As the PIPL has extraterritorial effect, the PIPL will not only apply to businesses that have a presence in the PRC, but also to those who process data for (1) providing products or services to natural persons in the PRC, and (2) analysing or evaluating the activities of natural persons in PRC. As a result, many businesses, including those in Hong Kong ("**HK**"), will need to comply with both the data privacy laws of their home jurisdiction, as well as the PIPL.

In this client alert, we explore some personal data issues (from both a HK law and a PRC law perspective) that we feel are particularly important to businesses operating in HK which provide services to individuals within the PRC. The primary data protection legislation in HK is the Personal Data (Privacy) Ordinance (the "**PDPO**"). The PRC legal position on the issues explored in this client alert is still evolving and may change in the near future.

The PIPL uses the term "personal information", whereas the PDPO uses the term "personal data". We will be adopting the same approach in this client alert.

1. To what extent do businesses outside of the PRC and HK have to comply with the PIPL and the PDPO respectively?

PIPL

As mentioned above, if a "**Personal Information Processor**", meaning an entity responsible for the processing of personal information under the PIPL, processes personal information outside the territory of the PRC for the following purposes, it must still comply with the PIPL:

(a) to provide products or services to natural persons located within the PRC; or

(b) to analyse or evaluate the activities of natural persons within the PRC.

If your business is located outside of the PRC but handles the processing of personal information of individuals within the PRC for the purposes stated above, a literal reading of the PIPL requires that you set up a specialised agency or designate a representative within the PRC, even if you have no physical presence in the PRC. The name, contact information, and other essential information of this agency or representative should be submitted to the relevant department performing personal information protection duties.

PDPO

In contrast, the PDPO does not contain a provision that states it has extraterritorial application. This is confirmed by the Administrative Appeals Board in the Google case in 2020. Therefore, only entities who can control the holding, process, or use of personal data, in or from HK, would be subject to the PDPO. As such (unlike the PIPL), the PDPO would not apply to businesses located outside of HK, even if they collect personal data on individuals within HK.

2. What should a business pay attention to after obtaining consent for the processing of personal information/data?

PIPL

Under the PIPL, a Personal Information Processor must inform individuals and obtain consent from the individual **again** if there is any change in (1) the purpose(s) for which their personal information is to be processed, (2) the method(s) by which their personal information is processed, and (3) the type of personal information processed.

In addition, the PIPL also requires Personal Information Processors to obtain separate and additional informed consent where the Personal Information Processor is:

(a) providing personal information to a third party;

(b) providing personal information to a party outside the territory of the PRC; or

(c) processing personal information that, if leaked, can easily lead to the infringement of personal dignity or cause harm to natural persons or property ("**Sensitive Personal Information**").

Personal Information Processors should also be mindful that any personal information collected can only be retained for the minimum period necessary for achieving the purpose for which the personal information was collected (the "**Retention Period**"), except where laws or administrative regulations provide otherwise. Personal Information Processors must also provide individuals with a convenient means of withdrawing their

consent. If any of the following occurs, then the Personal Information Processor must erase the relevant personal information on its own initiative:

(1) the Retention Period has come to an end;

(2) the purpose of processing that information has been achieved, is unable to be achieved, or no longer needs to be achieved;

(3) the individual has withdrawn his/her consent; or

(4) the Personal Information Processor has ceased to provide products or services.

PDPO

Similar to the PIPL, if personal data collected is intended to be used for a new purpose other than that for which it is originally collected, businesses that control the collection, holding, processing, or use of personal data ("**Data Users**") are generally required to obtain informed consent again from the individual who is the subject of the personal data (referred to as the "**Data Subject**" under the PDPO) (subject to certain exemptions). Further, a Data User must obtain the Data Subject's consent or indication of no objection if the personal data is subsequently used for direct marketing purposes.

Unlike the PIPL though, Data Users are not required to obtain additional specific consent to (1) transfer personal data to a third party, (2) transfer personal data overseas, or (3) process "sensitive" personal data (because the PDPO does not distinguish between sensitive and non-sensitive personal data), as long as the original consent granted is sufficiently clear to cover them. That said, the Hong Kong Office of the Privacy Commissioner for Personal Data (the "**HK PCPD**") recommends Data Users to notify Data Subjects of the above.

The PDPO also states personal data must not be retained by Data Users any longer than is necessary for the fulfilment of the purpose(s) for which the personal data was collected for. Individuals are also entitled to withdraw their consent by providing notice in writing to the Data User, but this does not mean that the Data User is obliged to delete the relevant personal data.

Takeaways

Generally speaking, the personal information protection regime of the PRC imposes a stricter requirement than that of HK, by designating a certain class of personal information as Sensitive Personal information and imposing stricter controls on cross-border data transfers. Businesses should be mindful that a Data Subject's consent can also be withdrawn under the PIPL, at which point not only the collection and processing of his/her personal information must cease, but the related personal information must also be deleted.

3. How should businesses handle its employee's personal information/data?

PIPL

The PIPL permits businesses to process the personal information of its employees without their consent if the processing is necessary for the conclusion or performance of a contract to which the employee is a party, or to implement human resources management in accordance with employment rules and regulations in the PRC. We recommend that businesses add clauses relating to personal information in its employment contracts and employment policies, standardise the collection and processing of employee information, and require employees to sign the necessary authorisations when or after they join the company.

As the day-to-day operations of a business will likely involve a flow of personal information between the business and its customers and trading partners, businesses should (1) clarify their rights and obligations in respect of the personal information with those third parties in writing, (2) maintain a privacy policy that clarifies the responsibility that they will take for the personal information it collects, and (3) provide guidance to their employees concerning the handling of personal information-related matters.

PDPO

The personal data of an employee should be treated like any other personal data. In other words, there are no rules that apply specifically to the personal data of one's employees. Same as any other person that collects personal data, employers should provide its employees with a Personal Information Collection Statement ("**PICS**"), informing the employee about the types of personal data that will be collected, the purposes for which it will be used for, and the classes of transferees etc.

Businesses should also have a privacy policy statement ("**PPS**") in place. The HK PCPD has also advocated for business to develop their Privacy Management Programme ("**PMP**") to treat data protection as part of their corporate governance. In March 2019, the HK PCPD published a best practice guide for the PMP. One of the HK PCPD's recommendations is that Data Users should appoint a data protection officer to oversee the business' compliance with the PDPO and PMP and to provide employees with up-to-date training and education about data protection.

Takeaways

Businesses should include clauses on personal information/data in their employment contracts and require employees to consent to the necessary collection of personal information/data when they join the company. Businesses should also maintain a privacy policy at all times and ensure their employees are well trained on matters concerning the collection of personal information/data.

4. What are the consequences of breaching the PIPL and PDPO?

PIPL

A company that contravenes the requirements under the PIPL may be subject to administrative penalties, civil liability, and criminal liability. Penalties include (1) the issuance of a rectification order or warning letter, (2) the confiscation of illegal gains, and (3) fines up to a maximum of RMB50 million or 5% of the annual turnover of the contravening company in the preceding year. Businesses may even be ordered to suspend or terminate their business or related businesses, and relevant competent departments may be notified to revoke the relevant business permit(s) or business license(s). Persons directly responsible for the contravention may also be restricted from serving as directors, senior managers, or persons in charge of personal information protection of related companies for a certain period.

If the company also infringes on the personal information rights and interests of individuals and fails to prove that it is not at fault, then a breach of the PIPL could also lead to civil liability, whereby the company would have to compensate the individuals for any losses that it has suffered or any profit that the company may have gained. If any violation constitutes a criminal offence, then the company may also be held criminally liable.

PDPO

In HK, a breach of the provisions of the PDPO could result in a maximum fine of HK$1,000,000 and imprisonment for 5 years. Examples include using a Data Subject's personal data in direct marketing or disclosing a Data Subject's personal data, in each case without the Data Subject's informed consent.

Further, if the HK PCPD receives a complaint or has reasonable grounds to believe there may be a contravention of the PDPO, it may conduct an investigation. If the investigation reveals a breach of the PDPO, the HK PCPD may issue an enforcement notice directing remedial or preventive steps to be taken. A failure to comply with an enforcement notice could lead to a maximum fine of HK$50,000 (on first conviction) or HK$100,000 (on subsequent conviction), and imprisonment of two years.

Data Users may also be subject to civil liability if a breach of the PDPO causes Data Subjects to suffer any loss or damage.

Recommendations

To ensure compliance with both the PIPL and the PDPO and to avoid such penalties, businesses need to have appropriate internal personal data policies in place, implement and enforce such policies, and regularly review them to ensure they remain up-to-date with the latest data privacy and protection laws of each relevant jurisdiction. If a data breach occurs, businesses are recommended to immediately gather information to assess the impact on Data Subjects, contact the relevant enforcement agencies, and adopt the necessary preventative/remedial measures. Data Users are also recommended to inform relevant Data Subjects about the data breach.

5. Will documents that comply with GDPR requirements also comply with the requirements under the PIPL and PDPO?

Despite certain similarities between the three regimes, compliance with the GDPR does not necessarily equate to compliance with the PIPL and/or the PDPO. Any rules or policies that were formulated according to the GDPR should be re-examined against the PIPL and PDPO.

6. What are the requirements relating to cross-border transfers of personal information/data?

PIPL

Although the PIPL does not clearly define what a cross-border transfer of personal information is, we consider both of the following circumstances to constitute a cross-border transfer of personal information:

(a) Personal information collected and generated within the PRC that is transferred outside the territory of the PRC; and

(b) A corporation outside the territory of the PRC can access or dispose of personal information physically stored in the PRC.

Where there is a cross-border transfer of personal information, the PIPL requires businesses to obtain separate consent and to take certain measures, for example, conducting security assessments or personal information protection certification, organising security audits and impact assessments on personal information protection, and signing contracts (i.e. standardised contracts formulated by the PRC Cyberspace Administration) with overseas recipients to agree on the rights and obligations of both parties.

PDPO

In contrast, there are currently no restrictions on the cross-border transfer of personal data in HK, as section 33 of the PDPO (prohibition against transfer of Personal Data to place outside HK except in specified circumstances) is not yet in force. It is currently unclear when section 33 will come into force. When it does, cross-border transfer of personal data will only be permitted if at least one of the following requirements is met:

(1) the place to which the data is transferred has in force any law which is substantially similar to the PDPO;

(2) the Data Subject has given consent for the cross-border transfer in advance;

(3) the Data User has reasonable grounds for believing that (a) the transfer is for the avoidance or mitigation of adverse action against the Data Subject, (b) it is not practicable to obtain the consent in writing of the Data Subject, and (c) if it were practicable for the Data Subject to give consent in writing, the Data Subject would give it;

(4) the cross-border transfer of data falls under one of the exemptions to section 33 prescribed under the PDPO; or

(5) the Data User has taken all reasonable precautions and exercised all due diligence to ensure that the personal data collected will not be dealt with in a manner that would constitute a contravention of the PDPO.

Of these requirements, the second one should, in most cases, be the easiest one to meet, as it can simply be included in the PICS that is given to the Data Subject at the time his/her personal data is collected.

In preparation for section 33, the HK PCPD recommends Data Users review their data transfer arrangements, control cross-border data flow activities through measures such as internal information barriers, keep an inventory of personal data transferred outside of HK, and conduct regular audits and inspections. Data Users are also recommended to notify individuals of any proposed cross-border data transfer and be transparent about its data processing activities. As with the PIPL, businesses should also sign contracts with overseas recipients regarding the rights and obligations of the transferor and transferee of personal data, although so far there are no standardised contracts prescribed by the HK Government.

Takeaways

The PIPL regime imposes a sweeping new set of obligations on businesses that control and process personal information. Like the PDPO, it is also centred around the theme of consent, albeit to a stricter standard. Most importantly, the PIPL has extraterritorial effect, whereas the PDPO does not, and therefore businesses should revisit and review their data-related policies and processes to ensure compliance with applicable laws and regulations. Where there is a conflict between two or more sets of data protection laws that businesses must abide by, they should comply with the legislation that imposes the stricter standard.

It remains to be seen how some of the more nuanced aspects of the PIPL will be interpreted and enforced.

How we can help

We routinely advise clients on the PRC and HK's data protection regimes. We can help ensure that your business is fully compliant with all its obligations under the PDPO and the PIPL. We also have teams in our other offices that are able to advise on the data protection laws of other jurisdictions such as the GDPR.

Contact us

Katherine Liu
Partner, Head of finance
T: +852 2533 2717
E: katherine.liu@shlegal.com

Zoe Zhou
Partner – Wei Tu Law Firm*
T: +86 20 8388 0590
E: zoe.zhou@shlegalworld.com

James Wong
Associate
T: +852 3166 6933
E: james.wong@shlegal.com

*Wei Tu (a PRC law firm registered in Guangzhou) and Stephenson Harwood (a law firm registered in Hong Kong) are in a CEPA association under the name "Stephenson Harwood - Wei Tu (China) Association". CEPA (Closer Economic Partnership Arrangement) is a free trade agreement concluded between Mainland China and Hong Kong. Under CEPA, Hong Kong based law firms are permitted to operate in association with Mainland Chinese law firms to provide comprehensive legal services in Mainland China governed by Chinese and non-Chinese laws.

Stephenson Harwood is a law firm of over 1100 people worldwide, including 190 partners. Our people are committed to achieving the goals of our clients – listed and private companies, institutions and individuals.

We assemble teams of bright thinkers to match our clients' needs and give the right advice from the right person at the right time. Dedicating the highest calibre of legal talent to overcome the most complex issues, we deliver pragmatic, expert advice that is set squarely in the real world.

Our headquarters are in London, with eight offices across Asia, Europe and the Middle East. In addition, we have forged close ties with other high quality law firms. This diverse mix of expertise and culture results in a combination of deep local insight and the capability to provide a seamless international service.

STEPHENSON HARWOOD
WEI TU (CHINA)
罗夏信-伟途 联营