THE
NATIONAL LAW REVIEW

China's Draft Data Security Measures and How They Compare to the GDPR

Monday, June 24, 2019

The Cyberspace Administration of China (the "CAC") launched a public consultation on the draft Administrative Measures on Data Security (the "Draft Measures") on May 28, 2019. This consultation falls in the middle of the publication of the drafts for two other data protection rules, namely the Measures for Security Assessment for Cross-border Transfer of Personal Information and the Measures for Cybersecurity Review.

Together, these three measures will implement a significant portion of the Cyber Security Law (the "CSL") and become the first set of binding laws focused solely on data protection, adopting certain rules from the non-binding Personal Information Security Specification. The Draft Measures were published just over a year after the General Data Protection Regulation (the "GDPR") came into effect in the EU and certain similarities between the two regimes are apparent.

Article By
Olivia Zhiying Zhan
Squire Patton Boggs (US) LLP
SECURITY & PRIVACY // BYTES

Communications, Media & Internet
Consumer Protection
Global
China

Extraterritorial Scope

The territorial scope of the CSL is repeated in Article 2 of the Draft Measures, to the extent that it shall apply to the construction, operation, maintenance and use of the network as well as the supervision and administration of cybersecurity within the country. However, Article 4 of the Draft Measures further stipulate that the State will

"*monitor, defend against and deal with data security* ***risks and threats from both inside and outside the territory*** *of the People's Republic of China, protect data from being divulged, stolen, falsified, damaged or used illegally, and punish the illegal and criminal activities that endanger data security in accordance with the law*".

It seems that China could take action against risks even outside of its borders, an extension of scope made even more powerful through the lack of a definition for the key term "risks and threats".

As the CSL takes precedence over the Draft Measures, the latter are not allowed to make any provisions inconsistent therewith or create new law going beyond the implementation of rules in the CSL. Additionally, State overreach into other jurisdiction in order to protect from security threats is a regular phenomenon that can be committed by any government around the world. Consequently, different from the GDPR, the Draft Measures may not be interpreted as providing extraterritorial effect for data protection. Further clarity on what actions the State may take has not yet been provided.While the GDPR was criticized by commentators for expanding jurisdiction to protect any EU citizen, the Draft Measures might go even further on the basis of dealing with data security risks from outside China.

Filing System/Registration Requirement

While, similarly to Art. 2(1), 4(6) and Recital 15 of the GDPR, the Draft Measures refer to "filing" requirements, the new procedure described in Article 15 is much more similar to the registration requirements under the implementation laws of the Data Protection Directive (the predecessor of the GDPR). How the filing system will work in practice is currently unclear and the government is seeking public opinion.

Perhaps the CAC may go in the direction the CNIL (France's data protection authority) took. Under French law, controllers had to register with the authority not only their own details, but also information on all processing and

data transfers they or a processor undertakes. This also encompassed a requirement for controllers to register all new transfers and purposes of processing with the CNIL and await their consent.

On the other end of the spectrum, the CAC may follow the ICO's example (the UK's data protection authority). The ICO had a template on its website with checkboxes, which would automatically generate statements when clicked. Thus, in contrast to drafting a complex registration document from scratch, as required in France, in the UK controllers simply had to decide which pre-existing statements applied to them. Also in contrast with the CNIL, the ICO did not need to provide consent for companies to process data, they only had to be informed. Considering the UK approach's advantage in efficiency and the CAC's fraternizing with potential offenders (which the ICO also formerly engaged in), the State will most likely consider the UK's implementation of the notification requirement.

It is worth noting that in line with Recital 89 GDPR, the requirement to register with local authorities in the EU was overturned in the GDPR. This served to replace the external accountability requirement of notification with internal accountability measures, such as maintaining accurate Records of Processing and conducting Data Protection Impact Assessments, which the authorities can access. Nevertheless, it can be argued that the ICO's current requirement to pay a data protection fee is a sort of work-around of the prohibition on a blanket registration requirement. Additionally, the CNIL (like the AEPD in Spain and the ADA in Lithuania) still has a form of Controller registration requirement and the Estonian data protection authority still requires the processing of sensitive data to be registered, perhaps reflecting the Article 15 requirement the most.

Big Data and VPN

Perhaps the biggest areas of divergence between the GDPR and the Draft Measures are their treatment of big data and the use of VPN. The GDPR covers big data and AI indirectly in Article 22, in its rights related to automated decision-making. Through t he right to object conferred therein, together with elements like data security requirements, the EU clearly opted to restrict big data in favour of consumer protection.

By contrast, through the Draft Measures, China seems to limit mass data collection only to where required for the sake of transparency. Article 16 of the Draft Measures explicitly requires network operators to abstain from interfering with automatic data collection and access, mandating that they only stop doing so when they "*seriously affect the operation of websites*". Article 24 adds a transparency requirement, that network operators automatically synthesizing media information indicate explicitly this process. The only restriction on big data and AI is contained in Sentence 2 of Article 24, which prohibits the aforementioned use in media information synthesis for the aims of causing profit increase or damage.

Thus, the Draft Measures seem to align more with the California Consumer Protection Act (the "CCPA") than the GDPR, which simply does not mention automated decision-making. The reasons thereof can perhaps be found in the high technological aims of their countries. Through lax regulation of big data, the CCPA may aim at supporting innovation in Silicon Valley and the Draft Measures at doing the same in Shenzhen.

However, the commercial advantage provided by Articles 16 and 24 may be undone by the strengthening of the Great Firewall in Article 29. This article generally prohibits the overseas routing of traffic on domestic internet by domestic users, which seems to be a direct attack on the use of VPN. Due to the internet censorship laws in China, most companies in the country have had to rely on VPN to access the outside world for crucial business operations, from connecting with customers outside the country to using services provided by foreign websites. The article seems to aim at strengthening the Great Firewall, which may dissuade companies with existing or future business outside of the country. Nevertheless, the article in the Draft Mearsures is too brief to guide practioners in this regard. Future regulation or guidelines may provide interpretations of the definition and limitations of the overseas routing of traffic.

Marketing Rules

Another similarity to the GDPR is likely to be the new marketing rules provided by Article 23 of the Draft Measures. Article 21 GDPR provides data subjects the right to object to direct marketing and adds some transparency requirements to be implemented by controllers and processors. Similarly, Article 23 of the Draft Measures requires network operators to explicitly indicate where data is used for targeted advertisement and gives users the right to object to receiving such advertisements. The Article also sets out the procedure to be followed, requiring operators to stop push advertising when the user opts out and delete their data.

The conditions for consent to marketing (and other processing) are also brought in line with the EU. In Article 7, the GDPR sets out the elements of free, informed and clear consent. Similarly, Article 11 of the Draft Measures prohibits consent by default, bundling and implied consent.

Nevertheless, Article 23 of the Draft Measures still provides some additional powers to the enforcement agencies

that the GDPR does not. Specifically, Paragraph 2 requires network operators engaged in targeted advertising to "*respect social morality and business ethic, abide by public order and good morals, and be honest and diligent*". The vague wording thereof may empower enforcement agencies to clamp down on businesses in a wide-ranging array of situations unless further guidance is provided.

Penalties

Ultimately, the potential for severe penalties in the cases of non-compliance is the biggest motivator of compliance. Compliance with the GDPR was undoubtedly so high due to the high value of potential fines. The Draft Measures followed this line in Article 37, increasing the seriousness of potential remedies, but nevertheless failing to reach the levels of the GDPR. Similarly to previous provisions, the Article sets out examples of the disciplinary action that enforcers can take, ranging from "*disclosing misconduct publicly, confiscating illegal incomes,* [and] *suspending relevant business operations*" to "*ceasing business operation for rectification, shutting down the websites,* [and] *revoking the relevant business permits or business licenses on it*".

Notably, the Draft Measures did not list the imposition of monetary penalties as one of the available enforcement tools and they did not set out the extent thereof in a separate article, like Article 83 of the GDPR. The reasons thereof remain unclear and will perhaps be explained in future guidance.

The Draft Measures are currently up for consultation. Any member of the public can provide comments until June 28, 2019. To submit a comment, either:

- Email security@cac.gov.cn;
- Log in on the Legal Information of Chinese Government website and click on the "Collection of Legislative Comments" tab; or
- Send post to the Office of Internet Security Coordination of the Cyberspace Administration of China, No. 11 Chegongzhuang Street, Xicheng District, Beijing, 100044, indicating "Comments on Administrative Measures on Data Security" on the envelope.

Co-authored by Daniel Csigirinszkij