China Releases Data Security Law: Some Expert Observations and Comments

China's Data Security Law was published on June 10, 2021, and will be formally effective starting September 1, 2021.

This law can be treated as another pillar of China's legal framework on information security and data (privacy) protection, besides the Cybersecurity Law (CSL) that was launched in 2017 and focused on network security and the Personal Information Protection Law (PIPL), which is at the second reading stage and expected to be published later this year.

It has been only two months since the second reading of the draft Data Security Law (in April of 2021), which indicates that Chinese legislative authorities are eager to publish it quickly to tackle emerging threats to data security.

In this article, we address the main changes in the published version of the Data Security Law as compared to its second draft. We also highlight the areas of concern for foreign companies running businesses in China.

China's Data Security Law: Key provisions

We have highlighted the changes made to the final version and the major concerns of the law as below:

- **Top-down strategy** – the law does not only specify the legal requirement details but also states that the government will implement the national data protection mechanism through "top-level design" with related organizations. There are still some ambiguities, such as the definition of "important data" and "core date", but we can expect more detailed regulation or rules to be issued by local authorities or industry-related ministry, such as the "Data Security Management Regulation", which has been listed on the State Council's legislative agenda for 2021 already.
- **Data classification and grading protection** – the law requests to establish the system to classify the data as "important data", "core data", and general data based on its sensitive nature, impact on national security, and potential damage in case of data breach. Each type of data needs to be protected with corresponding measures. For the companies in China that utilize the internet for data processing, MLPS (Multiple-Layer Protection Scheme, first introduced in the CSL) should be the foundation of data security management process to cover full data life cycle.
- **Data localization and cross-border transfer** – For CII (Critical Information Infrastructure) Operators, the important data should be saved in the territory of China and cross-border transfer is regulated by the CSL; for non-CII operators, the important data cross-border transfer is expected to be regulated by the measures announced from the Cyberspace Administration of China (CAC) and other authorities. However, those "measures" have still not yet been released.
- **Continuous data protection management** – the company should take organizational measures to provide enough resource for building the data protection management system through all business processes, specifying the person in charge of data security and related management agency to fully bear the data security responsibility.
- **Data utilization** – China admitted that data is a "new type of production factor" in 2020, and the

country's law encourages the development and commercial use of data. Consequently, under the state's "big data" strategy, the creative utilization of data in all industries has been supported.

- **Legal consensus** – both the company and the individual who oversees data protection will be subject to penalties and other administrative punishments specific for companies. The maximum penalty for the violation of the core data management system is RMB 10 million along with the revoking of the business license for companies, while the maximum penalty on the directly responsible person would be RMB 500,000.

How to avoid risk of non-compliance under the Data Security Law?

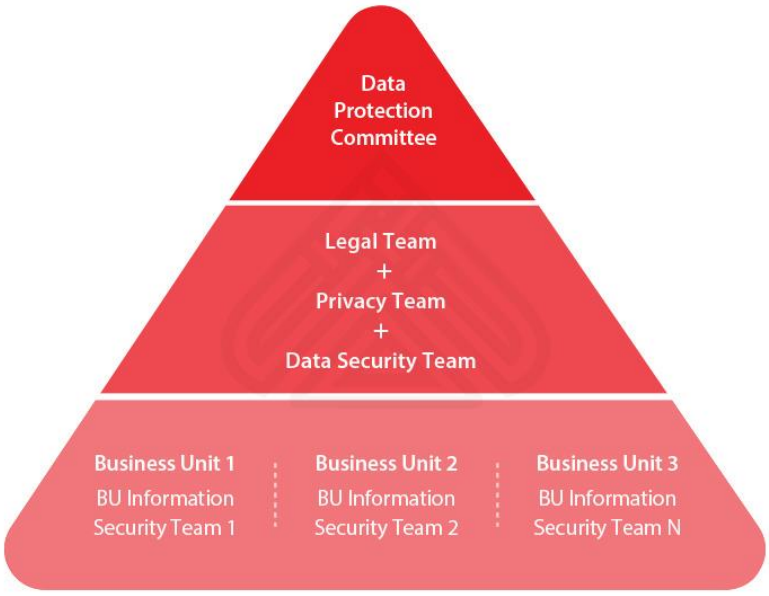
Here we provide few suggestions from the technical perspective on the methodology of compliance with the Data Security Law.

Organizational resource provision

Data protection brings new challenges for companies as it is beyond the traditional information security scope, therefore, existing resources inside the company (normally, the IT team or information security team) might be incapable of fulfilling the responsibility of data protection.

The company needs to assign the resource and build up the data protection management team with a top-down structure, such as the "information security committee", which involves legal, technical, and business departments on the top, followed by the professional team from the legal, privacy, and IT departments. For big companies, the information security team of each business unit needs to be involved as well.

Top-Down Structure of the Data Protection Management



Graphic© Asia Briefing Ltd.

Teamwork between IT and legal team

The compliance of data security apparently needs both IT and legal teams working together for compliance work. The legal team can interpret the legal clause and identify the detailed requirements (on an abstract level) that should be fulfilled by the company, and better convert such legalese into a format that can be easily understood by the IT department.

On its part, the IT team needs to locate the suitable technical control measures and toolkits to perform the actual data protection. When a company intends to seek the professional expertise of an external party, the capability and integration of both technical and legal resources should be considered on priority.

Identification of requirements by respective stakeholders

Besides the direct requirement from the law and regulation from authorities, there are many requirements from other stakeholders that need to be considered as well, such as external clients, partner, or supplier.

For B2C businesses, the consumer's personal information processing will be regulated by the Data Security Law. For B2B businesses, the business secrets and other business data is important data for protection as well.

Such assessments require the company to analyze their business model and identify all potential stakeholders, then further collect and identify their respective requirements on data protection.

Data asset inventory and data mapping

All data protection control measures, either technical (such as encryption) or organizational (such as requesting the staff to follow specific data processing procedures), should be applied to the target – which is the data itself; therefore, the inventory of the data is one important and basic step in the whole data protection process.

Before talking about how to protect the data, few questions should be answered first: what data does the company have, where is the data saved, how is the data collected and processed, who are accessing the data and in which ways?

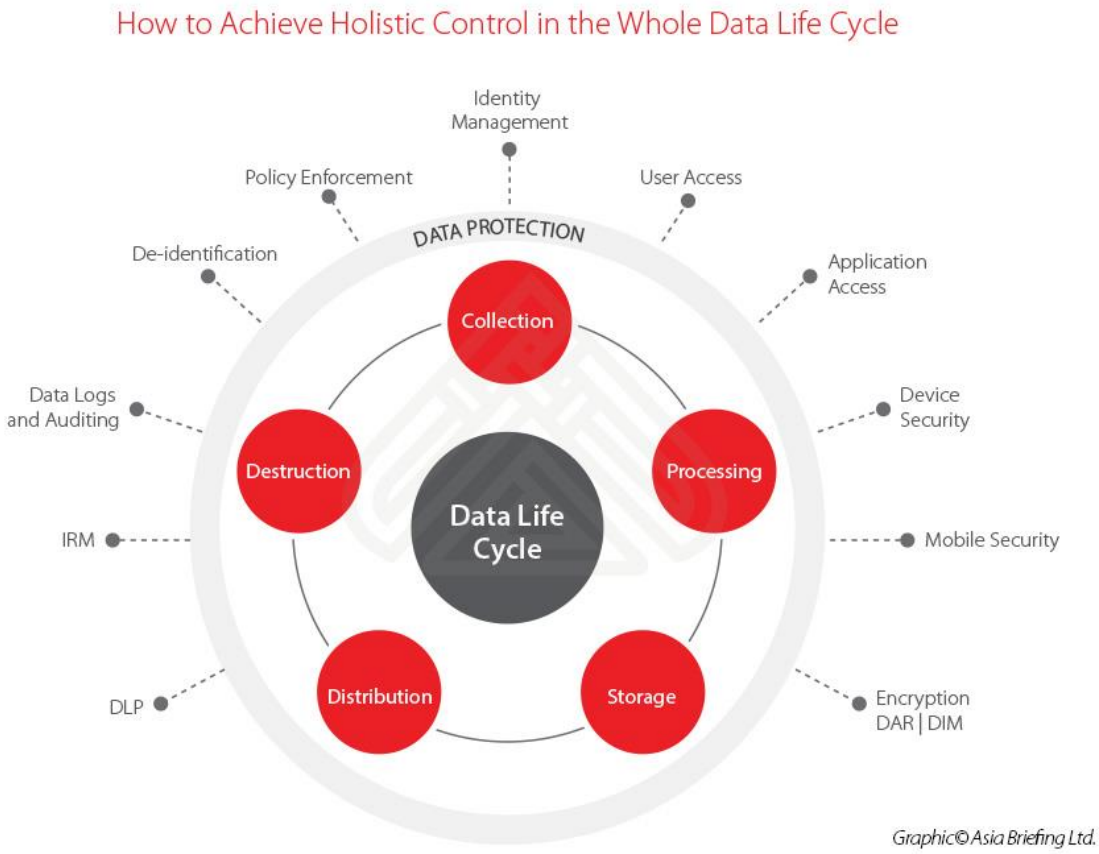
Data classification is another important step which classifies the data into different types based on its importance, purpose, source, and sensitivity; therefore, different levels of data protection control measures can be applied accordingly.

One clear data flow chart or data mapping which shows how the data is flowing inside the company and between the company and external parties will be very helpful to let the data protection team locate the key node/nodes that might need extra data protection measures. The company can consider using automatic tools to detect and identify the data type with auto-labeling, and further implement predefined control measures.

Holistic control in the whole data life cycle

The management strategy or control measures that just focus on a single or multiple nodes / points is always not enough as there are so many different potential problems in each phase of the whole data life cycle.

Different control measures should be adopted to align with the characteristics of different phases of data life cycle, or different stages. We give one simple illustration here for easier understanding:



Utilization of technical toolkits

More and more companies are dealing with large amounts of data in their daily operations nowadays and it is unrealistic to enforce the security control in a manual way. Adoption and deployment of advanced security toolkits is critical for data protection.

For example, companies should use a DLP (Data Loss Prevention) tool to classify and label the data with a pre-defined policy to prevent their sensitive data getting leaked out of the organization.

For the data that is necessary to be shared with an external party, deploying the tool like AIP (Azure Information Protection) can provide continuous protection even when the data is outside of the organizations' traditional security perimeter; implementing a Zero Trust-based security architecture can dramatically improve the overall data protection level. The company can consider utilizing Microsoft 365 productivity platform, which includes all features described in this section.

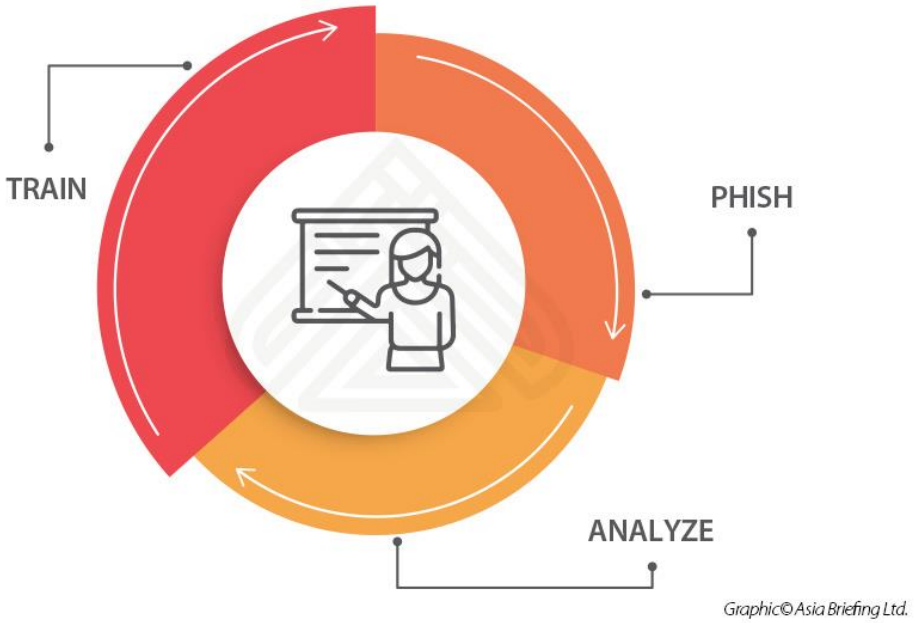
User training

The end user is always the last defense line for any data security incident. As part of organizational control measures, the security awareness training plus the training about how to utilize company-equipped technical toolkits for data protection is one important step of the overall data protection

process.

Some good platforms, such as KnowBe4, can be utilized to plan and develop the training program for all staff, detecting end users' real response on stimulated phishing for further analysis and improvement.

User Training as Part of Organizational Control Measures



Continuous improvement

Data protection is one long and endless journey, which requires continuous improvement. A suitable monitoring platform should be deployed to monitor and log the data activity, which should then send out the risk alert automatically to the data protection management team for manual intervention.

Internal review and external independent third-party audits should be done periodically and regularly to identify the potential weaknesses and the corrective actions that must be taken; the results should be further reviewed for the next round Plan-Do-Check-Action (PDCA).

Continuous Improvement in the Data Protection Management Strategy

Graphic© Asia Briefing Ltd.

This article was first published by China Briefing, which is produced by Dezan Shira & Associates. The firm assists foreign investors throughout Asia from offices across the world, including in China, Hong Kong, Vietnam, Singapore, India, and Russia. Readers may write to info@dezshira.com for more support.