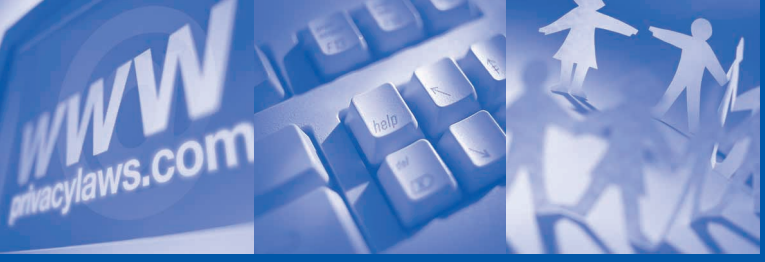

ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

China's new Standard Contract for international transfers

Yan Luo, **Xuezi Dan**, and **Vicky Liu** of Covington & Burling LLP explain what is required of an Overseas Recipient when the Measures take effect on 1 June.

On 24 February 2023, the Cyberspace Administration of China (CAC) released the final version of the *Measures on the Standard Contract for the Cross-border Transfer of Personal Information* (Measures), including a template contract (Standard Contract) accompanying the Measures. The Measures will take effect on 1 June 2023, but are subject to a six-month grace period to allow

Continued on p.3

Will the EU-US Data Privacy Framework end the saga around transatlantic data flows?

David Dumont and **Tiago Cabral** of Hunton Andrews Kurth LLP comment on the EU Commission draft adequacy decision, and reactions by other EU institutions.

On 13 December 2022, the European Commission officially initiated the process for adoption of an adequacy decision regarding the new EU-US Data Privacy Framework (DPF Adequacy Decision). The draft DPF Adequacy Decision marks the third

Continued on p.5

Issue 182 **APRIL 2023**

COMMENT
2 - EU-US adequacy decision is expected by summer

NEWS
13 - The future of DPA enforcement

ANALYSIS
1 - EU-US Data Privacy Framework
8 - Korea's closer to EU GDPR standards
11 - France: CNIL dismisses application of GDPR to US-based company
18 - Global data privacy 2023

LEGISLATION
1 - China: International transfers contract
15 - Slovenia finally adopts new DP Act

MANAGEMENT
24 - Events Diary

OBITUARY
22 - Dr David Flaherty

NEWS IN BRIEF
14 - China to establish privacy authority
14 - New EU regulation on the cards
17 - US FTC takes enforcement action against healthcare company
17 - Norway extends its Sandbox
24 - The CNIL's priorities for 2023
24 - EDPB: Guidelines on three topics
25 - Coordinated Enforcement Action on the role of DPOs
25 - Tesla adjusts camera privacy settings
26 - Canada: Investigation into TikTok
26 - EU, Singapore digital partnership
26 - Australia's Privacy Act review
26 - EU Parliament Opinion on health data
27 - Italy bans AI chatbot Replika
27 - Iowa passes a privacy statute

INTERNATIONAL report

ISSUE NO 182 APRIL 2023

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

ASIA-PACIFIC EDITOR
Professor Graham Greenleaf
graham@austlii.edu.au

REPORT SUBSCRIPTIONS
K'an Thomas
kan@privacylaws.com

CONTRIBUTORS

Yan Luo, Xuezi Dan, and Vicky Liu
Covington & Burling LLP, US and China

David Dumont and Tiago Cabral
Hunton Andrews Kurth LLP, Belgium

Kwang Bae Park, Hwan Kyoung Ko, Sunghee Chae and Kyung Min Son
Lee & Ko, Korea

Nana Botchorichvili
IDEA Avocats, France

Urša Horvat Kous
Jadek & Pensa, Slovenia

Professor Colin Bennett
University of Victoria, Canada

Published by
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Email: info@privacylaws.com
Website: www.privacylaws.com
Subscriptions: The *Privacy Laws & Business* International Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686
ISSN 2046-844X

comment

EU-US adequacy decision is expected by summer

There are still some procedural hurdles to clear before the EU-US Data Privacy Framework takes effect. It seems unlikely though that the remaining EU DPA reservations would put a stop to this agreement which has been in the making for years (p.1). However, their call for subsequent reviews to take place at least every three years is a sensible step, as well as monitoring how well the redress mechanism works in practice.

It is expected that EU-US Data Privacy Framework will be adopted in the summer of 2023 once the EU Member States have given their approval. While US organisations must self-certify, it is still less stringent than using Standard Contractual Clauses, for example. SCCs have also been developed in China but with important variations from the EU clauses (p.1).

Can we expect a US federal privacy law? In his State of the Union address at the beginning of February, President Joe Biden called for "bipartisan legislation to stop Big Tech from collecting personal data on kids and teenagers online, ban targeted advertising to children, and impose stricter limits on the personal data these companies collect on all of us." In the meantime, the trend of adopting state-level privacy laws continues with Iowa being the recent addition (p.27).

Data Protection Authorities keep enhancing their cooperation globally, both through networks created by law and international agreements, and by more informal arrangements (p.18). An example of the former is the European Data Protection Board which aims to further streamline its cross-border enforcement. The EU Commission is working on how to harmonise some aspects of the administrative procedures which have caused delays, for example in Ireland (p.14).

National level interpretations on what the GDPR means are always a fascinating read. In this issue we bring you a case study from France, where the DPA has ruled that the GDPR did not apply there to the operations of a US-based company (p.11).

I look forward to a discussion on this topic 3-5 July at *Who's Watching Me?* our 36th Annual International Conference in Cambridge, UK, with a EU Commission representative and a Member State national Data Protection Commissioner taking the stage (see p.27 and the conference programme at www.privacylaws.com/plb2023).

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura.linkomies@privacylaws.com.

China... from p.1

companies time to bring their activities into compliance.

Under the Measures, if an in-country personal information processing entity (equivalent to the concept of a "data controller" under the EU's General Data Protection Regulation) needs to adopt the Standard Contract as its lawful transfer mechanism, namely as a "data exporter," this entity is required to submit a filing to the provincial branch of CAC. This filing includes:

1. the signed Standard Contract; and
2. report that includes an impact assessment of personal information protection with respect to the transfer activities (DPIA).

Such a filing has to be made within ten working days from the effective date of the Standard Contract.

To help companies understand how to implement these Standard Contract requirements, this article first offers a high-level overview on the requirements under the Chinese laws and regulations for transferring personal information outside of China. After that, it analyses the obligations imposed under the Standard Contract on both data exporters and Overseas Recipients, with a focus on obligations on an Overseas Recipient. Finally, the article offers some practical suggestions for companies that wish to rely upon the Standard Contract to transfer data.

Background

China's Personal Information Protection Law (PIPL) provides three mechanisms that entities with operations in China may rely upon to transfer personal information out of China:

1. undergo a CAC-administered security assessment;
2. enter into the Standard Contract with the Oversea Recipient; or
3. obtain a certification from a CAC-recognized professional organization.

While all three of these mechanisms are generally available to entities processing personal information under the PIPL, those that transfer "important data," or are designated as Critical Information Infrastructure (CII) operators, or otherwise are processing or transferring certain threshold volumes of personal information, must file for the CAC-administered security assessment.

Thus far, many companies across a range of sectors have filed their security assessment applications with the CAC and the CAC has begun reviewing the applications submitted. By contrast, there have been no reported examples of companies seeking to obtain a certification from a CAC-certified body, as the rules are still evolving on how exactly this will work in practice.

In June 2022, a previous version of the Measures and the Standard Contract was published for public comments. The final version closely tracks the draft version, with a few changes that will be discussed below. With the rules implementing the Standard Contract now finalized, companies that are not required to file a security assessment application can decide to either adopt the Standard Contract or obtain a certification for their cross-border transfers.

Standard Contract Measures and the Template

Unlike the Standard Contractual Clauses (SCCs) of the European Union (EU), which offer four modules to address four different transfer scenarios, China's Standard Contract is limited to transfers from an in-country personal information processing entity to an Overseas Recipient, and do not differentiate the role of the Overseas Recipient (i.e. whether it is a data controller or data processor).

> The notification obligation is triggered in every breach scenario, regardless of the level of risk.

In addition to the filing requirement, the data exporter is subject to various obligations under the Standard Contract itself, such as the obligations to inform data subjects and obtain their separate consent (where applicable) for transferring personal information outside of China; take reasonable efforts to ensure that the Overseas Recipient is able to fulfill its obligations provided under the Standard Contract; respond to requests from Chinese regulators about the relevant processing activities; and carry out a Data Protection Impact Assessment DPIA) and retain the assessment report for at least three years.

At the same time, the Standard Contract imposes a range of obligations on Overseas Recipients that will be elaborated below.

Obligations imposed on Overseas Recipients

Data Security Incident Notification: Distinct from the EU SCCs, under China's Standard Contract, the notification obligation is triggered in every breach scenario, regardless of the level of risk. More specifically, in the event of a data security incident, the Overseas Recipient must promptly adopt appropriate remedial measures and immediately inform the data exporter in China. Further, if required by law, the Overseas Recipient should also notify the Chinese regulator and affected data subjects. While it is clear that if an Oversea Recipient is an entrusted party (equivalent to the concept of "data processor" under GDPR), it does not have the obligation to notify individuals, it is unclear from the text of the Standard Contract whether the Overseas Recipient still has an independent obligation to notify regulators.

Also, the Overseas Recipient is required to record all facts related to the data incident, including the remedial measures that have been taken. However, China's Standard Contract does not further clarify what would be considered relevant facts of a data security incident.

Onward transfers: The Overseas Recipient is not permitted to transfer personal information to third parties located outside of China unless the following requirements are met:

- there are real and legitimate business needs to provide personal information;
- the Overseas Recipient has informed data subjects about the third-party recipient and separate consent has been obtained (where consent is relied upon as the processing basis);

- the Overseas Recipient has entered into a written agreement with the third party to ensure that its processing can meet the level of personal information protection provided under Chinese laws and regulations, and assume liability for infringements of data subject rights caused by such provision; and
- the Overseas Recipient must provide a copy of the agreement to data subjects on request.

The Standard Contract keeps silent as to whether the provision of transferred personal information to authorities in the jurisdiction where the Overseas Recipient is located is governed by the onward transfer requirements listed above. That said, it specifically provides that the Overseas Recipient is required to immediately inform the data exporter if it receives a data request from local authorities.

Provide access to data exporter and cooperate with Chinese regulators: The Overseas Recipient is required to provide to the data exporter the information that is necessary to comply with its obligations under the Standard Contract. The Overseas Recipient must allow the data exporter to review its data files to the extent necessary for audit of its data processing activities.

Further, the Overseas Recipient must cooperate with Chinese regulators in connection with the implementation of the Standard Contract, including, for instance, responding to requests from regulators, facilitating regulators' inspections, complying with decisions made by regulators or providing documented proof (if necessary), and so forth.

Respond to requests from data subjects: Data subjects have the right to directly request the Overseas Recipient to facilitate the exercise of their privacy rights. In addition, when the data exporter is unable to facilitate requests from data subjects, the data exporter is required to ask the Overseas Recipient to provide assistance. The Overseas Recipient must fulfill these obligations within a reasonable period of time.

Record data processing activities: The Overseas Recipient is required to record its data processing activities and retain this record for at least three years. The Standard Contract does not clarify the exact scope of personal information processing activities. The obligation for the Overseas Recipient to keep all processing activities for three years might be burdensome.

Dispute resolution and jurisdiction: Under EU SCCs, in the controller-to-controller scenario, disputes must be resolved by a court of an EU member state, where in the processor-to-controller scenario, parties may choose a court of any jurisdiction. Under China's Standard Contract, the governing law must be Chinese law. However, the parties may choose, as an alternative to a Chinese court and the four Chinese arbitration institutions listed in the Standard Contract, an arbitration institution as long as the venue is located in a New York Convention signatory.

The EU SCC and China's Standard Contract both require the data importer/Overseas Recipient to submit to the competent authority's jurisdiction. China's Standard Contract further specifies the Overseas Recipient must agree to be subject to the supervision of regulators in China, as discussed above.

Practical considerations

The Measures emphasize that companies cannot circumvent the CAC-administered security assessment by simply "segregating" their cross-border transfers so that the total volume of personal information transferred does not reach the statutory threshold. Therefore, companies need to consider carefully when calculating the data volume for the purpose of analyzing whether the CAC-administered security assessment is triggered. As a good practice, companies may want to properly document the self-assessment process and the conclusion based on the self-assessment results.

The Measures explicitly state that no substantive deviation is allowed and only the CAC has the right to adjust the Standard Contract as needed. It is possible for parties to add terms to the agreement in the annex, even though such terms must not conflict with the terms in the main body of the Standard Contract. Thus, the parties of the Standard Contract may consider negotiating and having some additional clauses in the annex to clarify their respective obligations under the Standard Contract, to the extent permissible.

For companies who may be deemed as an Overseas Recipient, it is helpful to consider the contractual obligations imposed by the Standard Contract and be ready to comply with these terms in practice. For example, the Overseas Recipient will have a contractual obligation to respond to Chinese government's requests, cooperate with inspections and so on. Foreign companies need to evaluate the potential implications for their practices and businesses. In addition, as the Measures require the data exporter to complete and file the DPIA report together with the signed contract to CAC, the Overseas Recipient may also be required by the data exporter to provide necessary information and other support to complete the assessment report.

It is noteworthy that the Measures provide more light on how CAC plans to enforce these rules. It states that if and when the CAC discovers major risks involved in a company's transfer activities, or a security incident occurs, it can "summon" the company and ask it to rectify its conduct and eliminate risks. We assume that such exercises will focus on an in-country data exporter at least initially, but CAC's jurisdiction can extend to Overseas Recipients as well.

AUTHORS

Yan Luo is a Partner at Covington & Burling LLP, Beijing/Palo Alto, US, Xuezi Dan, is an Associate in Beijing, Peoples Republic of China, and Vicky Liu is an International Associate also in Beijing.
Emails: yluo@cov.com
xdan@cov.com
yliu@cov.com

Join the Privacy Laws & Business community

The *PL&B International Report*, published six times a year, is the world's longest running international privacy laws publication. It provides comprehensive global news, on 180+ countries alongside legal analysis, management guidance and corporate case studies.

PL&B's International Report will help you to:

Stay informed of data protection legislative developments in 180+ countries.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Find out about future regulatory plans.

Understand laws, regulations, court and administrative decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance and reputation.

Included in your subscription:

1. Six issues published annually

2. Online search by keyword
Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

3. Electronic Version
We will email you the PDF edition which you can also access in online format via the *PL&B* website.

4. Paper version also available
Postal charges apply outside the UK.

5. News Updates
Additional email updates keep you regularly informed of the latest developments in Data Protection and related laws.

6. Back Issues
Access all *PL&B International Report* back issues.

7. Events Documentation
Access events documentation such as *PL&B Annual International Conferences*, in July, Cambridge.

8. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.

privacylaws.com/reports

"The UK and International *PL&B* Reports have been my 'go to' resource for 20 years despite the wide choice of alternate resources now available. And have you tried the Annual Conference at Cambridge? I have seven IAPP certificates so a big IAPP supporter. But the *PL&B* Cambridge event each July, still knocks the spots off IAPP and other conferences!"

Derek A Wynne, SVP Privacy & Chief Privacy Officer, Paysafe Group

UK Report

Privacy Laws & Business also publishes *PL&B UK Report* six times a year, covering the Data Protection Act 2018, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Electronic Communications Regulations 2003.

Stay informed of data protection legislative developments, learn from others' experience through case studies and analysis, and incorporate compliance solutions into your business strategy.

Subscriptions

Subscription licences are available:

- Single use
- Multiple use
- Enterprise basis
- Introductory, two and three years discounted options

Full subscription information is at privacylaws.com/subscribe

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.