New GDPR Standard Contractual Clauses – the impact on businesses in Mainland China and Hong Kong

September 2021

The impact of Schrems II continues

There has been much uncertainty about cross-border data transfers following the much publicised *Schrems II*[1] decision in the Court of Justice of the European Union ("**CJEU**") on 16 July 2020. In order to satisfy their safeguard obligations under Article 46(1) of the General Data Protection Regulation ("**GDPR**"), some businesses have chosen to implement the European Commission's ("**the Commission**") pre-approved standard contractual clauses into their agreements. To add to the changing landscape, these standard contractual clauses are also being updated.

What are the new changes?

On 4 June 2021, the Commission published two sets of new standard contractual clauses ("**New SCCs**"):

- New SCCs to govern data transfer from the European Union ("**EU**") to third countries ("**Third Country SCCs**")[2], which are to replace the existing standard contractual clauses ("**Old SCCs**"). The New SCCs have been updated to reflect the changing regulatory landscape, including the recent *Schrems II* decision.
- New SCCs to govern the data transfer between controllers and processors (whether data will be transferred out of the EU) pursuant to Article 28 of GDPR ("**Article 28 SCCs**")[3]. Unlike the Third Country SCCs, Article 28 SCCs are optional. Yet, Article 28 SCCs may serve as a benchmark for companies to evaluate whether there are appropriate technical and organisational measures which govern the processing.

For the purposes of this article, we will focus on the compulsory changes which are likely to have the biggest impact in Mainland China and Hong Kong: The Third Country SCCs.

How does this impact me in Mainland China and Hong Kong?

The application of GDPR extends to companies in Mainland China and Hong Kong which collect and process personal data relating to the offering of goods or services to individuals and/or monitoring of behaviours of individuals in the EU. Mainland China and Hong Kong companies with a connection to the EU (e.g. having branch offices, employees, a business presence or business dealings in the EU) are subject to data protection obligations which are wider than those under the Personal Data (Privacy) Ordinance of Hong Kong (Cap 486) (the "**PDPO**") and in some instances differ to those under the new China Personal Information Protection Law ("**PIPL**") and other Mainland China related laws and regulations.

Further, there are contractual considerations for Mainland China and Hong Kong companies. Numerous Mainland China and Hong Kong companies process data on behalf of corporate customers in the EU. Under the GDPR, EU corporate customers are required to protect the data they have collected, including during transfer.

[1] CURIA - Documents (europa.eu)
[2] EUR-Lex - 32021D0914 - EN - EUR-Lex (europa.eu)
[3] EUR-Lex - 32021D0915 - EN - EUR-Lex (europa.eu)

pwc

A key element of this process is contractual protection. As Hong Kong and Mainland China are not deemed to have an adequate level of protection under the GDPR, EU data exporters must rely on alternative transfer mechanisms and safeguards provided in Article 46 of the GDPR. Standard contractual clauses are often a preferred method to demonstrate adequate protection[4].

This reliance on standard contractual clauses is only likely to increase in Mainland China and Hong Kong, due to the new PIPL. Under Article 38 of the PIPL, one of the conditions available for cross-border data transfer is entering into a standard contract formulated by the Cyberspace Administration of China ("**CAC**"). According to public information, the CAC is in the process of drafting the standard contract used for cross-border data transfer, but there is not a clear timeline when such standard contract will be finalised and ready to use. Whilst we wait further guidance from the CAC, global companies will hope these are compatible with the New SCCs going forward. It would be important to keep close watch on further development in this regard.

What are the highlights of the New SCCs?

"One single entry-point" – The New SCCs cover a broad range of transfer scenarios, replacing the separate sets of clauses adopted under the old SCCs which only captured two transfer scenarios (i.e. controller-to-controller and controller-to-processor transfers). The New SCCs combine the general clauses with the four modules set out below. Parties can add and remove clauses depending on the nature of the transfer.

"Modular approach" – The New SCCs effectively consolidate all four sets of clauses for each type of transfer (i.e., controller-to-controller, controller-to-processor, processor-to-processor and processor-to-controller) into one document, allowing more than two parties to join and use the clauses.

"Practical toolbox" – The New SCCs address the concerns raised in the *Schrems II* judgment, including the requirement to assess the laws of the third countries and implement any necessary supplementary measures; and provide an overview of the steps businesses have to take to comply with the judgment.

What should businesses in Mainland China and Hong Kong do?

Many EU data exporters to Mainland China and Hong Kong have relied on the Old SCCs as a means of complying with the GDPR and the cross-border data transfers. Given the potential extent of the obligations, businesses should start to understand the changes, communicate with counterparties and negotiate contracts to ensure timely adoption of the New SCCs. We recommend that businesses should consider taking the following next steps:

1. Assess data transfer arrangements

EU data exporters and Mainland China and Hong Kong data importers will need to start identifying all relevant data transfer arrangements by considering the following questions:

- Does any of your existing contracts rely on the Old SCCs?
- Does any of these agreements continue beyond 27 December 2022?
- Are the security arrangements sufficiently robust (see point (3) below)?

The answers to these questions will enable you to understand which contracts need to be remediated.

For new transfer arrangements, businesses will need to assess data flows and update templates to incorporate the New SCCs.

2. Conduct a transfer impact assessment

The New SCCs also require both parties to warrant they have carried out an assessment of the local laws in the jurisdiction to which the data is to be transferred and determine whether such local laws could prevent the data importer from fulfilling the obligations in the New SCCs. For Mainland China and Hong Kong importers, this will include an assessment of the protection offered by local laws, such as the PDPO, the PIPL, the China Data Security Law and the China Cybersecurity Law, and whether any laws may pose a risk to the data being transferred (e.g. local surveillance laws).

The situation for data importers is tricky because contractual clauses do not bind national authorities. In Mainland China and Hong Kong and elsewhere, data importers must balance their contractual obligations to EU data exporters with the local law requirements and satisfy themselves that they can comply with both.

[4] Article 46(2)(c) of GDPR

3. Consider supplementary measures

Businesses may need to supplement the New SCCs with additional security measures as suggested in the European Data Protection Board's ("**EDPB**") recommendations on supplementary measures 01/2020[5] to ensure compliance with the level of protection required under EU law, for example, encryption, pseudonymisation or split processing before transmission. These recommendations were recently adopted on 21 June 2021.

What is the timeline for these changes?

The Old SCCs were repealed on 27 September 2021.

Contracts concluded before 27 September 2021 using the Old SCCs could be deemed to have satisfied the safeguard requirement under Article 46 of GDPR until 27 December 2022.

For contracts executed after 27 September 2021, the New SCCs must be used.

All existing contracts need to be updated to the New SCCs by 27 December 2022.

How we can help

Our Data Privacy and Cybersecurity Team in Mainland China and Hong Kong includes privacy lawyers, operational specialists, RegTech consultants and project managers. We can help you understand more about the New SSCs and the related compliance measures. We can advise on transfer impact assessments and on your obligations under the standard contract clauses. Examples of how we can assist include:

Technology:

We have developed an AI tool to help you understand your existing data transfer contracts, which can help you address the questions raised above.

The AI Contract Review Tool empowers your legal compliance and contract management team by:

- Applying AI technologies to perform automated compliance regulation checking on contracts by the contract clause comparison engine with predefined standard data privacy and security rules.
- Performing full scan on contracts to auto-compare privacy clauses and analyse the level of compliance of the contract.
- Identifying non-compliant contract clauses, missing key phrases and contracts expiring beyond 27 December 2022, allowing us to provide recommendations to manage risks and enhance compliance.

By adopting the AI tool, your organisation can reduce the manual effort required for contract review and improve review accuracy and efficiency.

Global legal support:

The PwC global legal services network connects the expertise of over 3,700 legal professionals in nearly 100 territories, bringing the right combination of legal insight, business understanding and technological innovation. In Mainland China and Hong Kong, Tiang & Partners is an independent Hong Kong law firm with a close working relationship with PwC. Beijing Rui Bai Law Firm and Shanghai Xin Bai Law Firm are independent China law firms and members of the PwC global network of firms. Through this collaboration, Tiang & Partners, Rui Bai Law Firm and Xin Bai Law Firm can help you undertake the required impact assessment(s) and understand the local laws which may affect your ability to import and export data, as well as advise on additional measures and/or contractual obligations.

Cyber security:

We have over 350+ cybersecurity experts to advise your organisation on data security best practices (including measures recently circulated by the EDPB) to implement security by design solutions as early as possible in the system design and development processes. Examples of data transfer security design elements include access control management, secure data encryption, pseudonymisation using hashing, business continuity planning, security monitoring and controls, as well as data security incident response and management.

[5] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data | European Data Protection Board (europa.eu)

Let's talk

For a deeper discussion of how this impacts your business, please contact:

Barbara Li
Head of Corporate
TMT and Data Practice Lead
Rui Bai Law Firm
Tel: +86 10 8540 4686
barbara.xb.li@ruibailaw.com

Kenneth Wong
Cybersecurity and Privacy Leader
Risk Assurance
PwC Mainland China/Hong Kong
Tel: +852 2289 2719
kenneth.ks.wong@hk.pwc.com

Chiang Ling Li
Partner
Tiang & Partners
Tel: +852 2833 4938
chiang.ling.li@tiangandpartners.com

Lisa Li
Partner
PwC Mainland China
Tel: +86 10 6533 2312
lisa.ra.li@cn.pwc.com

Chris Cartmell
Counsel
Tiang & Partners
Tel: +852 2833 4913
chris.c.cartmell@tiangandpartners.com

Chun Yin Cheung
Partner
PwC Mainland China
Tel: +86 21 2323 3927
chun.yin.cheung@cn.pwc.com

Kris Fan
Counsel
Xin Bai Law Firm
Tel: +86 21 5368 4009
kris.fan@xinbailaw.com

Chris Mo
Partner
PwC Hong Kong
Tel: +852 2289 2941
chris.yw.mo@hk.pwc.com

www.pwchk.com
www.ruibailaw.com
www.xinbailaw.com
www.tiangandpartners.com

pwc

瑞栢律师事务所
Rui Bai Law Firm

信栢律师事务所
Xin Bai Law Firm

Tiang & Partners
程偉賓律師事務所