Synergize GBA series: Cross-border data transfers in mainland China

LC Lawyers LLP
Kareena Teh, Philip Kwok, Ken Lam

14 January 2022

LC Lawyers
林朱律師事務所
Law firm member of the EY global network

In 2021, we have seen significant changes in the data protection regime in mainland China. Specifically, the Data Security Law (DSL) and the Personal Information Protection Law (PIPL) came into effect on 1 September 2021 and 1 November 2021 respectively. They have far reaching implications for organizations, particularly those operating in or providing products and services to customers based in mainland China. Care needs to be taken to comply with the DSL and the PIPL in transferring data from mainland China to other jurisdictions, including Hong Kong. This article highlights several key issues which organizations doing businesses in and/or with organizations in mainland China should consider.

What are the key regulations for data export from mainland China?

There are a number of laws and regulations on exporting data out of mainland China. The key laws are the Cybersecurity Law (CSL), the DSL and the PIPL.

Under the DSL, any export of important data collected or produced by Critical Information Infrastructure Operators (CIIOs) in mainland China will need to comply with the CSL. Export of other data collected or produced by the data processors in mainland China will need to comply with the applicable implementing measures.

Under the CSL, personal information and important data (broadly defined as data that is closely related to national security, economic development or public interest) collected and produced by CIIOs during their operations in mainland China has to be stored in mainland China. If it is necessary to provide such information and data to overseas parties due to business requirements, a security assessment has to be conducted in accordance with the measures developed by the Cyberspace Administration of China (CAC) in conjunction with relevant departments of the State Council, unless it is otherwise prescribed by any law or administrative regulation.

Under the PIPL, CIIOs processing personal information (defined as various kinds of data related to identified or identifiable natural persons recorded by electronic or other means, excluding the data processed anonymously), and personal information processors that are processing personal information over certain thresholds prescribed by the CAC have to store the personal information collected or produced in mainland China domestically. Personal information processors that wish to transfer such information outside mainland China must either:

- pass the security assessment;
- obtain certification from a professional institution in accordance with the regulations set by the CAC;
- enter into a standard contract with the overseas recipient specifying their respective rights and obligations; or
- comply with other conditions imposed by laws, regulations or the CAC.

Additionally, they must also obtain the specific consent of the individuals concerned and inform them of the identity and contact of the recipient, purpose and method of processing, the type of personal information being transferred and the rights of the individuals concerned.

On 29 October 2021, the CAC published the Draft Measures on Security Assessment of Cross-Border Data Transfer (Draft Data Transfer Measures)[1] to provide more detailed rules on the security assessment requirements under the CSL, the DSL and the PIPL. The Draft Data Transfer Measures, if

[1] Draft Data Transfer Measures《数据出境安全评估办法（征求意见稿）》, http://www.cac.gov.cn/2021-10/29/c_1637102874600858.htm

passed, will require data processors meeting one of the following conditions to pass security assessment before exporting data outside the territory of mainland China:

- data processors that handle personal information and important data collected and produced by CIIOs;
- data processors that export important data;
- personal data processors that have processed personal information of more than one million persons;
- data processors that have cumulatively exported personal information of 100,000 persons or more, or have cumulatively exported sensitive personal data of 10,000 persons or more;
- data processors that fall within other circumstances as provided by the CAC.

Apart from the above restrictions, the DSL and the PIPL also prohibit the provision of data and/or personal data stored in mainland China to any foreign judicial or enforcement authorities without the approval of the relevant mainland China authorities. There is a similar prohibition in the Securities Law (2019 Revision) against the export of documents and information relating to securities business activities overseas without the approval of the China Securities Regulatory Commission.[2]

Which industries' data are relatively more sensitive?

Organizations can take guidance from the DSL, the CSL, the PIPL and their implementing measures on the type of data that is more sensitive and the industries that are likely to have such data.

The DSL defines data that is closely related to national security, economic development, people's livelihood or public interest as national core data (and hence require more stringent protection). While the DSL does not specifically define important data, it expressly mandates the need to strengthen protection to important data. Organizations could turn to the Draft Implementing Measures on Data Security Management (Draft Measures)[3] for reference as it defines important data as data that may directly affect national security, economic security, social stability, public health and safety. Examples include non-publicized government information and significant volumes of data related to population, genetics and health care, geographic, and/or mineral resources.

The CSL, together with the Regulations on Critical Information Infrastructure Security Protection (CII Regulations) (which took effect on 1 September 2021)[4], specify network operators in the following industries to be CIIOs, signifying the sensitivity of the data they hold: public communication and information services, energy, transport, water, finance, public services, e-government, defence technology[5] etc.; and other industries with facilities which, if destroyed, functionalities, which if lost, or data, which if leaked, would seriously harm state security, national economy, and people's livelihood, and/or public interest.

The PIPL also identifies certain types of personal information as being sensitive personal information. These include personal information that, once disclosed or used illegally, may easily cause harm to the dignity, security of individuals or their property. Examples include biometric characteristics, religious beliefs, special designation, health and medical record, financial accounts, location tracking information and the personal information of minors who are under the age of 14.

How should organizations prepare themselves?

The recent introduction of the DSL and the PIPL, when taken together with the CSL, now gives mainland China a comprehensive data protection regime governing the entire data cycle of businesses operating in mainland China. Organizations should closely monitor the implementation of the laws over time through implementation rules as well as enforcement actions. Now that industry regulators (which is also known as "Protection Departments") are delegated with the power to formulate the implementing rules for the identification of CII, organizations should closely monitor these implementation rules and assess whether their operations will fall under a CII classification. Further, it is essential for organizations, especially those engaged in cross-border operations, to devise and implement a comprehensive data governance framework to ensure compliance amidst the evolving regulatory landscape.

---

[2] Securities Law (2019 Revision)《证券法》（2019 年修订版）：https://flk.npc.gov.cn/detail2.html?ZmY4MDgwODE3MWU5ZTE4MTAxNzI3ZTMyYjk0ZDdkZTY%3D

[3] Draft Measures《数据安全管理办法（征求意见稿）》：http://www.cac.gov.cn/2019-05/28/c_1124546022.htm

[4] CII Regulations《关键信息基础设施安全保护条例》：http://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm

[5] Additional example added in the CII Regulations which came into effect on 1 Sep 2021

Key contacts

Kareena Teh
Partner
LC Lawyers LLP
kareena.teh@eylaw.com.hk
+852 2629 3207

Philip Kwok
Counsel
LC Lawyers LLP
philip.kwok@eylaw.com.hk
+852 2675 2160

Ken Lam
Associate
LC Lawyers LLP
ken.tl.lam@eylaw.com.hk
+852 3471 2671

Contact us

LC Lawyers LLP
Suite 3106,
31/F One Taikoo Place,
979 King's Road,
Quarry Bay, Hong Kong

Tel: +852 2629 3200
Fax: +852 2956 1980

https://www.eylaw.com.hk/en_hk

Follow us on WeChat

APAC no.: 03013887

ED None