UPDATE IN THE PRC DATA REGULATORY REGIME – A CLOSER LOOK AT THE SECOND DRAFT OF PRC DATA PROTECTION LAWS

Key issues

- The Draft DSL and the Draft PIPL both have extraterritorial effect which are important for international institutions to be aware of when operating in the PRC market.
- Based on the "consent-based" personal data protection regime laid down by the CSL, the Draft PIPL has introduced further subdivisions like "consent", "separate consent" and "written consent", to address different situations. This will need further implementation guidance.
- Data export activities may be allowed under additional permissible routes, but subject to stricter control.

On 29 April 2021, the Standing Committee of the National People's Congress released the second draft of the Data Security Law (Draft DSL) and the Personal Information Protection Law (Draft PIPL) for public comment until 28 May 2021.[1] The Draft DSL and the Draft PIPL mark another step by PRC[2] regulators and legislators towards protecting data sovereignty and regulating data-related activities in line with internationally recognised practice. These draft laws build on the PRC Cyber-security Law which came into force in 2017 (CSL).

The Draft DSL and the Draft PIPL demonstrate PRC regulators' focus on developing the regulatory environment with respect to data matters by adding more granularity to the existing legal framework. In this briefing, we highlight a few key regulatory developments that will be vital to international institutions in managing data issues with respect to their PRC businesses.

Extraterritorial effect

The CSL, which has been in place since 2017, applies to the construction, operation, maintenance and utilisation of networks as well as the regulation of cyber-security within the PRC[3]. Although articles 5 and 75 of the CSL empowered the PRC government to handle cybersecurity risks and threats originating from outside the PRC and sanction non-PRC entities/persons which attack PRC critical information infrastructure operators (CIIOs), these articles were viewed more as a statement of PRC data sovereignty than actual enforcement tools. Generally speaking, market participants did not expect PRC regulators to use the CSL to takeany action against non-PRC entities. By contrast, both the Draft DSL and the DraftPIPL, which will have equivalent force as the CSL in the PRC's statutory regime, capture

[1] See our alerters on (a) the first draft of PIPL: *China releases draft Personal Information Protection Law for public comment*; and (b) the second draft of data protection laws: *China releases second draft of data protection laws for public comment*.

[2] PRC stands for the People's Republic of China, which for the sole purpose of this briefing, excludes Hong Kong, Macao and Taiwan.

[3] See our client briefing on the CSL: *New PRC Cyber-Security Law comes into Force*.

data/personal information (PI) processing activities in the PRC and also expressly expand their scope to cover extraterritorial activities:

- the Draft DSL adopts a result-oriented approach, extending jurisdiction to data processing activities conducted outside the territory of the PRC that damage the PRC's national security or public interests or legitimate interests of PRC residents or organisations; and
- the extraterritorial jurisdiction of the Draft PIPL is linked to the purpose of PI processing – if any PI processing is to (i) provide products or services to, or (ii) analyse or assess behaviours of, natural persons within the territory of the PRC, the relevant overseas institution will be subject to the jurisdiction of the Draft PIPL and such institution will need to establish an office or appoint a representative within the PRC to fulfil regulatory duties under such law. This requirement will be difficult for entities without any existing presence in the PRC, as it will force them to set up a representative office in the PRC and/or wait for professional agency services for cross-border data matters to appear in the future. International institutions need to pay special attention if its overseas data processing activities involve processing PI of PRC citizens as the administrative penalties arising out of violation of the Draft PIPL can be up to 5% of annual turnover of the immediately preceding year.

Clearer regulatory framework for data, important data and personal information

The CSL introduced the golden rule for data collection/processing activities – the principle of "*legitimacy, appropriateness, necessity*". Since 2017, PRC regulators have issued various implementation rules under the CSL based on this principle toguide network operators to handle data protection matters, in response to emergingdata leaks and incidents on internet or mobile application programmes (Apps). However, it should be noted that the CSL regulates more than data issues – it coverscybersecurity matters as well.

The Draft DSL and the Draft PIPL, on the other hand, mark a change to the regulatory approach of PRC regulators – at the national legislation level, processorsof general data and PI will have clearer guidance on the following:

- the Draft DSL provides a regulatory framework for data protection generally, regardless of whether in electronic form or not. This fills in the gap under the CSL where non-electronic data may not have been covered. In addition, the Draft DSL states that the PRC government will establish a data classification andgrading system nationwide and issue a catalogue of important data with input from different industry regulators. Local regulators may further issue localised catalogue to guide local practice. The CSL was not clear on whether, in additionto CIIOs, normal network operators are also subject to export restrictions on important data. This seems to have been answered under article 30 of the DraftDSL, which empowers the PRC administration to formulate export rules for important data that are

applicable to data processors other than CIIOs; and

- the Draft PIPL develops a more advanced regulatory approach on PI processing.In addition to reaffirming the "legitimacy, appropriateness, necessity" principle governing data collection/processing activities under the CSL, minimising the impact on the rights and obligations of data subjects is introduced as a new requirement for PI processing. The Draft PIPL also introduces a stricter approach for sensitive PI processing activities.

Consent requirements

Under the CSL and its implementation rules, acquiring consent from the relevant data subject is one of the pre-conditions for data collection/processing activities. Although PRC regulators provided practical guidance on what actions might constitute "*collection and use of personal information without consent by therelevant App user*"[4], unified guidance on the formalities and substance of "consent"requirements under the current regulatory regime is lacking. In practice, a data subject may give consent by signing a written form, or by conduct, which would be subject to a case-by-case analysis.

The Draft PIPL provides further guidance on the consent requirements. On one hand, it introduces the concept of "separate consent" and "written consent" that apply in different situations, which can be interpreted as setting a lower standard forconsent in other situations :

- according to articles 24, 26, 27, 30, 39 of the Draft PIPL, a "separate consent" from the relevant data subject would be required for (i) sharing PI with a third party; (ii) public disclosure of PI; (iii) processing sensitive PI and; (iv) exporting PI; and
- according to article 30 of the Draft PIPL, a written consent is required for processing sensitive PI, if this is explicitly required under laws and regulations.

However, specific requirements for "separate consent" are still unclear. For example, data processors may wonder whether a standalone consent form is required, or whether a separate annex in the user privacy agreement/policy would be sufficient to fulfil such regulatory requirement.

On the other hand, the Draft PIPL does not require data subject consent for PIprocessing in the following circumstances:

- necessity for conclusion or performance of any contract to which the data subjectis a party;
- necessity for performance of statutory duties or obligations;
- necessity for responding to public health incidents or protection of personal andproperty security under emergencies;
- processing PI in the public domain (Public PI) within a reasonable scope in accordance with the Draft PIPL;

[4] See our alerter on the *Measures on Identifying the Illegitimate Collection and Use of Personal Information by Apps*: *China releases measures on identifying illegitimate collectionand use of personal information by apps*.

- activities to be considered in the public interest, such as news reporting and whistleblowing, provided that the processing is carried out within a reasonable scope; and/or
- other circumstances prescribed by laws and regulations.

The subsidiary legislation and regulatory guidance for the Draft PIPL needs to define or explain "reasonable scope" and "statutory duty or obligation" for clarity.On a related note, the *PRC Civil Code* which took effect in 2021 provides that (a) processing Public PI with no express objection from the relevant individual; (b) processing Public PI with no harm to the material interest of the relevant individual; and (c) reasonable activities for protecting the public interest or legitimate interest of the relevant individual, in the absence of the consent of relevant individuals, will not trigger civil liabilities.[5]

Emerging issues for cross-border activities

For international institutions with a global footprint, the interplay between local requirements on data in a specific jurisdiction and a unified global data policy is always a top compliance challenge. The CSL introduced export control on networkdata for the first time. The Draft DSL and the Draft PIPL further complete the regulatory framework on data export activities and upgrade the data export control regime as elaborated below.

Compared with the CSL, the Draft PIPL broadens the permitted routes for data export activities, which include:

- completion of security assessments organised by PRC regulators;
- obtaining PI protection verification issued by licensed institutions;
- entering into the standard contractual clauses issued by the Cyberspace Administration of China with overseas PI receiver with supervision to ensure thatits PI processing activities satisfy standards under the Draft PIPL; or
- satisfaction of other conditions prescribed by PRC laws and regulations.

However, the PRC government is seeking to enhance its supervisory approach on data export activities under the Draft DSL and the Draft PIPL by expressly empowering PRC regulators to:

- impose export control measures on data for the PRC's observation of international obligations and/or protection of national security and interests;
- impose equivalent counter-measures to the countries/regions which adopt prohibitions on or discriminatory measures against the PRC in terms of investment and trading activities relating to data and data development; and
- have the discretion to approve or deny data export requests from any overseasjudicial or enforcement agencies.

[5] See our alerter on the *PRC Civil Code*: *China codifies civil law rules on protection of right toprivacy and personal information*.

International institutions should keep a close eye on the relevant implementation mechanism once the PRC government releases its detailed arrangement to achieveits above supervision purpose.

Separately, the Draft PIPL does not specifically provide guidance on data import activities, which may result in regulatory uncertainty. For example, when an overseas institution transfers data to a PRC processor for further processing, the PRC processor would be required to fulfil contractual obligations with the overseasinstitution (which usually reflects certain overseas statutory requirements) and alsoto comply with the Draft PIPL, without a cross-border coordination mechanism – it would be advisable for international institutions to carefully navigate such arrangements with caution to ensure full compliance.

Conclusion

The Draft DSL and the Draft PIPL will introduce intricate compliance requirements for international institutions. Any PRC onshore operations of international market participants will need to be prepared for the incoming data classification and gradingsystem, and will need to re-design its consent forms with data subjects. Any exportof data, especially when dealing with requests from overseas administrative and judicial authorities, will need to be handled very carefully in order to balance the institutions' obligations to both PRC and non-PRC authorities. If any data/PI from the PRC is being processed outside of the PRC, it would be advisable to assess inadvance whether this would trigger the jurisdiction of the Draft PIPL and ensure the completion of the associated regulatory formalities or proper contractual arrangements.

CONTACTS

Terry Yang
Partner

T +852 2825 8863
E terry.yang
@cliffordchance.com

Kimi Liu
Counsel

T +86 10 6535 2263
E kimi.liu
@cliffordchance.com

Yan Li
Senior Associate

T +86 10 6535 2284
E yan.li
@cliffordchance.com

Jane Chen
Associate

T +86 10 6535 2216
E jane.chen
@cliffordchance.com

Roy Wang
Trainee

T +86 21 2320 7326
E roy.wang
@cliffordchance.com