



THE CHINESE DATA PROTECTION LABYRINTH: GUIDELINES FOR LEGAL DATA EXPORT

I. INTRODUCTION

Since the beginning of 2022, a large number of data protection laws have been enacted in China. Since there was initially a lack of necessary concreteness and harmonisation of these laws, their specific scope and significance was difficult to estimate for foreign enterprises in China.

In 2023 and 2024, there has been a large number of legal amendments and significant concretisation in data protection law. As a provisional final accord, the “**Chinese Cyberspace Administration**” last issued the “*Provisions on Promoting and Regulating Cross-border Data Flows*” on 22 March 2024.

The main focus for foreign enterprises under Chinese data protection law is to comply with the requirements for cross-border data transmission. This following newsletter is a guide to determine in what way and to what extent your enterprise is affected by the requirements for cross-border data transmission from China.

Please also find [attached](#) to this newsletter our [evaluation form on the Chinese data protection law](#). You are welcome to send this completed evaluation form to the contact person below. The Schindhelm team in China will then provide you with a free initial assessment of any need for action.

II. WHAT SCENARIOS MUST BE OBSERVED WHEN EXPORTING DATA FROM CHINA ABROAD?

1. The following enterprises must obtain **state approval for data export** within the “**Security Assessment**” framework:

- a. “**critical information infrastructure operators**” within the Regulation “*Rules on Critical Information Infrastructure Security Protection*” that export data abroad;
 - b. enterprises that export so-called “**critical data**” within the Regulation “*Measures on Security Assessments of Cross-border Data Transfers*”;
 - c. enterprises that export the “**personal data**” of 1,000,000 persons (or more) per year;
 - d. enterprises that export the “**sensitive personal data**” of 10,000 persons (or more) per year.
2. The following enterprises must conclude a written Standard Contract for data export with the foreign data recipient:
- a. enterprises that export the “**personal data**” of 100,000 persons (or more), but fewer than 1,000,000 persons per year;
 - b. enterprises that export the “**sensitive personal data**” of fewer than 10,000 persons per year.

If the (sensitive) personal data is exported to a large number of foreign data recipients, the Chinese enterprise may alternatively apply for a one-off **Protection Certification**. With this certification, the data may then be exported without a separate Standard Contract being concluded with all foreign data recipients.



3. In addition, all enterprises in China that collect and process personal data must fulfil the **legal information and disclosure obligations** towards the relevant persons and carry out and document a **data protection risk analysis**.

III. HOW ARE THE EXPORTED DATA AND DATA EXPORTERS CLASSIFIED IN CHINA?

The Regulation “*Rules on Critical Information Infrastructure Security Protection*” define “**critical information infrastructure operators**” as enterprises active in the areas of public communication and information services, energy, transport, water management, finance, public services and national defence. Since direct market entry for foreign enterprises is very limited in these areas, this complex is fundamentally not relevant for foreign enterprises.

“**Critical data**” within the Regulation “*Measures for Security Assessment of Outbound Data Transfers*” include collections and analyses of traffic data, collections and analyses of seller behaviour and collection of geolocation data.

“**Personal data**” within the meaning of the “*Personal Information Protection Law*” is all information that serves to identify a person and is stored in electronic or other form.

“**Sensitive personal data**” within the meaning of the “*Personal Information Protection Law*” is such data that can severely jeopardise personal well-being and property in the wrong hands (e.g. biometric data, religion, disabilities, data concerning health, financial data, place of residence and all personal data of minors under 14 years of age).

IV. UNDER WHAT CONDITION DOES AN EXEMPTION APPLY TO THE STANDARD CONTRACT OR PROTECTION CERTIFICATION?

Under the following conditions, enterprises can waive the execution of the Standard Contract or the Protection Certification:

- a. the export of personal customer information is necessary for the recipient to establish, fulfil and process contractual relationships (e.g. cross-border purchases, cross-border sales, cross-border payments, etc.);
- b. the export of personal employee information is necessary for purposes of implementing cross-border personnel administration;
- c. the export of personal data is necessary to protect the life and health as well as the property of the persons;
- d. the export of personal data (non-sensitive personal data) within one year amounts to fewer than 100,000 persons.



CONTACT

Austria

Philipp Leitner

P.Leitner@saxinger.com

Bulgaria

Cornelia Draganova

Cornelia.Draganova@schindhelm.com

China

Marcel Brinkmann

Marcel.Brinkmann@schindhelm.com

Czech Republic/Slovakia

Monika Wetzlerova

Wetzlerova@saxinger.com

France

Maurice Hartmann

Maurice.Hartmann@schindhelm.com

Germany

Rüdiger Erfurt

Ruediger.Erfurt@schindhelm.com

Hungary

Beatrix Fakó

B.Fako@saxinger.com

Italy

Tommaso Olivieri

Tommaso.Olivieri@schindhelm.com

Poland

Justyna Majchrzak,

Justyna.Majchrzak@sdzlegal.pl

Spain

Unai Mieza

U.Mieza@schindhelm.com

Turkey

Müge Şengönül

Muge.Sengonul@schindhelm.com