Update Data Protection in China

September 21, 2023 Dr. Thomas Pattloch, LL.M.Eur

TaylorWessing

1 Data processing and export

TaylorWessing

Measures for the Security Assessment of Outbound Data Transfers

- In force since 1 September 2022, issued by CAC
- Stipulates when and how an application for a security assessment by authorities is required, including
  - outbound transfer of important data by a data processor,
  - outbound transfer of personal information by a critical information infrastructure operator or a personal information processor who has processed the personal information of more than 1,000,000 persons,
  - outbound transfer of personal information by a personal information processor who has made outbound transfers of the personal information of 100,000 persons cumulatively or the sensitive personal information of 10,000 persons cumulatively since 1 January of the previous year.
- Measures also require the data processor to conduct a **self-assessment of the risks in the outbound data transfer** before applying for the security assessment of an outbound data transfer, and identify issues
- **Responsibilities and obligations must be clearly stipulated in a contract** executed with the overseas recipient
- Transferor must reapply for the security assessment where the security of outbound data transfer may be affected

Further departmental regulations

- Guide to Applications for Security Assessment of Outbound Data Transfers (First Edition), issued on 31 August 2022
- Announcement of the State Administration for Market Regulation and the Cyberspace Administration of China on Carrying out Certification for Data Security Management, promulgated on and in force since 6 June 2022

Measures for the Standard Contract for Outbound Cross-Border Transfer of Personal Information

- Issued by the CAC on 22 February 2023, in force since 1 June 2023
- Includes attachment Standard Contract for Outbound Cross-Border Transfer of Personal Information
- Additionally issued on 30 May 2023: Guidelines for Filing the Standard Contract for Outbound Cross-Border Transfer of Personal Information (First Edition)
- Deadline for meeting compliance through conclusion and registration of Standard Contract **until the end of November 30, 2023** (Art. 13 Measures for the Standard Contract for Outbound Cross-border Transfer of Personal Information)

2 Standard Contract

TaylorWessing

Standard Contract

- Measures Standard Contract in force now, sanctions in case of non-compliance based on PIPL
- Standard Contract as main justification basis for export of personal information, Art. 38 PIPL
- According to Article 4, the SCCs may be used as a legal basis for a domestic company to transmit personal information outside of China, if the following preconditions apply:

  (1) not a critical information infrastructure operator;

  (2) handling personal information of less than one million individuals;

  (3) having provided personal information of less than 100,000 individuals in aggregate to overseas recipients since January 1 of the previous year; and

  (4) having provided sensitive personal information of less than 10,000 individuals in aggregate to any overseas recipients since January 1 of the previous year.

  Where it is otherwise provided in any law or administrative regulations, or by the national cyberspace authority, those provisions shall prevail.
- Open questions as regards who is the “recipient” and who outside of China must conclude the Standard Contract with the data exporter

Art. 55 PIPL and Art. 5 Measures Standard Contract

The Measures repeat the statutory requirement for a Personal Information Impact Assessment under Article 55 of the PIPL before personal information is transmitted out of China, which shall include:

- the legitimacy, justifiability, and necessity of the personal information processing by both the personal information exporter and the foreign personal information recipients (e.g. purpose, scope, and method);
- the quantity, scope, category, and sensitivity of personal information to be exported, and respective risks;
- the responsibilities and obligations that foreign recipients have committed to, and their management/technical competence to perform their commitments and ensure personal information security;
- the risk of leakage, sabotage, alteration, and abuse of personal information if exported, and the availability of remedies for data subjects;
- the impact of data protection laws and policies in the jurisdiction of foreign recipients on the performance of the SCCs; and
- other factors jeopardising PI security.

According to the Measures, a PIA report shall be completed three months prior to registration with CAC and kept for at least three years. The SC shall be filed with CAC within ten days of its effectiveness.

Must apply Chinese law.

Supplementation or new SC required

New SC shall be concluded and filed again if:

1) there is any change in the purpose, scope, type, sensitivity, quantity, method, retention period, and storage location of the personal information transferred overseas, or any change in the purpose and method of the personal information processing of the overseas recipient, or an extension of the overseas retention period of the personal information;

(2) there is any change in personal information protection policies and regulations in the country or region where the overseas recipient is located, which may affect personal information rights and interests; or

(3) other circumstances that may affect personal information rights and interests.

3 Data classification

The scope of application of the Data Security Law, Art. 2 and 3 DSL

- DSL applies to all data processing activities conducted in China and related security supervision of such. Data processing is defined under the law to mean collection, storage, use processing, transmission, provision or disclosure of data.
- “Data” under the DSL includes not only electronic data, but also other data such as hardcopies, paper files etc.
- If data processing activities conducted outside China harm (i) China's national security; (ii) China's public interests, or (iii) the legitimate rights and interests of Chinese citizens or organizations, they will also be subject to the Data Security Law.
- As a result, according to Art. 27 DSL data processing on networks or over the Internet lead to
  (1) Obligation to establish and perfect a data security management system across the entire workflow;
  (2) Those conducting data processing by using the Internet or other information networks shall, **based on the graded cybersecurity protection system**, perform the data security obligations under the DSL;
  (3) Failure to comply with requirements of Art. 27 DSL leads to sanctions in accordance with Art. 45 DSL, i.e. corrections, warnings, fine between CNY 50,000 and 500,000 for an organisation and additionally a fine for the directly responsible officers and other persons in the amount of CNY 10,000 to CNY 100,000. In case of refusal of correction or major data leak, fine will increase to CNY 500,000 to 2 million, suspension of business/stopping of operation, revocation of business license and increased personal liability of responsible officer and other persons of CNY 50,000 to CNY 200,000.

DSL: Protection of core data and important data

- Art. 21 DSL refers also to a “classified and graded data protection system”, and stipulates that the “national data security coordination mechanism shall make overall planning for and coordinate relevant departments in formulating the catalogues for important data”.
  - **Each region and department shall, in accordance with classified and graded data protection system, determine the specific catalogue for important data** for the respective region and department, in relevant industries and areas, and undertake special protection for the data included in the catalogue
    - Meaning there is **not one definition in law of “important data”, but a multitude of (ministerial and other) catalogues** which may be amended, supplemented and interpreted differently over time
    - Draft standard Information Security Technology – Guidelines for Important Data Identification are added, but not yet in force and likely to be further amended
  - **Art. 21 DSL further defines “core data of the State”** as data that have a bearing on national security, the lifelines of national economy, people’s key livelihood and major public interests, which “shall be subject to stricter management system”

Important data

- Draft Circular CAC Regulations on Network Data Security Management promulgated on 14 November 2021 contained in its Art. 73 a generic definition of “important data”:
  - 3. “Important Data” means data, the tampering with, or sabotage, leakage, illegal acquisition or illegal use of which, if it happens, may cause harm to national security or the public interest, including the following data:
  - (1) government affairs-related data that have not been disclosed, official work-related secrets, intelligence data, and law enforcement or judicial data;
  - (2) export control data, data related to the core technology, design, production process or any such information involved in an **export control item, data on any scientific and technological advances in encryption, biology, electronic information, artificial intelligence** or any other field that has a direct impact on national security or economic competitiveness;
  - (3) **data on national economic performance, business data of an important industry, statistical data** and other data that are expressly required to be protected and controlled from dissemination by any national law, administrative regulations or departmental rules;
  - (4) **data on the production or operation safety in the industrial, telecommunications, energy, transportation, water resources, finance, national defense technology industry, customs, tax or any other key sector or field, data on any critical system component or the supply chain of any critical equipment**;
  - (5) **national basic data on the population and health or natural resources and environment**, such as **genetic, geographical, mineral, and meteorological data that reach the threshold amount or degree of precision** prescribed by the relevant state authority;
  - (6) data on the development or operation of national infrastructure or critical information infrastructure or its security data, data on the geographic location or security condition or other data of a national defense facility, military administration zone, national defense research or production unit or any other important sensitive area; and
  - (7) other data that may impact the nation’s security such as political, territorial, military, economic, cultural, social, scientific and technological, ecological, resource, nuclear facility, overseas interest, biological, space, polar or maritime security.

MIIT Circular Measures for Data Security Management 8 Dec. 2022

- Circular MIIT Issuing the Measures for Data Security Management in the Industrial and Information Technology Sector (for Trial Implementation), effective as of 1 January 2023
- Classification requirements and definition of criteria for determination of important and core data included
- Article 10 Data in respect of which the extent of harm meets any of the following conditions shall be deemed as important data:

  1. posing a threat to politics, land, military affairs, the economy, culture, society, science and technology, electromagnetics, network, ecology, resources, nuclear security, etc., and affecting overseas interests, biology, space, polar regions, deep sea, artificial intelligence, and other key fields related to national security;

  2. causing a serious impact on the development, production, operation, and economic interests in the industrial and information technology sector;

  3. causing any major data security incident or work safety accident, seriously affecting public interests or the legitimate rights and interests of individuals or organizations, and having great negative social impact;

  4. causing obvious cascade effects, involving multiple industries, regions, or multiple enterprises in the industry, or having a long duration of impact, causing a serious impact on industry development, technological progress, industrial ecology, and so on; and

  5. any other important data as assessed and determined by the Ministry of Industry and Information Technology.

MIIT Circular – definition of “Core Data”

Article 11 Data in respect of which the extent of harm meets any of the following conditions shall be deemed as core data:

1. posing a serious threat to politics, land, military affairs, the economy, culture, society, science and technology, electromagnetics, network, ecology, resources, nuclear security, etc., and seriously affecting overseas interests, biology, space, polar regions, deep sea, artificial intelligence, and other key fields related to national security;

2. having a significant impact on the industrial and information technology sector and its important backbone enterprises, critical information infrastructures, important resources, and so on;

3. causing material damage to industrial production and operation, telecommunications networks and internet operation services, radio business development, etc., and resulting in large-scale work stoppages and production shutdowns, radio business interruptions, network and service paralysis, loss of large-scale business processing capacity, etc.; and

4. any other core data assessed and determined by the Ministry of Industry and Information Technology.

Important data

- “Important data” inter alia leads to
  - (1) stricter requirements in terms of security measures,
  - (2) mandatory designation of a person in charge of data security and set-up of security department;
  - (3) periodic and regular risk assessments of data processing activities and regular reporting of assessment results to authorities,
  - (4) mandatory localization of data;
  - (5) export being conditional and requiring export security assessment by CAC with annual reports on safety of transfer and filing of such reports with local authorities,
  - (6) mandatory contractual agreements with recipient of data.
- Export in breach of the Cybersecurity Law (Art. 37 CSL) and other administrative provision of CAC (e.g. Measures for Security Assessment of Cross-border Data Transfer (Draft for Comment) issued 29 October 2021) leads to **sanctions of correction, warning, fine of CNY 100,000 to CNY 1 million plus fine for directly responsible officers and other persons between CNY 10,000 and CNY 100,000**. In serious circumstances (not defined) fine between CNY 1 million and CNY 10 million, order to suspend business, revocation of business license and direct liability of CNY 100,000 to CNY 1 million for directly responsible officers and other persons.
- Lack of cooperation with security organs carries similar sanctions, Art. 36,36 and 48 DSL

Further administrative regulations regulating different types of data and industries

- Several new types of data added in administrative regulations, e.g. “**network data**”, “**public data**” in Draft Circular CAC Regulations on Network Data Security Management promulgated on 14 November 2021, “**industrial data**” in Art. 2 of the MIIT Circular on Issuing the Guide to Classification and Grading of Industrial Data of 27 February 2020
- Measures for Cybersecurity Review, promulgated on 28 December 2021, applying to Critical Information Infrastructure Operators “CIIO” and data processing activities by a network platform operator, stipulating establishment of a national cybersecurity review mechanism (targeting inter alia companies listing abroad or exporting more than 1 million user’s personal data abroad)
- Specific industry rules, such as:
  - MIIT Circular on Strengthening the Network Security and Data Security of the Internet of Vehicles 15 Sept 2021
  - MIIT Circular Issuing the Guide to Classification and Grading of Industrial Data 27 February 2020
  - Several Provisions on Automobile Data Security Management (for Trial Implementation) Oct. 1, 2021
  - GB/T 39725 - 2020 Information Security Technology - Guide for Health Data Security
- Standards for data classification: Network Security Standards Practicing Guidelines - Network Data Classification and Grading Guidelines, issued December 2021 ("**Data Classification Guidelines**")
  - Three levels of data: General data, important data, core data
  - Important data and core data are mainly determined through national and industry data catalogues

Data classification under the DSL - Principles

- Data classification under the DSL – principles under the Data Classification Guidelines:
  - Data classification based on „**multiple dimensions**“ such as individual/public/data to be disseminated/industry-specific data/organizational data which can be „sub-divided“.
  - **Clear gradation and implementation of measures**: Different protective measures for different categories and the respective classification level of data.
  - If a dataset contains **multiple levels of data**, it should be classified according to the highest level of data in the dataset. For example, if a data set contains core data, important data, and general data, that data set should be classified at the core data level.
  - **Timely adjustment**: the classification and grading of data are subject to change and should be adjusted in a timely manner when circumstances change, such as changes in relevant guidelines or the occurrence of certain safety events.
  - When classifying network data, a **data processor should first consider whether the data is core or important data based on national and industry standards**. If there is no reference to it in the national or industry standards, the data processor can analyze the degree of impact if the data is tampered with, destroyed, leaked, unlawfully obtained or used, and decide whether the data is core data or important data based on the existing standards and regulations for identifying core data or important data. If the **data is a data set, the data processor should follow the principle of "subject to the highest level in classification."**

Minimum classification levels

- The minimum reference levels for specific general data:

(1) No less than level 4 for sensitive personal information and no less than level 2 for general personal information.

(2) Personal information of employees within the organization is not less than level 2.

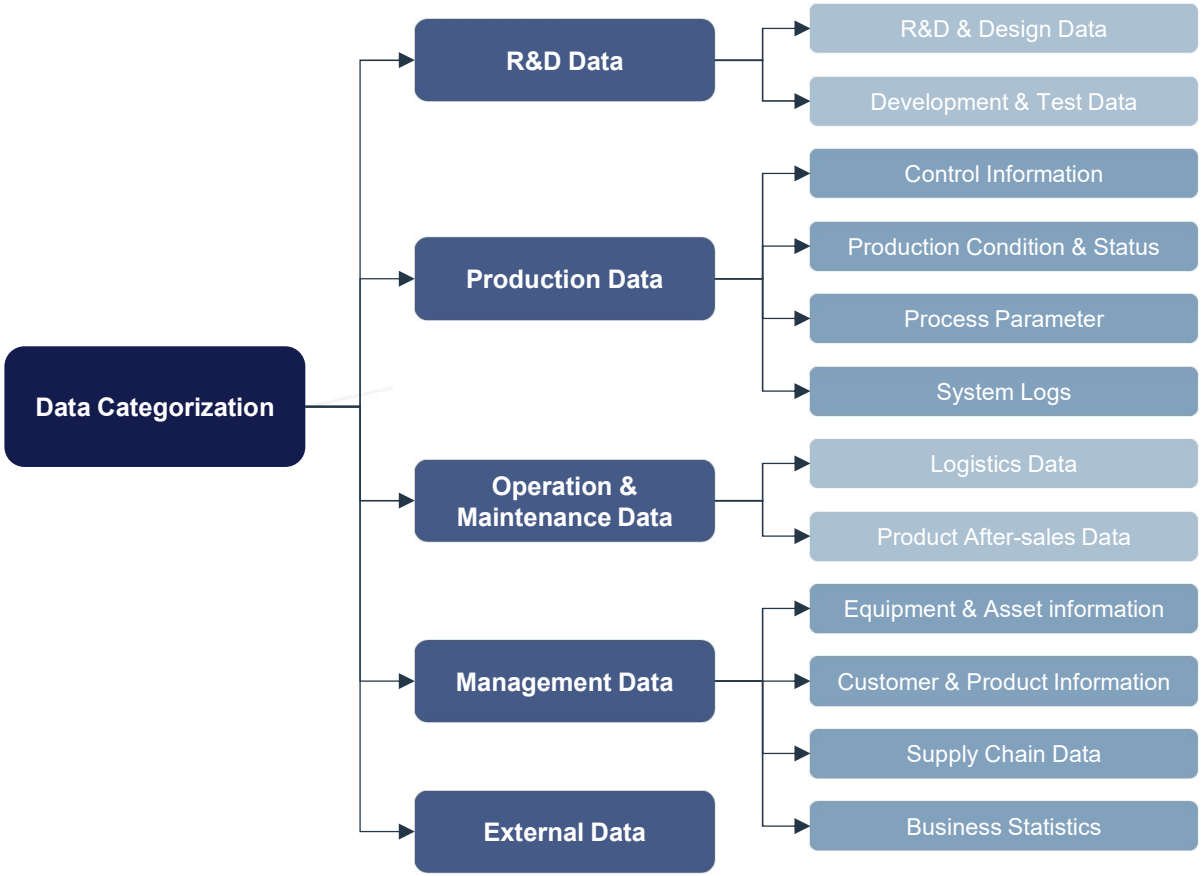
(3) The level of public data conditionally open/shared is not less than level 2, and open/shared is prohibited

(4) Public data is not less than level 4.

- "**Raw data**" can be graded according to the same method;
- The level of "**derivative data**" is graded against the level of the processed raw data set in principle according to the principle of higher and stricter, while the data can also be upgraded or downgraded according to the degree of processing.
  - The level of desensitized data can be reduced from the level of the original data set to no less than level 2 for de-identified personal information and no less than level 1 for anonymized personal information.
  - Label data level can be reduced from the original dataset level, with no less than 2 levels of individual label information.
  - Statistics that involve large-scale group characteristics or action trajectories should be set at a higher level than the original dataset level.
  - The level of derivative data ("fused data") should consider the result of data aggregation and fusion. If the result data aggregates more original data or mines more sensitive data, the level needs to be raised, but if the result data reduces the degree of identification, etc., the level can be lowered.

Data Categorization

Before classifying and grading the sensitivity, a data categorization system is recommendable according to prevailing industrial practice.



- It should first be checked if any applicable industrial standards on data categorization shall be followed.
- Applicable standards include *Guidelines for Categorization and Classification of Industrial Data (Trial)* which categorization is shown on the left and can be adjusted according to business operation.
- In the event that the categorization on the left does not suit the specific business operation upon assessment, other categorization may be implemented (e.g. categorizing data - from organizational perspective - into customer data, business data, operational and management data, system running and security data).

Classification of the categorized data - example

Type / class of data	Impaired interest			
	National interest	**Public interest**	**Rights of individuals**	**Rights of organizations and companies**
General data – Level 1	No hazard	No hazard	No hazard	No hazard
General data – Level 2	No hazard	No hazard	Low hazard	Low hazard
General data – Level 3	No hazard	No hazard	General hazard	General hazard
General data – Level 4	No hazard	No hazard	Serious threat	Serious threat
Important data	Minor hazard	Minor or general hazard	N/A	N/A
National core data	General or serious hazard	Serious threat	N/A	N/A

Re-classification principles

Measures or situations	Security level change
Increase in data volume to a specific size leading to significant social impact	Upgrade
Data to achieve the accuracy of the relevant national departments	Upgrade
Correlate data from multiple business units	Upgrade
Large amount of multidimensional data for correlation	Upgrade
Occurrence of specific events leading to increased data sensitivity	Upgrade
Data has been made public or disclosed	Downgrade
Data is desensitized or key fields are removed	Downgrade
Data is de-identified, pseudonymized, and anonymized	Downgrade
Data loss of sensitivity due to specific events in the data	Downgrade

Note: Data processors that handle personal information of more than one million people are managed in accordance with important data processors and should meet important data protection requirements

Process outline (further details apply to the specific procedure)

- A data processor should follow the steps below to categorize, classify and grade its data assets:
  1) Conduct an inventory of its data assets and create a list of data assets ("data (flow) mapping“ or „**data inventory**“).
  2) Categorization of data sets based on various dimensions in accordance with industry standards or other relevant data classification regulations (**"data categorization"**).
     - Identify core data, important data, general data and personal information.
     - Provide a grading based on sensitivity level for various benchmarks
     - Document the process
  3) Self-assessment of sensitivity screening based on the classification and grading, update the above classification and grading („**data classification**“ based on „**data impact assessment**“)
  4) Take appropriate measures to protect data of various levels and classifications („**data protection measures**“), including where required filing with governmental authorities for expert security assessment („**security review**“) or for registration prior to export
  5) Review in regular intervalls assessment, classification and related security measures („constant monitoring“ and „**reclassification**“ where indicated)