Employee Data Privacy – China

Cross-Border Data Transfer

Are there any restrictions on transferring personal data and how can these be overcome?

Cross-border data transfers affect all organizations that engage online IT services, cloud-based services, remote access services and global HR databases.

China's Personal Information Protection Law (PIPL) provides that data controllers (such as employers) may only transfer or access personal information outside of mainland China:

- if one of the following criteria is met: (a) the organization has passed a Cyberspace Administration of China (CAC) security evaluation; (b) the organization has obtained certification from a CAC-accredited agency; or, (c) the organization has put in place CAC standard contractual clauses (not yet published by Chinese Regulators) with the data recipient;
- to comply with laws and regulations or other requirements imposed by the CAC.

The employer (or other organization) must adopt necessary measures to ensure the data recipient's data processing activities comply with standards comparable to those set out in the PIPL. In practice this means initial due diligence, sufficient contractual protections and ongoing monitoring etc.

In addition to meeting one of the conditions above, the data controller (such as the employer) must (a) provide notice to, and obtain separate, explicit consent from the data subject (the employee); and, (b) conduct a personal information impact assessment.

The PIPL does not include a specific requirement to keep copies of personal information in China. However, certain personal information (and non-personal data) must still remain in (and cannot be accessed outside of) Mainland China. This includes (but isn't limited to):

- personal information processed by critical information infrastructure operators, unless a CAC-conducted security assessment has been completed;
- personal information processed by data controllers above a threshold/volume to be identified by the CAC (not yet published), unless a CAC-conducted security assessment has been completed;
- certain data under industry-specific regulations; and,
- restricted data categories (such as "state secrets", some "important data", geolocation, online mapping data, etc.).

Cybersecurity Law requires “critical information infrastructure” providers to store “personal information” and “important data” within China unless their business requires them to store data overseas and they have passed a security assessment. At this point, it remains unclear what qualifies as “critical infrastructure” and “important data,” although its inclusion in the text of the law alongside “personal data” means that it likely refers to non-personal data.

The National Standard of Information Technology – Personal Information Security Specification, (个人信息安全规范, GB/T 35273-2020), effective October 1, 2020, includes suggested best practices relating to personal data. When transmitting or storing sensitive personal information, the Specification recommends that security measures, such as encryption should be used.

The Draft Measures on Security Assessment of Cross-border Data Transfer was made available for public comment on October 29, 2021. The Draft Measures include a detailed description of when data that would be transferred out of China would be subject to a security assessment.

The Draft Measures have not yet been finalized and are therefore not binding at this time.

Last updated September 2022.