SQUIRE PATTON BOGGS

China Finalizes New Regulations to Relax Personal Data Exports from China

By: Lindsay Zhu, Scott Warren, Haowen Xu and Charmian Aw

APAC – March 2024

Nearly six months after the Cyberspace Administration of China (CAC) was first introduced for public consultation, with its draft regulations proposing to ease outbound data transfers from China (**Draft Regulations**) (see our article at China Releases Draft Regulation to Significantly Ease Cross-border Data Transfers | Privacy World), the much-awaited final rules on Regulating and Facilitating Cross-border Data Flows were published and came into effect on March 22, 2024 (New Regulations). The New Regulations largely repeat the Draft Regulations, but now have further relaxed personal data exports from China.

Meanwhile, on the same day, the CAC also released the Guide to the Application for Security Assessment of Data Exports (Second Edition) and the Guide to the Filing of the Standard Contract for Personal Data Exports (Second Edition) (collectively, the Second Edition Guides) which make corresponding adjustments pursuant to the New Regulations.

Exceptions to Signing Standard Contracts and Easing of Government Security Assessment Thresholds

The New Regulations largely implement exceptions set forth in the Draft Regulations, permitting certain cross-border transfers of personal data from China without the need to sign or file a standard contract (SC) or file a personal information privacy impact assessment (PIPIA) with the CAC. However, as compared to the Draft Regulations, the New Regulations further lessen export obligations requiring SCs and PIPIA filings by increasing the threshold from 10,000 individuals to 100,000 individuals for non-sensitive data.

The New Regulations further significantly raise the threshold requiring the exporter to apply for a mandatory government security assessment.

As a guide, we compare the old and new regulations as follows:

Control Measures	Old Regulations (before March 22, 2024)	New Regulations (from March 22, 2024)
New exceptions implemented for specific categories of personal data (no need to pass security assessment or the signing/filing a standard contract)	N/A	1. Export of employee personal data necessary for the purpose of HR management, pursuant to duly formulated HR policies and collective labor contracts 2. Export of personal data necessary for performing a contract for which the individual is a contracting party, such as online shopping, cross-border delivery, cross-border payment, hotel/flight booking, visa applications, examination services etc. 3. Export of personal data necessary for protecting the life, health and property safety of natural persons in case of emergency 4. Export by non-CIIOs[1] of less than 100,000 individuals' non-sensitive personal data annually.

1 Critical information infrastructure operator, which typically refers to an operator of critical infrastructure and IT systems to national security and public interest.

Mandatory government security assessment (these categories require getting government approval to export)	1. Export of Important data[2] 2. If the exporter is a CIIO, 3. If the exporter is a controller that processes one million or more individuals' data 4. Export of 100,000 or more individuals' data annually, 5. Export of at least 10,000 individuals' sensitive data annually.	Unless otherwise exempted under the Exceptions (1)-(4) above: 1. Export of Important data 2. If the exporter is a CIIO 3. Export of one million or more individuals' data annually 4. Export of 10,000 or more individuals' sensitive data annually Note: Item (3) was previously based on the volume of data processed by an exporter in its capacity as a controller of that data, whereas the threshold now is based purely on the volume of data that is exported from China. The earlier Item (4) has now been removed entirely.
Sign and file with the government a standard contract and personal information privacy impact assessment	Required for export of any other personal data	Unless otherwise exempted under the Exceptions (1)-(4) above, now required only for the: 1. Export of more than 100,000 but no more than one million individuals' data annually 2. Export of up to 10,000 individuals' sensitive data annually.

Other Clarifications

The New Regulations also make important clarifications that are commonly of concern to multinational companies and businesses:

- Business/marketing/scientific data (other than personal data and important data) can be freely transferred.
- The specific list or catalogue of "important data" will be provided by the government, either through public announcement or notice to specific entities. Accordingly, businesses will not need to make a self-judgement as to whether they possess or process important data.
- Exports of personal data originally collected and generated outside of China, and then transferred into China for processing is exempted from a government security assessment, as well as the signing and filing of a standard contract, provided that no domestic personal data or important data is introduced during the processing.
- The validity period for a government security assessment is extended from two years to three years, with the possibility of extending the validity period for another three years.
- Free trade zones may establish whitelists to further relax data flows among applicable jurisdictions therein.

Application to Foreign Controller?

While not stated in the New Regulations, the Second Edition Guides interpret "data exports" to include the extraterritorial processing of Chinese residents' personal data, as described in Article 3 of the Personal Information Protection Law (PIPL). This provision covers the processing of personal data of Chinese residents outside of China for purposes of providing services and products to Chinese residents or analyzing Chinese residents' behavior. You may note this is similar to the applicability of the EU/UK GDPR's extraterritorial effect. This interpretation seems to suggest that a foreign controller may also be required to pass a government assessment or sign a standard contract where the PIPL applies. It is, however, unclear how this will be implemented. For example, it is uncertain which party will be the "data exporter" and which party the "foreign recipient" if the personal data is collected directly from individuals. Moreover, given that the PIPL applies only for the purposes of providing products, services or behavior analysis, it seems that such purposes will qualify for Exception (2) above and thus be exempted from the government assessment as well as the signing and filing of SCCs.

2 "Important data" is defined under China's Data Security Law.

Recommendations

The New Regulations took effect immediately upon their publication, i.e., March 24, 2024. We strongly encourage companies to swiftly identify their data exports from China, including the categories and quantities of data transferred in each scenario described above to evaluate their compliance with New Regulations. Companies should also keep in mind that even if they are exempted from having to pass a government security assessment or sign and file a standard contract, they are still required to fulfill their ongoing statutory obligations of providing the requisite notifications to and obtaining individuals' relevant consents, as well as conducting PIPIAs for their data transfer activities. We would advise that these compliance measures be properly documented to demonstrate accountability with the PIPL and New Regulations.

Contacts

Lindsay Zhu
National Partner, Shanghai
T +86 21 6103 6303
E lindsay.zhu@squirepb.com

Scott Warren
National Partner, Tokyo
T +81 3 5774 1813
E scott.warren@squirepb.com

Haowen Xu
Associate, Shanghai
T +86 21 6103 6300
E haowen.xu@squirepb.com

Charmian Aw
Partner, Singapore
T +65 6922 8679
E charmian.aw@squirepb.com