DS NEWSLETTER savoir, faire
NEWSLETTER – LEGAL INFORMATIONS
PROPOSED BY DS AVOCATS

Data: manage it or risk it?

ASIE

Data issues have probably been on the agenda of many enterprises in China since last year, especially foreign invested enterprises ("**FIE**"). With major cyber laws such as the PRC Data Security Law ("**DSL**") and the PRC Personal Information Protection Law ("**PIPL**"), additional guidelines, national standards have been published giving a clearer view of what is required from enterprises. Enterprises are indeed required not only to protect personal information ("**PI**") but also to implement a comprehensive data compliance management. Since the end of 2021 and early 2022, several guides related to data compliance were released at Chinese national level and regional level respectively. They are different in content and focus but serve the same purpose. They can be used as guide in practice of delivering data compliance, because DSL and PIPL are clear on mandatory data obligations, but they stay vague in how to do it.

For instance, Shanghai Yangpu District authorities released a Guide on Data Compliance of Enterprises in late Jan, 2022 ("**Shanghai Guide**"). Yangpu District has strong educational and technological resources, and many FIE of Fortune 500. The Shanghai Guide mainly focuses on the methodology and principles of data compliance project inside an enterprise.

This article will focus on the main requirements of data compliance and will not dig into the details of how to approach PI protection (please refer our previous newsletter "Will the Chinese GDPR affect you? Get ready for the PRC Personal Information Protection Law").

- **WHAT IS DATA COMPLIANCE?**

The Shanghai Guide defines data compliance as the fact for the operation and management of an enterprise and its employees, to meet the requirements of data laws and regulations on PI protection, cybersecurity and data security. It is true that data compliance incorporates PI protection and is based on cybersecurity compliance, which is more frequently supervised by competent authorities by checking the enterprises' fulfillment of Multi-Level Protection Scheme per the PRC Cybersecurity Law ("**CSL**"). In other words, data compliance requires enterprises to comply with DSL and PIPL, as well as CSL.

Therefore, it is suggested for enterprises to know where they start from by conducting an audit led by professionals, and formulate a tailor-made roadmap.

- **WHO ARE CONCERNED?**

From the top management to each employee. The top executive of management (such as general manager) is responsible for data compliance, and therefore should allocate necessary and adequate resources (authorization/rights/power, HR and financial support) to build and implement data compliance strategies. Further, to avoid data compliance being an empty talk, the relevant accountability mechanism should be set and performance appraisal of relevant internal personnel should be linked with specific tasks of data compliance.

- **WHICH DEPARTMENT SHALL TAKE THE LEAD?**

The Shanghai Guide encourages enterprises to set dedicated data compliance department which is directly led by the Board level in a long term, but does not suggest to have the in-house legal department take charge of this topic. The dedicated department will formulate an overall data compliance strategy, organizational and technical measures internally, manage the external partners/clients on data issues, organize regular trainings and provide consultation to both management and employees internally. Besides, this department should be good at cross-departmental communication internally and handle public relationship with supervising authorities smartly.

Importantly, the Shanghai Guide stresses that it is indispensable and crucial of the involvement of external professionals with a cooperation relationship in a long term on data compliance.

- **DATA CATEGORIZATION**

In the end of 2021, a Chinese national standard guiding network data categorization and grading was released ("National Guide"). The National Guide aims to help enterprises to fulfill the basic but vague mandatory obligation, of data categorization and data grading required by both CSL and DSL. To put it simply, to manage data as an asset, the first step is to know its category and the level of risks attached to each category.

The National Guide mainly focuses on how to categorize and grade general data in practice.

1. For categorization, the criteria may vary depending on the actual situation of enterprises (business type, industry, scale etc.). However, the National Guide gives some universal criteria applicable to most scenarios, such as personal/non-personal data, public/social data, (non)/ public disseminated data. It is worthwhile to note that a set of data can fall into different categories per different criteria/dimensions (i.e. PI of employees may belong to the category of personal data as well as the category of internal user data of an ERP system).

2. For grading, the National Guide grades network data into 3 grades, the higher the grade the risker the impact of a data leakage: core data (highest grade), important data and general data.

   Enterprises should check whether they possess any core data and important data firstly; if so, such data should be managed carefully under professional advice because there are strict statutory obligations for the data controller.

   For general data, most enterprises may possess a certain volume of it, and it can be further graded into 4 grades. Still, the higher the grade, the riskier the impact of a data leakage on stakeholders. The National Guide gives some references:

   - Sensitive PI should be graded at least as General Data Grade 4;
   - Regular PI (including internal employees' PI) should be graded at least as General Data Grade 2;
   - Public data prohibited to be shared with 3rd parties should be graded at least as General Data Grade 4;
   - Public data shared with 3rd parties conditionally should be graded at least as General Data Grade 2.

To sum up, data categorization and data grading should be based on applicable official guidance (i.e. catalogue of core data and important data released by authorities and industry associations if applicable), otherwise enterprises should approach these tasks according to their own situations.

Obviously, data compliance takes patience. The better the project is planned, the more efficient the internal team is involved, the less budget will be needed. What makes this task more urgent is that there are limited good resource available on the market. Be an early bird!

For any additional information please contact:

ZHANG Beibei
Associate - Shanghai Office
beibeiZHANG@dsavocats.com

Isabelle DOYON
Lawyer- Shanghai Office
DOYON@dsavocats.com