ADVANT Beiten

CHINA PERSONAL DATA SECURITY: ESSENTIAL Q&As

Welcome to our new ADVANT Beiten edition of the China Personal Data Security Essential Q&As! With this publication, we aim to provide you with key information about China's Personal Data regulatory framework essentials and to explain some of its core principles. 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, Chinese legislation – such as certain EU laws – uses the terms "data processor" and "data controller" but under Chinese legislation the meaning of these terms differs from EU laws as follows: "Data processor" under Chinese legislation means the party who controls and determines the purpose and method of the data processing (i.e. "data controller" under the GDPR and various other data protection laws). "Entrusted party" under Chinese legislation means the party processing data on behalf of and at the instruction of the data processor (i.e. "data processor" under the GDPR and various other data protection laws). **We will use these terms in this publication in the way as they are defined under Chinese legislation, so please bear that in mind when digesting the information contained herein**.

2. What data categories are defined under Chinese legislation?

Chinese legislation distinguishes the following data categories, whereby the nature/categorization makes a difference in the level of regulatory requirements to be followed:

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 anonymized 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:

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 shall develop catalogue(s) of various grades 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

[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

that are only important or sensitive to an organization itself should not be considered 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.

3. What is considered "Data Processing" under Chinese legislation?

The PRC Data Security Law (**DSL**), effective since 1 September 2021, governs all data processing activities (irrespective of data categories) and 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.

4. What is considered "Outbound Data Transfer" under Chinese legislation?

Outbound (i.e. cross-border) data transfers 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 (**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 that "outbound data transfers" include e.g. the following two 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

Hence, also remote access from outside China of data stored within China for data processing constitutes outbound data transfers.

The Outbound Assessment Measures provide for a retroactive application for cross-border data transfers that have been carried out before 1 September 2022: if such transfers do not comply with the Outbound Assessment Measures, the rectification should be completed within 6 months as of 1 September 2022 (**hence latest by 28 February 2023**).

Data transfers (including transfer of PD) 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 under Chinese legislation.

5. If I access data stored and hosted in China from abroad, does this qualify as "Data Processing in China" under Chinese legislation?

Yes, if such data access involves any of the following activities, it is considered data processing in China: collection, storage, use, transmission, provision, disclosure and deletion of data (including PD).

6. When do I (not) need to obtain consent from a data subject concerning the processing of its PD according to Chinese legislation?

Generally, any PD processing requires consent by the data subject and such consent shall be given in an informed, specific, voluntary and revocable manner.

In addition, for the processing of Sensitive PD and for any outbound data transfer of any PD, separate consents shall be obtained by the data processor.

According to PIPL in the following exceptional circumstances a PD processor does not need to obtain consent from a data subject for processing of its PD:

- the data processing is necessary for the conclusion/performance of a contract with the data subject, or for the implementation of human resources management measures pursuant to legitimate PRC labour rules and regulations and/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
- purpose of news reporting, public opinion supervision or other acts conducted in public interest (all within reasonable scope)
- the processed PD has been voluntarily disclosed by the data subject or has been otherwise lawfully disclosed within a reasonable scope in accordance with PIPL
- other circumstances defined under applicable Chinese legislation

7. What content/form must such consents have according to Chinese legislation?

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, which can be accessed here: https://openstd.samr.gov.cn/bzgk/gb/newGbInfo?hcno=4568F276E0F8346EB0FBA097AA0CE05E

8. Can PD be freely transferred from the PRC to abroad under Chinese legislation?

No, regulatory restrictions exist concerning the transfer of PD from China to abroad.

PIPL allows the transfer of PD to organizations outside the PRC due to "business or other needs", provided the data processor has obtained the data subject's consent prior to the cross-border PD transfer and having informed the data subject regarding

- overseas PD data recipient's name and contact information
- purpose/method of PD handling
- types of PD processed
- methods/procedures for data subject to exercise its data privacy rights to-ward the overseas data processor/entrusted party

PIPL also provides that data processors shall satisfy one of the following conditions prior to such outbound data transfer:

- pass the CAC data security assessment (see Q&A No. 18 for details).
- obtain "PD protection certification" from CAC certified organizations
- enter into the CAC standardized data transfer agreement with the overseas data recipient (see Q&A Nos. 12 – 14 for details).
- comply with further requirements as set forth by CAC if and as applicable

PIPL also stipulates various data management, security, audit and risk assessment requirements, which require the setup of a holistic data security management system. These measures shall ensure that PD is protected throughout the whole lifecycle from unauthorized access, deletion, leakage, tampering or theft and include but are not limited to:

- IT compliance policies/procedures
- data classification system
- IT security such as encryption and de-identification
- IT training to key personnel
- emergency response plan for IT-security incidents

- designation of a data protection officer
- other measures as required by laws and regulations

The data processor must take all necessary measures to ensure that the activities of overseas data recipient meet the PD protection standards stipulated in the Chinese legislation. CAC can blacklist overseas data recipients if these engage in data processing infringing upon the PD protection rights of PRC citizens, or the PRC's public interest/ national security.

9. Does Chinese legislation mandate data localization in any case or only in certain cases?

Chinese legislation does not in all but in increasingly more situations require that data are localized in China. Matters pertaining to localization requirements and cross-border transfer of data are among others governed under PIPL and the PRC Cyber Security Law (**CSL**), effective since 1 June 2017.

Whether a data localization requirement exists in the PRC depends (a) on whether the data processor would qualify as a CIIO (see Q&A No. 10 for details) in China and/or (b) on the nature and amount of data subjects involved.

A data localization requirement under PIPL applies in the following cases:

- PD is collected and generated in the PRC by a CIIO, or
- PD is collected and generated in the PRC by a data processor who is not a CIIO but who reaches or exceeds the volume thresholds prescribed by CAC (see Q&A No. 15 for details)

Where a data localization requirement exists, such data can still be (also) transferred abroad if it is genuinely necessary to be provided to outside China. In such case the data processor in China must pass the CAC data security assessment, unless CAC rules that in a given case such assessment is not compulsory (see Q&A Nos. 15 – 18 for details).

Besides PIPL, CSL requires a localization of PD and Important Data processed by CIIOs.

Note: Besides legal considerations also practical aspects may warrant local hosting of data. E.g. 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). Also, any form of IoT services that requires authentication schemes via social login and that should be practically workable in China would in actuality require an access scheme that can be downloaded from App stores commonly used in China (e.g. Huawei App Market, Tencent My App, Oppo Software Store, VIVO App Store, 360 Mobile Assistant, MIUI App Store, Baidu Mobile Assistant, Samsung App Store, PP Assistant, Wandoujia, etc.). Thus, even if legally speaking no mandatory data localization requirement applies for a given case, practically speaking there may still be technical/operational reasons which may make a local hosting solution desirable or even necessary.

10. What is a CIIO under Chinese legislation?

A CIIO is the operator of a "critical information infrastructure (**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[2], 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.

11. Does Chinese legislation require to only enter into a Data Transfer Agreement if I transfer PD from China to abroad?

PIPL stipulates three different options for compliant outbound data transfers:

- pass the CAC data security assessment (see Q&A No. 18 for details),
- obtain "PD protection certification" from CAC certified organizations
- enter into the CAC standardized Data Transfer Agreement with the overseas data recipient (see Q&A Nos. 12 – 14 for details)

[2] 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.

Data processors not subject to mandatory CAC data security assessment (see Q&A No. 15 – 8 for details) can choose which of the three above options to follow and thus act in compliance with Chinese legislation if they only enter into a Data Transfer agreement.

Data processors subject to mandatory CAC data security assessment however cannot opt out of such assessment by only signing a Data Transfer Agreement and/or "PD protection certification" from CAC certified organizations.

12. If I enter into a Data Transfer Agreement, which minimum content must it have according to Chinese legislation?

CAC has issued a Chinese language standard contract for that purpose that can be downloaded under http://www.cac.gov.cn/2022-06/30/c_1658205969531631.htm

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

13. Do I have to register/record such Data Transfer Agreement with CAC and if yes, is this a condition precedent to the effectiveness of the Agreement?

According to the "Provisions for the Standard Contract for Outbound Transfer of Personal Data (Draft) (个人信息出境标准合同规定（征求意见稿）)" which were published on 30 June 2022 for public comment, PD processors are required to register the Data Transfer Agreement within 10 working days as of its effective date with the in-charge local CAC department if such provisions would be effectively promulgated.

According thereto, registration/recordal of these data transfer agreements with CAC would not be a condition precedent for the effectiveness of such agreements. However, in cases where a CAC data security assessment is legally required, the data transfer contract should ideally state that it only become effective as of passing the CAC data security assessment.

14. Must the Data Transfer Agreement be written in Chinese language?

Yes, it must be written at least in Chinese language but can also be written additionally in another language and both language versions can be made legally binding.

15. When is it mandatory to conduct a CAC Data Security Assessment under Chinese legislation?

According to the Outbound Assessment Measures a data processor must conduct a CAC Data Security Assessment for cross-border data transfers with the locally in-charge CAC department in any of the following circumstances of outbound data transfers:

- transfers of Important Data
- data transfers by CIIOs
- data transfers of PD of 1 million data subjects or more
- data transfers of PD of 100,000 individuals or more since 1 January of any given previous year
- data transfers of Sensitive PD of 10,000 individuals or more since 1 January of any given previous year
- other scenarios stipulated in Chinese legislation

16. Is there are difference between a Data Security Self-Assessment and a CAC Data Security Assessment under Chinese legislation?

Yes, these two assessments are different, and a data security self-assessment is required as a step before filing a CAC data security assessment.

Also, while according to the Outbound Assessment Measures, the data security self-assessment is only intended as a step before the filing for mandatory CAC data security assessment, a data security self-assessment (impact assessment) may still be needed

under scenarios not covered by the Outbound Assessment Measures if other pieces of Chinese legislation require such self-assessment. E.g. according to PIPL, a PD protection impact assessment must be conducted before any cross-border PD transfer, even if such transfer does not fall under any of the categories requiring a CAC data security assessment under the Outbound Assessment Measures.

17. What does a Data Security Self-Assessment under Chinese legislation comprise?

A data processor subject to a CAC security assessment filing also firstly conduct a data security self-assessment that addresses the following aspects[3]:

- the legality, propriety and necessity of the proposed outbound data transfer and processing conducted by the data recipient outside China; there is no clear definition of what constitutes "necessity" in the above sense but from a generally business-needs-test perspective this could probably be established if the outbound data transfer is necessary because the business / commercial goal cannot be reasonably completed without the cross-border data transfer or because the data subjects request to transfer their data overseas
- the scale, scope, type and sensitivity of the data to be transferred, and the potential risks to national security, public interests and the legitimate interests of individual and entities
- responsibilities undertaken by overseas data recipient and whether relevant management and technical measures implemented by the overseas data recipient will ensure the security of the data to be transferred abroad
- the risk of data tampering, damage, leakage, loss, transfer or illegal acquirement and usage during or after the outbound data transfer, and whether individuals may easily defend their rights
- whether the data transfer agreement or other legally binding documents adequately allocate the relevant responsibilities for data protection by the parties
- other matters that may affect the security of outbound data transfer

[3] Besides the Outbound Data Transfer Security Assessment Measures, see for details: Information Security Technology – Guidance for Personal Information Security Impact Assessment (信息安全技术 个人信息安全影响评估指南 GB/T 39335-2020), providing basic principles and implementation procedures for PD security assessment

18. What does a CAC Data Security Assessment under Chinese legislation comprise?

After the data security self-assessment, the data processor must submit the following materials to the locally in-charge CAC for filing of the CAC security assessment and CAC would focus in particular on the following aspects in carrying out such assessment:

- 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 favorable reviewed by CAC in the context of deciding whether a mandatory CAC data security assessment can be passed or not:

- information on internationally recognized security certifications, experiences and track records on data processing and protection, adequacy of the organizational 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 recognized by the China State Cryptography Administration)
- risk mitigation measures such as aggregation and pseudonymization 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

The locally in-charge CAC will conduct a first check of the application (to be completed within 5 working days as of acceptance of the application by CAC) and then submit compliant filings for further checking to the State-level CAC who shall decide whether or not to accept the filing within 7 working days. CAC will reject filings for outbound data transfers which are not within the scope of mandatory CAC data security assessment. In such a case of rejection because of an 'out of scope' application, the data processor in China can then implement the outbound data transfer based on either entering into a CAC standardized data transfer agreement with the overseas data recipient or based on obtaining the "PD protection certification" from CAC certified organizations. Hence, in cases where a data processor is not sure whether a CAC data security assessment is mandatory or not, filing such an application can be considered to obtain certainty on that question.

If CAC accepts the filing, it will instruct CAC certified organizations to conduct the security assessment which shall be completed within 45 working days after the CAC sends the acceptance notice to the data processor (such period can be extended if necessary).

If the data processor passes the CAC data security assessment, the outbound data transfers can then be implemented in accordance with the documents filed by the data processor with CAC. If however the data processors fails the CAC data 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 notice.

Once granted, the CAC data security assessment result remains valid for two years and can be re-applied for latest 60 working days prior to its expiry.

If material aspects of the application change during the validity period, a re-filing for security assessment must be carried out by the data processor.

19. Does Chinese legislation on data security have extraterritorial reach and if so, when?

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.

20. When do I need to appoint a data security officer in China according to Chinese legislation?

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.

PIPL requires that PD processors must designate PD protection officers (人信息保护负责人) and according to the PD Security Specification, in any of the following circumstances such position must be full-time:

- the main business of the PD processor involves data processing, and the number of employees exceeds 200
- the actual or 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

Also, a PD processor 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.

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

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 | HAMBURG | LONDON | MILAN
MOSCOW | MUNICH | PARIS | ROME | SHANGHAI

advant-beiten.com

08/2022