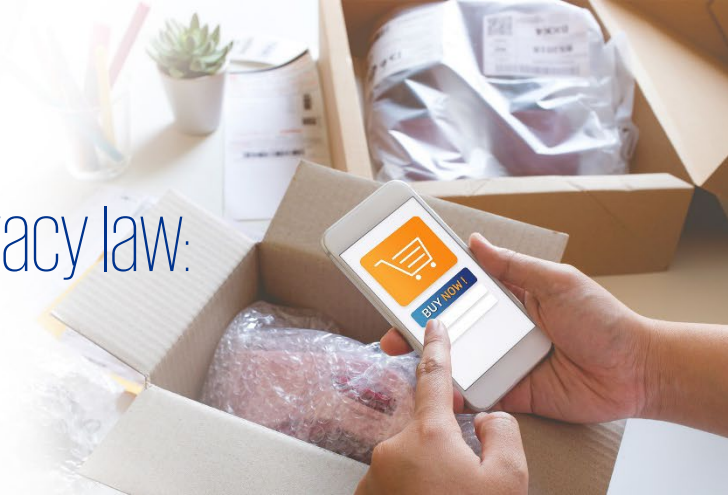
符涉莉律師事務所
SF Lawyers
In association with KPMG Law

China's new draft Data Privacy law: impacts on e-commerce providers



Introducing the Personal Information Protection Law

What's Happening?

China has over 610 million online shoppers (and growing)*. Unsurprisingly, massive volumes of personal data of Chinese consumers, such as names, mobile phone numbers, addresses and credit card numbers etc. are collected by e-retailers on a daily basis.

A brief look at China's history with data privacy and cybersecurity laws will highlight that the rules surrounding the topic span a number of laws and regulations such as the General Principles of Civil Law, Tort Liability Law, Law on the Protection of Rights and Interests of Consumers and more recently, the Cybersecurity Law (CSL) and E-commerce Law. There are also a number of national standards and sector specific regulations which also govern this topic. To navigate through the myriad of different regulatory requirements can be complex and challenging.

The new draft Personal Information Protection Law (PIPL), released on 21 October 2020 is meant to solve this problem while clarifying certain aspects in the data privacy rules. As online retailers hold a large amount of personal data of their consumers, they will need to keep updated with these latest developments.

*Source: https://www.chinadailyhk.com/articles/62/250/44/1551506282401.html as of December 2018.

So what's the big deal?

Things used to be quite straightforward before the internet became mainstream. In the past, consumers purchased their essentials locally and typically paid in cash. Thanks to the flourishing of e-commerce, Chinese consumers are now buying a variety of goods from online retailers around the world.

While the draft PIPL impacts on both domestic and foreign online retailers, the latter group will likely need to make the most adjustments to comply given they are currently not regulated by the CSL or other rules in relation to data privacy in China.

Under the draft PIPL, even if a foreign online retailer has no physical presence in China, as long as it processes the personal data of Chinese individuals to provide products or services to individuals in China, or to analyze or assess the behaviour of individuals in China or for other specified purposes under Chinese law, it will be captured by the PIPL.

Online retailers based outside China and shipping goods to customers in China, processing payments of Chinese consumers, or carrying out statistical, assessment or other similar processes will need to consider compliance with the PIPL.

Foreign online retailers will need to comply

What if we rely on a variety of third-parties to run our e-stores?

To offer the best shopping experience to customers, it is common for online retailers to engage third parties to provide key functionalities, such as the selling platform, or payment processing, logistics and delivering, or even customer data analytics to monitor customer preferences and for marketing purposes. These third party service providers help e-retailers to improve their efficiency and effectiveness in running their e-stores, However, they are involved in managing consumer privacy and need to comply.

One of the most frequently asked questions by online retailers is under what circumstances they will be held liable for the acts of these third party service providers in the event of a personal data breach.

Neither the CSL nor PIPL provide a definitive answer to this question. However, to minimize risks associated with the appointment of third party service providers, like the CSL, the draft PIPL imposes some obligations on retailers for using third party tools. These proposed obligations include the need for incorporating contractual measures and conducting risk impact assessments prior to the appointment of any third party.

It is worthy to note that the draft PIPL prohibits third party vendors from appointing sub-contractors to process customer data without the prior consent of the e-retailers who are presumed to be in control of such data. E-retailers are recommended to review their existing agreements with third parties to ensure compliance.

What if we (or our third party service providers) store or transmit data outside China?

To reduce costs and enhance efficiency, foreign online retailers operating in China often leverage global centralised IT or marketings systems, cloud or server storage to keep or back-up their customer data outside China. In some instances, their overseas affiliates may need to handle Chinese customer data. Such activities will inevitably involve the cross-border transfer of customer data.

Many foreign online retailers have been operating under the simplistic impression that data collected in China must always stay there. However, the position is more nuanced than that. The overall regulatory attitude, as exhibited by the draft PIPL, is to the permit the flow of data provided that relevant authorities are able to exercise supervisory powers. The CSL only imposes stricter overseas transfer compliance requirements on online retailers which are classified as an operator of critical information infrastructure (CIIO) as opposed to merely a network operator. The determination of a CIIO is never an easy exercise. An online retailer selling apparel will unlikely be a CIIO where retailers selling health care and pharmaceutical products may be regarded as one because of the health data they collected from customers may have important implication to the people's livelihood.

The draft PIPL seeks to provide clarity in this area by permitting the transfer of Chinese customer data to overseas on the conditions that online retailers have taken compliance steps, such as

a. obtaining explicit consent from customers,
b. Undertaking a personal information impact assessment,
c. conducting a security impact assessment approved by the authority and
d. obtaining a personal protection certification issued by the authority.

The first two steps are already stipulated under the CSL while steps (c) and (d) are new obligations proposed under the draft PIPL. We await the authorities providing more guidance on the scope of the impact assessments and how approval or certification can be obtained.

For online retailers, particularly non- CIIO retailers processing customer data overseas, they should be prepared to take the above compliance steps before the draft PIPL comes into force.

What can possibly go wrong if compliance with data privacy is not met?

The consequence of breaching the PIPL can be very serious.

Under the draft PIPL, any breach of the rules may attract a fine up to RMB 1 million, and in serious cases up to RMB 50 million or 5% of the entity's annual turnover for the previous financial year. However, it is unclear whether the annual turnover refers to global revenue or revenue generated within China. In addition, online retail stores may be ordered to suspend operations. Reputational damages may also be significant.

In view of this, we strongly suggest online retailers to take action early to ensure compliance. In this regard, we at SF Lawyers are more than happy to assist you in:

- reviewing current data privacy practices (including those of your affiliates and third-party partners)
- identifying whether you are considered to be a CIIO
- formulating a strategy to manage your customer data while taking into account compliance risk and practicalities
- constructing data privacy policies and providing training

Contact us

Feel Free contact our experts in data privacy for a discussion.

.

Leo Tian
Partner
SF Lawyers
T: +852 2847 5185
E: leo.tian@kpmglegal.com.cn

符莎莉律師事務所
SF Lawyers
In association with KPMG Law

www.kpmglegal.com.cn/hk/en/