China's Largest Potential Data Privacy Breach Provides Cautionary Tale for International Employers: 5 Steps Your Business Should Take

Insights
10.03.22

Hackers allegedly stole the personal data of over 1 billion Chinese residents from a police database in Shanghai earlier this year – and the largest potential data privacy breach in the nation's history should serve as a warning to all companies doing business in China. The breach came after China's Personal Information Protection Law (PIPL) took effect last year, which imposes stringent security safeguards on corporate and government entities that handle personal information. While the Shanghai police department whose data was breached is unlikely to be held liable for political reasons, the potentially severe penalties under the PIPL are real and more likely to be enforced against private-sector employers, especially those with foreign ownership. This Insight provides a five-step plan for businesses with operations in China or for those who manage information from that country to avoid critical consequences.

What is the PIPL?

The PIPL, which became effective on November 1, 2021, is China's first major piece of legislation tackling the protection of personal information.

Article 4 of the PIPL defines personal information as any information in any format, electronic or otherwise, relating to any identified or identifiable natural person, not including anonymized information. Article 4 also defines "processing" of that personal information as collection, storage, use, transmission, provision, disclosure, and deletion of personal information.

To Whom Does the PIPL Apply?

Article 73 of the PIPL defines personal information processors as any organization or individual that independently decides the purpose and method of processing personal information. Thus, anyone or any company – whether located in China or not – involved in such activities regarding individuals in China is subject to the PIPL.

The PIPL also applies to anyone or any company outside of China processing personal data from China to provide products or services to individuals in China or to analyze those individuals' behavior. American employers that control or process the personal information of their Chinese employees or customers are accordingly subject to this law as well.

Copyright © 2024 Fisher Phillips LLP. All Rights Reserved.

customers are accordingly subject to this law as well.

What are the Penalties for Data Breaches under the PIPL?

The potential penalties for data breaches under the PIPL vary widely and can be quite significant. For example, such breaches could result in fines ranging anywhere between $7.8 million USD (RMB 50 million) and up to 5% of a company's previous year's business revenue. A company could also be publicly shamed on the social credit system or even prohibited from conducting any further business in China.

Should a company be civilly prosecuted, the company will have the burden of proof of compliance and face unlimited liability. Further, company executives and data protection officers could be held individually responsible and be subject to penalties up to $157,000 USD (RMB 1 million) or even jail time.

With such grave consequences, individuals and companies that handle personal information or who are otherwise subject to the PIPL should be careful to review their policies and systems to prevent against breaches wherever possible.

What Can Employers Do to Stay Compliant? A 5-Step Plan

Below are five practical steps you can implement if you conduct business in China or manage significant personal information of Chinese employees or customers to stay compliant with the PIPL.

1. Understand the requirements

The PIPL includes a data localization provision requiring storage of personal information within China if the volume of data handled exceeds a certain threshold set by the Cyberspace Administration of China (CAC). Before the data could be transferred oversees, the data would first be subject to the CAC's security assessment. The ability to provide localized data to foreign regulators and courts is restricted as transfer of the data must first be approved by "the competent authorities" of the Chinese government.

2. Create data mapping and a clear data inventory

The PIPL requires companies to classify data into general, important, and core categories. Employers will want to implement data classification and management mechanisms for the categories of personal information processed.

Employers should implement reasonable security measures to protect the safety of personal information handled. Such measures may include anonymization, de-identification, or data minimization.

3. Appoint a data processing officer

Copyright © 2024 Fisher Phillips LLP. All Rights Reserved.

Employers will want to evaluate whether they may be required to appoint a data processing officer to supervise their personal information activities and protective measures taken. The appointment of a data processing officer is required should an employer's volume of personal information processing activities reach the threshold requiring data localization.

The CAC has not yet set the threshold, but recommended national standards suggest a data processing officer should be appointed if:

- the employer's main business is to process information and has over 200 employees;
- an employer currently or anticipates processing personal information of over 1,000,000 employees or customers in a 12-month period; or
- an employer processes sensitive personal information of over 100,000 employees or customers.

Data processors have strict reporting obligations to notify affected employers, consumers and regulators of the risk of data breaches, remedial actions taken in the event of any incidents. General incidents should be reported within three working days, while sensitive incidents must be reported to regulators within eight working hours.

4. Provide appropriate notices to consumers

Employers that process sensitive personal information of their employees and/or consumers will need to first obtain explicit consent from the individuals or their guardians that explains the reason and impact of processing the data.

5. Provide policy updates and training

Employers should prepare and regularly update a compliant data security policy along with an incident response plan, and should conduct a security assessment in line with the PIPL requirements at least annually. All employees involved in processing and supervising the processing of the personal information data should be adequately trained on the PIPL and updated regulations impacting the PIPL's enforcement.

Conclusion

The PIPL is one of the most restrictive data privacy laws in the world. If your organization does business or employs any individuals in China, or processes personal data from China, please contact your Fisher Phillips attorney, the authors of this Insight, or any attorney in our International Practice Group to learn more about the implications of this new law.

We will monitor these developments and provide updates as warranted, so make sure that you are subscribed to Fisher Phillips' Insights to get the most up-to-date information direct to your inbox.

Copyright © 2024 Fisher Phillips LLP. All Rights Reserved.

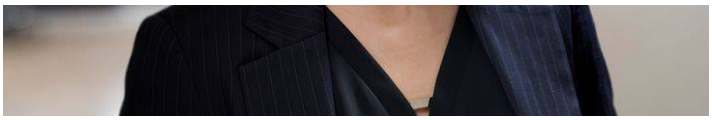
Related People

Nazanin Afshar
Partner
818.230.4259
Email

Ariella T. Onyeama
Of Counsel
213.402.9583

Email

Copyright © 2024 Fisher Phillips LLP. All Rights Reserved.



Nan Sato, CIPP/E, CIPP/C
Partner
610.230.2148
Email

Service Focus

Privacy and Cyber

International

Copyright © 2024 Fisher Phillips LLP. All Rights Reserved.