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

New Data Regulation: looks familiar, yet impactful

CHINA

On September 24, 2024, *the Regulation on Network Data Security Management* («***Data Regulation***» in Chinese 网络数据安全管理条例) was promulgated and will take effect on January 1, 2025. Given that this *Data Regulation* is relatively new and closely aligned with *Cyber Security Law, Data Security Law, and Personal Information Protection Law* ("***PIPL***"), we have compiled the following FAQs to provide a brief introduction and address common questions.

1. What are the major changes and/or impact brought by Data Regulation?

Data Regulation does not introduce entirely new changes to the current data regulatory regime. Instead, it provides implementing rules based on the existing principles set forth in relevant cybersecurity and data laws and regulations. Additionally, it emphasizes key data protection principles by establishing dedicated penalties for violations, affecting both the legal entity/violator and the person in charge.

In other words, *Data Regulation* transforms vague legal obligations for data controllers and processors into detailed, specific, and feasible tasks. By doing so, it brings data compliance obligations closer to controllers and processors. Consequently, a «*wait and see*» approach will no longer be viable after the implementation of *Data Regulation*.

Taking the entrusting of a third party for Personal Information (PI) processing as an example, *PIPL* requires controllers to set processing purposes, duration, methods, and other details with processors; however, *PIPL* is not clear on how to «*set*» these terms. *Data Regulation* addresses this by specifying that these terms should be established «*by entering into a contract or by other means.*» Violation of this provision may result in a penalty of up to RMB 1 million for the enterprise, and in severe cases, up to RMB 100k for the person in charge, as outlined in *Data Regulation*.

Similar detailed rules are provided in *Data Regulation* for various aspects, including:

- Important Data Management: Mandatory appointment of a Data Protection Officer (DPO) and a management organ; and stricter qualification requirements for the DPO and clarifying the obligations of the data management organ.
- Contingency Plan and Cyber Incident Response: Requirement to report incidents within 24 hours if they concern national security and/or public interests.
- PI Processing Policy: emphasizing dos and don'ts's for consent-based processing of PI and providing brief guide on how to respond to PI subjects' rights.
- Obligations for Large Online Platform Operators: Specific mandatory obligations for large online platforms.

These detailed rules ensure that organizations have a clear and actionable guidelines to follow, enhancing overall data compliance and security. Consequently, data controllers (e.g., enterprises and platforms) must respond to data regulations by implementing adjusted data protection measures. Conversely, data processors may take corresponding actions to meet legal requirements and/or contractual clauses stipulated by their clients/controllers.

Therefore, it is recommended that both data controllers and processors closely monitor data regulations and promptly adjust their current data management methods.

2. What's important about PI?

In addition to the example mentioned earlier, controllers should exercise with greater caution when formulating privacy policies or other privacy-related documents, regardless of whether they are consent-based. These documents must clearly inform PI subjects about how their PI is processed and include feasible procedures for PI subjects to exercise their PI rights. Failure to adequately inform PI subjects in consent-based processing can result in penalties for the legal entity and, in severe cases, the responsible individual. For B2C controllers, good news is that at the regulation level, it is confirmed enterprises may charge reasonable fees for responding PI subject's portable rights of PI.

In particular, large online platforms processing PI of 10 million individuals or more should appoint their own Data Protection Officer (DPO) and establish a dedicated internal data management organ. These platforms must assume responsibilities similar to those required for processing important data.

**For more detailed information about PI protection, please click the following newsletters:*
"How's your privacy policy(2024)?"
"Legal Updates on PI protection in 2023"
"Introduction of the Chinese GDPR- PIPL(2021)"

3. What's important about important data?

When entrusting important data to a processor, the controller should conduct a risk assessment and ensure that contractual safeguards are in place, outlining security obligations. The processor must meet data security standards, and if data is transferred abroad, a security assessment from the Cyberspace Administration of China (CAC) is required. Continuous monitoring and audits are essential, and both controllers and processors remain legally accountable for compliance.

Additionally, more detailed rules are provided for important data management. For example, beyond appointing a Data Protection Officer (DPO) and establishing an internal data management organ, *Data Regulation* specifies qualifications for the DPO. The DPO should be a member of the management team and possess adequate expertise and experience in data compliance. It also requires for important data controllers, a comprehensively annual risk assessment and report of the result to the competent authorities.

**For more detailed information about general data compliance, please click the following newsletters:*
"Introduction of the Chinese Data Security Law (2021)"
"Data: manage it or risks it? (2022)"

4. How about the cross-border data transfers?

The focus is primarily on the significant rules already established by existing laws and the *Provisions on Facilitating and Regulating Cross-border Data Flow* released in March 2024. There are no substantial changes or new developments regarding cross-border data transfer.

**For more detailed information about cross-border transfer, please click the following newsletters:*
"What to know about the Chinese Standard Contractual Clauses for Cross-border Personal Data Transfer(2023)?"
"What's new about cross-border data transfer from China in 2022 (about security assessment"
"How's the PI protection certification in China(2022)?"

5. What are the possible penalties in case of a violation?

Violating *Data Regulation* could result in penalties of up to RMB 10 million for the legal entity and RMB 1 million for the responsible individual. It is consistent with the "legal liability" provided in the *Data Security Law and PIPL*.

For any additional information, please contact:

Isabelle DOYON
Senior Associate- Shanghai Office
donyon@dsavocats.com

ZHANG Beibei
Senior Associate - Shanghai Office
beibeizhang@dsavocats.com

Enzo TRUPIANO
Intern- Shanghai Office
Enzotrupiano@dsavocats.com

12 November 2024