ADVANT Nctm

CHINA DATA PROTECTION REPORT

SUMMARY

1. INTRODUCTION

This short guide will help you navigate through the data security management laws and regulations of the People's Republic of China ("PRC").

Relevant laws and regulations
Cybersecurity Law of the PRC ("CSL"), effective from 1 June 2017, objectives: to ensure network security, safeguard cyberspace sovereignty, and national security;

Data Security Law of the PRC ("DSL"), effective from 1 September 2021, objectives: to standardize data handling activities, ensure data security, and promote data development and use.

Personal Information Protection Law of the PRC ("PIPL"), effective from 1 November 2021: to protect personal information rights and interests, regulate the processing of personal information, and promote the reasonable use of personal information.

Regulations
Regulations are second-tier legislation that is implemented by ministries or other state organs to enact law provisions. Regulations usually clarify details or procedures or certificates that are only mentioned in the main legislative provision.

Standards
Laws and regulations often establish general obligations or principles; however, they do not provide technical clarification or guidelines that may be needed. Therefore, as far as privacy is concerned, it is necessary to study the standards provided by the State Council Technical Committee (known as "TC260"). These standards are divided into mandatory standards (with the acronym of GB) and non-mandatory standards (with the acronym of GB/T).

2. CYBERSECURITY LAW
中华人民共和国网络安全法

The CSL is the PRC's fundamental law regulating cyberspace and focuses on a multi-level protection system of the Critical Information Infrastructures. The CSL also regulates some aspects of personal information protection, however, upon enacting the PIPL, now it mainly focuses on cybersecurity.

2.1. Useful Glossary

Critical Information Infrastructure (关键信息基础设施): Refers to important network facilities and information systems in important industries and fields such as public telecommunications, information services, energy, transportation, water conservancy, finance, public services, e-government and national defense science, technology and industry, as well as other important network facilities and information systems which, in case of destruction, loss of function or leak of data, may result in serious damage to national security, the national economy and the people's livelihood and public interests.

Network operator (网络运营者): Refers to the owner or manager of a network or the provider of network services. The "Network" is any system that is comprised of computers or other information terminals and relevant equipment that collect, store, transmit, and exchange and process information.

2.2. Network Operators Obligations

The CSL gives general obligations on data protection to the Network Operators:

- Formulate **internal security management systems** and operating rules, determine persons responsible for network security, and implement network security protection responsibility;
- Adopt technological measures to **prevent** computer viruses, network attacks, network intrusions, and other actions endangering network security;
- Adopt technological measures for **monitoring and recording** network operational status and network security incidents, and follow relevant provisions to store network logs for at least six months;
- Adopt measures such as **data classification**, backup of important data, and encryption;
- Other obligations are provided by law or administrative regulations.

These obligations are determined by specific regulations, guidelines, or standards that need to be examined case-by-case, according to the activities carried out by the Network Operator.

2.3. Information storage

These The Personal Information and other Important Data gathered or produced by Critical Information Infrastructure operators during operations within the mainland of the PRC, shall be stored within the mainland of the PRC. (art. 37).

3. DATA SECURITY LAW
中华人民共和国数据安全法

It defines the policies regarding data categorization and classification, data risk controls, contingency responses for data security, data security reviews, and outbound data transfer. The data categorization and classification systems will be established for the single industries by the relevant governmental departments from time to time when required

3.1. Useful Glossary

Important Data (重要数据): Refers to data that may have security implication in terms of national security, economic operations, social stability, public health, and safety.

Risk Assessment (风险评估): Refers to a risk assessment that must be conducted by subjects that collect important data

3.2. Scope of the Law

The DSL **regulates the processing of important data by any operator**, and the processing of important data by the **Critical Information Infrastructure Operators** ("CIIOs"), which shall be defined at the regional level. The important data handlers shall designate persons responsible for data security, and management bodies to implement data security protection responsibilities.
The DSL also applies to the data handling **activities outside the territory of the PRC** that harm the national security, the public interest, or the lawful rights and interests of citizens or organizations of the PRC.
The DSL also applies to the company whose business is the **trade of data** (Article 33):

- the source of the data must be indicated, and the data should have no ownership defects (meaning that the data is not acquired by theft or other illegal means);
- shall check the identity of both parties to the transaction;
- shall retain the examination and transaction records.

3.3. Important Data

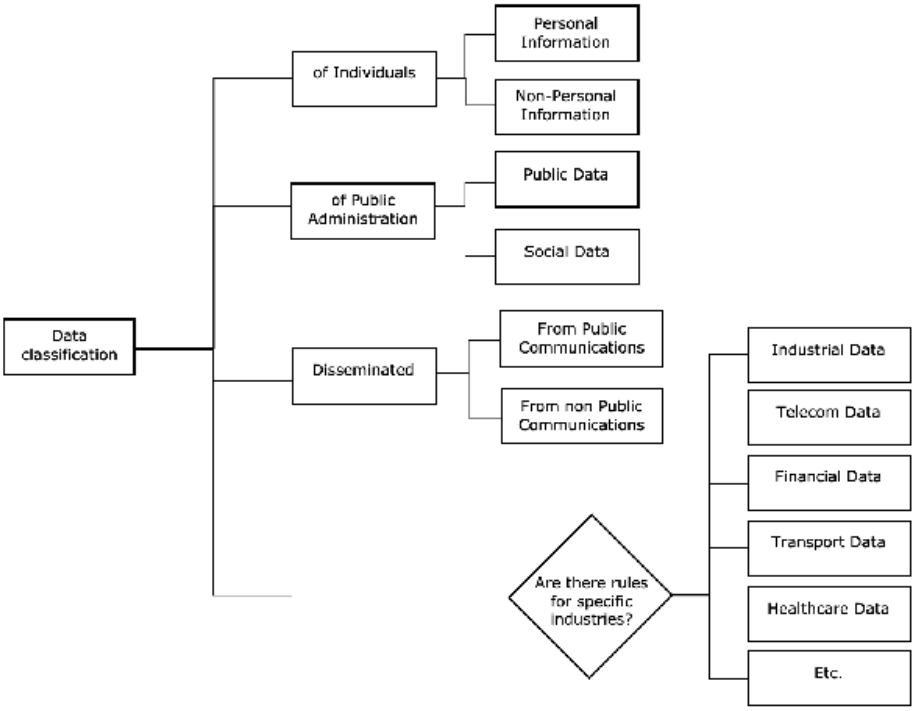
Important Data are not defined by the DSL, but from specific guidelines called "Guidelines for the identification of Important Data (draft)", according to which important dare identified following:

- their **security implication** in terms of national security, economic operations, social stability, public health and safety, etc. Data that is important or sensitive only to the organization itself is not considered important;
- the **comprehensive consideration of the risk** of a data leak, destruction, illegal access, or use;
- a **qualitative and quantitative approach** to the data.

3.4. Obligations of the DSL

The DSL obliges all the companies incorporated in the PRC to establish a **Data Security System** according to the data they are processing. The DSL gives no instructions for companies that do not process Important Data, but it gives a general obligation to adopt the technical measures and other necessary measures to ensure data security (Article 27).
The establishment of a Data Security System consists in establishing an internal data classification system, the company needs to be aware of what kind of data is processing and to whom it is transferring those data. The companies also need to establish guidelines to regulate a data security response in case of data breaches or system vulnerabilities. These obligations apply to all companies, not only to the ones processing important data.

Example of a data classification



3.5. Additional obligations for Important Data Processors

Some additional obligations may apply to the companies processing important data, including:

- **Appointment of a Data Processor Officer**: a person in charge of the data security, responsible for data security protection.
- **Risk Assessment**: the company must conduct a regular risk assessment, which covers the type, volume, data processed, and the activities concluded, and report them to the competent authorities.
- **Data storage obligations**: the important data collected and generated by Critical Information Infrastructure operators must be stored in China

3.6. Transfer of Important Data abroad

The Important Data collected, or when they are generated by Critical Information Infrastructure Operators within the PRC, shall be governed by the CSL, therefore whenever they need to be transferred overseas, a **security assessment** is required.

It is not allowed to transfer data to foreign judicial authorities without the approval of the competent authorities of the PRC.

3.7. Does the DSL apply to my business?

a. Do I process Important Data?

The DSL applies to companies that process Important Data, which are defined by central and regional administrative authorities as well as at an industry level:

- you need to check if the data of the industry you are operating in are considered important data by specific regulations or guidelines and, if so, comply with the specific regulation.
- if your data does not belong to any specific industry sector considered important, you need to check if they

can be considered important according to the principles for the identification of important data.

b. Am I a Critical Information Infrastructure ("CII") Operator?
Critical Information Infrastructure is infrastructures of particular importance for the public and national security and is identified at a governmental level. It is unlikely that wholly foreign-owned entities are allowed to run CII (such as entities in the following industries: telecommunication, transportation, finance, public services, etc.).

c. What can I do to make sure that I am DSL compliant?
If you do not collect Important Data, you need to adopt measures to ensure data security. For this reason, it is necessary to classify the data I am processing and the purpose of the treatment and to establish internal guidelines for data security management (Article 27 DSL).
If you collect Important Data, you must also conduct a Risk Assessment, appoint a DPO, and store important data in the territory of China.
Even though the obligations may be burdensome and costly, they are necessary to avoid sanctions from the authorities. In case of any control by the authority, the companies need to show the measures that they adopted to conform to the Data Security Law. The measures adopted, however, may vary a lot considering the type of data the company is processing. Therefore, it is important to know what kind of data my company is processing, to avoid unnecessary costs.

d. I am not a Critical Information Infrastructure Operator, nor do I directly collect important data, however, while doing my business, I may collect and process Important Data similar to those that are collected by a Critical Information Infrastructure, what can I do in this situation?
The DSL does not give a specific obligation to the processor of Important Data that is not a Critical Information Infrastructure operator. However, the DSL still gives a general obligation to adopt a data security system according to the data that are being processed.
It is always a good practice to establish an internal data classification system mechanism so that it is easy to classify which data your company collects and identify data that shall not be collected or requires protection measures.

e. I am a foreign company without a legal entity in China, but most of my business and customers are based in China, do I have to comply with the CSL?
The CSL applies to foreign entities only when the data handling harms the national security, the public interest, or the lawful rights and interests of citizens or organizations of the PRC.

Therefore, the DSL may apply if I handle any important data that falls under that category.

4. PERSONAL INFORMATION PROTECTION LAW

中华人民共和国个人信息保护法

4.1. Useful Glossary

Processing (处理): Include the collection, storage, use, processing, transmission, availability and disclosure of data, etc. (referring to data, where "data" refers to any recording of information by electronic or other means). As defined in the Data Security Law.

Personal Information (个人信息): All kinds of information related to identified or identifiable natural persons recorded by electronic or other means, excluding the information processed anonymously.

Sensitive Personal Information (敏感个人信息): Refers to the personal information that is likely to result in damage to the personal dignity of any natural person or damage to his or her personal or property safety once disclosed or illegally used, including such information as biometric identification, religious belief, specific identity, medical health, financial account and whereabouts, and tracks, as well as the personal information of minors under the age of 14

Impact Assessment (保护影响评估): Refers to a data security self-assessment that must be conducted before collecting sensitive personal information or transferring personal information abroad that need to be filed to the Cyberspace Administration of China.

Security Assessment (安全评估): Refers to a detailed security assessment that must be conducted and reported to the competent authority when personal information above defined quantitative thresholds are met.

4.2. Territory of Application

The PIPL applies to any subject who collects and processes Personal Information of **individuals** who are **inside the mainland** of the PRC. Therefore:

- The application of the PIPL does not apply only to Chinese nationals.
- The application of the PIPL does not apply to subjects who collect process Personal Information of Chinese individuals who are outside the mainland of the PRC.

The law also applies to the processing of Personal Information **outside the mainland** of the PRC under the following conditions:

- where the purpose is to provide products or services to natural persons in the mainland of the PRC.
- where the purpose is to analyze and evaluate the activities of natural persons in the mainland of the PRC.
- Other circumstances provided by laws and administrative regulations.

4.3. Principles for Personal Information Collection and Treatment

Every subject that is processing Personal Information of individuals inside the mainland of the PRC must respect the following principles:

- **Data minimization**: Personal information collection must be limited to the minimum necessary to provide the products or services.
- **Storage limitation period**: Personal Information must be stored for the minimum period necessary for achieving the processing purpose unless laws or regulations provide otherwise.
- **Transparency**: the processing of Personal Information must be conducted transparently and openly.
- **Accuracy**: the Personal Information processor must ensure the quality of the information collected.
- **Data security**: the Personal Information processor must ensure the security of the personal Information Processed.

4.4. Consent

4.4.1. When the consent is required

The consent is always required for collecting and processing Personal Information.

4.4.2. What does "Consent" mean

Consent in the context of personal information processing means that an individual (the subject of personal information) authorizes the processing of their personal information. This authorization can be either:

1. Active Consent (Explicit): The individual actively agrees to the processing. This could be through clear actions like saying "yes," ticking a checkbox, or clicking an "Agree" button.
2. Passive Consent (Implicit): The individual does not actively object or opt out of the processing. For example, they continue to use a service or remain in an area where information collection is taking place, without leaving or expressing disagreement, even after being informed about the data collection[1].

Explicit consent is a more specific form of consent where the individual actively and clearly authorizes the processing of their personal information. This can be done through:

- Written or Verbal Statements: Making a statement, either in writing or verbally, that clearly indicates consent[2].
- Affirmative Actions: Taking actions that unambiguously indicate consent, such as actively selecting a checkbox, clicking a button labeled "Agree," "Register," "Send," or "Call," or actively providing personal information in a form or survey.

4.4.3. When the consent is not required

The consent is not required when:

- Processing Personal Information is necessary for the **conclusion or performance of a contract** to which the individual concerned is a party. For example:
    - o A shopping website collects and uses a user's name, address, and contact number to deliver goods purchased online, as these details are essential for fulfilling the basic function of the delivery.
    - o An online rental platform collects a user's real-name information, mobile phone number, and other personal details to sign a rental contract, which is necessary for the realization of its basic functions.

  This includes circumstances where collecting personal information is essential for ensuring the safety, quality, and stable operation of products or services, and to prevent behaviors that could endanger operational safety. For example:
    - o A software application collects log information such as the user's device type, network operation logs, and crash reports. This data is used to analyze and improve the software's performance and ensure its safe and stable operation.
    - o Collection of user's device information, log information, and network access status to prevent malicious activities like fraudulent registrations and batch clicks that threaten operational security.
- To **implement human resources management** following labor law regulations;
- Processing Personal Information is necessary for the **performance of statutory duties** or statutory obligations;
- Processing Personal Information is necessary for **coping with public health emergencies** or for the protection of the life, health, and property safety of a natural person;
- **News reporting** and supervision by public opinions are carried out for the public interest;
- Processing Personal Information is **disclosed by individuals themself** or legally disclosed;
- Other circumstances provided by law or administrative regulations.

1 信息安全技术 个人信息告知同意指南 Information security technology - Guidelines for personal information notices and consent

2 信息安全技术 个人信息告知同意指南 Information security technology - Guidelines for personal information notices and consent

4.4.4. Additional mandatory consents

A **specific and separate consent** is required for collection and processing of Sensitive Personal Information.
An **additional and specific consent** is required for:

- processing Personal Information of people under 14 years old;
- transfer of Personal Information abroad.

4.5. Personal Information Protection Officer

4.5.1. When it needs to be appointed

If the **volume** of Personal Information processed goes **beyond a threshold established by the administrative authorities**, the Personal Information processor must appoint a Personal Information Protection Officer. This threshold has not been specified, however, some guidelines[3] provides that the Personal Information Protection Officer must be appointed when:

a) the main business of the organization involves the processing of Personal Information;
b) the organization has more than 200 employees;
c) the organization processes the personal information of more than 1 million people within 12 months;
d) the organization processes the sensitive personal information of more than 100,000 people.

Best practice may suggest the appointment of a Personal Information protection officer also where the proposed threshold is not achieved.

4.6. Data Classification

Personal information processors are required to develop an internal data classification and management system, as well as an appropriate technical security measures in accordance with the purpose of the processing, the type of personal information collected and the impact of the processing on the rights and interests of the individuals.

4.7. Impact Assessment and Security Assessment

4.7.1. Impact assessment

The personal information processor must conduct a Personal Information Impact Assessment ("**PIPIA**") before:

a) processing sensitive personal information;
b) using personal information in automated decision-making;
c) engaging an entrusted party to process personal information on the personal information handler's behalf;
d) providing personal information to another personal information handler;
e) disclosing personal information to the public;
f) transferring personal information outside of the mainland of the PRC; or
g) any processing activity will have a material impact on an individual's personal rights and interests.

The PIPIA must specify:

a) whether the purpose(s) and method(s) of processing are lawful, legitimate, and necessary;
b) the impact of the processing on individuals' rights and interests, the level of risk involved; and
c) whether the undertaken protective measures are lawful, effective, and commensurate to the degree of such risk.

4.7.2. Security Assessment

A separate Security Assessment is required whenever personal information of more than 1.000.000 individuals, or sensitive personal information of more than 10.000 individuals are transferred outside the PRC.

3 Personal Information Security Specification (GB/T 35273-2020)

4.8. Data Processed by Third Parties

When a personal information controller provides personal information to third parties, they must inform the subject of the personal about the type of personal information being provided, the purpose of the provision, and the recipient.

Prior explicit consent must be obtained from the individual before providing their personal information externally. This includes, but is not limited to, the following situations:

a) **Sharing for Business Needs**: The personal information controller shares personal information with a third party due to business requirements.

b) **Transfer Due to Business Changes**: The personal information controller transfers personal information to a third party due to business changes or other reasons and no longer retains the personal information.

c) **Public Disclosure**: The personal information controller discloses personal information to the public in a non-targeted manner.

d) **Other Cases of External Provision**: Other scenarios where the personal information controller provides personal information externally, except when the controller is providing the information to an entity commissioned by them or to an entity providing personal information processing services on their behalf[4].

When a third party is entrusted to handle personal information, establish a clear agreement with the agent (the party being entrusted) must be signed. This agreement should cover several key aspects:

1. **Purpose**: Define the specific purpose for which the personal information is being entrusted.
2. **Time Limit**: Specify the duration for which the agent is authorized to handle the personal information.
3. **Method of Handling**: Outline the methods or procedures the agent should use in handling the personal information.
4. **Type of Personal Information**: Identify the specific types of personal information being entrusted.
5. **Protection Measures**: Agree on the measures that will be put in place to protect the personal information.
6. **Rights and Obligations**: Clearly state the rights and obligations of both the personal information handler and the agent.
7. **Supervision**: The personal information handler must actively supervise the agent's handling activities to ensure they are in compliance with the agreed terms and protective measures[5].

4.9. Data Breach Notification

In the event of a suspected or actual data breach, the Personal Information Processor must immediately take remedial measures, and notify the affected individuals and relevant authorities.

4.10. Transfer of Personal Information Abroad

4.10.1. Requirements

Depending on the amount and type of personal information and sensitive personal information transferred abroad, a **separate consent** needs to be obtained and different requirements need to be satisfied:

a) A **Security Assessment** must be obtained by the relevant authorities whenever personal information of more than 1.000.000 individuals, or sensitive personal information of more than 10.000 individuals are transferred outside the PRC; OR

b) a **Standard Contract** need to be signed between with recipient abroad when the thresholds for the Security Assessment are not met; OR

c) a **Personal Information Protection Certification** awarded by a recognized institution must be obtained for specific circumstances provided by the law.

10.2. Exemptions

At present, a draft Regulations on the Facilitation of Cross-Border Data Flows of 2023 (the "**Amendment**

4 Article 21 PIPL and poin 5.3 of the "信息安全技术 个人信息告知同意指南 Information security technology - Guidelines for personal information notices and consent"

5 Article 21 PIPL

Regulation"), is removing the requirements above for in the following circumstances:

- If it is anticipated that the personal information of **fewer than 10,000 individuals** will be transferred outside the country within a year. However, when personal information is transferred based on the individual's consent, the consent must be obtained from the person whose information is being shared.
- When transferring personal information is necessary for the purposes of entering into or **fulfilling a contract** that the individual is a part of. This includes activities such as cross-border shopping, sending money across borders, booking flights and hotels, and processing visas.
- For the implementation of **human resources management** in line with labor laws and regulations, and **collective contracts** that are legally binding, where transferring employees' personal information outside the country is required.
- In situations where transferring personal information outside the country is necessary to protect the life, health, and property of individuals in emergency situations.

Exemptions to obtain the security assessment:

- If personal information of more than 10,000 but fewer than 1 million individuals is transferred outside the country within a year, and the recipient of the personal information signed Standard Contract for exporting personal information and either registers it with the provincial Internet information department or obtains a certification for personal information protection, there is no need to undergo a data export Security Assessment.

Finally, regardless of the number of individuals whose personal information is being transferred, if the transfer is based on individual consent, the consent must be obtained from the person whose information is being shared.

4.11. FAQ

- **Are cookies considered Personal Information?**

Yes, cookies are considered personal information. A cookie banner must be prepared and a cookie policy, or a specific section in the privacy policy, must be prepared.

- **I sell my product/services to Chinese customers from abroad, do I need to comply to the PIPL (i.e., obtain the consent, prepare the impact assessment, etc.)?**

PIPL applies to foreign entities only Chinese individuals are targeted. If you sell product/services through a website which is in Chinese, uses RMB as a currency, and has convenient shipping methods for individuals in China, you need to comply to the PIPL. On the other hand, if through your website there are some customers that are also from China, you do not need to comply to the PIPL.

- **I sell my products/services to individuals in China through a Chinese WFOE/Joint Venture, but my CRM is abroad, do I need to obtain separate consent?**

Yes, a separate consent is always required for the transfer of personal information abroad. If the customer refuses to provide the consent, the anonymization of the personal information is required before their transfer abroad.

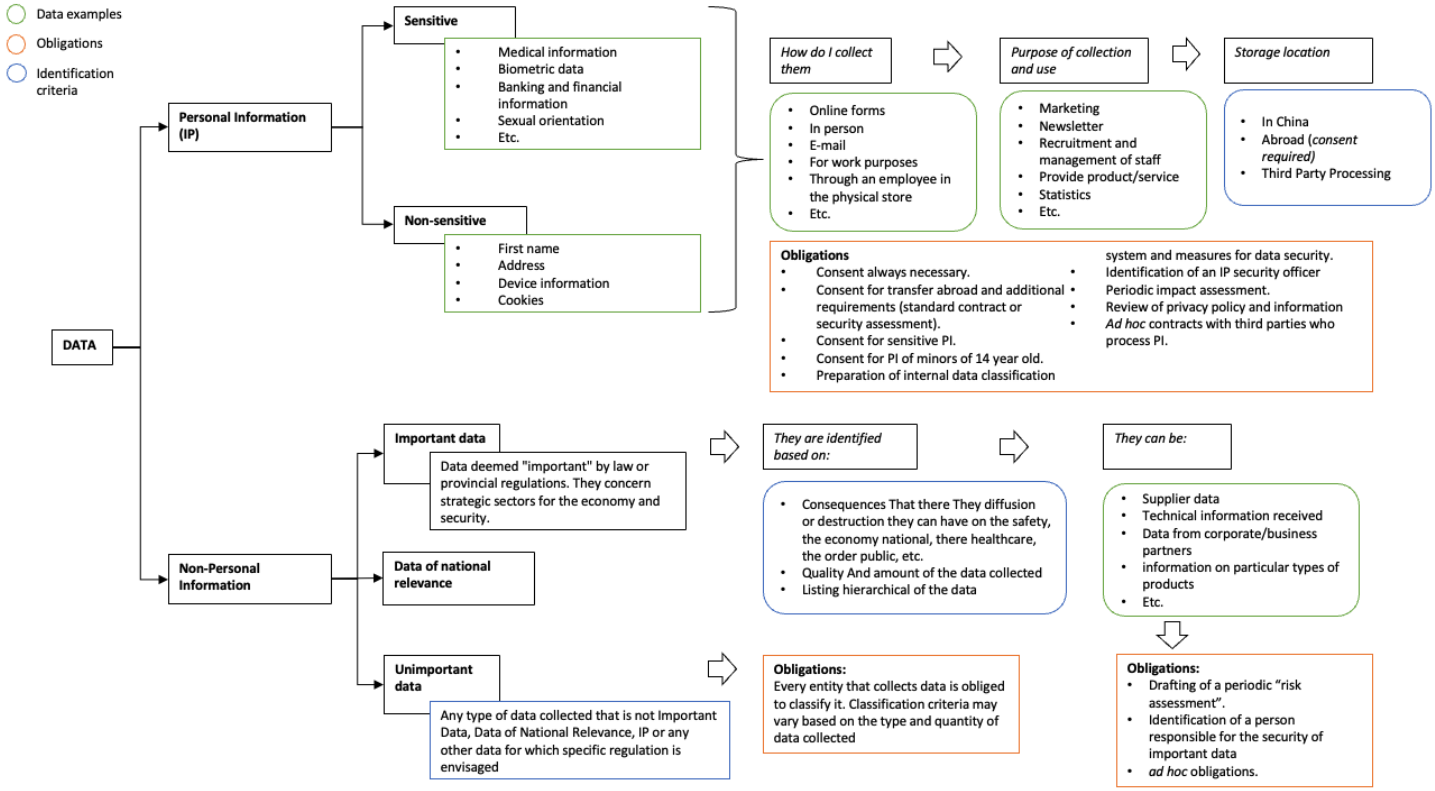
- **The personal information of my employees is managed by an HRM abroad, do I need separate consent from the employee?**

Yes. Even though consent is not required for HR management, it is still required for the transfer of the employee's data abroad.

- **My Chinese privacy policy is GDPR compliant, do I need to change it?**

Yes, you need to have it revised and made a PIPL complaint. Even though many aspects, such as the right of the individual may be similar, others, such as, for instance, the consent, the data retention period, and the legal age are different.

5. DATA CLASSIFICATION SCHEME



CONTRIBUTORS

Hermes Pazzaglini

hermes.pazzaglini@advant-nctm.com

Carlo Geremia

carlo.geremia@advant-nctm.com

Pierpaolo Canero

pierpaolo.canero@advant-nctm.com

ADVANT Nctm

Your European Advantage

www.advant-nctm.com

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