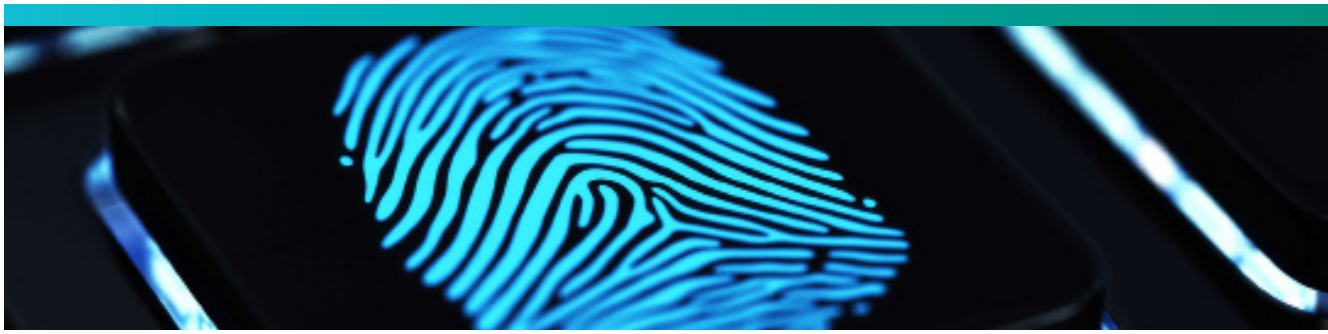
protiviti®
Face the Future with Confidence



China's Cybersecurity Law: Personal Information Protection Overview

As part of our series providing insights into the Cybersecurity Law of the People's Republic of China (PRC), this Point of View (POV) highlights a key area pertaining to personal information protection.

Personal information is defined as information that can be used individually or in combination with other information to identify a person. Requirements around the dissemination and management of personal information by network operators are prescribed within the Cybersecurity Law and are closely linked to the national standard of personal information protection, the Personal Information Security Specification ("the Specification").

The enforcement of personal information protection is primarily based on the Territoriality Principle: all legal entities operating in mainland China must comply with legal requirements, and authorities can prosecute offenses committed within the Chinese border. This means that both local and multi-national companies operating within mainland China are accountable for personal information protection and must comply with requirements outlined in the Cybersecurity Law and the Specification. It is therefore essential that companies understand these requirements and address the potential compliance challenges discussed in this POV.

Overview of Personal Information Protection

Both the Cybersecurity Law and the Specification prescribe a set of principles for network operators around personal information protection. Although the Specification is neither a law nor a regulation and cannot legally make any official judicial interpretations of the Cybersecurity Law, it is one of the most important national standards concerning the protection of personal information in China. Corporations are recommended to comply with the Specification to demonstrate compliance with the personal information protection requirements under the Cybersecurity Law.

Since late 2018, the Cybersecurity Law has been referenced by the Ministry of Public Security, the Ministry of Industry and Information Technology, the Cyberspace Administration of China (CAC), and State Administration for Market Regulation during investigations and prosecutions of illegal acts. Going forward, the Specification and other upcoming rules and measures will be utilized and developed by regulatory authorities to facilitate law enforcement.

Compliance Requirements of Personal Information Protection

Under the Cybersecurity Law, network operators are required to fulfill certain technical security measures and compliance procedures to protect personal information. Furthermore, the Specification, along with other laws and administrative rules[1] from regulatory authorities, are applied to the Cybersecurity Law for clarification, interpretation, and stipulation.

The following table summarizes the personal information protection requirements:

Article	Legal Requirements
No. 40	Network operators must establish and complete user information protection systems and maintain the confidentiality of user information they collect.
No. 41	Network operators must abide by the principles of legality, propriety and necessity in collecting and using personal information. They should not gather personal information unrelated to the services they provide, and they must abide by the provisions of laws, administrative regulations, and agreements with users when using or processing the personal information they have stored.
* No. 42	Network operators must not disclose, tamper with, or destroy personal information they gather. They must not provide personal information to others without the consent of the person whose information has been collected, unless the information cannot be used to identify a specific individual. Network operations must also adopt technical and other necessary measures to ensure the security of personal information they gather, and to prevent personal information from being leaked, destroyed, or lost.
No. 43	Network operators should have measures for deleting or making corrections to the personal information they collect, on reported violation of laws, administrative regulations or agreements between the parties in the collection or use of personal information, or any errors in the collected personal information.
* No. 44	Individuals or organizations must not steal or use other illegal methods to acquire personal information. They must not unlawfully sell, or unlawfully provide others with personal information.
* No. 45	Legally responsible departments and staff must keep personal information, private information, and commercial secrets strictly confidential. They must not leak, sell, or unlawfully provide it to others.
No. 49	Network operators must establish network information security complaint and reporting systems, as well as accept and handle complaints and reports relevant to network information security.

* Warning: violations of these provisions may lead to criminal prosecution based on Article 253 & 286, Criminal Law Amendment 9 of the People's Republic of China

[1] These laws and rules include the Criminal Law, Public Security Administration Punishment Law, Self-Assessment for Illegal Personal Information Collection, and Provisions on the Cyber Protection of Children's Personal Information.

Privacy Protection Comparisons between the Cybersecurity Law and General Data Protection Regulation (GDPR)

While there are similarities between the Cybersecurity Law's obligations around personal information protection and the European Union's (EU) GDPR, there are also some distinct differences. Below is a comparison of the Cybersecurity Law and GDPR in various areas:

Jurisdiction Principles

CYBERSECURITY LAW

The Cybersecurity Law is based on a Territoriality Principle, requiring compliance by any company processing personal information within mainland China. As such, even multi-national companies within mainland China must comply with the personal information protection requirements outlined in the Cybersecurity Law even if they only process personal information belonging to citizens of other countries. In addition, industries or business functions in marketing and sales, data analysis, medicine, customer relationship and others related to personal information processing are obligated to comply with those requirements.

GDPR

GDPR is based on a Personality and Protective Principle. It stipulates that entities in countries beyond the EU providing services or goods to its citizens can fall under GDPR requirements.

Legislative Perspective

CYBERSECURITY LAW

The Cybersecurity Law considers personal information protection as part of the network operator's responsibilities. Administrative authorities can take legal enforcement actions on network operators whom they believe have not fulfilled obligations around personal information protection and can require network operators to provide evidence of compliance.

GDPR

GDPR tends to regard privacy protection as the data subject's right. Therefore, to justify penalties for infringements of GDPR, administrative authorities in the EU must prove with solid evidence that a violation against the regulation and data subject rights exists or a data breach has led to the disclosure of private data.

Sources of Law

CYBERSECURITY LAW

As the Cybersecurity Law is a law with Chinese sources of law, this has several implications. First, the Cybersecurity Law will have effect within the territory of mainland China, and no national regulations, rules or local legislation can override it. Secondly, when not conflicting with the Cybersecurity Law, administrative regulations and rules enacted by state councils of the PRC and subordinate ministries and commissions can prescribe detailed specifications, standards, and procedures to enforce the Law.

GDPR

GDPR should be regarded as an administrative regulation or international agreement created by the European Parliament and the Council of the European Union. Although GDPR claims to be effective in the EU and the European Economic Area, it cannot conflict with the laws of sovereign states within the EU. Furthermore, there is no unified EU enforcement agency for GDPR, nor are there unified specifications, standards and procedures. Thus, each sovereign state in the EU has the right to lay down rules on penalties applicable to GDPR infringements, and each supervisory authority shall take legal enforcement actions on their own.

Legal Penalties

CYBERSECURITY LAW

The Cybersecurity Law may refers to both the Public Security Administration Punishment Law and the Criminal Law of the PRC to determine penalties for legal violations and offenses, which include administrative fines, custody, and, in the worst cases, criminal sentences. Because of the differences between Administrative Punishment Law and Criminal Law, the severity of penalties vary depending on which is broken.

GDPR

The typical penalties issued under GDPR are administrative fines that generally fall below €1 million ($1.08 million USD) for a single case. Notable exceptions include a fine of €204 million ($220 million USD) issued to British Airways for a data breach; €50 million ($54.1 million USD) issued to Google for transparency violations in France; and €2.6 million ($2.8 million USD) issued to the National Revenue Agency in Bulgaria for stolen personal data.

When comparing the Cybersecurity Law and GDPR, it is clear that personal information protection clauses in the Cybersecurity Law prescribe more severe penalties for the violation of the respective personal information protection clauses. Organizations' senior leadership should pay close attention to the request of comments on the Public Security Administration Punishment Law, since the public security agency has the authority to perform administrative adjudication without public defense and judgment, and it is possible that the ruling may include a period of jail time.

Compliance Challenges

Cybersecurity Threat

Cybersecurity threats present a potential challenge for companies trying to achieve compliance to personal information protection regulations. According to The Internet Security Threat Report from Symantec, there is one phishing email in every 3,208 emails in China, and the country's spam rate is up to 62.2 percent. Of 545,231 ransomware attacks globally, 16.9 percent were targets in China, among the top three targets for these

attacks. China also contributed 19 of 49 espionage indictments by U.S. authorities, and is one of the top sources of Internet of Things (IoT) attacks at 24.0 percent. As cybersecurity is a part of personal information protection, it is imperative that companies take measures to defend against security threats.

However, this is complicated by a shortage of security professionals in China. The CAC reported in September 2018 that the gap in security professionals would reach 1.4 million by 2020. Without enough security professionals to work on technical solution development and security processes adjustment, it is difficult for legal compliance to be effective and continuous.

Economy and Business Environment

The progress of digitalization in China has deeply impacted all aspects of the economy and enabled rapid market expansion. The increasing reliance on internet technology saw the monthly active users of China's mobile internet reaching 1.136 billion as of June 2019, according to data from QuestMobile. Market penetration of social media reached 87.2 percent as of December 2018, with WeChat reported as the most used platform.

A challenge resulting from these trends is that when designing technical solutions for legal compliance, especially for personal information protection, companies must consider both business functional operation and user experience in the development phase. Otherwise, businesses will expose themselves to legal risks when compliance solutions are abandoned due to poor user experience, operation performance pressure, and market competition.

Data and DevOps Lifecycle Management

The Specification provides detailed technical requirements regarding data, development, and data lifecycle management, which may not be compatible with companies' existing application systems.

Companies may realize that compliance with personal information protection regulations will be needed beyond firewalls at the network border and anti-virus application in endpoints, while supply chains will make the compliance with privacy regulations even more complicated.

While the Cybersecurity Law holds network operators accountable for personal information protection, the Specification prescribes compliance requirements for controllers, not processors. Therefore, not only will each network operator need to comply with personal information protection, they will also have to provide specific instructions to prevent suppliers from intentionally or accidentally violating the legal requirements. This is especially important in China, where the rule of law may sometimes be neglected in favor of political or financial considerations.

To comply with these requirements effectively and efficiently, technical control solutions designed for compliance must be integrated into some processes to provide continuous implementation.

Data Security and Privacy Protection Technology

Although there is some overlap, data security and privacy protection may apply different technologies and solutions from those used in infrastructure and application security. While infrastructure and application security uses sessions to manage access control, data access is controlled by cryptographical algorithms and keys. Privacy protection complicates matters further as it relies on technology such as de-identification and tokenization. As such, securing infrastructure and applications does not automatically mean that data and personal information are protected.

Application developers and system administrators need to align with suppliers, select proper technical solutions, re-design infrastructure and application systems, and make multiple changes in order to fulfill compliance requirements. This will likely require additional technical resources and investment.

Furthermore, enterprises in mainland China will likely find it difficult to find technical professionals in data security and privacy protection. The reason for this shortage is the historical lack of value attached by management to data and personal information. Even though they are increasing in importance, data and personal information can be legally, or to some extent illegally, acquired and exchanged in the market. Investment in data and personal information protection is seen by management as having a poor return on investment, thus there is less interest in hiring for data security and privacy protection. Furthermore, most security professionals are former system administrators and software developers who may be reluctant to step into a relatively new environment.

Protiviti Cybersecurity and Privacy Protection Services

IT Specialized Audit	• Often included in the overall audit co-sourcing or outsourcing program • More in-depth and technical than Information Technology General Control (ITGC) audit • Often focused on a specific part of IT operations such as Cybersecurity or Disaster Recovery
Security Risk and Compliance Assessment	• International Security Standards: ISO/IEC 2700x, NIST Cybersecurity Framework, CSA Cloud Control Matrix • Payment Card Security Standards: PCI DSS 3.x • Other Regulations/Standards: China Cybersecurity Law, HKMA, SFC, MAS, COSO SOX, ISO/IEC 27701
Data Privacy Services	• Compliance assessment against privacy regulations: Hong Kong PDPO Cap.486, China Personal Information Protection, EU GDPR, US CCPA • Managed privacy services: Privacy-as-a-service • Personal data inventory advisory
Attack and Penetration Service	• Vulnerability scan and penetration test • Source code review • Red team test • Phishing and social engineering test
Security Program and Strategy Design	• Design and revision of cybersecurity strategy and program • Design and revision of security policies, such as data and information classification • Design, revision, and implementation of security procedures
Security Architecture and Control Design	• System hardening review and enhancement • Security architecture design: on-premise, cloud platform • Security control design and review: firewall, data loss prevention, privileged access management, event log analyzer
Security Implementation Services	• Security tools design and selection • Project management and support for security tools implementation • Leverage Protiviti global partnerships with OneTrust, SailPoint, CyberArk, Palo Alto, ServiceNow, Carbon Black, Splunk, LogRhythm, etc.
Managed Security Services	• Security resource augmentation • Managed security operations • Third-party risk outsourcing
Incident Response and Forensics	• Security incident response advisory and support • Security incident investigation and root-cause analysis • Compromise assessment
Security Awareness and Capability Advisory	• Blueteam security assessment and advisory (e.g. SOC, MSSP) • Cyber incident handling and mitigation review • Security awareness assessment and support

How Protiviti Can Help

Protiviti aids businesses in ensuring their IT services meet legal requirements and regulatory rules on both national and industry-specific levels. With our IT security professionals, compliance experts, auditors, as well as other IT professionals, we are able to quickly react to constantly evolving regulations based on industry innovations, environmental trends, and emerging risks.

Protiviti security and privacy services will evaluate your existing state of compliance in accordance to relevant legal requirements and regulations before developing technical solutions corresponding to your current technology, procedures, as well as resources competency. We expect to close any gaps in your IT technology and processes within budget while preventing disruptions to normal IT and business operations from compliance activities.

Contacts

Beijing

Unit 718, China World Office 1
No. 1 Jianguomenwai Street
Chaoyang District
Beijing 100004, China
Tel: (86.10) 8515 1233

Shanghai

Rm. 1915-16, Bldg. 2, International Commerce Centre
No. 288 South Shaanxi Road
Xuhui District
Shanghai 200030, China
Tel: (86.21) 5153 6900

ShenZhen

Unit 1404, Tower One, Kerry Plaza
No. 1 Zhong Xin Si Road
Futian District
Shenzhen 518048, China
Tel: (86.755) 2598 2086

HongKong

9th Floor, Nexxus Building
41 Connaught Road
Central, Hong Kong
Tel: (852) 2238 0499