dahui

DaHui Lawyers

37/F China World Tower A
1 Jianguomenwai Avenue
Beijing 100004, China

T +86 10 6535 5888
F +86 10 6535 5899
W dahuilawyers.com

BEIJING
NEW YORK
SHANGHAI

China Releases Draft Regulations on Network Data Security

19 November 2021

On 14 November 2021, the Cyberspace Administration of China ("**CAC**") released a draft of the *Administrative Regulations on Network Data Security* ("**Draft Regulations**"); the public comment period is set to last until 13 December 2021. On the one hand, the Draft Regulations reiterate and refine key requirements under the *Cybersecurity Law*, *Data Security Law* ("**Data Law**") and *Personal Information Protection Law* ("**PIPL**"); on the other hand, the Draft Regulations define terms and clarify provisions under these laws as well as adding to data security obligations for certain operators. This Newsletter summarizes key points of the Draft Regulations.

Definitions of Terms

1. The Draft Regulations apply to "processing" of "network data" ("**Data**") – and thus to any individual or organization that autonomously determines the purpose and manner of such "processing" ("**Data Processor**"). "Processing" is defined, like in China's existing cybersecurity framework, as "collecting, storing, using, processing,[1] transferring, providing, publishing, deleting, etc.", while Data is defined, much like in the latest cybersecurity laws and regulations, as "any record of information in electronic form". The Draft Regulations also provide definitions for terms used in the existing cybersecurity framework but not yet defined, such as "specific consent" and "large internet platform operator" (see further below).

2. The Draft Regulations draw a threefold distinction of Data: "core data", "important data" ("**ID**") and "general data" – though these terms are also not entirely new to the existing cybersecurity framework. Briefly, "core data" refers to Data relevant to state security, key branches of the national economy, key areas of people's livelihood and significant public interest. As for ID, the Draft Regulations define it much as other recent (draft) regulations do: Data that may endanger national security or public interests if tampered with, destroyed, leaked, illegally obtained or illegally used, including but not limited to:

   (a) non-public government Data, work secrets, intelligence Data and law enforcement and judicial Data;

   (b) export-controlled Data, Data related to export-controlled items' core technology, design solutions, production processes, etc., Data on scientific and technological achievements that have a direct impact on national security and economic competitiveness in cryptography, biology, artificial intelligence and other areas;

   (c) national economic operation Data, important industry business Data, statistical Data, etc. whose dissemination is (to be) protected or controlled under national laws, administrative regulations,

[1] The Chinese term corresponding to "processing" here is "加工", whereas the Chinese word corresponding to the more general word "processing" used in all other places in this Newsletter (and generally in English-language versions of China's cybersecurity laws, regulations, etc.) is "处理".

departmental regulations, etc.;

(d) Data for safe production and operations in industrial, telecommunications, energy, transportation, water conservancy, finance, national defense, science, technology, customs, taxation and other key industries and areas;

(e) national basic Data concerning the population, health, natural resources and environment, such as genes, geography, minerals and meteorology, at the scale or accuracy stipulated by the relevant authorities;

(f) Data concerning construction and operation of national infrastructure and "critical information infrastructure" ("**CII**")[2] and their security, Data of the geographic location and security of important and sensitive areas, such as national defense facilities, military administration areas, national defense research and production units, etc.;

(g) other Data that may affect national political, territorial, military, economic, cultural, social, scientific, technological, ecological, resource, nuclear facility, overseas interest, biological, space, polar, deep sea and other security.

3. Finally, "general data" is not defined in the Draft Regulations or any other provision in the PRC cybersecurity framework, but there are indications that it refers to all Data not falling under the category of "core data" or ID. In addition, however, the Draft Regulations seem to introduce a term "public data", defining it as Data collected or generated during the performance of public management functions or the provision of public services by government authorities or other organizations that have been authorized with management functions of public affairs under PRC laws and regulations. Setting aside state-owned entities and other parties connected or working closely with government bodies, most companies are unlikely to process "core data" or "public data".

Extraterritorial Effect

4. The Draft Regulations would extend the recent trend of PRC legislation containing provisions purporting to impart extraterritorial affect. The Draft Regulations provide three circumstances in which they would apply to processing of Data of individuals or organizations within China done outside China (plus a catch-all "other circumstances provided for by [other] laws and administrative regulations"):

(a) the processing is for the purpose of providing products or services within China;

(b) the processing is for analyzing and evaluating the behavior of individuals or organizations within China; or

(c) the processing involves onshore ID.

The PIPL already provides for (a) and (b) above, though only with respect to "personal information"

[2] The *Cybersecurity Law* defines "critical information infrastructure" as infrastructure "used for public communications, information services, energy, transport, water conservancy, finance, public services, e-government affairs, and other important industries and fields and other critical information infrastructure that will result in serious damage to the national security, national economy, people's livelihood and public interests if they are destroyed, there are lost functions or they are subject to data leakage."

("**PI**"),[3] while the Draft Regulations, in addition to expanding (a) and (b) by applying it to Data, add (c).

General Data Security Requirements

5. The Draft Regulations would impose somewhat generic obligations, most being largely redundant under the existing cybersecurity framework, on all Data Processors, *e.g.*, employing measures such as encryption, access control and emergency response mechanisms and more generally strengthening security protection of Data processing, transmission and storage systems. They would also impose several new general obligations, *e.g.*, a time limit for reporting information about a data security incident to Data subjects and government authorities.

Corporate Change Reporting and Cybersecurity Review

6. The Draft Regulations would also require reporting in the context of certain corporate changes. Specifically, in any of the following circumstances, the relevant parties would need to report to the CAC for a so-called "cybersecurity review":[4]

   (a) Any merger, restructuring or spin-off that affects or might affect state security and that involves an Internet platform operator that controls a "large amount of data resources" concerning state security, economic development or public interests;

   (b) Any listing done on a stock exchange outside the country involving a Data Processor with PI of more than 1 million users; or

   (c) Any listing that is done on a Hong Kong stock exchange and that affects or might affect state security.

While the second requirement merely repeats a requirement in the draft *Measures for Cybersecurity Review* issued by the CAC on 10 July 2021, the first and third requirements are new. However, the Draft Regulations do not elaborate on when a merger, restructuring, spin-off or listing in Hong Kong affects or might affect state security. In addition, when a Data Processor dissolves or enters bankruptcy, it would have to report to the relevant authorities, and hand over or delete Data as required by the authorities.

Reinforced Requirements for Processing PI

7. The Draft Regulations reiterate key rules regarding PI under the existing cybersecurity framework (*e.g.*, processing of PI may only be done to the extent necessary for providing services or fulfilling legal obligations, and functionality cannot be withheld for failure to provide non-necessary PI). They would also reinforce the existing framework by specifying expanded or additional rules, such as the following:

   (a) A privacy policy would be required to specify, *inter alia*: (i) the purpose, use, method, type,

[3] The PIPL defines "personal information" as "all kinds of information recorded by electronic or other means related to identified or identifiable natural persons", explicitly excluding anonymized information.

[4] The *Cybersecurity Law* introduced the concept of a "cybersecurity review", but the only currently binding specific rules are in the *Measures for Cybersecurity Review*, which were issued on 13 April 2020 (effective as of 1 June 2020) and ostensibly applied only to operators of CII and only when purchasing network products or services that affect or may affect state security; on 10 July 2021, a draft revision of the *Measures for Cybersecurity Review* was issued and would significantly expand the scope of application of the "cybersecurity review".

frequency, timing and storage location of PI with respect to each function as well as the impact to functionality of a user refusing to provide PI; (ii) the storage term or at least the way to determine it; and (iii) detailed information for any plug-in, including the plug-in operator's name and processing rules.

(b) In any dispute regarding whether user consent has been obtained, the Data Processor would bear the burden of proof.

(c) PI would have to be deleted or anonymized within 15 working days of (i) the purpose for PI processing being realized or no longer necessary, (ii) expiry of the storage term as agreed or determined under the privacy policy, (iii) termination of the service or deregistration of the account, or (iv) the automated collection of PI without user consent. However, if certain PI could not be deleted or anonymized due to technological or business difficulties, a Data Processor could keep it but not process it (except to store it) and would have to provide the PI subject(s) a "reasonable explanation".

(d) Biological characteristics (*e.g.*, fingerprints, faces, voices, gaits) could not be used as the sole method for personal ID verification, and when used, the Data Processor would be required to conduct a risk assessment on the necessity and safety of the use.

Requirements Related to ID or to PI of More than One Million Users

8. The Draft Regulations specify additional obligations on processors of ID ("**ID Processors**") and processors of PI of more than one million users ("**Volume PI Processors**"). Such obligations include:[5]

(a) Data Protection/Security Officers and Departments. One or more data protection officer(s) ("**DPO**") and a data security management department ("**DSMD**") would need to be designated, and the DPO/DSMD would be required to, *inter alia*, propose data security–related resolutions, formulate data protection plans and emergency response systems, supervise data security risk, handle data security risk events, conduct trainings, accept and handle complaints and reporting, and report to the CAC and other authorities regarding data security.

(b) Reporting. Within 15 working days after the identification of any ID or PI, the following would have to be reported to the competent authorities: certain information about the processor, its DPO and DSMD as well as purpose, scale, method, scope, type, storage term and location information about the processed Data. In addition, any merger, restructuring or spin-off would need to be reported to the competent authorities.

(c) Training. Technical staff and management staff would have to receive no less than 12 hours of training, per year, *concerning* data security.

(d) Annual Security Assessment. A "data security assessment" ("**Annual Security Assessment**") would need to be conducted, by either the processor or a data security service institution, each year and reported to the relevant authorities by January 31 the following year. The Annual Security Assessment, which would need to be retained for 3 years by the Data Processor, would

[5] According to Article 26, Volume PI Processors must abide by the rules applicable to ID Processors, which would include all the following rules, although it is questionable whether the regulators intend for all processors of more than one million users' PI – which likely characterizes many businesses processing PI in China – to carry out all the required reporting procedures – which may entail a large expenditure of resources not only for such processors but also for regulators.

have to cover such matters as data security management policies, risks, events, etc.; if the processor carried out certain enumerated activities (*e.g.*, sharing, "transacting",[6] processing on behalf of others, etc.), the Annual Security Assessment would have to cover additional matters, such as whether the contractual obligations and technical measures undertaken by the recipient are sufficient to prevent Data breaches. The Draft Regulations provide that the Annual Security Assessment requirements would also apply to any Data Processor (not only ID Processors and Volume PI Processors) listing overseas (possibly including in Hong Kong); therefore, certain overseas-listing Data Processors would have to undergo a "cybersecurity review" and carry out and report Annual Security Assessments.

9. In addition, sharing, "transacting" or entrusting others to process ID would be subject to pre-approval by competent authorities.

10. Finally, the Draft Regulations provide that any government department or operator of CII purchasing cloud computing services would be subject to a "security assessment" – though unclear, "security assessment" here likely refers to the cybersecurity review under the *Measures for Cybersecurity Review*.[7]

Restrictions on Cross-Border Data Transfers

11. With respect to provisions specifically on cross-border data transfers, the Draft Regulations for the most part merely repeat the restrictions or prerequisites under the existing cybersecurity framework or at least recently released draft regulations, *e.g.*, the draft *Measures Concerning the Security Assessment for Cross*-Border *Data Transfer* released by the CAC on 29 October 2021. One addition, mentioned above, is the requirements regarding the Annual Security Assessment in relation to cross-border transfers of ID (and of PI) of more than one million users.

12. However, the Draft Regulations may mark a major milestone in terms of the PRC legal regime: it would contain one of the first – if not the first – public-facing rule relating almost explicitly to the so-called "Great *China* Firewall", *i.e.*, the set of technological measures employed by the country to impede domestic users from accessing certain internet content hosted offshore. Article 41 of the Draft Regulations provides: "The State established a cross-border data security gateway to block the spread of information that originates from outside the PRC and is prohibited by laws and regulations from being released or transmitted." Article 41 further prohibits all individuals and organizations from providing programs, tools, routes, etc. for passing through or circumventing the cross-border data security gateway and from providing internet access, server hosting, technology services, marketing, payment settlement or application downloading services for any activities passing through or circumventing the gateway. Finally, Article 41 provides that the traffic of domestic users visiting onshore networks may not be routed overseas.

Enhanced Requirements for Internet Platform Operators

13. The Draft Regulations would impose additional obligations on operators of platforms for online services ("**Internet Platform Operators**"), *e.g.*, online publishing, social networking and e-commerce, especially those with at least 50 million users, processing large amounts of PI and ID, and having strong social mobilization ability and market dominating status ("**Large Internet Platform Operators**"). Such obligations include:

[6] The Chinese word is "交易" and it is a term neither significantly used before in existing or draft cybersecurity laws, regulations, etc. nor defined in the Draft Regulations.
[7] See footnote 4.

(a) User Terms and Privacy Policy. New or significantly updated user terms or privacy policies would, before taking effect, need to be published in a prominent place on the platform for public comment for at least 30 working days, public comments should be adopted to improve the terms or policies and information about such adoption (or reasons for rejection) would also have to be published. Furthermore, Large Internet Platform Operators with more than 100 million daily active users would be required also to submit new or significantly updated terms or policies for an assessment by a third party designated by the CAC and for the approval of the CAC and the Ministry of Industry and Information Technology (MIIT) at the provincial level.

(b) Liability for Third-Party Products and Services. Internet Platform Operators would be liable for data security violations arising from third-party products and services connected to the platforms, including to compensate users for any losses caused by connected third-party products and services.

(c) Instant Messaging Interfaces. Internet Platform Operators providing instant messaging services would need to provide interfaces for users to transfer data to other instant messaging service providers.

(d) Annual Auditing. Large Internet Platform Operators would be required to entrust third parties to conduct annual audits of data security, platform rules, enforcement of undertakings, PI protection, etc., and would also have to publish the results of such annual audits.

(e) Processing Data via New Tech. If artificial intelligence, virtual reality, deep learning or other new technologies would be used by an Internet Platform Operator for processing data, it would need to undergo a "security assessment" – whether of the same kind as other "security assessments" provided for under the Draft Regulations is not clear.

Supervision and Penalties

14. The Draft Regulations reiterate and might possibly expand the scope of application of the relatively wide powers of the CAC and other government authorities to supervise and investigate data protection and security activities for violations, including by:

    (a) Interviewing employees of Data Processors;

    (b) Retrieving and reviewing documents and logs concerning data security; and

    (c) Auditing Data Processors' security measures, including through third-party professional agencies.

15. According to the Draft Regulations, the state supports the establishment of associations for PI protection, for exposing activities violating PI protection, reporting violations to authorities, etc.

16. Finally, for each requirement in the Draft Regulations, liability is also specified. Penalties, such as fines and measures such as revocation of business licenses, generally match those provided for under the Data Law and PIPL (which were heightened compared to the *Cybersecurity Law*).

Takeaways

17. China has for years been building up its data security and privacy protection legal framework, much like many other jurisdictions, but mostly with relatively small and often imprecise building blocks. If the Draft Regulations were to be issued more-or-less in their present form, they would represent

a comparably large and clear addition to the legal framework, although they might also introduce some new uncertainties, at least until further regulations or interpretations would arrive. Key yet hitherto undefined terms (such as the "specific consent" required from data subjects for some of their personal information to be collected, processed or transferred) would finally have official, binding definitions. The categorization of data, into "core", "important" and "general", would be significantly though still not completely clarified. Many so far missing details about the restrictions and requirements in processing data would be specified, *e.g.*, the timing and other details of the required response to a data breach and the threshold amount to PI processed before certain obligations are triggered.

18. The Draft Regulations, however, appear to take a further step: they would add obligations on certain Data Processors in certain circumstances. Some of these have already been heralded, *e.g.*, by vague or abstract references in earlier legislation or by other draft regulation recently released, but others appear to be largely or entirely new. The need for companies to undergo a "cybersecurity review" before certain mergers, restructurings, spin-offs and listings on overseas stock exchanges (including Hong Kong) is among the most notable examples, as is the need for certain companies to undertake and submit an Annual Security Assessment. The provisions concerning a "cross-border data security gateway" – likely one of the clearest references to the so-called "Great China Firewall" in any PRC legislation or regulation – is another novelty of the Draft Regulations.

19. In its relatively measured construction of the cybersecurity framework, China has on occasion released draft rules that were significantly pared down or simplified before being formally issued (or were never formally issued) – this occurred especially when the draft rules were particularly novel, complicated or controversial. On the one hand, the same may apply to the Draft Regulations, though on the other hand, China may be at or near the point of having formal rules that adequately cover details of such sensitive matters as cross-border data transfers, especially if the formal rules would track existing or emerging practices in reality and therefore at least afford a degree of transparency and predictability. For now, parties collecting, processing or transferring data in or across China's borders may wish to take a close look at the Draft Regulations, but bearing in mind not only that they are still in draft form but also that several of the rules – and the most notable amongst them – may not come into effect anytime soon (if ever).

******

 The authors from DaHui Lawyers involved in producing this Newsletter include: Richard Ma, Managing Partner (firm bio); Joanna Jiang, Partner (firm bio); and Dimitri Phillips, Associate (firm bio).