Cataloguing of Important Data

July 2022

Executive summary

The term 'Important Data' was first mentioned in the *China Cybersecurity Law*, where it requires that personal information and Important Data gathered or created by critical information infrastructure operators ('**CIIOs**') during operations in the People's Republic of China ('**PRC**') be stored in the PRC. However, the term has never been defined, whether in the *China Cybersecurity Law*, the new *China Data Security Law* (which is the key law on data security administration and established a classified and graded data protection system), or other China laws and regulations.

More recently, the different drafts of the regulation entitled *Information Security Technology – Identification Guide of Important Data* as well as the latest draft entitled *Information Security Technology – Identification Rules of Important Data*, which was not publicly released, finally define Important Data. The latest draft regulation defines Important Data widely to cover not just government data.

The draft regulation is subject to further review and amendment, but reportedly the wide definition not likely to substantively change.

Definition of Important Data

The latest draft regulation defines Important Data as '*data that are domain-specific, group-specific, region-specific, or of a certain precision and scale, where national security, economy, social stability, public health or safety would be directly harmed in the event that the data are leaked, tampered with, or destroyed*.' State secret is outside of the scope of Important Data.

This definition of Important Data is significantly wider than the definitions in the previous draft regulations which defined Important Data as data where national security and public interests would be harmed in the event that they are tampered with, destroyed, leaked, or illegally obtained or used.

Cataloguing principles

The basic principles for cataloguing of Important Data as prescribed by the draft regulation include:

(1) focusing on impact on security: considering from the perspective of national security, economic stability, social stability, public health and safety. Data which are only important and sensitive to an organisation (for example, data in relation to internal management of a company) would not be deemed Important Data

(2) highlighting the focus of data protection and facilitating the free flow of data (after ensuring security)

(3) linking up existing local rules

(4) evaluating risks holistically

(5) using both quantitative and qualitative methods

(6) constant evaluation.

Factors for cataloguing

The draft regulation lists a number of factors as examples to be taken into account when cataloguing Important Data. Data that may influence national politics, sovereignty, military, economy, culture, society, technology, environment, resources, nuclear equipment, overseas interests, biology, outer space, polar region or deep-water would be classified as Important Data.

Data classification and grading system

Important Data represents one grade (level 2) under the data classification and grading system under the *Network Security Standard Practice Guide – Guidelines for Data Classification and Grading* (v1.0-202112) (TC260-PG-20212A) issued by the National Information Security Standardisation Technical Committee on 31 December 2021:

	Impacted Subjects			
	National Security	**Public Interests**	**Personal Lawful Interests**	**Organisational Lawful Interests**
Core Data	Harm or significantly harm	Significantly harm	-	-
Important Data	Slightly harm	Harm or slightly harm	-	-
General Data	No harm	No harm	No harm, slightly harm, harm, significantly harm	No harm, slightly harm, harm, or significantly harm

The *Draft Measures for Security Assessment of Cross-border Data Transfer* issued on 29 October 2021 and the *Draft Regulation on Network Data Security* issued on 14 November 2021 prescribe for (a) prior Chinese government approval for cross-border transfer of important data by even companies who are not CIIOs, and (b) notification to the regulators within eight (8) hours and full reporting to the regulators within five (5) business days in case of a data breach relating to Important Data.

With the definition of Important Data being wider than government data, the burden on companies is immense. Companies should therefore monitor this and other developments relating to Important Data to update data cataloguing to ensure compliance.

Let's talk

For a deeper discussion of how this impacts your business, please contact us.

PwC Hong Kong

Kenneth Wong
Mainland China and Hong Kong Digital Trust & Risk - Cybersecurity and Privacy Leader
PwC Hong Kong
+852 2289 2719
kenneth.ks.wong@hk.pwc.com

Kristine Chung
Partner
PwC Hong Kong
+852 2289 1902
kristine.ky.chung@hk.pwc.com

Patrick Mulholland
Associate Director
PwC Hong Kong
+852 2289 1974
patrick.mulholland@hk.pwc.com

Tiang & Partners

Chiang Ling Li
Partner
Tiang & Partners
+852 2833 4938
chiang.ling.li@tiangandpartners.com

PwC China

Kris Fan
Associate Director
PwC China
+86 21 2323 8352
kris.k.fan@cn.pwc.com

www.pwc.com

www.tiangandpartners.com

pwc

Tiang & Partners
程偉賓律師事務所