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

Review of Legal Updates on Data Protection and Cybersecurity in 2021

ASIE

2021 is a big year for data protection and cybersecurity, especially a milestone for personal information ("PI") protection. In addition to the famous *Data Security Law* ("DSL") and *Personal Information Protection Law* ("PIPL"), there are also other regulations and guidelines in official or draft version, which may to some extent affect the enterprises' business in China. So, what is the trend of 2021? This article will take a peek of some important and interesting legal updates.

CYBERSECURITY

- *Cyber Security Law* ("***CSL***", *effective in 2017*) sets the basic obligations (i.e. Multi-Level Protection Scheme, "***MLPS***") for network operators, but it is absent on details of how to manage risks. On the other hand, facing more and more cyber incidents and frauds, it was in urgent need of a regulation on management of loopholes and risks discovered. On July 12th, 2021, the *Administrative Provisions on Security Vulnerabilities in Network Products* was promulgated and took effect on September 1st, 2021.

  It regulates network products (hardware and software) providers, network operators and other entities (organizations, individuals). Where any loophole is found, the enterprise concerned shall investigate it, report to competent authorities within 2 days, immediately take remedial measures and notify the relevant parties who may be affected. Relevant logs of loopholes found shall be kept for at least 6 months, which is consistent with one of the basic obligations set by *CSL* about network logs. It is notable that violation can lead to severe administrative punishment (pecuniary fine to the enterprise and sometimes person in charge as well, revocation of business license, etc.) according to *CSL*.

- Per *CSL*, critical information infrastructure operators ("CIIOs") have more and stricter obligations regarding cybersecurity and data management than those for normal network operators. However, *CSL* remains vague in most of the obligations of CIIO. Since September 1st, 2021, the *Regulation on the Security Protection of Critical Information Infrastructure* became effective. It, to some extent, solves the non-clarities of the obligations of CIIOs and sets more administrative punishments besides those already included in *CSL* for CIIOs.

  Though in practice, it is less likely for foreign invested enterprises to be considered as CIIOs, they may commercially cooperate with some CIIOs who will or already have stricter requirements for their suppliers through background audit or clients through KYC (Know Your Client) process. Thus, it is advisable for foreign invested enterprises to check the compliant level regarding cybersecurity, especially the status of MLPS compliance, which is mandatory for all network operators and more frequently supervised by authorities in practice.

DATA MANAGEMENT AND PERSONAL INFORMATION PROTECTION

It is no longer news that China released its first law governing data security and its first law regulating PI protection, namely the *DSL* (effective on September 1st, 2021) and *PIPL* (effective on November 1st, 2021). They are all with extraterritorial legal effect and have impact on the daily operations of most multinationals who have subsidiaries in China.

At present, both *DSL* and *PIPL* are too general to guide enterprises in their compliance projects. However, in 2022, there would be more supportive regulations, guidelines and instructions to solve these unclear issues. For example, the following two drafts released in October and November 2021 shed some light on cross-border data transfer.

- *Regulation on Network Data Security Management (Draft)*
  Per the current *Draft*, enterprises who are data controllers should fulfill their obligations on documentation (making data flow traceable

by keeping logs), conducting self-assessment in scenarios like data incidents, sensitive PI processing, profiling, transferring data to third countries etc., communicating with competent authorities where security assessment and reports of data events are required.

As for PI protection, the following parts in the *Draft* call for attention.

- Enterprises who process PI of more than 1 million data subjects shall pass cybersecurity review (which is more comprehensive than security assessment) conducted by competent authorities before launching any overseas IPO projects.
- There are timeframe and restrictions on the rights of data subjects of PI. For instance, data controllers should respond to data subjects' requests within certain days and the requests should be reasonable in frequency, otherwise the data controllers may charge data subjects reasonable fees.
- When it comes to the hot topic of cross-border PI transfer, it gives the threshold amount of data subjects of PI triggering the security assessment organized by Cyberspace Administration of China ("**CAC**") for data controllers. Furthermore, to prevent unlawful flow of PI, this *Draft* strengthens the requirements that "*it is not allowed for any individual or organization to provide programs, tools, lines, etc. for penetrating and bypassing the data cross-border security gateway, Internet access, server hosting, technical support, dissemination and promotion, payment and settlement, application download and other services for penetrating and bypassing the data cross-border security gateway*".
- Data controllers shall not force data subjects for their consent by the purpose of improving service quality, improving user experience, developing new products, etc.
- Biometrics (sensitive PI), including face, gait, fingerprint, iris, voiceprint, etc., shall not be used as the only way of personal identity authentication.

- *Measures for Security Assessment of Cross-border Data Transfer (Draft)*

  Cross-border data transfer is in no doubt the hot topic of concern for multinational enterprises with subsidiaries in China. Ever since the *CSL*, security assessment remains a mystery. This draft could be the draft mostly close to the official measures guiding the security assessment organized by CAC in the future.

  Scenarios related to any of the following, namely CIIOs, important data, PI data controllers who process PI of more than 1 million data subjects or accumulatively transfer PI of more than 0.1 million data subjects or sensitive PI of more than 10,000 data subjects, would trigger the security assessment organized by CAC.

  Per the *Draft* at least two documents are required for the security assessment besides the application form (which could be provided by authorities by templates later). They are the self-assessment report and contracts entered between the data exporter and the foreign data recipient. In practice, some multinationals already start to integrate the Chinese regulatory framework of cross-border data transfer into their global data flow strategy per the current laws and regulations, which can already improve the legitimacy of data export from China to other countries.

OTHERS

- *Facial recognition*

  With *PIPL* and a judicial interpretation (released by the Supreme People's Court of China and became effective on August 1st, 2021), entities using facial recognition are facing more compliance issues and disputes with data subjects. The judicial interpretation clearly lists scenarios infringing rights and interests of data subjects by illegal processing of their facial data, and the users of facial recognition (i.e. enterprises, institutions etc.) are to prove their compliance where disputes occur (reversed burden of proof). Thus, considering the increasing number of civil disputes and administrative punishments in China, relevant stakeholders are advised to check if relevant facial recognition is necessary and legitimized per the current laws and regulations.

- *Algorithm*

  At national level, the *Administrative Provisions on Algorithm Recommendation of Internet Information Services* was just released on January 4th, 2022 and will be effective on March 1st, 2022. It requires algorithm service providers to assess the algorithm mechanism, monitor the security status and implement data security and PI protection measures, and record-filing with competent authorities if such algorithm affects public opinion etc. In addition, algorithm models inducing users to indulge or consume at a high price shall not be set by service providers.

  At regional level, Shanghai authority released a guidance on supervision of algorithm used in digital marketing of e-commerce. Per this guidance, algorithm should not be used to unfairly affect price or unreasonably affect consumer treatment, etc., which will more or less restricts the profiling and other forms of digital marketing activities.

***

The above is only a glimpse on a few aspects of data protection and cybersecurity measures in 2021. Some industries (automotive, pharmaceutical etc.) in China also released some specific rules during 2021 (you may found our previous newsletters on these topics via the following links). With no doubt, there will be more to come in 2022. We will keep observing and sharing from time to time during the coming year.

Previous newsletters:

Health data: control your risks!
EN: https://www.dsavocats.com/mailing/Asia%20News/Newsletter%20Asie%2020210930%20EN.pdf
FR: https://www.dsavocats.com/mailing/Asia%20News/Newsletter%20Asie%2020210930%20FR.pdf

What to know about data of connected vehicles?
EN: https://www.dsavocats.com/mailing/Asia%20News/Newsletter%20Asie%2020211104%20EN.pdf
FR: https://www.dsavocats.com/mailing/Asia%20News/Newsletter%20Asie%2020211104%20FR.pdf

"Face Pressure": what's new about facial recognition in 2020 and 2021?
EN: https://www.dsavocats.com/mailing/Asia%20News/Newsletter%20Asie%2020210629%20EN.pdf
FR: https://www.dsavocats.com/mailing/Asia%20News/Newsletter%20Asie%2020210629%20FR.pdf

Seek a quick path to know the new PRC Data Security Law? Check the FAQs!
EN: https://www.dsavocats.com/mailing/Asia%20News/Newsletter%20Asie%2020210715%20EN.pdf
FR: https://www.dsavocats.com/mailing/Asia%20News/Newsletter%20Asie%2020210715%20FR.pdf

Will the Chinese "GDPR" affect you? Get ready for the PRC Personal Information Protection Law
EN : https://www.dsavocats.com/mailing/Asia%20News/Newsletter%20Asie%2020210901%20EN.pdf
FR : https://www.dsavocats.com/mailing/Asia%20News/Newsletter%20Asie%2020210901%20FR%20.pdf

For any additional information please contact:

ZHANG Beibei
Associate - Shanghai Office
beibeiZHANG@dsavocats.com

Isabelle DOYON
Lawyer- Shanghai Office
DOYON@dsavocats.com