

DJINGOV
GOUGINSKI
KYUTCHUKOV
VELICHKOV

ATTORNEYS AND COUNSELLORS AT LAW



China Has Its Own Standard Contractual Clauses on Cross-border Personal Data Transfers:

What Do They Include and Mean to Business Cooperation between Organizations in EEA and China?

Recently, **the Republic of China has adopted its own set of standard data protection contractual clauses as an appropriate safeguard for transfer (export) of personal data to third countries.**

The cross-border trading relations of organizations operating within the People's Republic of China inevitably lead to international transfers of personal data. According to Article 38 of the China's Personal Information Protection Law (the "**PIPL**"), the three major mechanisms that can serve as a legal basis for domestic Chinese entities to engage in cross-border data transfers are (i) the security assessment led by the Cyberspace Administration of China (the "**CAC**"); (ii) the certification by licensed professional institutions; and (iii) the Chinese standard contractual clauses (the "**CN SCCs**").

On 24 February 2023, the CAC released **Regulation on the Standard Contract Measures for Exporting Personal Information** (the "**Regulation**") as well as an **annexed standard contractual clauses contract**. This serves as a final step to close the three-way mechanism defined under Article 38 of PIPL providing important details of applying the SCCs to outbound transfer of personal information from China.

Pursuant to the Regulation, **the CN SCCs apply where the respective companies in China:**

- (i) are not "*critical information infrastructure operators*";
- (ii) do not process the personal information of more than 1 million individuals; and
- (iii) have not transferred the personal information of 100,000 individuals or sensitive personal information of more than 10,000 individuals out of mainland China since 1 January of the previous year, regardless of the transfer destination.

Further, to adopt the CN SCCs mechanism, the data transferring company should **go through three main steps:**

1. it must conduct a personal information impact assessment before signing the CN SCCs for the personal information outbound transfer;
2. it must sign with the foreign recipients the CN SCCs without any modification, but for additional terms, which are not in conflict with the main text of the CN SCCs; and
3. after the signed CN SCCs take effect, the company must file the executed CN SCCs with the provincial CAC office for records, submitting both the executed CN SCCs and related personal information impact assessment within 10 working days. The impact assessment shall consider various explicitly provided factors, such as the validity, necessity, and appropriateness of the cross-border data transfer.

It is worth noting that a company must follow the CAC procedures if the data transfer has triggered the CAC-led security assessment scenario - the SCCs structure would not be a valid legal basis for the cross-border transfer in that case.

The Regulation will come into effect on **1 June 2023**, and the market players in China will have an additional 6-month (i.e., by 30 November 2023) grace period to conclude and implement the CN SCCs for existing cross-border data transfers.

Why the CN SCCs are important to Bulgarian and other European organizations that deal with Chinese vendors and/or customers or belong to Chinese corporate groups?

Because:

- The CN SCCs constitute a legal ground for exporting personal information from mainland China to other jurisdictions. In this relation, note that when the data exporter is located within the EEA, and the data importer is in China, the appropriate legal grounds for the international transfers of personal data would be those set forth in the GDPR, such as for example, the EU SCCs, pursuant to Article 1 of the EU Commission Implementing Decision on SCCs from 2021. It is therefore critical for businesses to understand the differences between the CN SCCs and the EU SCCs and mind possible parallel application of both regimes.
- When the CN SCCs come into effect and operation, the EEA data controllers transferring personal data to China would be able to add a favorable point in their updated transfer impact assessments when assessing the laws of China and, thus, reduce the risk of non-compliance claims regarding their personal data transfers to China.
- EEA clients and affiliates of Chinese companies should be aware and understand the significant efforts, time and costs that Chinese businesses and other organizations would have to invest in data protection assessments, measures and documentation to bring existing personal data processing into compliance throughout 2023 year.
- the CN SCCs mechanism will impact all the foreign investment companies in China and all Chinese companies that are doing international businesses.
- In mid-term perspective, business cooperation between companies and other organizations in the EEA and China may be expected to increase and diversify because of the increased export and use of personal data originating from China.

The potential benefits of CN SCCs for the international businesses partnering with Chinese organizations are to be seen. The European Commission and the European Data Protection Board have not taken the opportunity to comment on the CN SCCs yet.

QUESTIONS?



Ralitsa Gogleva

Counsel and Head of
Data Protection Practice

E: ralitsa.gogleva@dgkv.com



Anita Dangova

Associate

E: anita.dangova@dgkv.com



Sofia | 10 Tsar Osvoboditel Blvd. | Sofia 1000 | Bulgaria

T: +359 2 932 1100 | F: +359 2 980 3586

Berlin | Schlegelstrasse 29 | 10115 Berlin (Mitte) | Germany

T: +49 30 2758 1561 | F: +49 30 2758 1562

[WEB](#) | [LINKEDIN](#) | [YOUTUBE](#)