Data Privacy Detective Podcast – Episode 20 – China's New Data Privacy Standards

May 16, 2018

Categories:

Blogs
Podcast
Publications
Technology Blog

Authors:

Joseph J. Dehner

Let's explore China's approach. It reaches far beyond the sectoral approach taken by the U.S., Japan and other countries that lack an overarching personal data privacy protection law. It follows generally much of the European model but embodies differing restrictive and protectionist principles that reflect Chinese culture and political order. Businesses inside and outside China must pay attention.

New Standards Fill the Gaps of the Network Security Law

The May 1 standards are not "regulations" directly enforceable as understood in western countries. They are instead standards that Chinese authorities will use in judging data privacy measures of businesses that deal with personal information. These standards arise as a kind of "gap-filler" implementation of the Network Security Law of the PRC that took effect on June 1, 2017. This law, also called the Cybersecurity Law, applies directly only to "network operators." It provides a framework for regulating goods and services marketed over networks as well as the operation and maintenance of data networks. Announced by the Cyber Administration of the PRC, it was accompanied by Measures for the Security Review of Network Products and Services that likewise took effect on June 1, 2017. This second framework called for all network products and services to meet national PRC standards that would be set over time for all "owners, operators, and service providers of networks." This is a deliberately broad definition of what businesses are regulated by standards as they are issued.

Wide Application and Enforcement

Businesses covered by standards that are issued must address security leaks and defects, inform users and authorities, and

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

remediate. A network operator or service provider must maintain security for customers, inform users, and obtain consent from persons whose personal information is collected and processed. If a network service or product implicates national security, Chinese authorities will conduct a security review of the system. The Law and Measures will most likely be applied to any business or person with a website, mobile app or online platform operated or used in China. If a user has relevant records of information prohibited by the Law that it publishes, it must report the data to the authorities.

Unlike the EU's GDPR, the Chinese Law has a data localization requirement that requires Critical Information Infrastructure Operators (CIIOs) to keep important data and personal information within China, data that cannot leave China without a legitimate business need and only after a security review. While Article 31 of the Law has a list of Critical Information Infrastructure (CII), the list is not exhaustive and the definition of CII is not clear. Different Chinese economic sector regulators have lists of CIIs under their jurisdiction, most of which are state-owned enterprises.

Before the May 1 standards became effective, actions were taken against non-Chinese companies under the Law. One example was the shutdown of Marriott's Chinese website for a week because the site listed Taiwan as a "country." Non-Chinese airlines, including Delta and Qantas, were criticized for similar listings and were ordered to remove such "illegal content" from their sites, which they promptly did and made public apologies. This example shows how China does not regard cyberspace as immune from territorial sovereignty but will instead be treated like any other type of activity that takes place within China.

A Comparison With the GDPR

While the May 1 standards for personal information protection generally follow the GDPR approach to strict and comprehensive protection of personal data, including an emphasis on obtaining express consent from those whose personal information is collected and processed, there are significant differences from the GDPR:

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

- The Chinese definition of "sensitive personal information" is much broader than the EU meaning – extending to any personal data that would cause harm to persons, property, reputation or mental and physical health.
- The GDPR does not insist upon a data subject's prior consent to the use of personal data but allows a controller's or processor's legitimate interests as a basis for collection and use. The Chinese standards do not have the GDPR's flexible "legitimate interest" exception to consent, though there are limited exceptions listed to the consent requirement, including the need for troubleshooting of goods and services.
- Privacy notices must meet more specific requirements than demanded by GDPR, and Chinese privacy notices must be presented to a person "one by one."
- The Chinese standards demand specific security testing and validation procedures for processing personal information, consistent with the Chinese Government's overriding interest in national security that means more intrusive governmental access to and control over personal data than is generally the case in western countries.

How Companies Can Prepare for Ensuing Data Privacy Laws in China

Non-Chinese companies that market or sell within China must take heed. Even though the May 1 standards are not legally binding in the sense of GDPR or the law-plus-regulation approach in western societies, the standards amount to central guidance to the variety of Chinese Ministries and enforcement officers that deal with personal information. It is expected that when China adopts further formal laws about data privacy, the standards will be the starting point for what becomes binding legislation. Even the word "standard" as used here can be misunderstood, as a better translation may be "specification." A non-Chinese company intending to grow serious business in or with China should view the May 1 standards as guidance of what is and is not required and allowed. Businesses wishing to conform to Chinese data privacy principles should consider the following:

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

- Design systems to obtain consent from users for use and cross-border transfer of personal information of Chinese persons;
- Meet network security rules and be vigilant about emerging standards;
- Offer a means of resolving complaints about information to which the Chinese government may object;
- Consider the particular authorities that may regulate them; and
- Team with local Chinese partners to keep data within China when required.

This last point – data localization – differs from the European approach that permits data transfers outside of the EU if to a country or business that is deemed "adequate" and committed to enforce data protection rules similar to those of the EU. It indicates a protectionist and territorial approach to controlling data privacy of Chinese nationals that could become a major issue in trade negotiations.

Conclusion

China has the world's largest web-connected native population, and e-commerce is growing rapidly there. Businesses that operate in or wish to offer goods and services in China will need to design data protection systems to conform with Chinese expectations. The May 1 standards are the best indicator of how a compliant system can be designed.

For more information, please contact Joe Dehner or any attorney in Frost Brown Todd's Privacy and Information Security Law Practice Group.

View the original article as a Frost Brown Todd Legal Update: Data Privacy Detective Podcast – Episode 20 – China's New Data Privacy Standards.

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

FBT Gibbons