

# Global Cybersecurity Apparatus Development: Comparing the Chinese and European Models

*Can vague legal criteria for personal information protection spark innovation?*

[Based on the event "Understanding China's Emerging Data Protection Regime" on September 26, 2018](#)

## Highlights and Key Takeaways

- ◆ Compliance with different cybersecurity laws across borders has emerged as a top challenge in global business.
- ◆ The ambiguity of China's Personal Information Security Specification ("the Specification"/ [个人信息安全规范](#)) could disadvantage many foreign businesses.
- ◆ While Europe's GDPR prioritizes individuals' right to data privacy, China's Cybersecurity Law and the Specification hold national security as the ultimate goal.

## Executive Summary

As some of the first major regulations on cybersecurity, the EU's recently implemented [General Data Protection Regulation \(GDPR\)](#) and China's [Cybersecurity Law \(CSL\)](#) have inevitably set standards for the rest of the world to consider when determining how to govern cyberspace. Despite some differences, these two laws both take government-oriented, onerous approaches to data protection. This, coupled with the lack of a comprehensive cybersecurity law in the US, has necessitated that US businesses operating abroad develop reactionary plans. For those global businesses that operate in both Europe and China, it is important to understand the key similarities and differences between the GDPR and the CSL.

## The Personal Information Security Specification

As previously discussed in the first Insights, "[Navigating the Chinese Cybersecurity Law](#)," the CSL serves as an overarching legal framework for cybersecurity while key terms such as "personal data" await clearer definitions. The Specification, an effort by the Chinese government to regulate personal information and data, took effect on May 1, 2018.

The Specification has come under the spotlight for three major reasons:

- ❖ There has been **public outcry** for better data privacy rights protection (e.g., misuse of user data by Chinese ride-hailing company DiDi), making the release of the Specification timely.
- ❖ Some, including AmCham China members, have raised concerns that the **ambiguity** of the Specification could allow the government to give certain tech companies – those who thrive on big data – some leeway, while closing doors on others. Some members worry that this could leave foreign companies in a **vulnerable position** as “**Made in China 2025**” takes off at full steam. However, insiders familiar with the matter have suggested that the intention behind the vague wording is to encourage more innovation.
- ❖ It is unclear how strictly the Specification will be enforced. In general, standards (标准) like the Specification are supposed to be optional. Some argue that, in practice, businesses in China **have been asked to comply** with measures and standards that claim to be not mandatory. This is the case especially for government agencies and SOEs.

## The Specification vs. GDPR

Many refer to the Specification as the Chinese version of GDPR because they are similar in several ways, including their use of ambiguous language and protection of the right to request corrections and deletions of personal data and information.

Despite some common elements, the similarities are predominantly superficial. What really sets the Specification apart from its European counterpart is the ultimate intention behind the regulations. The GDPR sets **individual privacy protection** as the top priority, whereas the Specification and the CSL in general are designed with **national security interests in mind**. However, there is a consensus that certain efforts were made to **strengthen** Chinese users’ control over data.

Major differences between the two regulations:

Differences	Personal Information Security Specification	GDPR
❖ Definition of consent	❖ Although consent is defined similarly as in the GDPR, it can be implied or silent	❖ Explicit consent with affirmative actions (e.g., checking a box)
❖ Other grounds for consent	❖ Lower compliance risk as consent can be inexplicit and therefore present more pathways for companies to utilize user data	❖ High costs and regulatory risks for meeting explicit consent requirements
❖ Enforcement	❖ Open to interpretation by authorities from the local to central level	❖ GDPR is binding to all EU members

It is important to remember that the Specification is a national standard that falls under the umbrella of the CSL, an overarching framework that is still taking shape. The Specification, like other standards and

measures, will continue to evolve. AmCham China members are advised to **stay vigilant** with upcoming changes, review all network security rules in China, and **cross reference** them with the GDPR.

---

*If you have questions about the event and or would like to join AmCham China's Information and Communications Technology Forum, please contact [Evan Schmitt](#).*

*For inquiries on Insights, please contact [Chloe Ma](#).*