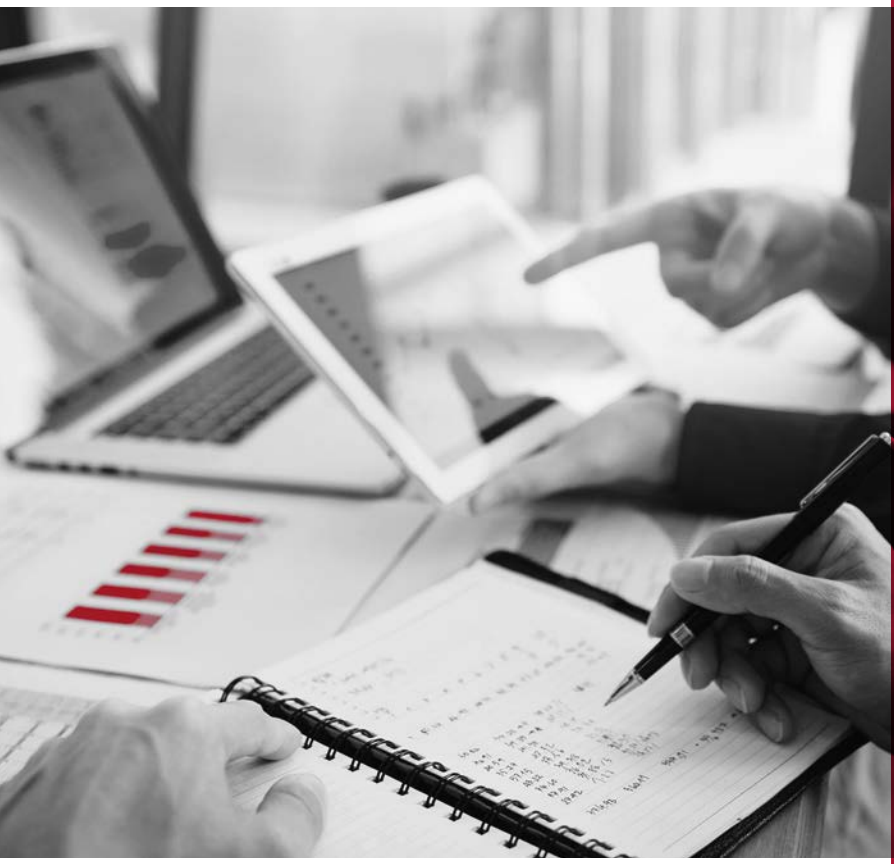
ADVANT Beiten



# CHINA
# DATA SECURITY: ESSENTIAL Q&As

Welcome to our revised April 2024 edition of the China Personal Data Security Essential Q&As! We aim to provide you with key information about China's Personal Data regulatory framework essentials. We do this intentionally in a way which seeks to draw your attention to key issues impacting foreign and domestic enterprises doing business in, or with, China. Hence, what we set out in this publication deals with some of the most common questions and situations brought to our attention. What can make China's personal data security framework challenging is the clattered legislative documentation which can apply based on specific cases and situations. Thus, please read this publication to get a first understanding on how personal data are protected in China and for any specific question, please contact us anytime!

# 1. Is the term “data processor” used uniformly under EU GDPR and Chinese legislation?

No! In Chinese legislation, “data processor” means the party who controls and determines the purpose and method of the data processing (= “data controller“ under GDPR). “Entrusted party” under Chinese legislation means the party processing data on behalf of and at the instruction of the data processor (= “data processor“ under the GDPR). We will use these terms in this publication in the way as they are defined under Chinese legislation.

# 2. What data categories are defined under Chinese legislation?

Chinese legislation distinguishes the following data categories:

**Personal Data** (**PD**) refers (according to the PRC Personal Information Protection Law (**PIPL**) effective since 1 November 2021) to various types of information related to an identified or identifiable natural person that is recorded electronically or otherwise, excluding anonymised information that can identify a specific natural person either alone or in combination with other information, including the natural person’s name, date of birth, residential address, phone number, email address, medical information, location information, etc..

**Sensitive PD** is PD that, once leaked or used illegally, may easily infringe on the personal dignity of natural persons, or endanger personal or property safety, including biometrics, religious beliefs, specific identities, medical health, financial accounts, whereabouts tracking and other data, as well as all PD of minors under the age of 14. Appendix B “Determination of Sensitive PD“ of the **PD Security Specification**[1] provides a non-exhaustive list of Sensitive PD as follows:

[1] The “Information Security Technology-PD Security Specification“ (信息安全技术 个人信息安全规范 GB/T 35273-2020) (PD Security Specification) specifies rules for implementing PD protection and processing, PD categories and requirements for PD transfers.

| | |
|---|---|
| **Personal Property Information** | Bank account, identification information (passwords), deposit information (including the amount of funds, payment and collection records, etc.), real estate information, credit records, credit information, transaction and consumption records, flow records, etc., as well as virtual currency, virtual transactions, game redemption codes and other virtual property information |
| **Personal Health Physiological Information** | Personal records related to illness and treatment, such as symptoms, hospital records, doctor's orders, inspection reports, surgery and anesthesia records, nursing records, medication records, drug and food allergy information, fertility information, previous medical history, diagnosis and treatment, family medical history, current medical history, history of infectious diseases, etc. |
| **Personal Biometric Information** | Personal genes, fingerprints, voiceprints, palmprints, auricles, irises, facial recognition features, etc. |
| **Information of Personal Identification** | ID card, military ID card, passport, driver's license, work permit, social security card, residence permit, etc. |
| **Other Private Information** | Sexual orientation, marriage history, religious beliefs, unpublished criminal records, communication records and content, address book, friend list, group list, whereabouts, web browsing records, accommodation information, precise positioning information, etc. |

**Important Data** are data important for the economic and social development and that may endanger national security, economic operation, social stability, public health and safety, etc. once they are tampered with, destroyed, leaked, or illegally obtained or used. Government agencies define catalogue(s) of various sorts of Important Data based on their respective regions and sectors and from the perspectives of national security, economic operation, social stability, public health and safety. Data that are only important or sensitive to an organisation itself should not be considered Important Data. Data that are not defined by any government agencies as Important Data are generally not considered to be Important Data.

**National Core Data** are a class of data subject to stricter regulations than (Sensitive) PD and Important Data due to their relevance for national security, national economy, citizen's livelihoods, and important public interests, etc. Data that are not defined by any government agencies as National Core Data are generally not considered to fall in such category.

# 3. What is considered "data processing" under Chinese legislation?

The PRC Data Security Law (**DSL**), effective since 1 September 2021, PIPL and DSL define data processing as the collection, storage, use, transmission, provision, disclosure, and deletion of data (including PD). Hence, from a PRC legal perspective hosting (storing) data alone is already considered as data processing activity. If one accesses data stored and hosted in China from abroad, this qualifies as "data processing in China" provided it involves any of the afore mentioned activities related to data handling.

# 4. Do I need to obtain consent from an individual if I want to process its PD?

Generally yes! Any PD processing requires consent by the data subject and such consent shall be given in an informed, specific, voluntary and revocable manner. For the processing of Sensitive PD and for any outbound data transfer of any PD, separate consents shall be obtained and for outbound data transfers these consents must encompass the overseas PD data recipient's name and contact information, the purpose/method of PD handling, the types of PD processed, the methods/procedures for data subjects to exercise data privacy rights towards overseas data processors/entrusted parties.

In the following circumstances however, no consent from the data subject is required[2]:

- the data processing/transfer is necessary for the conclusion/performance of a contract with the data subject, or for the implementation of HR management measures pursuant to lawful company rules or collective contracts;
- the data processing is necessary for the performance of statutory duties/obligations;
- the data processing is necessary to respond to public health emergencies, or to protect the data subject's life, health and property in an emergency situation;
- reasonably disclosures in news reporting, public opinion supervision or other acts serving public interest;

[2] The "Guidelines for Security Assessment of Data Export (Second Edition)" (数据出境安全评估申报指南（第二版）) require that if an application for CAC Security Assessment involves separate consent, supporting documents must also be provided even if it meets the mentioned exemptions.

- reasonable voluntary disclosure by the data subject or other reasonable lawful disclosures;

- other circumstances defined under applicable Chinese legislation.

Where required, consents must be given in a tangible form, e.g. electronically, in written form, etc. They must be given in Chinese language and can be additionally given in other languages, whereby in a China domestic context, in general the Chinese version will prevail. The details to be covered in any such consents and related data privacy policies are in particular defined in the "Information Security Technology Standard – PD Security Specification" (《信息安全技术 个人信息安全规范》GB/T 35273-2020, "**PD Security Specification**"), effective since 1 October 2020, accessible here: https://openstd.samr.gov.cn/bzgk/gb/newGbInfo?hcno=4568F276E0F8346EB0FBA097AA0CE05E.

# 5. What is a CIIO?

CIIOs are operators of "critical information infrastructures (**CII**, 关键信息基础设施)", a term broadly defined under CSL as any information infrastructure which if destroyed, disabled, or leaks data may seriously endanger national security, national welfare or the public interest as CII. According to the CII Regulations[3], CIIs refer to public communication and information services, power, traffic, water, finance, public services, electronic governance, the national defense technology industry and other important industries and sectors, as well as other important network facilities and information systems for which the destruction, loss of function, or data leakage might seriously endanger national security, national welfare and the people's livelihood, or the public interest. In practice, the government will notify a company if it is a CIIO. Before being notified, the company may generally be safe to assume it is not a CIIO.

# 6. What is considered "outbound data transfer"?

Outbound (i.e. cross-border) data transfers/exports from China to abroad are governed in detail under the Outbound Data Transfer Security Assessment Measures《数据出境安全评估办法》which here issued on 7 July 2022 and are effective as of 1 September 2022

[3] Matters pertaining to the protection of critical information infrastructure and cybersecurity are provided in the "Regulations on Critical Information Infrastructure Security Protections" (关键信息基础设施安全保护条例) (**CII Regulations**), effective since 1 September 2021.

(**Outbound Assessment Measures**). Although the Outbound Assessment Measures themselves do not define what constitutes "outbound data transfers", the Cyberspace Administration of China (**CAC**) clarified in a Q&A and the Outbound Data Transfer Security Assessment Declaration Guide (Second Edition)/数据出境安全评估申报指南（第二版）that "outbound data transfers" include e.g. the following scenarios:

- data processors transfer to or store outside China data collected and generated during operations within China;

- data collected and generated by data processors are stored within China but can be accessed or used by natural/legal persons from outside China for data processing (–> remote access from outside China of data stored within China constitutes outbound data transfer);

- data processing outside China that involves PD of natural persons located within China

Data transfers from China to the SAR Hong Kong, SAR Macao and/or the Region of Taiwan are considered as outbound data transfers and must comply with all related regulatory requirements.

# 7. Can PD be freely transferred from the PRC to abroad?

No, regulatory restrictions exist concerning the transfer of PD from China to abroad. China established the main regulatory framework for outbound data transfers with the enactment of PIPL, PRC Cyber Security Law (**CSL**), effective since 1 June 2017 and DSL. Under this regulatory framework, data transferors need to meet one of the following requirements (which one depends on the nature and volume of the data to be transferred) before exporting data out of China:

- passing the CAC security assessment (**CAC Security Assessment**, see below Sec. 11 for details);

- signing and filing the standard CAC contract (**Standard Contract Filing**, see below Sec. 10 for details);

- obtaining PD protection certification from qualified institutions (**Protection Certification**).

The three above measures are hereinafter referred to as "**Data Transfer Clearance Procedures**", for exemptions from the necessity to undergo these Data Transfer Clearance Procedures, please refer to Sec. 8 below.

## 8. Are there exemptions from the Data Transfer Clearance Procedures?

Yes! In the years of 2022 and 2023, CAC introduced several measures to guide the implementation for the Data Transfer Clearance Procedures. Still, it was quickly felt that such framework caused severe bottlenecks and extreme workload for companies and authorities alike. Therefore, the need for exemptions from the Data Transfer Clearance Procedures became evident. This issue was addressed with the "Provisions on Regulating and Promoting the Cross-border Flow of Data" ("**Exemption Regulations**")[4]. While the export of Important Data always requires CAC Security Assessment, exports of data is exempted from the Data Transfer Clearance Procedures in the following cases:

- Data Transit: PD collected/generated overseas is routed through China for processing and then exported without involving Important Data or PD;

- Necessity in Contracts with Natural Persons: there is a legitimate need to export PD in the performance of contracts to which natural persons are a party (e.g. cross-border e-commerce & logistics, payments, bank account openings, travel reservations, visa processing, examination services, etc.);

- Lawful cross-border HR Management: PD is exported for cross-border HR management according to lawfully implemented company policies and/or collective contracts;

- Emergencies: PD exports are necessary to protect life, health and property of natural persons;

- Negligible PD Volumes for Non-CIIOs: PD of less than 100,000 data subjects is exported by one data processor within one calendar year (this exemption does not apply in case of Sensitive PD, Important Data and other qualified data categories and does generally not apply to CIIOs: CIIOs always must pass CAC Security Assessments for any data exports);

[4] Provisions on Promoting and Regulating Cross-border Flow of Data (《促进和规范数据跨境流动规定》), issued by the CAC, effective as of 22 March 2024.

- General data: data collected and generated in activities such as international trade, cross-border transportation, academic cooperation, cross-border manufacturing and marketing, as long as no form of PD or Important Data is involved.

Further, the Exemption Regulations allow PRC Free Trade Zones (**FTZs**) to promulgate individual "*negative lists*" to formulate exemptions from the Data Transfer Clearance Procedures. Such negative lists shall be approved by the provincial-level Network Security and Informatisation Committees and must then be registered with CAC and other in-charge authorities before being implemented. The exemptions granted under such negative lists apply only to entities registered in the given FTZ. Whether they would only apply to data generated, collected and stored within such FTZ or not lacks clear guidance at this stage and this further monitoring is advised to ensure compliance.

# 9. Do I have to localise all my data in China?

No! Chinese legislation does not require that all data but only certain data are localised in China. Whether data localisation requirements exist depends (a) on whether the data processor is e.g. a CIIO and (b) on the nature/amount of data and data subjects involved. Data localisation requirements apply e.g. in the following cases:

- for National Core Data & Important Data;
- for PD collected/generated in China by a CIIO;
- for PD collected/generated in China by any data processor under the volume thresholds prescribed by CAC.

Besides legal considerations also practical aspects may warrant local hosting of data. Some platforms used outside China for data hosting (Google, Microsoft, Facebook, to name a few) are not accessible in China (except with VPN access, which on a larger domestic scale is not used in China). Any form of IoT services that requires authentication schemes via social login require an access scheme that can be downloaded from App stores commonly used in China. Thus, even if legally speaking no data localisation requirement applies, practically speaking there may still be technical/operational reasons which may make a local hosting solution desirable or even necessary.

## 10. When can/need I conduct the Standard Contract Filing?

That depends: As said above, there are generally three Data Transfer Clearance Procedures available if one wants to transfer data from China to abroad:

- CAC Security Assessment (this is considered the "hardest" of the three options);
- Standard Contract Filing (this is considered the "easiest" of the three options);
- Protection Certification.

Data processors not mandatorily subject to the CAC Security Assessment (see below Sec. 11 for details) can choose which of the Data Transfer Clearance Procedures they apply. Standard Contract Filing or Protection Certification can be applied e.g. for:

- PD transfers of more than 100,000 individuals but fewer than 1 million individuals (excluding Sensitive PD) since 1 January of the current year;
- Sensitive PD transfers of fewer than 10,000 individuals since 1 January of the current year.

PD transfers involving fewer than 100,000 individuals since 1 January of the current year will not require Standard Contract Filing / Protection Certification until that threshold is exceeded.

CAC has issued a Chinese language standard contract for that purpose that can be downloaded under https://www.cac.gov.cn/2023-02/24/c_1678884830036813.htm.

If you require an English reference translation thereof, please send an email request to beijing@advant-beiten.com.

## 11. When is CAC Security Assessment mandatory?

CAC Security Assessment is mandatory in the following cases of outbound data transfers:

- transfer of Important Data;

- transfer of any amount of PD by CIIOs;
- transfer of PD of ≥ 1 million individuals or since 1 January of the current year;
- transfer of Sensitive PD of ≥ 10,000 individuals since 1 January of the current year;
- other scenarios stipulated in Chinese legislation.

Exemptions to these rules are granted where transfers of PD are necessary for HR management or where such transfer is necessary for the conclusion/performance of a contract with an individual. Data transfers for these purposes will not count towards the above volume thresholds. These exemptions will relieve a data exporter from the obligation to undergo CAC Security Assessment, undergo Standard Contract Filing or obtain Protection Certification even if the cumulative volume in a year exceeds the 1 million individuals' PD (CAC Security Assessment), 10,000 individuals' Sensitive PD (CAC Security Assessment) or < 100,000 individuals' PD (Standard Contract Filing), provided that the only data being transferred is within any of the exempted categories.

## 12. What aspects does a CAC Security Assessment comprise?

A CAC Security Assessment shall address the following aspects:

- the legality, propriety and necessity of the outbound transfer's purpose scope and method;
- the data protection laws and regulations of the overseas data recipient's jurisdiction, the security of the data being transferred, and whether the protections provided by the data recipient satisfy Chinese legislation and standards;
- the scale, scope, type and sensitivity of the data being transferred and the risk of data tampering, damage, leakage, loss, transfer or illegal acquirement and usage during or after outbound data transfer;
- whether the data security and interests of the transferred data can be adequately and effectively protected;
- whether the legal documents adequately allocate responsibilities for data protection compliance with Chinese legislation; the content of these legal documents shall stipulate provisions regarding data processing beyond the agreed storage time, re-

transfer of data by the overseas data recipient, substantial changes in the data recipient's actual control and/or business scope, changes in data security policies and network security environment at the data recipient's location, emergency response requirements in case of data breaches, etc.;

- other matters that are deemed necessary by CAC.

The following factors would be favourable reviewed by CAC in the context of deciding whether a mandatory CAC data security assessment can be passed or not:

- information on internationally recognised security certifications, experiences and track records on data processing and protection, adequacy of the organisational structure and internal control measures (e.g., independent audit reports) of the data processors in China and abroad;

- reliable and trusted encryption and security protocols to ensure the security of the data transferred abroad (note: in China these must be commercial encryption products recognised by the China State Cryptography Administration);

- risk mitigation measures such as aggregation and pseudonymisation of data prior to the transfer abroad;

- application of robust data protection policies offered to data subjects granting all legal rights to data subjects in an efficient, understandable and comprehensive manner;

- viable, advanced and well documented emergency response plans for potential data breaches.

If the data processor passes CAC Security Assessment, the outbound data transfers can then be implemented in accordance with the documents filed by the data processor with CAC. CAC Security Assessments remain valid for three years and can be re-applied at latest 60 working days prior to expiry. Further three-year extensions of the same data transfers can thus be sought without undergoing a further complete CAC Security Assessment. If material relevant aspects change during any such validity period, a new application must be done.

If the data processors fails CAC Security Assessment, it may not conduct the outbound data transfer but it can file an application for re-assessment with CAC within 15 working days upon receipt of the rejection.

# 13. When do I need to appoint a data security officer in China?

PIPL requires PD processors to designate PD protection officers (人信息保护负责人). In any of the following circumstances such position must be full-time:

- the main business of the PD processor involves data processing and it has over 200 employees;
- the actual/expected number of data subjects whose PD is processed reaches 1 million or more during any 12 months period;
- Sensitive PD of 100,000 or more data subjects is processed.

PD processors residing outside China and processing PD of PRC data subjects shall designate a representative or agency within China for data security matters related to PD protection of PRC data subjects.

CSL requires network operators not only to formulate internal security management systems and operating procedures but also to appoint data security officers (网络安全负责人). CIIOs must in addition appoint safety management officers (安全管理负责人).

DSL requires data processors of Important Data to designate data security officers (数据安全负责人) and management bodies for data security.

# 14. Does Chinese legislation on data security have extraterritorial reach?

Yes, among others e.g. DSL and PIPL have an extraterritorial reach because they do not only apply to data processing activities within China but also to those outside China if the data processing may harm the legal interests of Chinese nationals and/or entities.

# Contacts

**Susanne Rademacher**
Rechtsanwältin | Partner
**ADVANT Beiten**
Susanne.Rademacher@advant-beiten.com

**Dr Jenna Wang-Metzner**
Juristin | Partner
**ADVANT Beiten**
Jenna.Wang@advant-beiten.com

**Lelu Li**
Rechtsanwältin | Partner
**ADVANT Beiten**
Lelu.Li@advant-beiten.com

**Kelly Tang**
Juristin | LL.B. | LL.M.
**ADVANT Beiten**
Kelly.Tang@advant-beiten.com

**ADVANT Beiten** in Beijing
Suite 3130 | 31st Floor
South Office Tower
Beijing Kerry Centre
1 Guang Hua Road
Chao Yang District
100020 Beijing, China
T: +86 10 85298110
www.advant-beiten.com

# Our offices


**BEIJING**
Suite 3130 | 31st floor
South Office Tower
Beijing Kerry Centre
1 Guang Hua Road
Chao Yang District
100020 Beijing, China
beijing@advant-beiten.com
T: +86 10 85298110

**BERLIN**
Luetzowplatz 10
10785 Berlin
Germany
berlin@advant-beiten.com
T: +49 30 26471-0

**BRUSSELS**
Avenue Louise 489
1050 Brussels
Belgium
brussels@advant-beiten.com
T: +32 2 6390000

**DUSSELDORF**
Cecilienallee 7
40474 Dusseldorf
PO Box 30 02 64
40402 Dusseldorf
Germany
dusseldorf@advant-beiten.com
T: +49 211 518989-0

**FRANKFURT**
Mainzer Landstrasse 36
60325 Frankfurt/Main
Germany
frankfurt@advant-beiten.com
T: +49 69 756095-0

**FREIBURG**
Heinrich-von-Stephan-Strasse 25
79100 Freiburg im Breisgau
Germany
freiburg@advant-beiten.com
T: +49 761 150984-0

**HAMBURG**
Neuer Wall 72
20354 Hamburg
Germany
hamburg@advant-beiten.com
T: +49 40 688745-0

**MOSCOW**
Turchaninov Per. 6/2
119034 Moscow
Russia
moscow@advant-beiten.com
T: +7 495 2329635

**MUNICH**
Ganghoferstrasse 33
80339 Munich
PO Box 20 03 35
80003 Munich
Germany
munich@advant-beiten.com
T: +49 89 35065-0



Imprint
This publication is issued
by BEITEN BURKHARDT Rechtsanwaltsgesellschaft mbH
Ganghoferstrasse 33, 80339 Munich, Germany
Registered under HR B 155350 at the Regional Court Munich/
VAT Reg. No.: DE811218811
For more information see:
https://www.advant-beiten.com/en/imprint

EDITOR IN CHARGE:
Susanne Rademacher



ADVANT member firm offices:
BEIJING | BERLIN | BRUSSELS | DUSSELDORF
FRANKFURT | FREIBURG | GENOA | HAMBURG | LONDON
MILAN | MOSCOW | MUNICH | PARIS | ROME | SHANGHAI

**advant-beiten.com**


04/2024