BÄR & KARRER

BRIEFING FEBRUARY 2022

CHINA'S NEW PRIVACY LAW - WHAT SWISS COMPANIES SHOULD KNOW

Over the past year, many countries around the globe have implemented new privacy laws. On 1 November 2021, the Personal Information Protection Law of the People's Republic of China („PIPL") entered into force. The main purpose of PIPL is to establish additional rules and to clarify existing rules for processing personal information. It also defines the obligations of so-called „personal information processors" and the rights of „personal information subjects". In addition, the PIPL expands specific data localization requirements, defines measures which the enforcement authority may take in order to protect personal information and stipulates fines for violations of this law.

CHINA'S NEW PRIVACY LAW HAS ENTERED INTO FORCE

In the past few years, China has been pushing forward with a digital law framework that – much like EU data protection law – will affect companies both in and outside of China. The data protection, cybersecurity and data security framework of China was, until recently, mainly based on the Cybersecurity Law of the People's Republic of China („**CSL**", in effect since 1 June 2017) and the Data Security Law of the People's Republic of China (in effect since 1 September 2021). On 1 November 2021, China's new privacy law, the Personal Information Protection Law of the People's Republic of China („**PIPL**") entered into force. The PIPL essentially amends and adds extra details to the two mentioned existing laws and complements the overall data security framework.

Much like its European counterpart, the EU General Data Protection Regulation („**GDPR**"), the PIPL is based on the following goals:

> Protecting the rights and interests of individuals;
> Regulating processing activities related to personal information;
> Safeguarding the lawful and „orderly flow" of data; and
> Facilitating the reasonable use of personal information.

However, the PIPL also provides certain national security requirements (covering data localization obligations) and aims at digital sovereignty (e.g., blacklisting companies outside of China which endanger the personal data rights of individuals or the security of China).

HOW DOES THE PIPL AFFECT SWISS COMPANIES?

The PIPL applies to any processing of personal information. „Personal information" refers to any kind of information related to an identified or identifiable natural person whether held electronically or otherwise recorded, with the exception of anonymised information. This definition is largely in line with Swiss and European standards. However, the definition of sensitive personal data under the PIPL is slightly broader, as it includes personal information that, once leaked or illegally used, may cause discrimination against individuals or grave harm to personal or property security, including information on race, ethnicity, religious beliefs, individual biometric features, medical health, financial accounts, individual location tracking, etc.

The PIPL primarily applies to the processing of personal information in China. Additionally, it applies to the processing of personal information outside China, when: (i) products or services are provided to natural persons located within China (ii) the behaviour of a natural person located within China is assessed or analysed or (iii) other circumstances provided in laws or administrative regulations apply. This allows the Chinese government to extend the territorial scope even further. Accordingly, Swiss companies without a physical presence in China but doing business in China are likely to be subject to the PIPL.

Similar to the GDPR and the Swiss Federal Data Protection Act („**FADP**"), the PIPL provides data protection principles that must be met when processing personal information and requires a legal basis for the processing of personal information such as the data subject's consent. This consent remains the primary legal basis for certain processing activities such as sharing data with a third party or when using facial recognition technology in the public space. However, other than the GDPR or the FADP, the PIPL does not recognise an overriding legitimate interest as a lawful basis for the processing of personal information.

In the PIPL, the term „personal information processor" is introduced, which is comparable to the term controller under the GDPR and the FADP. Personal information processors domiciled outside of China may be obligated to establish a dedicated office or to appoint a representative in China who is responsible for data subject matters. Additionally, if these personal information processors process a specific volume of personal data (the exact volume still to be defined), they need to appoint a personal information protection officer, resembling the DPO under the GDPR and FADP. Notably, the PIPL introduces additional duties for personal information processors operating „important" internet platform services to „large amounts" of users (so-called „gatekeeper obligations for internet giants" similar to the proposed EU Digital Services Act).

The PIPL expands the scope of data localization and security assessment requirements, already set out in the CSL, by providing that critical information infrastructure operators („**CIIO**"), i.e. operators in critical sectors such as information service, energy, transport, financial services etc., and personal information processors whose processing of personal information reaches a large volume should store the personal information collected and generated in China within the territory of China.

For the CIIO or other personal information processors to be able to transfer personal information outside the territory of China, the planned transfer needs to pass a necessity test. Accordingly, they need to: (i) obtain separate consent (not a package consent covering all processing purposes) and notify the affected individuals, (ii) conduct an impact assessment and (iii) meet special conditions (such as obtaining certification, passing a security exam or the conclusion of a contract in accordance with Chinese standard contractual clauses). To date, the competent authority has not yet issued or adopted standard contractual clauses and it remains unclear whether they will be similar to what is required under the GDPR and the FADP.

Before fulfilling these requirements for cross-border data transfers, the CIIO must additionally undergo a security assessment. On 29 October 2021, the Cyberspace Administration of China published draft guidelines outlining when and how these security assessments need to be done. The draft guidelines require personal information processors to conduct a risk assessment and further specify that the security assessment must include a declaration form, self-assessment report and the agreed contract between the data importer and exporters when it is submitted to the competent authorities for review. Regarding the data processing agreement, the draft guidelines prescribe several clauses which need to be included, such as data transfer restrictions concerning the receiving party or security measures which ensure data security even when the circumstances of the foreign recipient, e.g. the legal environment, change. Furthermore,

the guidelines state that the competent authority's assessment should be completed 45 days after submission of the materials and will generally be valid for two years. Finally, the draft guidelines provide the possibility for any organisation or individual to make a complaint to the competent authority, should they discover a violation of the duties under the draft guidelines. However, the final guidelines have not yet been adopted.

Irrespective of these requirements, when transferring personal information outside of China, personal information processors must ensure that the data protection rights of individuals are not endangered and that national security or public interests of China are not violated. If this were the case, such transfers could be prohibited and could lead to the personal information processors being blacklisted in China.

Alongside the rules on the transfer of personal information abroad, the PIPL also provides rather strict rules on processing personal information of children and when engaging in automated decision-making. Furthermore, it stipulates data security, data breach notification and risk assessment obligations for personal information processors and gives individuals similar rights as under the GDPR and the FADP. In cases of breach of the PIPL, the enforcement authority, which will consist of several (state) departments, may take measures in order to protect personal information. Such measures include conducting on-site inspections, consulting contracts, records, receipts and „other relevant material" or conducting interviews with the parties handling personal information.

Finally, violating the requirements under the PIPL could lead to administrative liabilities of up to CNY 50 million (approx. CHF 7.2 million) or 5% of the annual turnover of the prior year for entities. For responsible individuals within an organisation this could result in fines of up to CNY 1 million (approx. CHF 144'000.-). Behaviour or acts deemed illegal under the PIPL will be recorded and made public in a so-called social credit system. In addition, the PIPL establishes the standard of „presumptive fault", which means that a personal information processor actively needs to prove that it is not at fault for an alleged breach of the PIPL. Hence, the burden of proof lies with the personal information processors and not the competent authority. The PIPL also provides certain administrative sanctions such as orders to stop processing or confiscation of unlawfully obtained profit, individual rights to obtain compensation, and civil public interest litigation cases through a public prosecutor. Only two days after the PIPL entered into force, China's Ministry of Industry and Information Technology announced that it had ordered a total of 106 applications to be removed across app stores for violating user privacy.

WHAT ARE THE NEXT STEPS FOR SWISS COMPANIES DOING BUSINESS IN CHINA?

Companies should bear in mind that the PIPL, while similar to the GDPR and the FADP, does not *tel quel* mirror the provisions therein with which market participants in Europe or Switzerland may already be familiar. Therefore, Swiss companies are well-advised to analyse their obligations carefully under the PIPL irrespective of whether they are established in China or not.

Firstly, Swiss companies should clarify whether they fall under the scope of the PIPL, i.e., whether they offer services or products to persons in China or whether they monitor the behaviour of persons in China. If a Swiss company concludes that it is subject to the PIPL, all data processing activities relating to personal information collected in China and processed should be carefully assessed for compliance under PIPL principles.

Secondly, Swiss companies are advised to identify the volume and kind of data they process in China, as depending on the outcome thereof, additional obligations may apply to them. This analysis is also helpful if any segregation of certain data may be envisaged, in order to limit the impact of the PIPL. Furthermore, such an analysis helps to decide if appointing a DPO or point of contact in China is required and to identify if the specific gatekeeper obligations for internet platforms apply.

Thirdly, if Swiss companies with a domicile or other establishment in China want to transfer and process personal information outside of China, including remote access, they need to ensure that this transfer fulfils all the requirements for cross-border data transfers under the PIPL. A particular challenge companies may face is the requirement to obtain separate consent for cross-border data transfers.

Finally, if a Swiss company is qualified as a CIIO, it falls under the data localization requirements and therefore needs to store its data on Chinese territory.

It must be highlighted that the strict rules regarding data localization requirements and the multi-level process for processing personal information outside the territory of China may lead to widespread access rights of the Chinese government. As a result, companies should review all data that is stored and processed in China and assess what data must be stored locally in China and what data can be transferred / stored outside of China.

It remains to be seen how several undefined terms or parameters (e.g. regarding the volume of processed personal information or concerning the term CIIO) will be interpreted. Similarly, it is currently unclear how exactly the scope of the obligations under the PIPL may be extended or how certain requirements such as data localization obligations and cross-border security assessments will be interpreted. Therefore, close attention must be given as to how the PIPL is applied in practice and whether further guidance may be made available by the competent authorities.

AUTHORS

Dr. Jan Kleiner
Partner
T: +41 58 261 53 84
jan.kleiner@baerkarrer.ch

Jan Kleiner co-heads our firm's sport, media and data protection practice groups. His practice covers contentious and non-contentious matters in the fields of national and international sports law as well as media, entertainment and data protection law. He also advises clients on technology and telecommunication law matters.

Dr. Rehana Harasgama
Senior Associate
T: +41 58 261 54 51
rehana.harasgama@baerkarrer.ch

Rehana Harasgama is an expert in domestic and international privacy law and also advises clients on media and technology law. She advises clients on complex data protection and privacy questions, such as major cross-border disclosure requests, the adoption and implementation of privacy-by-design in new technologies and data breach response plans.

Viviane Berger
Junior Associate
T: +41 58 261 55 28
viviane.berger@baerkarrer.ch

Viviane Berger is a Junior Associate at Bär & Karrer and advises clients on data protection law as well as real estate matters.