國浩律師（北京）事務所
GRANDALL LAW FIRM (BEIJING)

Cyber Security and Personal Information Protection in Cross-border Business

March 27, 2023

- Speaker:
  Catherine Liu
  Partner, Grandall Law Firm (Beijing)

GRANDALL

CONTENTS

I. Data Privacy Legislative System in Medical Device Industry

Basic Legal System

Cybersecurity Law
Effective Date： 06/01/2017

- Cybersecurity Review Measures (2021)
- Security Protection Regulations for Critical Information Infrastructure
- ……

Data Security Law
Effective Date： 09/01/2021

- Security Assessment Measures for Outbound Data Transfers
- Regulations for the Administration of Network Data Security (Draft for Public Comment)
- ……

Personal Information Protection Law (PIPL)
Effective Date： 11/01/2021

- Provisions on Standard Contracts for Cross-Border Transfers of Personal Information
- Guide to Practice on Cyber Security Standards - Security Certification Specification for Cross-Border Processing of Personal Information V2.0
- ……

Legal System for Compliance Regulation in Medical Device Industry

- Biosecurity Law of the People's Republic of China (2021)
- Law of the People's Republic of China on Basic Medical Care and Health Promotion (2020)
- Measures for the Management of Scientific Data (2018)
- Regulation on the Supervision and Administration of Medical Devices (Revised in 2021)
- Administrative Regulations on Human Genetic Resources of the People's Republic of China (2019)
- Administrative Measures on Standards, Security and Services of National Healthcare Big Data (for Trial Implementation) (2018)
- Information Security Technology-Guide for Health Data Security (GB/T 39725-2020)
- Guiding Principles for the Cybersecurity Registration Review of Medical Devices (2022)
- Pharmaceutical Industry Compliance Management Practices (PIAC/T 00001-2020) (2021)

II. Key Points of Data Compliance and the Compliance Structure in Medical Device Industry

Cybersecurity Review

Compliance subjects and obligations under the basic data privacy laws

Subject

- **A Network Operator** refers to the owner or manager of a network or the provider of a network service.

  ——*Cybersecurity Law, Article 76*

- **An Internet Platform Operator** refers to a data processor who provides Internet platform services such as information releasing, social networking, transaction, payment, or audio-visual services.

  ——*Regulations for the Administration of Network Data Security (Draft for public comment), Article 93*

- **Critical Information Infrastructure Operator (CIIO):**
  Critical Information Infrastructure (CII) refers to the 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 the national security, economy and the people's livelihood and public interests.

  ——*Security Protection Regulations for Critical Information Infrastructure, Article 2*

Cybersecurity Review

Jurisdiction

- Those who carry out data processing activities within the territory of PR China.
- Those who carry out data processing activities outside the territory of PR China, which endanger the national security, public interests or the legitimate rights and interests of citizens and organizations.

Data Security Review

Obligations

Establish a whole-process data security management system

Processors of important data:

- specify the person (s) responsible for data security and the management organization;
- carry out risk assessment on data processing activities on a regular basis and submit a risk assessment report to the relevant competent authority.

Risk monitoring

Personal Information Protection

Subject

- **Personal information** refers to all kinds of information related to identified or identifiable natural persons recorded by electronic or other means, excluding the information processed anonymously.

- **Personal information processor** refers to an organization or individual that independently determines the purpose and method of the processing in the processing of personal information.

Definitions

Information Security Technology-Guide for Health Data Security（GB/T 39725-2020）

- **Personal Health Data**

  Relevant electronic data that can identify particular natural persons or reflect the physical or mental health of particular natural persons, either alone or in combination with other information.

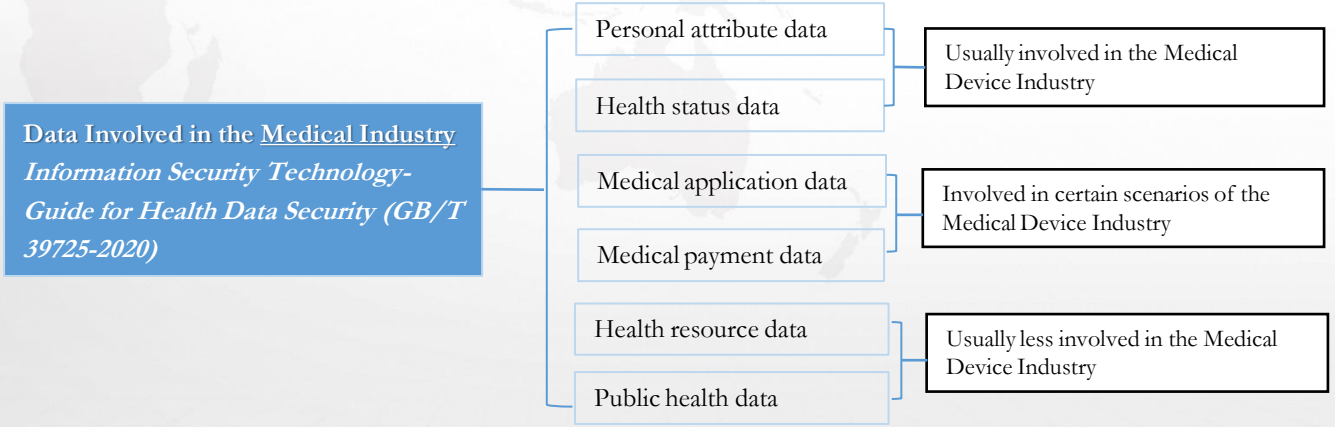
  Note: Personal medical data concerning health involves the individual's past, present or future physical or mental health conditions, the medical care services received, and the cost of the medical care services.

- **Health Data**

  Personal health and medical data and health-related electronic data are obtained after processing personal health and medical data.

  Examples: Results of population analysis, trend prediction, disease prevention statistics, etc., obtained after processing group's health and medical data.

Type of Data Involved in the Medical Device Industry



Type of Data Involved in the Medical Device Industry

Data Involved in the Medical Device Industry

- **Medical data:** the data (including logs) related to medical activities generated or used by medical devices
  - Sensitive medical data: medical data containing personal information
  - Non-sensitive medical data
- **Device data:** the data (including logs) recording the operation status of medical devices, which are used to monitor and control the operation of medical devices or the maintenance and upgrading of medical devices and shall not include personal information.

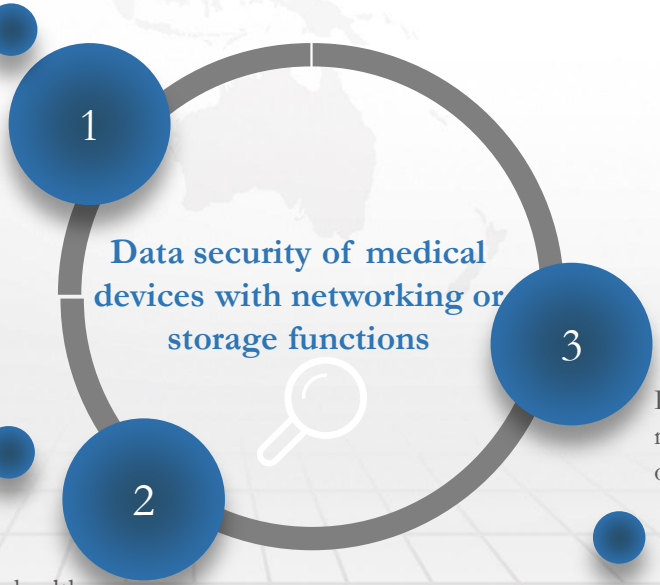
Guiding Principles for the Cybersecurity Registration Review of Medical Devices（2022）:

*Medical data are usually important data, especially sensitive medical data containing personal information, and the processing of medical data shall comply with the relevant regulations on the processing of important data, personal information and human genetic resources.

*** Sensitive personal information**

Article 28 of the *PIPL*: Sensitive personal information 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.

Parties Involved in the Medical Device Industry



Production

Medical device manufacturers and relevant suppliers.

Use

Medical device operators in medical institutions, health care professionals who need access to data, target systems and patients.

Remote maintenance personnel, medical device manufacturers, medical institutions, device operators in medical institutions, and patients.

Maintenance

Key Points of Data Compliance in Medical Device Industry

Key points of Compliance: Collection of Data

Collection of personal information

✓ **Inform**

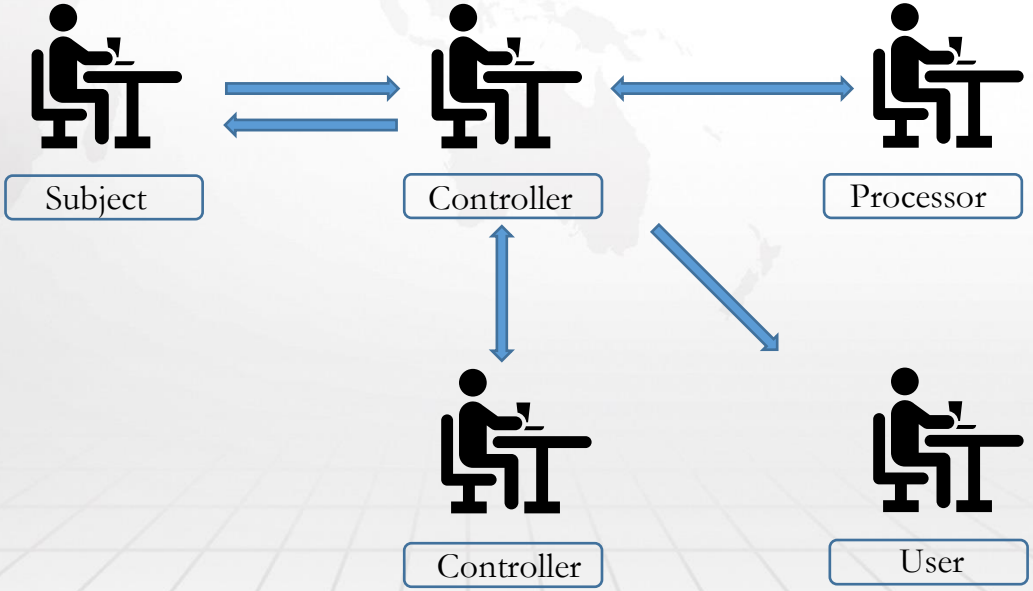
*sensitive personal information: inform the individual of the necessity of processing his/her sensitive personal information and the impact on his/her personal rights and interests

✓ **Consent**

* sensitive personal information: separate consent

* minor under the age of 14: the consent of the minor's parents or other guardians

1. Data Flow



——Information security technology-Guide for health data security（GB/T 39725-2020）

2. Key Points of Compliance of Data Flow and Commercial Development on Health and Medical Treatment

1) Inform and Consent (Article 13, 17, 20-23 of *PIPL*)

- Without authorization from the individual, a controller may use or disclose relevant personal data on health or medical treatment under the following circumstances: 1) Provide the subject with its own data; 2) treatment, payment or healthcare care; 3) for public interest or requirements by laws and regulations; 4) limited data set for scientific research, medical/health education, public health or healthcare practices. (*Information Security Technology-Guide for Health Data Security, GB/T 39725-2020,* Article 7.b)
- If personal data is involved in the maintenance of the medical devices, the individual's consent is not required in principle; however, it is recommended to obtain the individual's consent if the involved data is required to be used for other purposes. (*Information Security Technology-Guide for Health Data Security, GB/T 39725-2020,* Art. 11.8.4.1)

2) Impact Assessment on personal information protection (Articles 55 and 56 of *PIPL*)

3) Enter into a Data Processing Agreement to specify the rights and obligations of both parties and data security responsibilities. (Articles 20-23 of *PIPL*)

- Medical device manufacturers shall enter into maintenance contracts with medical institutions to specify the rights and obligations of both parties and carry out data security assessments in accordance with GB/T 35273 and the medical security standards ISO 80001. (*Information security technology-Guide for health data security, GB/T 39725-2020,* Art. 11.8.4.1)

Key points of Compliance: Data Cross-Border Transfer

Three Dimensions of Data Cross-Border Transfer

Data Category

Personal information, important data, core data, other data……

Industry

Medical device, human genetic resources……

Company

Critical Information Infrastructure Operator, Internet Platform Operator

Key points of Compliance: Data Cross-Border Transfer

1. Identify the Category of the Cross-Border Transferred Data

- Personal Information
- Important Data
- Core Data

Key points of Compliance: Data Cross-Border Transfer

Definition

Core Data: refers to data concerning national security, lifelines of the national economy, important people's livelihood, major public interests, etc. are core data, and shall be subject to a stricter management system.

——*Data Security Law,* Article 21

Important Data: refers to data that exists electronically and that, once tampered with, destroyed, disclosed, or illegally obtained or exploited, may endanger national security or the public interest.

*Basic data reflecting the group's health and physiological status, population characteristics, genetic information and others, such as population survey data, information on human genetic resources and original data on gene sequencing, are important data.

——*Information Security Technology, Important Data Recognition Guide (Draft for Public Comment)*, Articles 3.1 and 5.h

Personal information: refers to all kinds of information related to identified or identifiable natural persons recorded by electronic or other means, excluding the information processed anonymously.

——*PIPL*, Article 4

*The medical device industry usually does not involve the processing of Core Data.

Compliance Requirements for Cross-Border Transfer of Different Categories of Data

Personal Information

a. Obtain legitimate basis according to Article 13 of *PIPL*.

b. Adopt a transfer regulatory approach stipulated in Article 38 of *PIPL*, including security assessment, certifying by specialized agency for protection of personal information, concluding Standard Contract or other approaches.

c. Perform the duty of informing the individual, including informing the abroad receiver's name, contact address, processing purpose, processing method, the category of personal information, the methods and procedures with which individuals are able to exercise the rights according to this law, and other issues.

d. Carry out influence assessment on the personal information protection in advance.

e. To cross-border transfer personal information under the following circumstances, a data processor shall declare security assessment for its cross-border transfer to CAC through the local cyberspace administration at the provincial level:

1)CIIO or data processor processing the personal information of more than one million people cross-border transfer personal information;

2)a data processor has cross-border transferred personal information of 100,000 people or sensitive personal information of 10,000 people in total since January 1 of the previous year.

Compliance Requirements for Cross-Border Transfer of Different Categories of Data

Important Data

Cybersecurity Law:

Article 37 Personal information and important data collected and generated during the operation of CIIO within the territory of the PR China shall be stored within the territory of the PR China. Where such information and data have to be cross-border transferred for business purpose, security assessment shall be conducted pursuant to the measures developed by the CAC together with competent departments of the State Council, unless otherwise provided for in laws and administrative regulations, in which such laws and administrative regulations shall prevail.

Measures for the Security Assessment of Outbound Data Transfers:

Article 4 To cross-border transfer data under any of the following circumstances, a data processor shall declare security assessment for its cross- border data transfer to the Cyberspace Administration of China ("CAC") through the local cyberspace administration at the provincial level:

(I) where a data processor cross-border transfer important data;…

Compliance Requirements for Cross-Border Transfer of Different Categories of Data

Three Approaches of Data Cross-Border Transfer

Declaring Security Assessment

- *Security Assessment Measures for Outbound Data Transfers*
- *Guide to Applications for Security Assessment of Outbound Data Transfers (First Edition)*

Concluding Standard Contract and Applying for Filing

- *Measures for the Standard Contract for Outbound Transfer of Personal Information*

Seeking Certification for Protection of Personal Information

- *Cybersecurity Standards Practice Guide-Security Certification Practice v2.0 for Cross-border Processing Activities of Personal Information*

Compliance Requirements for Cross-Border Transfer of Different Categories of Data

Application Scenarios

Declaring Security Assessment

Security Assessment Measures for Outbound Data Transfers

Article 4

To provide data abroad under any of the following circumstances, a data processor shall declare Security Assessment for its outbound data transfer to the Cyberspace Administration of China ("CAC") through the local cyberspace administration at the provincial level:

(I) where a data processor provides **critical data** abroad;

(II) where a **Critical Information Infrastructure Operator** or a data processor processing the **personal information of more than 1,000,000 people** provides personal information abroad;

(III) where a data processor has provided **personal information of 100,000 people** or **sensitive personal information of 10,000 people** in total abroad since January 1 of the previous year; and

(IV) other circumstances prescribed by the CAC for which declaration for Security Assessment for outbound data transfers is required.

Under circumstances not required to declare Security Assessment, the companies could choose other two regulatory approaches:

Seeking Certification for Protection of Personal Information by a Specialized Agency

Cybersecurity Standards Practice Guide-Security Certification Practice v2.0 for Cross-border Processing Activities of Personal Information

Article 4.f

Voluntary Certification Principle: Personal information processors who carry out cross-border processing activities of personal information **are encouraged to voluntarily apply for** Certification for Personal Information Protection.

Concluding Standard Contract

Measures for the Standard Contract for Outbound Transfer of Personal Information

Article 4

Any personal information processor transferring personal information abroad by entering into the Standard Contract shall meet all of the following conditions:

(1) it is **not a Critical Information Infrastructure Operator**;

(2) it processes the **personal information of less than 1,000,000 individuals**;

(3) it has cumulatively transferred abroad **the personal information of less than 100,000 individuals** since January 1 of the previous year; and

(4) it has cumulatively transferred abroad the **sensitive personal information of less than 10,000 individuals** since January 1 of the previous year.

Key points of Compliance: Data Cross-Border Transfer

2. Identification of the Industry → **Medical device**

Administrative Measures on Standards, Security and Services of National Healthcare Big Data (for Trial Implementation) (2018)

Healthcare big data shall be stored in the secure and reliable servers within the territory of PR China and shall carry out security assessment and review according to relevant laws, regulations and requirements if it is necessary to cross-border transfer such data for business concerns.

Guiding Principles for the Cybersecurity Registration Review of Medical Devices (2022)

Medical data are usually important data, especially sensitive medical data containing personal information, and the cross-border transfer of medical data shall comply with the relevant regulations on important data, personal information and human genetic resources.

Key points of Compliance: Data Cross-Border Transfer

2. Identification of the Industry → **Medical device**

Information Security Technology-Guide for Health Data Security (GB/T 39725-2020)

7. o) Where a Controller needs to conduct cross-border transfer of relevant data due to academic research needs, non-confidential and non-important data, the amount of which is not more than 250 pieces, may be provided after necessary de-identification processing and upon the discussion and approval of the data security committee; otherwise, it will be recommended to be submitted to relevant departments for approval.

p) Where no state secrets, important data or other data prohibited or restricted to be cross-border transferred are involved, the controller may, upon authorization and consent by the subject, and consent by the data security committee upon discussion and examination, provide the personal health and medical treatment data outside of PR China and the accumulative data shall preferably be controlled within 250 pieces, otherwise, it will be recommended to be submitted to relevant departments for approval.

Measures for the Management of Scientific Data

Article 2 For the purpose of the present Measures, scientific data mainly includes data produced from basic research, application research, pilot development and others in such areas as natural science and engineering technology science, and the original data as well as derived data acquired via observation and monitoring, survey and investigation, and inspection and detection and used for scientific research activities.

Article 25 Any scientific data involving a state secret, state security, social public interests, commercial secret or personal privacy may not be disclosed and shared; where disclosure is indeed needed, the purpose, user's qualification, conditions of confidentiality and other factors shall be reviewed, and the informing scope shall be strictly controlled.

Key points of Compliance: Data Cross-Border Transfer

2. Identification of the Industry

Human Genetic Resources

Administrative Regulations on Human Genetic Resources of the People's Republic of China

Article 22

The international cooperation in scientific research carried out by utilization of China's human genetic resources shall meet the following conditions, and the two cooperative parties shall jointly submit an application, which shall be approved by the administrative department of science and technology under the State Council:
(1) There is no harm to the public health, State security or public interest of PR China;
(2) The two parties are a Chinese entity and a foreign entity, both of which shall have legal person status, and have the basis and capability to carry out the relevant work;
(3) The purposes and contents of the cooperative research are clear and legitimate, and the cooperation period is reasonable;
(4) The cooperative research plan is reasonable;
(5) The sources of human genetic resources to be utilized are legal, and the types and quantities of such human genetic resources are consistent with the research contents;
(6) They have passed the ethical review of the respective countries (regions) where the parties are located; and
(7) The research achievements are clearly identifiable and there are reasonable and clear arrangements for the distribution of benefits.

Where clinical institutions, in order to obtain the marketing licenses of relevant drugs and medical devices in PR China, makes use of China's human genetic resources to carry out international cooperation in clinical trials by utilization of China's human genetic resources by the clinical institutions, not involving the exit of human genetic resource materials, approval is not needed. However, the two parties shall, before conducting clinical trials, submit the types, quantities and uses of the human genetic resources to be used to the administrative department of science and technology under the State Council for filing. The administrative department of science and technology under the State Council as well as the administrative departments of science and technology of the people's governments of the provinces, autonomous regions and centrally-administered municipalities shall strengthen the supervision over the filing matters.

2. Identification of the Industry

Human Genetic Resources

Administrative Regulations on Human Genetic Resources of the People's Republic of China

Article 28

The provision or open access of information on human genetic resources to foreign organizations, individuals and institutions established or actually controlled thereby shall not endanger public health, State security and public interest of China; and those that are likely to affect public health, State security and public interest of PR China shall pass the security review organized by the administrative department of science and technology under the State Council. Those that provide or offer open access of information on human genetic resources to foreign organizations, individuals and the institutions established or actually controlled thereby shall file for record with the administrative department of science and technology under the State Council and submit such information for backup.

Information on human genetic resources generated by international cooperation in scientific research by utilization of human genetic resources of PR China may be used by the two parties.

Key points of Compliance: Data Cross-Border Transfer

3. Identification of the Company

CIIO

OR

Network Operator

Key Points of Compliance: Security Measures

- ✓ In the process of product research and development: Medical device manufacturers shall refer to the relevant international, national standards and technical reports to build their cybersecurity capabilities. Medical device manufacturers may consider the applicability of their cybersecurity capability requirements based on the characteristics of specific medical devices;

- ✓ Personnel authorized access mechanism shall be established, under which only the personnel who have passed security certification can remotely access authorized medical devices; a safe link shall be established to obtain maintenance records and log information, as needed;

- ✓ Application information security: it is necessary to obtain the authorization of the medical device operator or the staff of the medical institution to access application information through remote desktop;

- ✓ Encryption technologies, identity verification technologies and data integrity check technologies shall be used for data transmission to ensure that data is transmitted to the designated objects in a safe manner; and

- ✓ Organizational management measures: security strategies, procedures and management processes shall be established; security risk assessment and management shall be conducted on a regular basis; emergency management strategies shall be formulated and regular exercises shall be conducted on such strategies; and safety management, safety training and assessment shall be conducted on employees.

Data Compliance Structure:
Personal Information Protection as an Example

Stored within/ outside the territory of PR China

Inside/ cross-border transfer

Collect → Store → Process → Transfer → Delete

Legitimate basis

Jointly process/ Entrust others

Whole Procedures of Personal Information Processing

Compliance Structure:
Personal Information Protection as an Example

Legitimate Basis

Principle: Personal information processor shall obtain the consent of the individual concerned to process personal information.

Exceptions: under the following circumstances, such consent is not required for processing personal information:

a. it is necessary for the conclusion or performance of a contract to which the individual concerned is a party, or for the implementation of human resources management in accordance with the labor rules and regulations formulated in accordance with the law and the collective contract concluded in accordance with the law;

b. it is necessary for the performance of statutory duties or statutory obligations;

c. it is necessary for the response to a public health emergency or for the protection of the life, health and property safety of a natural person in an emergency;

d. such acts as news reporting and supervision by public opinions are carried out for the public interest, and the processing of personal information is within a reasonable scope;

e. it is necessary to process the personal information disclosed by the individual concerned or other personal information that has been legally disclosed within a reasonable scope in accordance with the provisions of *PIPL*;

f. other circumstances prescribed by laws and administrative regulations.

Compliance Structure:
Personal Information Protection as an Example

Storage of Personal Information

1. Requirements for storing personal information within or outside the PR China.

2. Retention period of personal information shall be the shortest period necessary to realize the purpose of processing.

A. CIIO and

B. Personal information processor whose quantity of processing of personal information reaches that as prescribed by CAC

shall store personal information collected and generated within the PR China

if it is necessary to provide such information and data to an overseas party

shall pass the security assessment organized by the CAC

where the laws, administrative regulations and the provisions of the CAC stipulate that security assessment is not required, such stipulation shall prevail

Compliance Structure:
Personal Information Protection as an Example

Processing of Personal Information

- Change: when the purpose and method of processing personal information and the type of personal information to be processed changes, whether the individual's consent has been re-obtained

- Joint Processing: when deciding the purpose and method of processing personal information jointly with other personal information processors, whether the respective rights and obligations have been clearly agreed upon by way of agreement

- Entrusted Processing:

1) In the case of entrusted processing of personal information, whether the purpose, duration, and method of entrusted processing, type of personal information and protection measures as well as the rights and obligations of both parties have been agreed upon with the entrusted party in a written agreement;
2) In the case of entrusted processing of personal information, whether the personal information processing activities of the entrusted party are supervised in the performance of the entrustment contract so that the entrusted party shall not process personal information beyond the agreed purpose and method of processing.
3）Whether an assessment on the impact of personal information protection is conducted in advance prior to entrusted processing of personal information and a record of processing is kept.

Compliance Structure:
Personal Information Protection as an Example

Providing Personal Information

Provide Within PR China

When the Company is the provider:

- Inform
- Obtain separate consent
- Impact assessment on personal information protection in advance and record of the processing: sensitive personal information; automatic decision-making; entrusted processing and publicizing; cross-border transfer, etc.

When the Company is recipient:

- Make an agreement on the purpose, time limit and the method of entrusted processing, type of personal information, etc
- Process personal information as agreed

When the recipient changes the original purpose and method of processing:

- Re-obtain the individual's consent

Compliance Structure:
Personal Information Protection as an Example

Cross-border Transfer of Personal Information

Providing Personal Information

Requirements

Security Assessment
or
Certified by a specialized agency for personal information protection
or
Conclude standard contract formulated by CAC
or
others

+

Take necessary measures to ensure the security of personal information

Procedure

Evaluate and keep a record on the impact on the protection of personal information

+

Inform specific issues

+

Separate consent of the individual concerned

Processor

Processor who process the personal information of natural persons within PR China, from outside of the territory of PR China,
When(1) the purpose is to provide domestic natural persons with products or services or ;(2) the activities of domestic natural persons are analyzed and evaluated or; (3)other circumstances as prescribed by laws and administrative regulations, it shall:
Set special agency or designate a representative within PR China

+

Submit the name and contact information of the relevant agency or the representative to relevant authorities

Compliance Structure:
Personal Information Protection as an Example

Deletion of Personal Information

Under any of the following circumstances, a personal information processor shall take the initiative to delete personal information; if the personal information processor fails to delete such information, the individual concerned is entitled to request the deletion of such information:

- the purpose of processing has been achieved, it is impossible to achieve such purpose, or it is no longer necessary to achieve such purpose;
- the personal information processor ceases to provide products or services, or the storage period has expired;
- the individual withdraws his/her consent;
- the personal information processor processes personal information in violation of laws, administrative regulations or the agreement; or
- other circumstances stipulated by laws and administrative regulations.

If the storage period as stipulated by laws and administrative regulations does not expire, or the deletion of personal information is difficult to be realized technically, the personal information processor shall stop the processing other than storage and necessary security protection measures.

III. Compliance Practice in other Industries

Compliance Practice in other Industries: AI Industry

Legal System of AI Industry -Current Laws and Regulations

—By 2020, China has initially established laws and regulations, ethical norms and policy systems related to AI, and developed the ability to assess and control the safety of artificial intelligence.

Guiding Opinions on Accelerating Innovation in Scenarios to Promote High-level Economic Development through High-level Application of Artificial Intelligence

Ministry of Science and Technology on Supporting the Development of Demonstration and Application Scenarios for New-Generation Artificial Intelligence

New Generation Artificial Intelligence Development Plan

Code of Ethics for the New Generation Artificial Intelligence

Guide to the Construction of National New Generation Artificial Intelligence Standard System

Administrative Provisions on Algorithm Recommendation for Internet Information Services

Compliance Practice in other Industries: AI Industry

Guide to the construction of national new generation artificial intelligence standard system

— Security and Privacy Protection Framework

H Ethics / Security	**HA Protection of Security and Privacy**	HAA Fundamental Safety	AI concepts and terminology, security reference structure, basic security requirements, etc.
		HAB Data, algorithm, and model security	Data security, privacy protection, reliability of algorithm model, etc.
		HAC Technology and System Security	Security of AI open-source frameworks, security projects of artificial intelligence systems, security of AI computing facilities, security technologies of AI, etc.
		HAD Security Administration and Services	Security risk management, supply chain security, safe operation AI, safe service capability of AI, etc.
		HAE Security Testing and Evaluation	AI algorithm models, system and service platform security, data security, application risks, testing and evaluation, etc.
		HAF Products and Application Security	Guarantee the security of AI technologies, services and products in specific application scenarios.

Compliance Practice in other Industries: AI Industry

Application Scenarios and Key Compliance Points

Ten Demonstration Application Scenarios

- Smart farms
- Smart ports
- Smart mines
- Smart factories
- Smart home
- Smart education
- Autonomous driving
- Smart diagnosis and treatment
- Smart courts
- Smart supply chains

--Guiding Opinions on Accelerating Innovation in Scenarios to Promote High-level Economic Development through High-level Application of Artificial Intelligence

Key Compliance Points

- Data collection issues
- Data theft prevention issues
- Data intervention and elimination issues

Compliance Practice in other Industries: AI Industry

Application Scenario: Data Compliance for Smart Home as An Example

Smart Home

In view of personalized and intelligent demands for household appliances, diets, accompanying, health management and so on in future family life, it is encouraged to apply cloud-side intelligent decision-making and active services, scenario engines, adaptive perception and other key technologies, strengthen comprehensive demonstration applications including active reminding, intelligent recommendation, health management and intelligent zero operations, and promote the realization of the whole-house integrated intelligence control coverage ranging from single smart product to the whole-house smart product, and from passive control to active learning as well as compatible development of various smart products.

Compliance Practice in other Industries: AI Industry

Application Scenario: Data Compliance for Smart Home as An Example

Smart Home

(I) Data Collection

- In scenarios where speech sounds and semantic recognition are required, data collection shall comply with the scope of users' authorization and should not exceed the authorized scope;
- Excessive collection of data shall be avoided, and the type of personal data collected shall be directly related to the realization of the business functions of the products or services;
- When it is necessary to collect users' facial recognition data, fingerprint data and other personal biometric information, the requirements in the Information Security Technology - Personal Information Security Specification shall be followed, and the data shall be collected and used at the front end only, and the data shall be anonymized in the back-end storage.

Compliance Practice in other Industries: AI Industry

Application Scenario: Data Compliance for Smart Home as An Example

Smart Home

(II) Data Storage

- Data collected in smart home scenarios are mostly stored in the cloud, and it is important to pay attention to whether the cloud system is located within the territory of PR China. The storage period shall follow the principle of the shortest storage period ;
- Good technical support measures shall be adopted, including encrypted storage, physical separation, control of access authority, etc.;
- For sensitive personal information such as facial recognition and fingerprint information, desensitization measures shall be taken to anonymize or de-identify such information, and the relevant personal data shall be deleted upon the expiry of the storage period.

Compliance Practice in other Industries: AI Industry

Application scenario: data compliance for Smart Home as an example

Smart Home

(III) Data Sharing

- With respect to data sharing, it is important to pay attention to the data protection capability of the entrusted third party and the security and compliance issues in data processing;
- With respect to the compliance requirements of cross-border data transfer, it is important to pay attention to the different obligations of an enterprise as different types of data processing subject, and the enterprise shall comply with relevant national regulations and standards on cross-border data transfer;
- Necessary technical measures and security measures shall be adopted to ensure the security of the data transfer process and avoid the risk of data leakage.

Compliance Practice in other Industries: Autonomous Driving

Legal System of Autonomous Driving Industry - Current Laws and Regulations

- Several Provisions on the Management of Autonomous Driving Data Security (for Trial Implementation)
- Information Security Technology - Connected Vehicle —Security Requirements of Data (Draft)
- Information Security Technology —Security Requirements of Vehicle Collected Data (Draft)
- Notice on Strengthening the Production, Test, Application and Management of Maps for Autonomous Driving
- Notice of the Ministry of Industry and Information Technology on Strengthening the Cybersecurity and Data Security of the Internet of Vehicles
- Opinions of the Ministry of Industry and Information Technology on Strengthening the Administration of the Access of Intelligent Connected Vehicle Manufacturers and Products

Compliance Practice in other Industries: Autonomous Driving

Laws Coming into Effect

- *Information Security Technology - Connected Vehicle —-Security Requirements of Data*

Items	Content
Application Scope	a. The design, production, sales, use, operation and maintenance of automobiles by **automobile manufacturers**; b. The supervision, administration and assessment on the vehicle data collection and processing activities by **the regulatory authorities** and/or **the third-party assessment institutions**.
Classification of the Data Collected by Vehicles	• Off-vehicle Data • Cockpit Data • Operation Data • Location Trajectory Data
Requirements	On **transferring**, **storage**, **outbound transfer** and other aspects

- *Information Security Technology —Security Requirements of Vehicle Collected Data*

Items	Content
Basic Requirements	**Data processing activities that are unrelated to** vehicle administration and driving safety **shall not be carried out** based on data collected by and processed by network-connected vehicles.
Requirements on the Data of the Vehicles	On **transferring**, **storage**, **outbound transfer** and other aspects

Compliance Practice in other Industries: Autonomous Driving

Data Classification in the Automobile Industry

Automobile Data	• Includes personal information data and important data involved in the design, manufacturing, sales, use, operation and maintenance of the automobiles.
Processing of Automobile Data	• Includes the collection, storage, using, processing, transferring, provision and publication of Automobile Data
Processor of Automobile Data	• Refers to organizations carrying out Automobile Data processing activities, including automobile manufacturers, components and software suppliers, distributors, maintenance agencies and travel service providers, etc.
Personal Information	• Refers to all kinds of information related to the identified or identifiable vehicle owners, drivers, passengers and persons outside vehicles recorded by electronic or other means, excluding the information that has been anonymized.
Sensitive Personal Information	• Refers to the personal information that, once disclosed or illegally used, may lead to discrimination or serious harm to the personal and property safety of the owners, drivers, passengers and persons outside the vehicles, including vehicle whereabouts and tracks, audio, video, images and biometric features, etc.
Important Data	• Refers to the data that may endanger national security, public interests or the legitimate rights and interests of individuals or organizations once they are tampered with, damaged, disclosed, illegally obtained or illegally used, including: (I) geographic information, passenger flow, vehicle flow and other data of important sensitive areas such as military administrative zones, entities of science, technology and industry for national defense, and Party and government organs at the county level or above; (II) data reflecting economic operation such as vehicle flow, logistics, etc.; (III) operational data of the automobile electricity charging network; (IV) video and image data outside the vehicles that contain face information, license plate information, etc.; (V) the personal information of more than 100,000 persons as the subjects of personal information is involved; and (VI) other data that may endanger national security, public interests or the legitimate rights and interests of individuals or organizations as determined by the Cyberspace Administration of China ("CAC") and the authorities of development and reform, industry and information technology, public security and transport, etc., under the State Council

Compliance Practice in other Industries: Autonomous Driving

Different Processing Requirements Depending on the Data Processed

<table>
<tr><th>Automobile Data</th><th>Classification</th><th colspan="4">Requirements</th></tr>
<tr><td rowspan="3">Personal Information Data</td><td>Personal Information</td><td colspan="4">The Processor shall inform and obtain consent regarding: (I) types of personal information processed; (II)specific collection scenario and collection ceasing method; (III) purposes, use and methods of processing; (IV) storage place, period and rules for determining them; (V) how to consult, copy and delete data….</td></tr>
<tr><td>Sensitive Personal Information</td><td colspan="4">• The processing shall meet the following requirements: (I) directly serving the individuals, including enhancing driving safety, intelligent driving and navigation, etc.; (II) efficiently informing the necessity and impact on individuals; (III) obtaining the individual's consent; (IV) reminding the collection status; and (V) upon request, deleting Personal Information within ten working days after receiving the request.
• Only for the purpose and sufficient necessity of enhancing driving safety may a Processor collect biometric information such as fingerprints, voice prints, faces and heart rhythm</td></tr>
<tr><td></td><td>Data Processing</td><td>Outbound Transferring</td><td>Reporting</td><td>Assessment</td></tr>
<tr><td>Important Data</td><td>Important Data</td><td>Conduct risk assessment and submit a risk assessment report to the relevant authorities.</td><td>Go through the Security Assessment conducted by the authorities.</td><td>Annually report to the relevant authorities the information on Automobile Data security management.</td><td>Assessment authorities are: the CAC, relevant authorities of development and reform, industry and information technology, public security, transportation and so on under the State Council.</td></tr>
</table>

Compliance Practice in other Industries: Autonomous Driving

Principles on the Processing of Automobile Data

- In-car processing, unless it is really necessary to provide outside the car
- Non-collection by default: the default is set to the non-collection status every time driving unless the driver sets it independently
- The application of accuracy scope, i.e. the coverage scope and resolution of the camera and radar, etc., shall be determined according to the data accuracy requirements of the provided functional services
- Desensitization, i.e. anonymization and de-identification shall be conducted as much as possible

Compliance Practice in other Industries: Autonomous Driving

Requirements on the transferring, storage and cross-boarder transferring of Automobile Data

-- National Standard*: Information Security Technology —Security Requirements of Vehicle Collected Data* (Not Yet in Force)

- **Transfer Requirements**

✓ Without the individual's consent, other than anonymized data of video and image, the motor vehicles shall not transfer off-vehicle data that contains personal information through network.

✓ The motor vehicle shall not transfer cockpit data through network

✓ The circumstances satisfying the following requirements may serve as the exceptions of the above situations:

a) Where the anonymization processing operation needs to be executed in real time through a remote platform in order to realize the above-described anonymization processing function.

b) Where the cockpit data needs to be processed in real time through a remote platform in order to realize functions that directly serve the needs of the driver or an occupant, such as speech recognition, etc.

c) Where the data has to be transferred or stored in cloud given that the user has to remotely monitor the inside and outside of the vehicles or to use the cloud storage to store data, etc.

d) Where data transferring is required by the authorities under legal circumstances, e.g., in a traffic accident.

- **Storage Requirement**

✓ The off-vehicle data and position and track data shall be stored in the remote platform and other external locations for no more than fourteen (14) days.

✓ The data satisfying the following requirements may serve as the exceptions of the above situations:

a) Specific scenario data stored to optimize driving safety functions.

b) Where the data is stored remotely by the user when using functions that directly serve the user, e.g., cloud storage service.

c) The data collected by the special collection vehicle for collecting training data or the special test vehicle driven in the specific area

d) Data stored by vehicles using new energy, road transport vehicles and taxis subject to online booking system in accordance with relevant administrative requirements.

e) Location trajectory data generated for vehicles used in the production and operation and are controllable by production operators

- **Cross-boarder Transfer Requirements**

✓ The off-vehicle data, cockpit data and location trajectory data shall not be transferred abroad. The operation data, where necessary, may be transferred abroad after going through the Security Assessment for Outbound Data Transfers.

Compliance Practice in other Industries: Autonomous Driving

Limitation for Foreign Investors to Engage in Research on Autonomous Driving

Surveying and Mapping Law

- **Definition for Surveying and Mapping**

Surveying and mapping include the activities conducted to determine, collect and formulate the key elements of physical geography or the shapes, sizes, space positions, attributes, etc. of man-made surface installations, as well as to process and provide the data, information and results gained therefrom.

- **Limitation to conduct Surveying and Mapping**

Foreign organizations or individuals that wish to conduct surveying and mapping in the territory under the jurisdiction of China shall be subject to **approval by the competent departments**.

Foreign organizations or individuals that wish to conduct surveying and mapping in the territory under the jurisdiction of China shall **cooperate with the relevant departments or entities** of China and such surveying and mapping **may not** involve State secrets or jeopardize state security.

- **Penalty**

Where any foreign organization or individual, in violation of the provisions of the law and **without approval or without cooperation with the relevant department or entity of China**, engages in surveying and mapping activities, the organization or individual shall be ordered to desist from the violation; its/his unlawful gains, surveying and mapping results and tools shall be confiscated, and it/he shall be fined not less than 100,000 yuan but not more than 500,000 yuan; if the circumstances are serious, it/he shall be fined not less than 500,000 yuan but not more than one million yuan and shall be ordered to leave the country within a specified time limit or expelled from the country; and if a crime is constituted, it/he shall be investigated for criminal liability in accordance with the law.

Special Administrative Measures (Negative List) for Foreign Investment Access (Edition 2021)

- **NO.21**

It is prohibited to invest in: geodetic surveying, marine surveying and mapping, aerial photography for surveying and mapping, ground moving surveying and mapping, surveying and mapping of administrative boundaries, preparation of topographic maps, world administrative maps, national administrative maps, administrative maps at or below the provincial level, national teaching maps, local teaching maps, true three-dimensional maps and electronic navigation maps, regional geological mapping, mineral geology, geophysics, geochemistry, hydrogeology, environmental geology, geological disasters, geological remote sensing and other surveys (mining right holders which carry out work within the scope of their mining rights are not subject to this special administrative measure).

Compliance Practice in other Industries: Autonomous Driving

Limitation for Foreign Investors to Engage in Research on Autonomous Driving

- *Notice on Strengthening the Production, Test, Application and Management of Autopilot Maps*

- Article 2

Without the approval of the administrative authorities of surveying, mapping and geoinformation at or above the provincial level, map data may not be provided to or shared with foreign organizations and individuals as well as wholly foreign-owned enterprises, Sino-foreign equity or contractual joint ventures registered in China.

- *Information Security Technology - Connected Vehicle —-Security Requirements of Data (Draft)*

- Article 7.1

Data on roads, buildings, terrain, traffic participants, etc., collected by network-connected vehicles from the external environment through cameras, radars and other sensors, as well as data relating to vehicle location and tracks, shall not be transferred abroad. Outbound transfer of network-connected vehicles' driving status parameters, abnormal warning information and other data shall comply with the relevant provisions.

Q&A

THANK YOU!