符沙莉律師事務所
SF Lawyers
In association with KPMG Law

China's new draft Data Privacy law: Not just an administrative issue for Employers

What's Happening?

A brief look at China's history with data privacy and security laws will find that the rules surrounding the topic span a number of laws and regulations, such as the General Principles of Civil Law, Tort Liability Law and more recently, the Cybersecurity Law. There are also a number of national standards and sector specific rules which also govern this topic. It can be complex to navigate through and ensure compliance with a myriad of different legal requirements..

The new draft Personal Information Protection Law (PIPL), released on 21 October 2020 is meant to solve precisely this problem while clarifying certain aspects in the data privacy rules. Employers hold a large amount of personal data in relation to their employees and it is incumbent on them to keep updated with these latest developments.

So what's the big deal?

At first glance, one might think that data privacy should not really be such a big issue for employers. Unlike in a consumer context, there is often little resistance from individuals when the human resources department of any company asks for personal data. However, just because there is very little resistance does not mean that employers should not be paying attention to the data privacy reforms. In fact, we would say that because the type of data collected by employers in order to carry out HR tasks often involves sensitive personal data (for example, mobile phone numbers and bank account numbers), data privacy is a much bigger issue for employers than at first glance.

The draft PIPL requires data processors who process sensitive personal data to obtain express consent, provide the reasons for processing such data, and its implications. More onerously, data processors are required to conduct a prior risk assessment and maintain related records for at least 3 years.

Meeting these requirements can be quite challenging for employers for two reasons. First, employers generally do not conduct risk assessments before collecting/processing sensitive personal data. The second is that since much of the data collected from prospective candidates contain sensitive personal data, employers must be reminded to keep proper records of that data for 3 years, even where the candidate is rejected.

It remains to be seen how the PIPL will be interpreted and applied in practice. However, there is a real prospect that the PIPL could be applied to existing information held by employers at the time the law is passed, requiring them to maintain such data in accordance with the new PIPL standards.

What if we are headquartered in another part of the world?

One of the most frequently asked questions by multinational companies is in relation to cross-border transfers of personal data. Many employers utilize HR systems, or HR teams not located within China. As a result, one of the ongoing challenges is to navigate through the complex web of data privacy laws to ensure compliance, prior to the sharing or transmittal of such personal data.

In this regard, the draft PIPL is welcomed in that it seeks to provide some clarity on this long uncertain area. Specifically, the PIPL sets out various requirements and mechanisms to be taken for the purposes of cross-border transfers of information. What employers need to continue to be cautious of is the meaning of "cross-border" transfer. In the modern day where data may be stored on servers or backed up outside China, or where communication is via email or instant messaging, it is very easy for personal information to be sent "cross-border" (e.g., if the recipient happens to sit in a different jurisdiction). A click of a button may potentially cause an employer's need to comply in China. Processes should be in place to minimize such risks and appropriate actions to be taken if this does occur.

What if we outsource our HR Function?

Running a global business has never been easy, and equally difficult as an employer with employees in a foreign jurisdiction. In order to minimize compliance risks, the outsourcing of HR functions and processes to local specialists has soared in recent years. In some instances, to minimize costs, some companies have chosen to use offshore HR specialists in less expensive jurisdictions to handle these matters.

While the benefits are obvious, given the increased requirements arising out of the PIPL, employers may need to revisit whether the benefits of using an HR specialist outweighs the risk.

Based on the current draft PIPL, a risk assessment must be conducted prior to sharing the data with a third-party. Separately, the data can only be shared after obtaining the explicit consent of their employees. In addition, employers must ensure that the third party engaged will not further pass on the personal data without the consent of the employees. Additional care must be taken in order to protect employees' data if the third party operates outside of China.

What should you do?

What is becoming obvious is that governments around the world are taking data privacy extremely seriously and it is for good reason. Personal data has much more use cases than one or two decades ago. The advancement of technology has turned personal data from mere data to a key to a person's private life, wealth and livelihood, and unlike other "keys", it is not one which you can simply lose and replace.

While this may seem overwhelming, this is only the tip of the iceberg. 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 (whichever is greater). Reputational damage may also be considerable too.

In view of this, we strongly suggest employers 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 critical information infrastructure organisation
- formulating a strategy to manage your employee 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/