Six Highlights MNCs Need to Know about China SCC Route

By Xun Yang | Yuwei Xia

On 24th February 2023, the Cyberspace Administration of China ("**CAC**") released the *Measures on the Standard Contract for Outbound Transfer of Personal Information* (the "**SCC Measure**"), which will become effective on 1 June 2023. A standard contract for outbound transfer of personal information ("**SCC**") is attached to the SCC Measure. The issuance of the SCC Measure indicates the final establishment of the three "legitimate grounds" for outbound transfer of person information, being:

(1) to undergo security assessment organized by CAC (the "**CAC Assessment Route**");

(2) to undergo personal information protection certification by a professional institution (the "**Certification Route**"); and

(3) to enter into a data transfer agreement ("**DTA**") in conformity with SCC with the foreign recipient of personal information (the "**SCC Route**").

This briefing highlights the major issues which MNCs need to pay attention to in relation to the adoption of the SCC Route.

Application of SCC Route

The SCC Route applies to the outbound transfer of personal information by a personal information handler if the volume of personal information to be transferred below the statutory threshold and no important data are involved in the transfer.

Firstly, the SCC Route applies to the outbound transfer of personal information by a personal information handler. Art. 38 of the Personal Information Protection Law ("**PIPL**") provides for "*Where personal information handlers need to provide personal information*

如果您需要本出版物的中文本,
请联系:

Publication@llinkslaw. com

For more Llinks publications, please contact:

Publication@llinkslaw.com

out of the jurisdiction of the People's Republic of China for business or other such requirements, they shall meet one of the following conditions" of which the SCC Route is one. This article suggests that the SCC Route does not apply to outbound transfer of personal information by an engaged processor.

Secondly, the SCC Route applies to outbound transfer of personal information which falls below the statutory threshold. According to Article 4 of the SCC Measure, the SCC Measure applies if the personal information handler (which is not a critical information infrastructure operator) (i) handles personal information about less than 1 million individuals; (ii) since January 1 of last year, transfers outbound accumulatively personal information fewer than 100,000 individuals in total; and (iii) since January 1 of last year, transfers outbound accumulatively sensitive personal information about 10,000 individuals in total. CAC Assessment Route would be required if the volume of personal information exceeds said threshold.

Thirdly, the SCC Route does not apply to outbound transfer of data where important data are involved. According to the *Security Assessment Measure for Data Export*, the outbound transfer of important data requires the data exporter to undergo the CAC Assessment Route. Therefore, the SCC Route does not satisfy the compliance requirement of outbound data transfer where important data are involved. Since no catalogue of important data has been officially released, except for obvious or extreme scenario, it would be difficult for MNCs to determine if the information they wish to export contain important data. A consultation with the relevant regulator is usually helpful.

Performance of PIA

The SCC Route appears to be simplest way to form the legitimate ground to outbound transfer of personal information. However, it is much more than entering into a DTA consistent with SCC.

According to Article 55 of PIPL, personal information handlers must perform personal information protection impact assessment in advance of, among others, outbound transfer of personal information. Article 5 of the SCC Route also provides that "*Prior to providing personal information outbound, a personal information handler must perform a personal information protection impact assessment.*" In other words, a personal information protection impact assessment is required if an MNC adopts the SCC Route.

This requirement is similar to the privacy impact assessment requirement in Europe developed from the decision made by the European Court of Justice in Schrems II case where additional due diligence is required vis-à-vis data protection environment and level where the data recipient is located. The personal information protection assessment under the SCC Measure appears to be more comprehensive. It requires due diligence on all segments on outbound transfer of personal information and, based on the due diligence, assess the legitimacy, justifiability and necessity of the outbound transfer as well as the risks arising from such transfer.

Filing of SCC

A DTA is a private contract but it needs to be filed with the local cyberspace administration at the provincial level (the "**Local CAC**"). According to Article 7 of the SCC Measure, "*a personal information handler must, within 10* *business days after the standard contract becomes effective, file the standard contract with the local cyberspace administration at the provincial level for records."* The documents which are required to be submitted for filing includes the signed DTA (SCC) and the personal information protection impact assessment report. The filing requirements suggest that the adoption of the SCC Route is not only a private matter and government is involved. It remains uncertain as to how close the Local CAC will look into the signed DTA (SCC) and the personal information protection impact assessment reports.

Deviation from SCC

When adopting the SCC Route, a personal information handler must sign a DTA with the overseas recipient in strict conformity with the SCC attached to the SCC Measure except that they parties may add additional clauses which are not inconsistent with the SCC.

According to Article 6 of the SCC Measure, the DTA must be concluded in strict conformity with the template SCC attached to the SCC Measure, which the national cyberspace administration may adjust the Annex in light of the actual circumstances. The personal information handlers may agree on additional clauses with overseas recipients, which clauses must not conflict with the SCC. This article indicates: (i) all clauses in the SCC must be included in the DTA and no deviation can be made on them; (ii) CAC has the authority to amend the SCC from time to time, which suggest that the parties need to make sure that the DTA they sign retain the flexibility to be adjusted according to CAC's amendment to the SCC; and (iii) the parties may add more clauses to the extent that these clauses are not conflicting with the SCC.

This suggests that when adopting the SCC Route, MNCs would need to develop their DTA from the SCC but not their global template used for GDPR regions or elsewhere.

Dispute Resolution

It is worth noting that, according to Section 2 of Article 9 of the SCC, a DTA must be governed by the PRC law. Section 4 of Article 9 of the SCC further provides that disputes arising from the construction or performance of DTA can be resolved, at the election by the parties, either by a PRC court or an arbitration institution recognized under the New York Convention provided that, if an arbitration is selected to the dispute resolution measure, only institutional arbitration (not ad hoc arbitration) is allowed.

This means that MNCs may need to have DTAs specifically for China outbound transfers which are governed by the PRC law whilst other outbound personal information transfers governed by a foreign law.

Implementation of SCC Route

The SCC Measure provides for a six-month grace period to rectify existing outbound personal information transfers.

According to Article 13 of the SCC Measure, outbound transfers of personal information carried out before the effective date of the SCC Measure (which is 1 June 2023), in noncompliance with the provisions of the SCC Measure, must be rectified within six months as of the effectiveness of the SCC Measure. In other words, it leaves about 9 months for MNCs to rectify the noncompliance. As such, we suggest that MNCs consider the following:

(1) to streamline their outbound data flows and to assess the legitimacy, justifiability and necessity of these data flows;

(2) to perform personal information protection impact assessment on outbound transfers of personal information; and

(3) to review and amend their existing DTAs to ensure the consistency with the SCC.

If you would like to know more information about the subjects covered in this publication, please contact:

Xun Yang
+86 21 3135 8799
xun.yang@llinkslaw.com

SHANGHAI

19F, ONE LUJIAZUI
68 Yin Cheng Road Middle
Shanghai 200120 P.R.China
T: +86 21 3135 8666
F: +86 21 3135 8600

BEIJING

30F, Central Tower, China Overseas Plaza, 8 Guanghuadongli,
Chaoyang District
Beijing 100020 P.R.China
T: +86 10 5081 3888
F: +86 10 5081 3866

SHENZHEN

18F, China Resources Tower
2666 Keyuan South Road,
Nanshan District
Shenzhen 518063 P.R.China
T: +86 755 3391 7666
F: +86 755 3391 7668

HONG KONG

Room 3201, 32/F, Alexandra House
18 Chater Road
Central, Hong Kong
T: +852 2592 1978
F: +852 2868 0883

LONDON

1/F, 3 More London Riverside
London SE1 2RE
United Kingdom
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

www.llinkslaw.com

Wechat: LlinksLaw

WE LINK LOCAL LEGAL INTELLIGENCE WITH THE WORLD