

Highlights of Personal Information Export Standard Contract (Draft for Comment)

By David Pan | Susan Deng | Shana Sha

On 30 June 2022, the Cyberspace Administration of China (CAC) released the long-awaited draft of *Personal Information Export Standard Contract (Exposure Draft)* (the “SC Draft”). Deriving from article 38 of the *Personal Information Protection Law* (the “PIPL”), the SC Draft elaborates on one of the three personal information export mechanisms, which is expected to be frequently used by MNCs for data export. This briefing focuses on the application scope and key points of the SC Draft.

1. The last missing piece to the personal information export puzzle

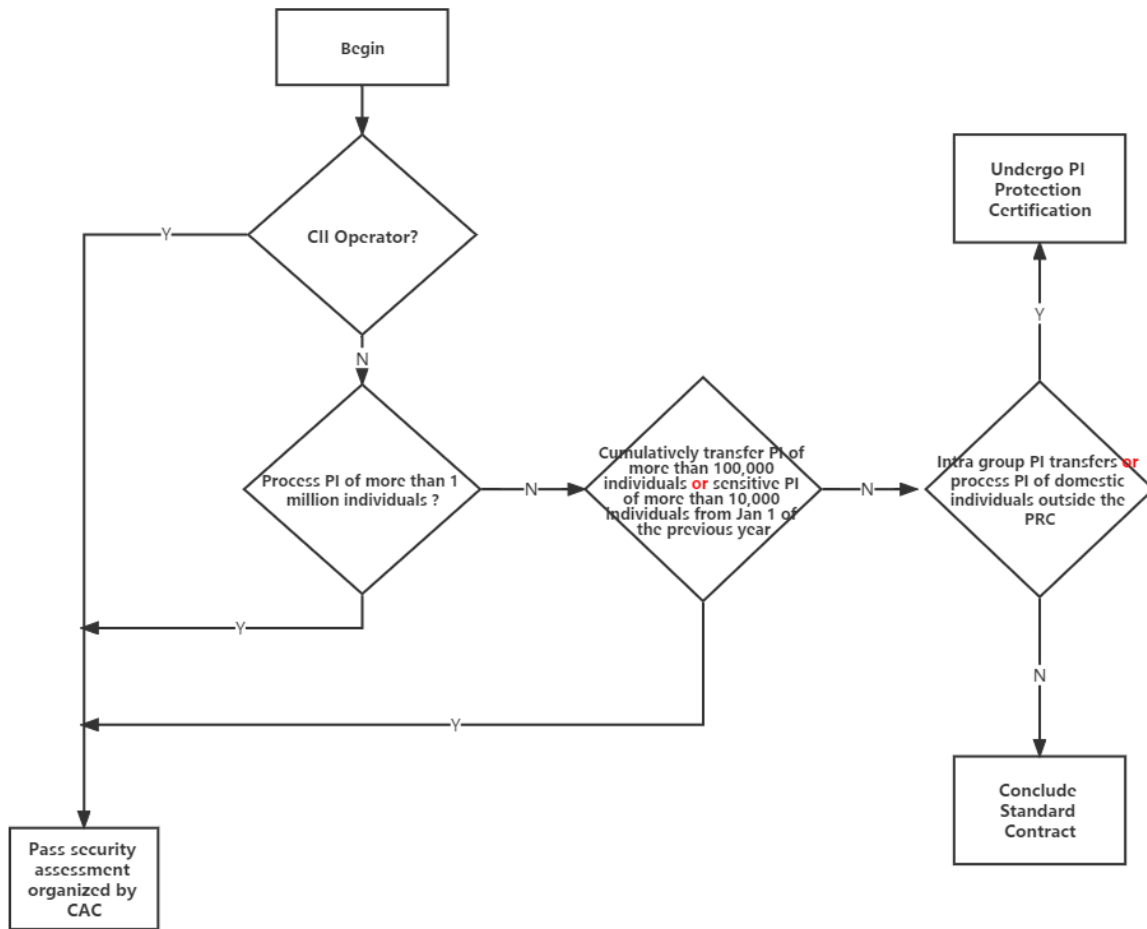
Measures on Data Export Security Assessment (Exposure Draft) (the “Data Export Draft”), *Practice Guidelines for Cyber Security Standards – Technical Specifications for Certification of Cross-Border Processing of Personal Information*, and the SC Draft respectively elaborates on the three mechanisms stipulated by article 38 of the PIPL, which are (1) assessment, (2) certification, and (3) standard contract. Below we prepared a flow chart for identifying which mechanism to apply:

.....
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



2. Scope of application

Consistent with the preconditions and thresholds stipulated in the Data Export Draft, the SC Draft limit the use of Standard Contract to a Personal Information Processor that:

- (1) is not a Critical Information Infrastructure Operator,
- (2) processes personal information of less than 1 million individuals,
- (3) has not exported personal information of more than 100,000 individuals cumulatively since 1 January of the preceding year, and
- (4) has not exported sensitive personal information of more than 10,000 individuals cumulatively since 1 January of the preceding year.

3. Nine clauses

The SC Draft also provides a 16-page and 9-clause Standard Contract Provisions (the “SC Template”). Because the SC Template is not mandatory, companies are allowed to draft their own standard contracts and prepare bilingual versions, as long as they do not contradict the SC Template.

The nine clauses basically reflect the provisions in the PIPL and *Information Security Technology Personal Information Security Specifications*. The key terms include:

Personal Information	The purposes, scope, types, sensitivity, quantity, means, retention period and storage location of personal information to be exported out of China
Personal Information Processor	- The basic information of the PI Processor - The responsibilities and obligations of the PI Processor, and the technical and management measures taken by them to prevent security risks
Overseas Recipient	- The basic information of the overseas recipient - The responsibilities and obligations of the overseas recipient, and the technical and management measures taken by them to prevent security risks - The impact of the personal information protection policies and regulations of the country or region where the overseas recipient is located on compliance with the terms of the SC Template
Personal Information Subject	Personal Information subjects' rights, and the ways and means to protect these rights
Other General Terms	Remedy, termination, liability and dispute resolution

4. Nexus with other data export contracts

Although the SC Draft stipulates that, entities which meet the four conditions may transfer personal information abroad by signing the standard contract, it does not waive the condition of signing data export contracts in other circumstances of personal information export. Entities still must sign data export contracts if they (1) undergo the government-led personal information security assessment; or (2) undergo the personal information protection certification.

Data Export Mechanism	Requirements
Personal Information Security Assessment	The contract concluded between the data processor and the overseas recipient shall fully stipulate the responsibilities and obligations of data security protection.
Personal Information Protection Certification	Relevant parties involved in personal information export must sign legally binding and enforceable documents to ensure that the rights and interests of personal information subjects are fully protected.

5. Calculation of personal information amount

Article 4 of the Data Export Draft stipulates that personal information processors: (1) who process personal information of more than 1 million individuals; or (2) accumulatively provide personal information of more than 100,000 individuals or sensitive personal information of more than 10,000 individuals abroad, need to apply for the government-led security assessment. The Data Export Draft does not specifically explain how

to define “processing 1 million individuals’ personal information”, or how to define “accumulatively”. As a helpful clarification, the SC Draft stipulates in article 4 that “January 1 of the preceding year” should be the starting point for accumulative calculation. This provision narrows down the time range for calculating the number of individuals involved in outbound data, and adopts rolling calculation principle. As a result, if the Data Export Draft does not make amendments or explanations to the calculation mechanism accordingly, it will cause contradiction. For example, if the number of individuals involved in outbound data since January 1 of the preceding year has reached 80,000, and the number of individuals involved in the outbound data since January 1 of the year before the preceding year was 90,000, the company may adopt the standard contract mechanism for data export according to the SC Draft. However, the number of individuals accumulated has reached 170,000, which triggers the threshold for government-led security assessment according to the Data Export Draft. We expect that the formally effective *Personal Information Export Standard Contract* will resolve this contradiction by taking a unified position.

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



David Pan
+86 21 3135 8701
david.pan@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

This publication represents only the opinions of the authors and should not in any way be considered as legal opinions or advice given by Llinks. We expressly disclaim any liability for the consequences of action or non-action based on this publication. All rights reserved.

© Llinks Law Offices 2022