CHINA

"In addition to a rocketing administrative workload, the proposed regulations would also give rise to a disproportionate compliance burden for overseas entities that collect only a small amount of personal information on an irregular or random basis."

—JAMES GONG, senior associate, Herbert Smith Freehills, Beijing

"The measures have been under heated debate during the period of public comment as to whether it is reasonable to require network operators to go through the mandatory security assessments regardless of the volume of personal data that would be transferred outside of China."

—DORA LUO, counsel, Hunton Andrews Kurth, Beijing

China's draft Measures on Security Assessment of the Cross-border Transfer of Personal Information

The Cyberspace Administration of China (CAC) released the draft Measures on Security Assessment of the Cross-border Transfer of Personal Information on June 13, 2019. The Measures, which refer to the GDPR, apply to all network operators, i.e., "owners and managers of networks as well as network service providers." The comment period ended on July 13, 2019.

Under the draft measures, network operators should undergo security assessment with the CAC prior to the transfer of personal information collected in China to an overseas recipient. They should also file their security assessment report with the CAC for evaluation. If results show that the cross-border transfer may "impact China's national security, endanger public interest or ineffectively protect personal information," the transfer will not be allowed.

Network operators should also have data transfer agreements containing specific clauses with all overseas recipients. Among these clauses are that the data subjects are the beneficiaries of the contract and they can bring infringement claims against either the network operator or the recipient or both and claim damages.

Additionally, the measures specify that network operators should develop an incident response plan, report serious data security incidents immediately and keep a record of all cross-border data transfers for at least five years, among others.

In the case of a foreign entity, appointing a local representative who will help the organization to comply with Chinese data protection and security policies may be beneficial.

According to James Gong, senior associate at Herbert Smith Freehills in Beijing, there will be challenges once the measures are enacted.

"The measures do not provide any exemption for random or limited transfers of personal information. This will further increase the number of applications and also the compliance burden for companies that only export personal information on an occasional basis. Measures seem to apply to all overseas entities that collect personal information from China, irrespective of the amount of personal information collected or whether Chinese data subjects are targeted. In addition to a rocketing administrative workload, the proposed regulations would also give rise to a disproportionate compliance burden for overseas entities that collect only a small amount of personal information on an irregular or random basis," says Gong.

He also mentions that some of the provisions to be included in the export contract seem to be inconsistent with the general contract law or tort law. Thus, problems in enforcement may arise.

He cites other gaps in the draft measures: "The draft regulations do not expressly specify whether the overseas entities must also apply to the CAC for assessment and pre-approval for the collection of personal information."

Dora Luo, counsel at Hunton Andrews Kurth in Beijing, agrees with Gong. "The measures have been under heated debate during the period of public comment, for instance, as to whether it is reasonable to require network operators to go through the mandatory security assessments conducted by the competent authority regardless of the volume of personal data that would be

transferred outside of China," she says.

Gong continues: "In addition, the 2019 Draft Measures do not expressly provide a grace period within which network operators can complete the evaluation and approval process. If implemented strictly, network operators may have to cease current transfers and wait for the export applications to be evaluated and approved. This would give rise to serious operational difficulties for a number of companies."

Luo sees additional challenges considering the complexity of cross-border data transfers.

"For instance, the measures only address cross-border transfer of personal data rather than the much larger amount of non-personal data," says Luo. "Before the measures were issued, back in April 2017, the China Administration of Cybersecurity also released the Draft Measures on Assessment of Cross-Border Transfer of Personal Information and Important Data. Even though the relationship between these two drafts still remains unknown, it seems that cross-border transfers of personal data and cross-border transfers of important data would be subject to different regulations."

She also believes that some organizations which need to transfer large amounts of personal data outside of China will have to review their IT structures. In case data cannot be delivered out of China, the organization may even be forced to build a data center on Chinese soil.

Despite these however, Luo believes the draft measures serve a purpose.

Singling out the security assessment process as a smart move, Luo says, "the security assessment is a reasonable option in the initial stage of the establishment of a cross-border data transfer mechanism in China. It is hard to reach a unanimous agreement as to the global standard of national security which might vary by the change of volume, type, scope of data, network security environment of the receiving nation, data security laws, foreign relations, international political and economic situation and development of new technology. The specific standard of assessment of national security is difficult to confirm in the preliminary stage of drafting the cross-border data flow, so the security assessment is a smart way for exploration."

In totality, Luo says that the issuance of the draft measures shows China's commitment to continuously improve its data protection laws. Her firm also believes that the orderly data flow will promote data privacy and data compliance in Asia Pacific.

Citing the Snowden incident of 2013, Luo says, "conditions such as geopolitics, national security, privacy protection, industry capabilities and market access inevitably influence and drive such policies. The issuance of the measures reflects the burgeoning demand of data protection as well as cybersecurity compliance in China. On one hand, China wants to promote the free flow of data. On the other hand, China also needs to ensure security. China is trying to seek orderly data flows in the complex political environment and with the rapid development of technology."—**ESPIE ANGELICA A. DE LEON**

EUROPE

"Supervisory authorities will focus on claims where there is a clear link between the data subject and the EU, for instance where the data subject is a citizen or resident in the EEA. So practically speaking, individuals from outside the EEA will not have access to this right."

—GABRIEL VOISIN, partner, Bird & Bird, London

"It may be possible for the right to be forgotten to limit freedom of speech and expression because the individual has complete control over their personal data, notwithstanding that it may have been commented on by others or be important for the public to view."

—SHEENA JACOBS, managing partner, JurisAsia, Singapore

ECJ: The right to be forgotten, but only in the EU

The European Court of Justice (ECJ) has recently ruled in favour of Google, saying that it does not have to remove links of sensitive information of people worldwide,

but only for those within the boundaries of the European Union. In its ruling, the top court claimed that the dispute known as the *right to be forgotten* or *the right to erasure* could be ill-treated by authoritarian governments should it be implemented outside Europe.

With this win, individuals can see litigious entries de-listed from Google results at a worldwide level if the competent EU data protection regulator or court determines that, in the light of national standards, global de-listing would be required.

Gabriel Voisin, a partner at Bird & Bird in London, explains further that this ruling means that under EU laws, everyone has a right to data protection.

"In practice, however, supervisory authorities will focus on claims where there is a clear link between the data subject and the EU, for instance where the data subject is a citizen or resident in the European Economic Area (EEA)," he says. "So practically speaking, individuals from outside the EEA will not have access to this right."

If visiting the EU, the General Data Protection Regulation (GDPR) applies only to data subjects when they are in the EU, and this includes the right to be forgotten – Google is not required to remove the search results in other countries outside the EU. However, if visiting other countries outside the jurisdiction of the EU, for instance, and a different address for Google is put in, then any sensitive information still appears.

"Indeed, this search will be deemed to be outside the EU via your IP address, which will show that you are in other countries outside EU," says Voisin. "This happens regardless of your nationality. This also explains why you may see from time to time the following disclaimer at the bottom of Google result web pages: 'Some results may have been removed under data protection law in Europe.'"

On the other hand, if Google removes an individual from searches in Europe, the possibility of showing up on Google in the US, Hong Kong or the Philippines, for example, may depend upon the search engine.

"An important distinction here is that individuals cannot just request a blanket wipe of 'their data' from the internet," says Voisin. "The right to be forgotten requests are linked to particular items that individuals want to see de-listed from Google results. Google reviews every request. If Google believes that arguments can be made to resist to someone's request (e.g. there are freedom of information or speech considerations that override the individual's rights), then it may decline to remove the requested item. If Google does remove the requested item, it would do so only in relation to EU-wide results, meaning that if you Google the search term outside of the EU, it will appear."

Voisin adds that if a competent EU data protection regulator or court approached by the individual determine that, in the light of national standards, global de-listing would be required, then the item may no longer be listed and Google will have to remove it from results displayed in Europe, US, Hong Kong, the Philippines or anywhere else in the world.

Meanwhile, according to Sheena Jacobs, managing partner of JurisAsia in Singapore, the difficulty with this right is that it is quite complicated to accomplish when you also consider other rights such as freedom of information or the public interest.

"It may be possible for the right to be forgotten when taken to the extreme to limit freedom of speech and expression because the individual has complete control over their personal data, notwithstanding that it may have been commented on by others or be important for the public to view," she says. "While this would not arise in every case, the public also has a competing right to have access to such information. For example, a totalitarian government may use this right to censor content that they do not want their citizens to have access to."

She adds that in the near future, it is quite possible that the right to be forgotten may be implemented in other countries' data protection laws in the same way as rights of access and correction.

In 2016, Google was fined approximately US$110,000 by the Commission Nationale de L'informatique et des Libertés (CNIL), a private, France-based organization designed to protect personal data, support innovation and preserve individual liberties, for its failure to delist search engine results globally. This came after the EU's right to be forgotten in 2014 that says that search engines should have the right to remove results that are deemed inappropriate and vulgar, such as criminal records.

In view of the ruling, the top court considered two cases. The first looked at the territorial scope of de-listing requests (the right to be forgotten on Google). The second examined requests to de-list sensitive personal data (special category data) and criminal offenses and convictions data and Google's obligation to consider the interests of freedom of information.—**EXCEL DYQUIANGCO**

TAIWAN

"The implementation of the patent linkage will definitely raise the protection strength for pharma IP holders. It is the nature and intended purpose of the policy. Once