ZTE

Deloitte.

White Paper on Compliance Governance of Cross-Border Data Flows

2021

Preface

Digital economy is speeding up the transformation and integration of industries, further boosting economic growth. During the rapid development of the digital economy, data flows are playing an increasingly important role. Accordingly, many countries have promoted market-based allocation of data resources when formulating macro strategies. To balance "data security" and "data dividends", and build advantages in the era of digital economy, major countries and regions have been stepping up efforts in optimizing their own rules for cross-border data flows, and facilitating the formulation of global rules. As a result, various compliance policies for cross-border data flows have been developed around the globe.

Under the global regulatory framework, no enterprises can ignore the profound impact brought by the rules for data flows. Enterprises should attach great importance to the current situation and development trend of cross-border data flows, and adhere to compliance regulations proactively in global business activities to reduce risks and address uncertainties. In addition, a mechanism for risk management has become a priority of enterprises.

In this context, risk-oriented compliance governance is key to addressing the challenges posed by global rules for cross-border data flows. To ensure business sustainability, equal attention should be paid to compliance management and the pursuit of profits. Specifically, systematic reforms should be carried out in compliance management on the basis of enhanced cross-border data governance, thus preventing risks in a proactive way. In addition, the OPEX of enterprises can be reduced by leveraging the unified compliance control baselines and inclusive bilateral and multilateral rules. In a new digital world, enterprises should work together to explore compliance governance of cross-border data flows, learn from the best practices, and make continuous efforts in compliance building, to enhance data compliance systems and jointly build an ecosystem for industrial digitalization.

Spencer Shen
Chief Legal Officer
ZTE Corporation

Content

White Paper on Compliance Governance of Cross-Border Data Flows

(2021)

1. Global Rules for Cross-Border Data Flows and Development Trend

1.1 Global Rules for Cross-Border Data Flows

The rules for cross-border data flows depend on the policy preference for data security. The existing rules are broadly divided into two categories:

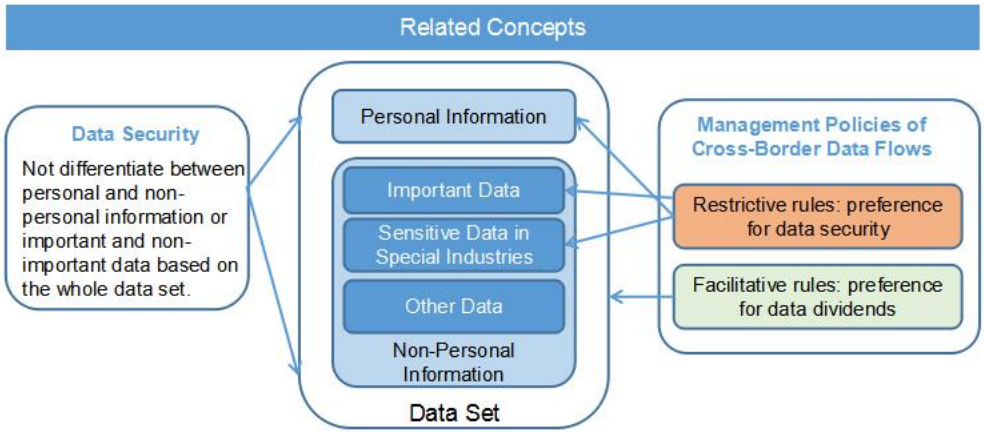
Restrictive rules are often used by a country or region to restrict the export of important data or personal information in order to maintain data security or data sovereignty, indicating a preference for data security.

Facilitative rules are bilateral/multilateral international agreements or treaty frameworks established by bilateral, multilateral, or international organizations to facilitate secure and frictionless cross-border data flows and maximize the value of data, indicating a preference for data dividends.

For data subjects, the data that are subject to restrictive rules are generally personal information, important data, or sensitive data in special industries. The types of the data are not clearly defined in the facilitative rules.

For enterprises, both restrictive and facilitative rules are of practical significance, while the restrictive rules, mainly adopted by major countries, will become the focus. In accordance with the restrictive rules, enterprises strictly implement the compliance governance and the management and control over data exports to avoid any violations to the maximum extent. Furthermore, while ensuring effective compliance management and control, enterprises can take advantage of the flexibility of facilitative rules to reduce the pressure and cost of control over cross-border data flows.

Note: The facilitative rules are "non-mandatory" and only binding on "the parties involved in the formulation of the rules."



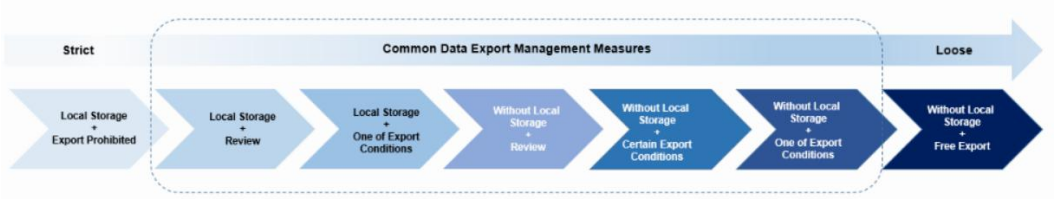
1.1.1 Restrictive Rules in Major Countries

Restrictive rules of data exports are applied by a country/region with varying degrees of strictness in accordance with the local legal system, history and traditions, and risk appetite. So far, no country/region has completely prohibited or allowed data exports.

Most of the countries/regions are in between. For example, by valuing both national security and digital dividends, India and Russia promote the development of digital economy while implementing data localization measures; By placing equal emphasis on market freedom and digital rules, the European Union (EU) and Singapore advocate free flows of data across borders while establishing diversified data export mechanisms.

Refer to Appendix 1 *Major Modes of Global Restrictions on Cross-Border Data Flows.*

1.1.2 Facilitative Rules by International Organizations



International organizations proactively develop rule frameworks for cross-border data flows, to facilitate the orderly and frictionless flows of data across countries/regions and make the most of digital data. Such international organizations as the Organization for Economic Cooperation and Development (OECD) and the Asia-Pacific Economic Cooperation (APEC) have established a number of principles and representative frameworks for cross-border data flows.

International organizations are open to cross-border data flows among member countries and aim to further enhance the efficiency of data flows within the organizations through unimpeded channels, while being cautious about cross-border data flows outside the organizations. At present, the European *General Data Protection Regulation* (GDPR) provides the only compliance framework for extra-territorial application, and has been promoted in a continuous and substantial manner worldwide, bringing a significant impact on the relevant rules in many countries/regions around the world.

Refer to Appendix 2 *Frameworks of International Organizations for Cross-Border Data Flows.*

1.1.3 Differentiated and Tiered Management in China

China has been continuously enhancing its laws and regulations on cross-border data flows. With the publication of the *Cybersecurity Law of the People's Republic of China*, *Data Security Law of the People's Republic of China*, and *Personal Information Protection Law of the People's Republic of China*, the legal framework of data protection has been formed in China. The rule system of data protection has been built based on the issued normative documents and national standards.

China adopts tiered management as evidenced by its rule system for cross-border data flows, and makes a differentiated design for the compliance control of important data and personal information. Specifically, for the specific types of data in particular industries, the requirements for data localization are clearly defined; The large number of personal

information and important data shall be stored in China and can be exported after being reviewed by supervisory authorities; For the export of general personal information, various compliance measures such as standard contract signing and security certification are formulated.

Refer to Appendix 3 *Regulations on Cross-Border Data Flows of Special Industries in China* and Appendix 4 *List of Global Laws and Regulations on Cross-Border Data Flows.*

1.2 Development Trend of Cross-Border Data Flows

1.2.1 Category- and Class-Based Data Management Becoming the Mainstream

Different types of data, such as personal information, important data, and core data, involve different legal risks, thus requiring different protection measures. Major countries have tried to supervise data flows by category and class, shaping different control policies with varying degrees of strictness.

1.2.2 Exploration of Unified Regulations on Cross-Border Data Flows

With the increasing cross-border data flows, various countries and regions have tried to incorporate the governance of cross-border data flows into the international trade rules. The existing international data governance framework hardly meets the characteristics and needs of global data governance. It is necessary to establish a new governance structure for the new digital world dominated by intangible assets to maximize the value of data.

1.2.3 Continuous Impact of Long-Arm Jurisdiction on Data Sovereignty

The long-arm jurisdiction allows local courts to exercise jurisdiction in another country in which the data are located, which will have a great impact on the implementation of data protection laws in the country and the principles of judicial application. Furthermore, the long-arm jurisdiction has a far-reaching impact on the global data security and compliance framework, and greatly changes the rules for data sovereignty globally.

1.3 Types of Cross-Border Data Flows

Currently, there are still differences in the definition of cross-border data flows. The cross-border data flows are generally understood as "the act of transferring data from one jurisdiction to another" or "the processing of machine-readable data stored in computers across national borders." Based on the "contact with overseas entities", cross-border data flows are mainly divided into two types:

Type I: the transmission and transfers of data across national borders.

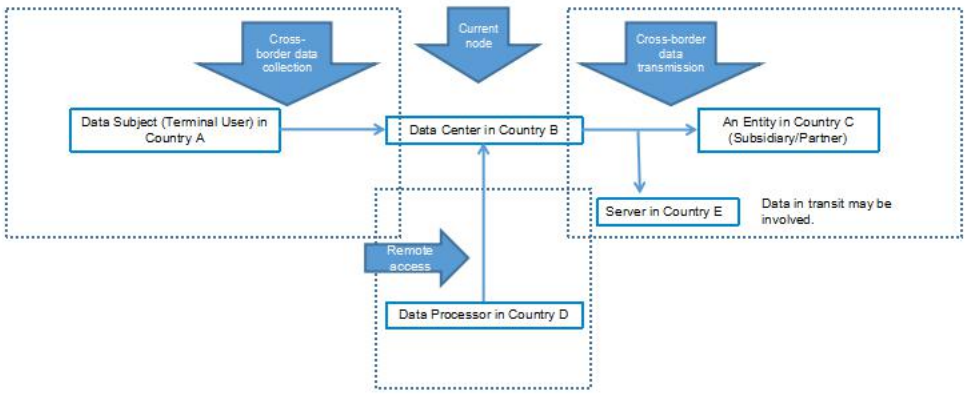
Type II: the access of data by overseas entities although the data have not been transferred across national borders.

One particular case is the direct collection of data across the borders, that is, the data are collected directly from the data subject in country A to the data center in country B, and are not stored in country A. As it is difficult to deploy servers globally in practice, there is a great a great amount of data collected across borders.

Concept	Definition	Scenario	Example
Cross-Border Data Flows	Any act of transferring data to another jurisdiction, or re-transferring after data are transferred to another jurisdiction.	**1. Cross-border data transmission** The recipient of the data receives the data from other jurisdictions on the basis of the contract or other basis.	A subsidiary of a multinational enterprise transmits data through the internal system to the headquarters located in another jurisdiction.
		*Cross-border data collection Cross-border collection is a special case of cross-border data transmission: Based on certain needs, the data collector collects the data directly from	An employee of a multinational enterprise fills in personal information in the internal system, whose server is not within the

Concept	Definition	Scenario	Example
		the jurisdiction in which the data subject is located to another jurisdiction in which the data processor is located, without any processing behavior in the jurisdiction of the data subject.	jurisdiction in which the employee is located.
		2. Cross-border data access Based on certain needs, the accessing party of the data accesses the system server located in another jurisdiction, reads some or all the data in its database, and performs certain automated processing actions.	A multinational enterprise provides remote operation and maintenance services in China for customers located in the EU.

Cross-Border Data Flow



1.4 Data Localization Models

Data localization is a measure of cross-border data management, to restrict data exports by a country/region through the formulation of rules or legal requirements.

Data localization requires the data server to be located within the jurisdiction where the data are stored or processed. So far, a number of countries/regions have put forward data localization requirements with varying degrees of strictness as shown in the table below.

Model	Specific Situation	Representative Country	Type of Data Involved
No localization requirements, but restrictions on data exports	Compliant data flows are permitted in principle.	the EU, Japan	General personal information
Local storage of copies, and no restrictions on data transfers or exports	Only data copies are required to be stored on the device that is physically present within the borders, and there are no restrictions on transfers or processing of data copies outside the borders, so that the regulatory requirements can be met.	India (2018 draft *Personal Data Protection Bill*)	General personal information
Local storage, and data processing allowed	The data shall be stored within the borders. The	Russia	General personal information

outside the borders	data can be transmitted and processed outside the borders if the export requirements are met.		
Local storage and processing	The data can only be stored and processed within the borders, and can only be exported after the required approval is obtained under certain conditions (such as national security requirements).	the U.S, Turkey, Australia	Special types of non-personal information/important data

Data localization requirements are usually implemented with degrees of restrictiveness based on the following classification:

(1) Data types: Different protection requirements are proposed for different data types. The most common types of data that are subject to localization requirements are biological health, finance, and credit information.

Example: The Government of India divides the data into key personal information, sensitive personal information, and general personal information. The key personal information shall be stored in India, with several exceptions. For sensitive personal information, it must be stored in India, but its copy can be transmitted outside India in accordance with the regulations on cross-border data flows.

(2) Data collectors: Different local storage requirements are put forward for different data collectors.

Example: The Government of Indonesia requires that only public electronic system operators place their electronic systems and data in Indonesia. The U.S. Department of Defense stipulates that all cloud computing service providers serving this department store data in the U.S., and the U.S. Internal Revenue Service requires that the servers of tax information systems should be located within the U.S.

2. Typical Scenarios and Key Control Points (KCPs) of Cross-Border Data Flows for Enterprises

2.1 Main Pain Points of Cross-Border Data Flow Compliance

With the development of economic globalization and digitalization, enterprises are facing stricter supervision of cross-border data flows. To address the pain points of cross-border data flow compliance has become the focus of data compliance governance.

2.1.1 Data Variety and Difficulties in Identifying Legal Attributes and Classifying Data

Data Variety: In the era of big data, the data generated in the enterprises' production and operation processes have been growing explosively with various data types. Based on data subjects, data are divided into customer data, user data, partner data, supplier data, internal staff data, etc. Based on business operations, data are divided into product data, daily operation data, R&D data, internal affairs management data, etc. As a result, the difficulties in and cost of data management for enterprises are greatly increased.

Difficulty in identifying legal attributes: The personal information and important data are usually defined by supervisory authorities in a "general" manner, which provides a certain degree of flexibility for enterprises, but also brings ambiguity and uncertainty to identify the legal attributes of data. Different jurisdictions have different or even conflicting definitions of personal information and important data, which makes it difficult for enterprises to identify the legal attributes and apply control.

Example: If a mobile phone manufacturer in China collaborates with a telecommunications operator in the EU, the Chinese manufacturer may encounter difficulties in data compliance. The operator in the EU requires the Chinese manufacturer to provide the identifiers like International Mobile Equipment Identity (IMEI) numbers of its mobile phones, so as to guarantee the use of the devices. As the hardware identifiers like IMEI numbers are personal information in accordance with the Chinese regulations, the Chinese manufacturer requests the telecommunications operator to sign the *Data Processing Agreement* (DPA). However, as the operator only obtains the IMEI numbers of the devices, the operator is unable to identify the specific users of the devices through such identifiers. In accordance with the EU laws, the IMEI number is not personal information for its nonidentifiability. As a result, the operator may refuse to sign the DPA.

Difficulty in classifying data: Multiple types of unstructured data may be carried by the same carrier or distributed in different carriers, so it is difficult to split, merge, and accurately identify such data. Enterprises face the challenges of classifying the unstructured data based on data source, content, and use, to ensure compliance control of cross-border data flows.

Example: The internal document management platform of a company stores a large number of documents including project and business materials, business contracts, financial documents, etc. The business materials may involve important data of other countries if the information on the traffic network, energy nodes, and sensitive locations of other countries is contained. The business contracts may contain personal information of the legal entities. The financial documents may involve sensitive personal information. However, as the volume of data is large and the data are unstructured, it is difficult to accurately identify each data type.

2.1.2 Diverse Business Scenarios, Complex Data Flow Routes, and Different Legal Definitions of Data Processing Roles

Diverse business scenarios: During the development of enterprises, their business landscape and fields are continuously expanding or changing, and the supporting processes are also refined accordingly. With the interaction of the business scenarios, the business data are converged as well, which increases the difficulty in identifying the data flow routes and relevant responsible parties.

Example: A large enterprise may have many business sectors, involving a large number of data processing activities: The financial sector involves banking, insurance, securities, etc.; the non-financial sector involves system product development, supply chain management, marketing, etc.; and the functional sector involves human resources, financial management, administrative management, legal and compliance, internal control and audit, etc.

Complex data flow routes: In the context of digital transformation, the business data of the enterprises are often processed and transmitted through the business systems. Meanwhile, because of the cost and efficiency, the system servers of the enterprises are usually deployed and managed in a centralized manner, which leads to the frequent and complex cross-border data flows during the global business development.

Example: The system servers of an enterprise are deployed and managed at the location of its headquarters, leading to a large number of cross-border data flows during the business activities overseas. For example, the data are transmitted from the overseas branch office to the server located in the headquarters; The overseas branch office fetches data from the server, and directly accesses the server. If multiple overseas branches are within the scope of control over cross-border data flows, the data may also be transferred/accessed between the branches through the server located in the headquarters.

Different legal definitions of data processing roles: As data processors and data controllers have different responsibilities and obligations, it is important to accurately identify the responsibilities and obligations of the two data processing roles, and the roles of enterprises. The definitions, responsibilities, and obligations of data processing roles vary

from different jurisdictions. Faced with complex data flows, enterprises may have difficulty in accurately identifying their roles, responsibilities, and obligations, affecting the compliance control of cross-border data flows.

Example: The GDPR specifies responsibilities of the controller and processor of personal data, while the *Personal Information Protection Law of the People's Republic of China* does not distinguish between the roles of the data controller and data processor which are collectively referred to as "personal information processors." The *Personal Information Protection Law of the People's Republic of China* stipulates that "Where personal information processors jointly processing personal information infringe the rights and interests on the personal information and cause damages, they shall be jointly liable in accordance with law."

2.1.3 Differentiated Regulations, Conflicts of Laws Across Different Jurisdictions, and Dynamic Change of Rules

Differentiated regulations around the world: A consistent governance framework for cross-border data flows has not been established globally. Considering national security, data sovereignty, human rights protection, geopolitics, and trade modes, many countries/regions have formulated their own regulations on cross-border data flows with different priorities, leading to great differences in data governance and cross-border data flow policies. Also, the countries/regions have been actively expanding their respective data ecosystems, making it more difficult for enterprises to research and comply with the rules for cross-border data flows.

Conflicts of laws across different jurisdictions: When conducting activities involving cross-border data flows, enterprises need to take into account the laws of the place to which the data are exported, and the place from which the data are imported. However, the varying laws of cross-border data flows in different jurisdictions make it difficult for enterprises to ensure compliance across multiple jurisdictions. Because of the long-arm jurisdiction or other factors, the data processing activities in one jurisdiction may also need to comply with the laws of multiple jurisdictions, which may lead to potential legal conflicts and pose higher requirements for enterprises' capabilities in the governance of cross-border data flows.

Example: The legal basis that is required for data processing varies in each jurisdiction. The processing of European citizens' data in China shall meet the *Personal Information Protection Law of the People's Republic of China* and the GDPR. In order to avoid overly broad interpretation, the legal basis of "interests of a data subject" and "legitimate interests of a controller," which are difficult to distinguish, is not included in the scope of the articles in the *Personal Information Protection Law of the People's Republic of China*. If data processing is conducted on the basis of "legitimate interests" in China, the activity may violate the laws because of the lack of a legally recognized basis.

Dynamic change of rules: Since the official release of the GDPR, the legislation and update of privacy and data protection laws have been promoted worldwide, and the importance of data protection has been widely recognized in various countries and regions. The rules for cross-border data flows based on civil rights, national security, data sovereignty, and other factors tend to be more detailed and concrete, further increasing the cost of designing, implementing, and maintaining the enterprises' compliance systems for cross-border data flows.

Example: The GDPR specifies that "Where possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data." Two years later, Spain released the *Guidelines for Data Protection by Default*, which provided detailed configuration requirements for the "privacy panel". Even if it is not mandatory, it has great value for reference. Spain, as a member of the EU, has taken the lead in giving the user control over the configuration options, which will influence the progress of other countries in refining their regulations, significantly increasing the cost of corporate compliance.

Refer to Appendix 5 *List of Global Management and Control Requirements for Cross-Border Data Flows* and Appendix 7 *Contact Information of Major Global Supervisory Authorities.*

2.2 KCPs of Typical Scenarios of Cross-Border Data Flows

2.2.1 Typical Scenarios of Cross-Border Data Flows

Based on the common business activities of enterprises and the basic models of cross-border data flows, several typical scenarios are involved.

(1) Cross-border data flows in corporate management: In the daily operations and management activities of a multinational enterprise, the headquarters needs to adopt centralized management of its branches' data; Also, the branches need to obtain data from the headquarters. The flows of large volume of data across borders become a necessary and frequent activity during the enterprise's operations. Common scenarios of cross-border data flows include:

Business Scenario	Scenario of Cross-Border Data Flows	Relevant Field
Supplier management	For supplier management, the enterprise needs to collect related personal information of its global suppliers and enter the information into the supplier management system at headquarters for maintenance.	Name, position, telephone number, fax number, email address, financial account, and other information of suppliers', contact persons and senior management
Procurement management	To negotiate procurement matters and fulfil the obligations under a contract, the enterprise collects the personal information of relevant contact persons worldwide and transmits it to the headquarters' procurement department for management and use.	Name, nationality, address, zip code, contact, and other information of customer contact persons
Financial management	The headquarters of the enterprise uniformly manages the remunerations, reimbursement, and tax declaration of employees of overseas subsidiaries. The cross-border data transmission involves employee account information and reimbursement documents.	Employee account information, salary, reimbursement documents, tax documents, and other information
Human resource management	For unified human resource management including recruitment, the enterprise needs to upload the personal information of the overseas employees or candidates to the headquarters.	1) Employee information including name, telephone number, position, education background, work performance, and salary and benefits 2) Candidate information including name, telephone number, qualification certificate, education background, and work experience
Document management	To facilitate the sharing and management of internal documents, the enterprise usually establishes a global document management platform.	Personal information that may be contained in the internal documents, including enterprise internal systems and regulations, contracts, and process documents

(2) Cross-border data flows in business activities: The enterprises' business activities also involve a large amount of cross-border data flows. To expand overseas

markets, the enterprises need to deal with massive cross-border flows of data generated from product sales, brand promotion, and aftersales maintenance. Furthermore, the cross-border data flow routes become more complex as enterprises deploy their supply chains globally to save costs. Common scenarios of cross-border data flows include:

Business Scenario	Scenario of Cross-Border Data Flows	Relevant Field
Supply chain	The enterprise collects the personal information of suppliers, consignees, contact persons of warehouses, and other related personnel from supplier sourcing, international freight, and warehousing, and uploads the information to the supplier department of the headquarters for management and use.	Name, nationality, contact information, and address of the suppliers, consignees, and contact persons of warehouses
Marketing and sales	The enterprise needs to collect, use, and maintain customer information for research on global markets and customer relationship maintenance.	Personal information of customers/potential customers, including name, telephone number, and email address
Remote operation and maintenance	The enterprise accesses the system network of the overseas customer remotely to conduct the technical support, troubleshooting, and so on, which involves the processing of customer personal information.	Customers' phone number, International Mobile Subscriber Identity (IMSI), IP address, call record, etc.
E-commerce platform	The e-commerce platform is generally operated and maintained by the headquarters or the third party. When the enterprise conducts online product sales business globally, the headquarters needs to process the information of user orders and logistics on the e-commerce platform.	Platform users' name, telephone number, order information, shipping addresses, etc.
Brand management	When conducting brand promotion and exhibition activities abroad, the enterprise collects the personal information of the participants and transmits it to the place where the organizers are located.	Personal information of participants, including name, gender, nationality, telephone number, email address, and other information

2.2.2 KCPs of Cross-Border Data Flows

The scenarios of cross-border data flows for each enterprise are different, and the rules for cross-border data flows in each jurisdiction are not scenario-oriented. Usually, the unified baselines are specified for the compliance control. As each scenario may bring different risks, the focus may be different when the unified compliance control baselines are incorporated into specific business activities. For the enterprises, the compliance control landscape generally consists of two parts:

First, the compliance control baselines for all business activities, which are built based on the classification of the rules in each jurisdiction.

Second, the special KCPs, which are set up for special scenarios.

(1) General compliance KCPs

Refer to the KCPs of cross-border data flows that are formulated based on the laws and regulations and relevant industry standards.

- Assessment before cross-border data flows
- Execution during cross-border data flows
- Management after cross-border data flows

Scope of Application	Stage	Compliance KCP
	Assessment	1.1 Sorting of data fields
		1.2 Identification of cross-border data flows routes

Scope of Application	Stage	Compliance KCP
Compliance KCPs for Cross-Border Data Flows	Assessment before cross-border data flows	1.3 Data recipient identification and compliance capability assessment
		1.4 Legitimacy and necessity assessment on the purpose of cross-border data flows
		1.5 Minimization assessment on data fields
		1.6 Screening and interception of special data (national secrets, core data, personal information, etc.)
		1.7 Agreement on the obligations to protect data security between data sender and overseas recipient
		1.8 Review by internal relevant parties of the enterprise
		1.9 Report to/Authorized by supervisory authorities
		1.10 Training for related personnel
	Execution during cross-border data flows	2.1 Strengthened mechanism for the protection of cross-border data flows (signing of the *Data Transfer Contract* (DTC), privacy notice, etc.)
		2.2 Guaranteeing of data transmission safety
		2.3 Recording of data processing activities
		2.4 Strict control over access permissions
		2.5 Monitoring and prevention of data breaches
		2.6 Safeguarding of response to Data Subject Rights (DSRs) requests
	Management after cross-border data flows	3.1 Timely deletion/destruction of data in time after the purpose is achieved
		3.2 Compliance re-assessment if beyond the scope of the specified purpose
		3.3 Compliance audit on cross-border data flows

(2) Compliance KCPs in special scenarios

Refer to the KCPs that are set up for special scenarios, facilitating the formulation of scenario-oriented control measures.

Example: The overseas branch office needs to transmit the customer data to the headquarters for processing when conducting business with the local customer. In order to ensure the legitimacy of cross-border data flows, the overseas branch office signs the DPA with the customer and provides a list of sub-processors, so that the headquarters can participate in the data processing with the specific authorization as the sub-processor. Meanwhile, the overseas branch office signs the DTC with the headquarters to agree on the obligations of both parties in the cross-border data flows.

3. Enterprise Roadmap and Practices of Compliance Governance of Cross-Border Data Flows

3.1 Roadmap of Compliance Governance of Cross-Border Data Flows

With the further development of the digital economy, enterprises are bound to be involved in the global compliance system for cross-border data flows and must rise up to the compliance challenges. Enterprises need to determine the KCPs of compliance governance concerning cross-border data flows by comparing their involvement in cross-border data

flows against external regulation requirements. In addition, enterprises should establish a risk-oriented compliance control mechanism for cross-border data flows, and build an efficient, cost-effective, flexible, and sustainable compliance system that fits the enterprise's characteristics and enables coordination with supervisory authorities.

The roadmap of corporate compliance governance of cross-border data flows includes specifying the scope of data under compliance governance, identifying key business scenarios, understanding external compliance requirements, assessing risks and formulating a risk governance plan, and tracking additional information on the compliance governance of important data.

3.2 Practices of Compliance Governance of Cross-Border Data Flows

3.2.1 Specify the Scope of Data Under Compliance Governance

An enterprise needs to sort out and identify the types of data under compliance governance, including personal information and important data.

(1) Identify personal information

According to the definitions of personal information in the GDPR, and in laws and regulations of China including the *Personal Information Protection Law* and the *Personal Information Security Specification*, "directly or indirectly identifiability" is the fundamental criterion for determining personal information. Examples of directly identifying information are basic identity information such as names and IDs, and biological identity information like fingerprints, voiceprints, iris, and facial features.

The difficulty in identifying personal information lies in the uncertainty of the scope of "indirectly identifying" data, more precisely, the uncertainty of whether such data as equipment data and location data, can be used, in combination with other information, to identify a specific individual. "Indirectly identifying" data are interpreted differently in different jurisdictions.

For example, there is an international controversy about the identifiability of device identifiers. Because device identifiers can be used, in combination with other information, to identify an individual. Therefore, system versions, software versions, and log information are all personal information. But in many scenarios, the above information and other information which are collected in a piece of software are not sufficient for the collector of the information to identify a specific individual.

Therefore, in scenarios involving hardware identifiers or indirectly identifying information, rather than applying the definition rigidly, an enterprise should take the following two points into account to decide whether certain information is personal information.

- For hardware identifiers such as the IMEI and GAID, their relevance to personal identity should be considered. If the processor cannot access other information, the hardware identifier should not be deemed personal information.
- For indirectly identifying information, the data pool managed by the processor should be considered. If the processor cannot identify any individual by combining the information under discussion with other data under its management, the information in question should not be deemed personal information.

(2) Identify important data

Currently, the international community has yet to come to a universal definition on important data. Enterprises need to pay close attention to the issuance and interpretation of the regulatory policies on important data, and adjust compliance strategies accordingly in a timely manner.

- **Laws and regulations in China**

According to the *Cybersecurity Law*, important data refer to the data that, once leaked, may directly affect national security, economic security, and social stability. Examples of such data are undisclosed government information, large-scale demographic information, information on genetic health, geography, and mineral resources.

The *Information Security Technology — Guideline for Identification of Critical Data (Draft)* specifies the features of important data, and divides important data into such types as data on economic operation, population and health, natural resources and environment, science and technology, security protection, application services, and government affairs. The Guideline also puts forward for the first time the basic principles for identifying important data, the identification process, and the description format for important data, providing references for enterprises to sort their own directories of important data.

In the *Measures for Data Security Management in Industry and Information Technology (Trial Implementation)*, it is proposed to categorize data before classifying them, and form and maintain a data classification list. In the Measures, data in the industrial and ICT fields are classified into three levels based on the level of damage to national security, public interests, or legitimate rights and interests of individuals and organizations caused by the tampering, destruction, breaches, or illegal access/use of such data. It is stipulated in the Measures that important data collected and generated in China shall be stored in China in accordance with laws and administrative regulations. If data need to be exported, security evaluation shall be conducted on the export in accordance with laws and regulations. Data can only be exported when data security is ensured, and the tracking of the exported data shall be strengthened. Core data shall not be exported.

- **Laws and regulations in other jurisdictions**

In other countries/regions, though important data have yet to be clearly defined, there are compliance requirements with different degrees of strictness for special data or the data in special industries. For an enterprise, the commercial data generated in daily operations and limited amount of personal information are usually not deemed important data. However, in some special industries, such as the surveying and mapping, exploration, and telecommunications industries, commercial data in daily operations may be deemed important data.

3.2.2 Identify Key Scenarios

Key action 1: Identify scenarios involving cross-border data flows through researches

The identification of scenarios involving cross-border data flows in an enterprise provides a solid factual basis for the enterprise to analyze the gap between external compliance requirements and current internal compliance governance (hereinafter referred to as "the compliance gap") and determine the KCPs for its compliance governance. The following methods are commonly used in internal researches:

- Information collection and personnel interview: Formulate a cross-border element identification form, and send the form to business units to investigate the needs for the cross-border data flows in business activities, and understand the current status of data protection and data flows.
- Regulation, process, and document review: Review the current regulations, processes, privacy notices, and related documents, and understand the current compliance status.
- Onsite inspection and observation: Conduct onsite inspection on the existing processes for cross-border business. Pick a random business scenario or a specific scenario of concern involving cross-border data flows, track the entire process of collecting, transmitting, and receiving data in the scenario, and learn about the compliance control measures and the actual implementation of such measures at each link of the data flow.

Key action 2: Identify the routes of cross-border data flows and develop information collection tools

As cross-border data flows are complicated, information collection tools can be helpful. Forms and data flow diagrams are needed to record and sort out information on cross-border data flows, for example:

- Create a cross-border scenario identification form: Sort out the current internal situation of cross-border data flows based on the information from the forms filled in by business units, including the specific business scenarios, involved departments, forms of documents, specific fields of data, areas of data sources, cross-border data identification, and involved systems. Specify the types of cross-border data flows in each business scenario: cross-border transmission, cross-border access, cross-border collection, and cross-border transit (if any).
- Draw a cross-border data flow diagram: Draw cross-border data flow diagrams based on the scenario identification form, specify the logic and routes of cross-border data flows in each business scenario, including the involved system, location of data subject, and other information on cross-border data flows, and summarize the aforementioned information in a cross-border data flow landscape of the enterprise.

In addition, a mechanism shall be set to update the above tools, review their conformity and practicability, and adjust the tools regularly.

3.2.3 Understand Key Points of External Compliance Requirements

After the above two steps, the enterprise has had a clear understanding of its current condition of cross-border data flows and its compliance needs. On the basis of its business scenarios involving cross-border data flows, the enterprise shall collect and study the compliance requirements of external supervisory authorities to identify the key points of its compliance governance of cross-border data flows.

Key action 1: Identify and study external regulatory rules for cross-border data flows

On the basis of compliant operation, the enterprise can greatly reduce its cost of cross-border O&M by making full use of international rules for cross-border data flows. Through a

research on the regulatory rules in more than 50 countries, ZTE has identified the main structures of the regulatory rules worldwide:

1) Supervision modes: There are usually three measures to manage cross-border data flows, namely data exports prohibited, data exports conditionally allowed, and free data exports. The "data exports conditionally allowed" is the most common measure, and also the focus of the following compliance actions;
2) Core requirements: Data protection decrees all over the world often include core requirements for cross-border data flows in the first paragraph of the corresponding section, including consent, equal/adequate protection, and approval/evaluation. In a jurisdiction, the core requirement is usually one of the above or a combination of two;
3) Adequate protection measures: Protection conditions prevail in countries with equal protection as the core condition. In some countries, the measures of adequate protection have been specified in such forms as Standard Contractual Clauses (SCCs) and corporate rules. In other countries where the measures have not been specified, enterprises may adopt best practices to meet the requirements of adequate protection;
4) Conditions for derogations: If certain conditions are met, derogations may apply, and the obligation of adequate protection may be exempted. However, some countries have not stipulated any conditions for derogations, such as China.

Take the EU as an example, its rules on cross-border data flows can be interpreted as follows:
1) The core requirements of cross-border data flows in the GDPR: equal/adequate protection;
2) The GDPR allows for diversified forms of fulfilling the conditions for adequate protection and provides SCCs for cross-border data flows;
3) The GDPR also stipulates the conditions for derogations, including consent. Only with a clear understanding of the rationale behind the regulatory rules around the world, can an enterprise form an explicit interpretation on the application of the rules from different levels of supervisory authorities.

For example, Russia's core requirements for cross-border data flows are equal/adequate protection; However, Russia provides only one form of adequate protection measures, that is white lists. In practice, if an enterprise is to transmit data to a country not included in any white lists of Russian supervisory authorities, it must meet the conditions for a derogation.

Key action 2: Classify risk levels of cross-border data flows in each jurisdiction

The strictness of the rules varies among countries/regions. Therefore, the difficulties in the control implementation and the compliance risks facing enterprises differ among countries/regions.

1) In some countries, such as Egypt and Russia, data exports are allowed only if the data are exported to countries deemed to provide adequate protection, or if the export is approved by corresponding supervisory authorities. In Zambia, data exports are allowed only when the SCCs are registered in supervisory authorities, that is the involvement of supervisory authorities, which makes it difficult for an enterprise to meet compliance requirements.
2) In other countries, a wide range of compliance conditions are stipulated for data exports, which include the conditions not involving supervisory authorities. Enterprises can choose which conditions to meet, which means the difficulty in meeting compliance requirements is relatively low.
3) Compliance measures taken in countries of the same risk level are generally the same.

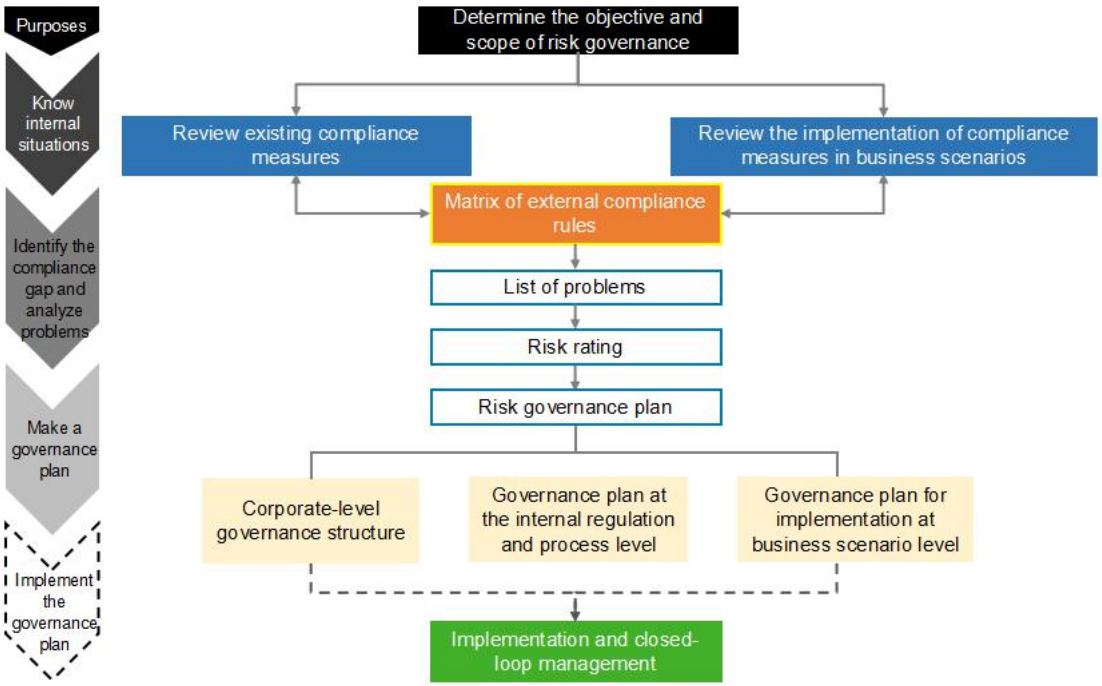
Given the above considerations, based on the compliance requirements on cross-border data flows in major countries, the risks of cross-border data flows may be classified into the following levels: high, medium, and low. Uniform compliance measures may be taken in countries of the same risk level, and a risk governance matrix may be formed, consisting of different levels of compliance measures: strict control (level 3), moderate control (level 2), loose control (level 1) (as shown below).

Risk Level	Country	Risk Detail	Coping Principle
Level 3	Egypt, Russia, Ukraine, etc.	Data exports are allowed only if the data are exported to countries deemed to provide adequate protection, or if the export is approved by corresponding supervisory authorities.	Obtain authorization for cross-border data flows from supervisory authorities. If the authorization is not obtained, take measures to meet the conditions for a derogation; Otherwise, avoid cross-border data transmission.
Level 2	Brazil, Singapore, the European Economic Area (EEA) Countries, etc.	Measures of adequate protection have been specified. Enterprises may choose from various measures such as applicable SCCs, measures abiding by the Binding Corporate Rules (BCRs), and other compliance measures (stipulated by supervisory authorities or formulated by the enterprise). If measures of adequate protection are not specified, enterprises may adopt self-formulated templates of SCCs.	Sign SCCs for cross-border data transfer; take measures to meet the conditions for a derogation; otherwise, avoid cross-border transfer or assess the risks and keep records.
Level 1	Indonesia, Bangladesh, Vietnam, etc.	There are currently no compliance requirements for cross-border data flows.	Not the top priority in compliance governance. Enterprises may track the legislative updates in these countries.

Meanwhile, by referring to the above risk governance matrix, an enterprise needs to formulate compliance strategies and KCPs for cross-border data flows, including guidelines on cross-border data flow routes, relevant examples/tools, and responsible parties and auditors, based on its management practices, business scenarios, and risks appetite, as well as the law enforcement by each country/region.

3.2.4 Assess Compliance Risks

An enterprise needs to carry out risk assessment on its business scenarios with reference to regulatory requirements for cross-border data flows, to evaluate the compliance risks in its business activities involving cross-border data flows, improve its capability to manage cross-border data, and lay a solid foundation for business development. The overall process is shown in the following figure:



Key action 1: Establish a risk assessment scale for cross-border data flows

Based on the regulatory rules and international standards, the enterprise shall establish a risk assessment matrix for the full lifecycle of cross-border data flows with reference to the best practices of the industry. The general assessment items before, during, and after cross-border data flows are as follows:

1) Before cross-border data flows: Whether the following have been internally reviewed and cleared: the data field/information on the flows, minimization assessment, legitimacy assessment, third-party compliance, etc.

2) During cross-border data flows: Whether the flows have been filed to/approval has been obtained from supervisory authorities, whether the SCCs have been signed, whether the data subject's consent has been obtained, and whether the cross-border data flows are completely documented, etc.

3) After cross-border data flows: Whether the data are deleted in time after the fulfillment of the designated purpose, whether there is any use of the data beyond the purpose of flows, etc.

Key action 2: Determine risk rating methods

Make a list of issues based on risk assessment, classify the issues into different levels in accordance with the risk-oriented compliance strategy. Based on experience from practices, two dimensions may be considered in the classification, namely the severity of risk impact and the probability of risk occurrence. The methods are as follows:

Risk Level				
Risk Impact	High	Medium	High	High
	Medium	Low	Medium	High
	Low	Low	Low	Medium
		Low	Medium	High
		Probability of Risk Occurrence		

The specific criteria for judging the severity of risk impact are as follows:

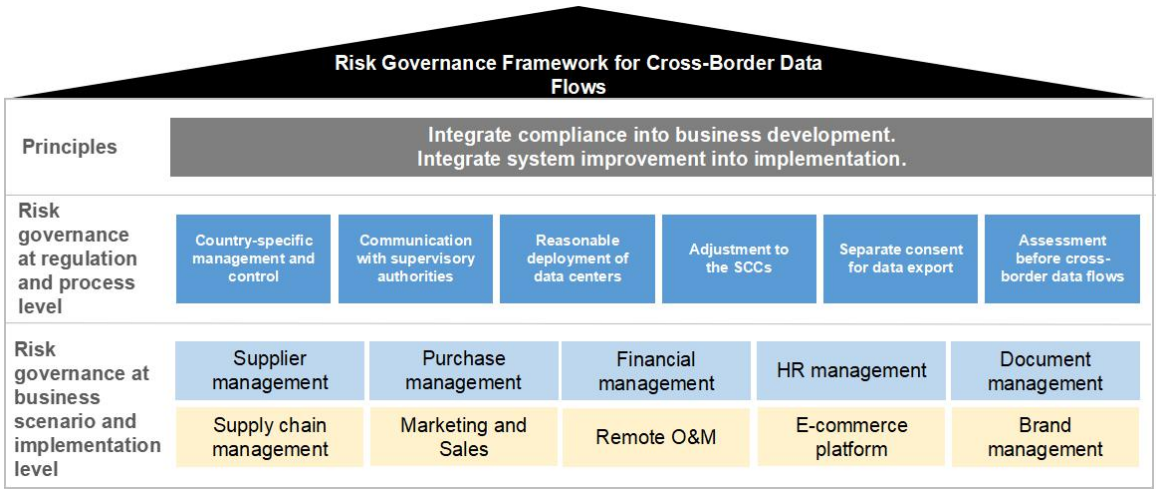
Definition of Risk Impact Level	
Severity Level of Risk Impact	**Description**
High	High-risk items may cause high compliance risks in cross-border data flows, which are the focus of the attention of supervisory authorities. If an item of this kind is investigated by supervisory authorities, the proper operation of the related business module will be severely hindered; or if such an item is discovered and exploited by any entity, it will directly lead to data breaches, which will cause significant economic loss or major reputation risk to the company and hinder the operation of the relative business module.
Medium	Medium-risk items correspond to general compliance risks in cross-border data flows. If an item of this kind is investigated by supervisory authorities, there is a medium or high probability that the proper operation of the relative business module will be affected; or if such an item is discovered and exploited by any entity, it will directly lead to data breaches, which will cause certain economic loss to the company, and affect the operation of the relative business module.
Low	Low-risk items correspond to low compliance risks in cross-border data flows. The mishandling of such an item has only a small impact on the proper operation of the relative business module and on personal information security, and causes small corporate economic losses, and the probability of the occurrence of such consequences is low. The mishandling of such an item has only limited impact on the relative business module, and can cause relatively severe impact only in concurrence with other problems. Thus, the probability of the occurrence of such a risk is lower than that of a medium level risk.

3.2.5 Formulate a Compliance Risk Governance Plan

An enterprise needs to formulate a risk governance plan covering process design and implementation based on the risk assessment result and with consideration of regulatory requirements and best practices in the industry. The following two aspects should be considered in the formulation of a governance plan:

1) Risk control and governance: Formulate a risk governance plan based on the risk assessment result and prioritize risks to be managed. Risks of major impact and high urgency shall be prioritized, while risks of minor impact and low urgency can be dealt with in a less urgent manner. Implement the governance plan with both technical and management measures, including rectifying problems in implementation and optimizing existing compliance control baselines.

2) Integration of risk governance in operation and long-term O&M: Ensure compliance in business development and improve systems during their implementation. Develop feasible, scalable, and sustainable rules, guidelines, methods, and tools for the risk control and compliance governance of cross-border data flows to gradually optimize the risk governance system for cross-border data flows.



Key action 1: Communicate with, report to, and obtain approval from supervisory authorities

In most countries/regions, the fulfillment of the compliance requirements for cross-border data flows requires the involvement of supervisory authorities, such as their approval prior to cross-border data flows and the reporting of the SCCs to supervisory authorities. At present, supervisory authorities in some countries have issued specific guidelines on the reporting process, such as the approval process specified in the BCRs of the EU; In other countries/regions, the reporting process is not specified, and enterprises need to actively communicate with supervisory authorities.

Refer to Appendix 7 *Contact Information of Major Global Supervisory Authorities.*

Key action 2: Deploy data centers reasonably

When deploying a business system server, a multinational enterprise should, on the basis of compliance, consider multiple factors such as cost and technology, and choose a proper location for deployment.

- **Compliance considerations**

Data localization requirements must be met. Depending on the data localization requirements for general personal information or sensitive personal information, there are two situations:

1) In countries with data localization requirements for general personal information, such as Russia, if an enterprise has a large amount of personal information in its human resources management system and supplier management system, local deployment is recommended.

2) In countries with data localization requirements for sensitive personal information, such as India, Pakistan, the United Arab Emirates, and Zambia, if an enterprise has large amount of sensitive data in its business systems, it is recommended that the enterprise deploy the server locally.

In countries without data localization requirements, the data protection capacities of countries/regions should be considered in choosing the deployment location. An enterprise should establish data centers or data ports in countries where data are considered by the international community as "adequately protected" for the convenience of data storage and rational data use, striking a balance between business development and data protection. In this way, compliance risks and compliance costs of cross-border data flows can be reduced.

- **Cost and technology considerations**

Factors like cost and technology need to be considered for choosing an overseas location of a data center, such as:

1) Policies on enterprises: Tax, enterprise incentive policy, business environment, etc.

2) Local environment: Climate and environment, culture and education, energy and communication, population density, etc.

3) Local network level: Number of fixed/mobile network users, traffic data, number of backbone network nodes, number of local data centers, etc.

4) Technical cost: Cost of public cloud services and the rent of data centers.

Key action 3: Adjust the template system of SCCs

In some countries, enterprises are required to sign the SCCs issued by local supervisory authorities, such as Dubai, or to sign the SCCs endorsed by local supervisory authorities, such as Zambia. If an enterprise has adopted a unified version of SCCs for all business scenarios involving cross-border data flows, it cannot meet the special requirements of some countries. In countries with lower compliance requirements, SCCs with a lower level of compliance requirements may be considered.

In the short term, make adjustments to the SCCs that have been "pre-approved" by the European Commission (hereinafter referred to as "the EU version of SCCs") with consideration of regulatory rules that are specified and ready to be implemented:

1) In countries/regions without specified rules, the enterprise may sign the EU version of SCCs as a provisional solution.

2) In countries/regions with special regulatory requirements, the enterprise may sign the SCCs issued by the local supervisory authorities.

3) In countries/regions where approval or reporting is required, the enterprise may confirm the approval procedure for the SCCs with supervisory authorities and have the existing SCCs certified and approved.

In the long term, consider the differences in compliance requirements in different countries and the differences in the roles of enterprises in cross-border data flows, and adjust the template of SCCs and the use guidelines accordingly:

1) Establish a template system for SCCs: Design several sets of templates of SCCs to meet different requirements for SCCs in various countries/regions.

2) Formulate rules and guidelines about the use of the templates.

3) Track the regulatory changes in each country/region and update the templates of SCCs in a timely manner.

Refer to Appendix 8 *European Control Mechanisms for Cross-Border Data Flows.*

Key action 4: Obtain individual consent prior to data exports

If an enterprise uses individual consents as its legal basis for data processing, it shall obtain the individuals' consents separately for the export of their personal information. The enterprise shall fully fulfill its obligation of informing the data subject of the name and contact information of the receiving party abroad, the purpose of data processing, method of processing, the type of personal information, and the method and procedure for the individual to exercise lawful rights to the recipient abroad.

Key action 5: Establish a mechanism for assessment before cross-border data flows

The enterprise shall establish a mechanism for assessment before cross-border data transfer. The following aspects shall be assessed prior to cross-border data flows:

1) Feasibility: Assess the legality, legitimacy, and necessity of the purpose, scope, and mode of cross-border data flows, and evaluate the capability of the overseas recipient to ensure data security.

2) Data minimization: Judge whether the data to be transferred is minimized and whether sensitive information is involved.

3) Data security: Evaluate the security control capability from the aspects of organizational management and technology control, such as control of access permission, transmission channel, desensitization, and encryption.

In addition, specific procedures for assessment should be established, specifying the assessment triggering mechanism, participants in the assessment, use of assessment tools, application of assessment results, and closed-loop management of the assessment process.

3.2.6 Track Additional Information on the Compliance Governance of Important Data

At present, countries/regions have yet to come to a clear-cut definition of important data, and the regulatory rules concerning the cross-border flows of important data are vague. There are many uncertainties in the supervision and enforcement in this regard.

In terms of the identification of important data, there is no globally recognized definition of important data. An enterprise should analyze its business scenarios and identify important data in the context of local laws and regulations, make a list of important data and maintain it separately. At the same time, an enterprise should stick to a "conservative" definition of important data to address the uncertainties of regulatory enforcement.

In terms of external rules, rules for the cross-border flows of important data boil down to the following two requirements:

1) Local storage and processing are required. In principle, important data are not allowed to be exported.

2) Important data can only be exported for certain purposes, approval needs to be obtained, and the approval systems are strict.

Apart from the above requirements, there is no substantial difference between the regulatory requirements for important data and those for personal information, both including prior risk assessment and protection measures. Therefore, local deployment may be prioritized in the compliance governance involving important data, so that risks are avoided from the start. Besides, an enterprise should evaluate the necessity and legality of the cross-border flows of important data. If such flows are necessary, the enterprise should file an application to supervisory authorities in accordance with regulatory rules, and take security measures at organizational and technical levels. Meanwhile, an enterprise shall track, sort out, and study regulatory rules for cross-border data flows, so that the enterprise is ready to deal with the compliance risks concerning important data anytime.

Appendix

Appendix 1: Major Modes of Global Restrictions on Cross-Border Data Flows

Mode	Country	Legislative Overview	Legislative Details
Balancing national security and digital dividend by promoting the development of digital economy while seeking data localization measures	India	It is advocated that personal data should be classified and different data localization requirements be applied to general personal data, sensitive personal data, and critical personal data.	From the changes of rules for cross-border data flows in the two personal data protection bills of 2018 and 2019, it can be seen that India does not want to implement strict "data protectionism," nor does it allow the free data flows. As a result, its data localization strategy aims to not only integrate into the trend of data globalization and stimulate digital economy in India, but also protect data security. Its final middle way is as follows: While implementing localization requirements, India advocates classification of personal data and strict localization requirements for sensitive data, critical personal data. For example, copies of the data shall be stored within India and cross-border data flows are allowed only in rare and specific circumstances, where critical personal data are subject to more stringent conditions than sensitive personal data. There is no requirement for the cross-border flows of general personal data.
	Russia	According to the data localization policy, the first data storage must be conducted in Russia and be transferred outside the country under compliance requirements.	In 2014, Russia adopted the *Data Localization Law*, which requires all operators who collect and process Russian citizens' personal data to use data centers located in Russia and that the first data storage be conducted on servers located in Russia. Regarding law enforcement, Russia also hopes to strengthen government enforcement and control of data through local storage. The "Yarovaya Law" requires organizers disseminating information over the Internet to retain Russian users' communication data on the Internet, personal data and certain data of user activities within the Russian territory for 6 months, and to disclose the data to the Russian authorities upon request.
Advocating cross-border free data flow and promoting the formation of relevant rules	the U.S.	It is advocated that the "free cross-border data flow" be incorporated into the terms of agreements, and important technical data be restricted, and that long-arm extraterritorial jurisdiction be determined.	In accordance with its current leading edge in the information and communications industry, computer industry, and digital economy, the U.S. adopts the data flows policy that pays more attention to the free cross-border flow of personal data. The main purpose of this policy is to leverage its leading edge in global digital industry to dominate the future data flows. The U.S. therefore advocates the inclusion of "free cross-border data flows" in the terms of agreements in the new rounds of trade negotiations with different countries, aiming to remove market access barriers set by these countries. At the same time, the U.S. limits exports of important technical data and foreign investment in specific data-related areas. In addition, the U.S. expands the scope of application of the domestic laws through the "long-arm extraterritorial jurisdiction" and further extend data sovereignty to meet the law enforcement needs of the U.S. government for cross-border data retrieval in new circumstances.

Mode	Country	Legislative Overview	Legislative Details
	the EU	Implement the digital single market strategy within the EU and set up a more flexible model for cross-border data flows externally.	The cross-border data flows policy aims to remove obstacles to the free flow of data within the EU and to implement the EU digital single market strategy. In order to realize the digital single market, the EU, through the direct application of the GDPR among the member states, eliminates the discrepancy of data protection rules and realizes the free flow of personal data within the EU. Through the *Regulation on a Framework for the Free Flow of Non-Personal Data in the European Union*, the EU strives to remove the barriers set by the data localization requirements in member states. For data transfer outside the EU, the EU provides enterprises with data transfer mechanisms that ensure appropriate safeguards, including legally binding and executable documents of public authorities or agencies, BCRs, standard data protection provisions (approved by the European Commission or approved by member states' supervisory authorities and recognized by the European Commission), approved codes of conduct, approved certification mechanisms. Among these mechanisms, enterprises collecting and processing personal data in the EU can choose applicable ones for cross-border data flows.
	Singapore, Japan	Advocate the combination of data protection and free data flows, set up diversified conditions for enterprises' data exports, and actively participate in the cooperation mechanism for cross-border data flows.	Singapore has set up flexible cross-border data transmission requirements similar to those of the EU, making it easier for multinational enterprises to establish their Asia-Pacific data centers. At the same time, Singapore has actively joined APEC's Cross-Border Privacy Rule System (CBPRs) to promote free flows of data within the region. Although Japan has referred to the EU in the formation of rules on cross-border data transfer, its interpretation of the rules is more flexible and provides more space for free cross-border data flows. At the same time, Japan actively participates in the TPP, a Trans-Pacific partnership agreement dominated by the U.S., and APEC's CBPR system. By making supplementary data protection rules to bridge the differences with the EU, Japan has realized mutual recognition of data protection rules with the EU in 2019.

Appendix 2: Frameworks of International Organizations for Cross-Border Data Flows

International Organization	Overview	Framework Details
OECD	Facilitate cross-border data flows within member states.	In 2013, the OECD conducted a comprehensive revision of the *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (OECD 1980 Guidelines), and formed the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD 2013 Guidelines). The OECD 2013 Guidelines define "transborder flows of personal data" as "movements of personal data across national borders". Part three of the guidelines stipulates the basic principles of free data flows and legitimate restrictions (Article 15-18), including the obligations of member states for re-export impact assessment, obligations to ensure uninterrupted and secure data flows, security, management and protection responsibilities, and obligations to avoid creating obstacles to transborder flows of data and ensure proportionality of restrictions and risks. In 2007, on the basis of the OECD 1980 Guidelines, the OECD adopted the *Recommendation on Cross-Border Co-operation in the Enforcement of Laws Protecting Privacy*. According to the Recommendation, member states should implement the laws relating to cross-border privacy protection cooperation and put forward operational requirements for enterprises to facilitate implementation of cooperation. It can be seen that the OECD is generally open to cross-border data flows within member states.
APEC	Establish a rule system of cross-border data flow rules and form specific evaluation criteria.	In 2013, the APEC passed the *Cross-Border Privacy Rules* (CBPR) *System*. The CBPR aims to "ensure the free flow of personal information across borders while providing meaningful protection for the privacy and security of personal information" and requires that "Governments should ensure that there are no unreasonable obstacles to cross-border data transmission, and that the privacy and security of personal information of their citizens should be protected domestically and in cooperation with foreign governments internationally." As the first collaborative framework for data protection in Asia Pacific, APEC's CBPR is a relatively mature mechanism in current multilateral regulatory cooperation. It establishes the evaluation criteria, which include domestic privacy laws, privacy protection law enforcement agencies, trust-mark providers, consistency between the domestic privacy laws and APEC privacy frameworks, requiring member states to ensure that there are no unreasonable obstacles to cross-border data transmission.
Association of Southeast Asian Nations (ASEAN)	Through the digital governance framework, ASEAN implements supervision on and provides guidance to its member countries, and focuses on the development of standard contract terms and cross-border data flows certification.	The *ASEAN Data Management Framework* (DMF) and the *ASEAN Model Contractual Clauses for Cross Border Data Flows* (MCCs) were approved and released at the first ASEAN Digital Ministers' Meeting (ADGMIN). This is to facilitate the data-related business operations in ASEAN, reduce negotiation and compliance costs, and to ensure personal data protection in the cross-border data transmission process. The DMF is formulated to flexibly adapt to the different levels of maturity of member states in terms of data and privacy protection regulation, but is not binding domestically or internationally. In 2018, based on the *ASEAN Economic Community Blueprint 2025* and the *ASEAN Framework on Personal Data Protection*, ASEAN issued the ASEAN Framework on Digital Data Governance, which sets out the strategic priorities, principles, and initiatives to provide guidance for ASEAN member states on their policies and regulatory approaches to the data governance (including personal and non-personal data) in the digital economy. In November 2019, ASEAN adopted the *Key Approaches for the ASEAN Cross-Border Data Flows Mechanism* and recommended that ASEAN member states focus on the development of two of

		these approaches, namely MCCs and *ASEAN Certification for Cross Border Data Flows*.

Appendix 3: China's Relevant Laws and Regulations on Cross-Border Data Flows

Name	Relevant Terms	Key Provision	Time	Nature	Status
Cybersecurity Law of the People's Republic of China	Article 37	1. The framework stipulates that the personal information and important business data collected and produced by critical information infrastructure operators in China shall be stored within the jurisdiction. 2. A security assessment shall be conducted if data export is truly necessary.	Came into force in 2017	Law	In force
Security Assessment Measures for Outbound Personal Information and Critical Data Transfer (Draft)	Full text	1. There is no differentiation between personal information and important data. 2. Specific contents of self-assessment. 3. Supervision on standards for security review. 4. Circumstances in which data export is prohibited.	Draft for Consultation released in 2017	Administrative Regulation (Cyberspace Administration of China)	Draft for consultation
Information Security Technology-Guidelines for Data Cross-Border Transfer Security Assessment (Draft for Consultation)	Full text	1. Specific processes of self-assessment. 2. Key points for personal information and important data assessment (lawfulness and fairness, risk controllability). 3. Requirements for the exporter's technical and management ability. 4. Security protection capability of importer and regional political and legal environment requirements.	Draft for Consultation released in 2017	National Standards (National Standards Committee)	Draft for consultation
Security Assessment Measures for Outbound Personal Information Transfer (Draft for Consultation)	Full text	1. Only personal information is involved. 2. Application materials for security assessment. 3. Key assessment contents. 4. Requirements for data export records. 5. Circumstances in which data export is prohibited.	Draft for Consultation released in 2019	Administrative Regulation (Cyberspace Administration of China)	Draft for consultation
Data Security Management Measures (Draft for Consultation)	Article 28	1. There is no differentiation between personal information and important data. 2. The network operators shall assess the risks and submit them to the regulatory department for approval before issuing, sharing, trading or providing important data abroad. 3. The provision of personal information abroad shall be carried out in accordance with the relevant provisions.	Draft for Consultation released in 2019	Administrative Regulation (Cyberspace Administration of China)	Draft for consultation
Measures for Cybersecurity Review	Article 6	1. If an operator who controls more than one million users' personal information prepares to go public overseas, it must report to the Cybersecurity Review Office for cybersecurity review.	Came into force in 2020	Administrative Regulation (Cyberspace Administration of China)	In force

Data Security Law of the People's Republic of China	Article 36	1. Data refers to records of information in various forms and no other differentiation is made. 2. Without detailed regulations, it only stipulates the basic position in promoting effective utilization of data and promoting the development of digital economy. 3. Overseas transfer is subject to approval.	Came into force in 2021	Law	In force
Personal Information Protection Law of the People's Republic of China	Article 36 Article 38 Article 39 Article 40 Article 41 Article 42 Article 43	1. The personal information processed by the government agencies shall be stored in China; Security assessment shall be conducted if it is truly necessary to provide data abroad. 2. Legal basis of providing data abroad: security assessment, certification, standard contract, and others. 3. Obligation to inform. 4. Key information infrastructure operators and processors who process personal information up to the specified amount shall store data in China and data export shall be evaluated. 5. Judicial assistance shall be subject to approval and complies with international treaties. 6. Actions which may be taken against overseas organizations. 7. Countermeasures to overseas organizations.	Came into force in 2021	Law	In force
Measures for Evaluation of Data Export Security (Draft for Consultation)	Full text	1. Conditions and situations of data export security assessment. 2. Data export risk self-assessment and key points of assessment. 3. Materials, process, expiry period and precautions for the data export security assessment.	Draft for Consultation released in 2021	Administrative Regulation(Cyberspace Administration of China)	Draft for consultation
Regulations on Network Data Security Management (Draft for Consultation)	Chapter V	1. Necessary conditions for data processors to provide data abroad. 2. Data export requires consent from data subjects. 3. Data export security assessment requirements. 4. Compliance requirements for data processors who provide data abroad. 5. Requirements for enterprises to report data security to the municipal network information departments. 6. Data processors engaging in cross-border data activities shall establish and improve relevant technical and management measures.	Draft for Consultation released in 2021	Administrative Regulation (Cyberspace Administration of China)	Draft for consultation

Appendix 4: Regulations on Cross-Border Data Flows of Special Industries in China

Industry	Name	Released by	Specific Requirements
Finance	*Notice on Financial Institutions' Protection over Personal Financial Information*	People's Bank of China	Personal financial information collected in China shall be stored, processed, and analyzed in China.
	Personal Financial Information (Data) Protection Trial Method	People's Bank of China	Personal financial information collected in China shall be stored, processed, and analyzed in China. No one shall provide domestic personal financial information to overseas organizations, unless required by laws, regulations, rules, and regulations of relevant competent departments. If a domestic financial institution handles cross-border business, it shall obtain the explicit consent of the data subject and carry out a data export security assessment in accordance with the laws. After personal financial information is transmitted abroad, financial institutions in China shall create data transmission records of the personal financial information and keep them for at least five years.
	JR/T0171-2020 Personal Financial Information Protection Technical Specifications	People's Bank of China	If personal financial information needs to be provided to overseas organizations due to business needs, the specific requirements are as follows: The information shall comply with national laws and regulations and relevant regulations of the competent industry departments. The explicit consent of the individual financial information subject shall be obtained. The outbound security evaluation of personal financial information shall be conducted in accordance with the regulations and standards formulated by the relevant national and industrial departments to ensure that the data security protection capabilities of overseas organizations meet the security requirements of national, industry departments, and financial institutions. Agreements with overseas organizations shall be signed and onsite checks shall be conducted to clarify and supervise that overseas organizations effectively fulfill their obligations such as protection of personal financial information confidentiality, data deletion, and case investigation.
	Implementation Measures for the Protection of Financial Consumer Rights of the People's Bank of China	People's Bank of China	Consumers' financial information collected in China shall be stored, processed, and analyzed in China. If it is required to provide overseas consumer financial information due to business needs, the following conditions shall be met at the same time: It is necessary for handling cross-border business. Written authorization by financial consumers is required. The information receiving party is the associated organization (including the head office, parent company, branch, and subsidiary) required for completing the business. By signing agreements and conducting onsite checks, overseas organizations are required to keep the

Industry	Name	Released by	Specific Requirements
			obtained consumer financial information confidential. The laws and regulations, and rules of relevant regulatory departments shall be observed.
	Insurance Company Opening and Acceptance Guidelines	China Banking and Insurance Regulatory Commission	Important data, such as business data and financial data, shall be stored in China, and there shall be independent data storage devices and corresponding security protection and remote backup measures.
	Regulation on the Administration of Credit Investigation Industry	State Council	The information collected by credit agencies in China shall be sorted out, saved, and processed in China.
Transportation	*Interim Measures on the Administration of Online Taxi Reservation Business Services*	Seven ministries including the Ministry of Transport and the Ministry of Industry and Information Technology	Online ride-hailing platform companies shall comply with relevant national regulations on network and information security. The collected personal information and generated business data shall be stored and used in Chinese mainland for no less than two years. Unless otherwise specified by laws and regulations, the above information and data shall not be exported.
Medical Care	*Management Regulations on Population Health Information (Trial)*	National Health and Family Planning Commission	It is not allowed to store population and health information in servers outside China, or to host or rent servers outside China.
Publishing	*Management Regulations on Network Publishing Service*	National Press and Publication Administration, National Radio and Television Administration, and Ministry of Industry and Information Technology	When a book, audio, video, electronic, newspaper, or periodical publishing entity engages in network publishing services, it shall meet the following condition: There is necessary technical equipment required for network publishing services, and the relevant servers and storage devices must be within the territory of the People's Republic of China.
Surveying and Mapping	*Map Management Regulations*	State Council	Internet map service companies shall set the server that stores map data within the territory of the People's Republic of China, and formulate regulations and safeguards for the security management of Internet map data.

Appendix 5: List of Global Laws and Regulations on Cross-Border Data Flows

Country/Region	Name
the EEA	European *General Data Protection Regulation*
the UK	European *General Data Protection Regulation* *UK General Data Protection Regulation* (UK GDPR)
Mexico	*The Federal Law on Protection of Personal Data held by Private Parties*
Turkey	*Law on Protection of Personal Data (LPPD)*
Brazil	*LEG Geralde Proteçãode Dados (LGPD)*
Colombia	*Statutory Law No. 1581 2012* *Statutory Law No. 1377 2013*
Peru	*Personal Data Protection Law No.29733 (PDPL)*
Russia	*Federal Law 152-FZ* *Federal Law No. 242-FZ* *Federal Law No. 405-FZ*
India	*Personal Data Protection Bill 2019*
Indonesia	There is no personal data protection law. The *Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions ("GR 71")* set certain requirements for public electronic systems, but there is no requirement for private databases.
Japan	*The Act on the Protection of Personal Information (APPI)*
Philippines	*Data Privacy Act of 2012* or *Republic Act No. 10173*
Pakistan	*Personal Data Protection Bill 2020 (draft)*
Bangladesh	There is no written personal information protection law, and only the *Digital Security Act 2018*, where there is no content related to cross-border data transmission.
Vietnam	No written personal information protection law is available.
Myanmar	No written personal information protection law is available.
Thailand	*Personal data Protection Law 2020*
Malaysia	*Personal Data Protection Act 2010 (PDPA)*
Ukraine	*Law No. 2297-VI on Protection of Personal Data* *Law No. 4452 -VI (Amendment)* *Law No. 5491-VI (Amendment)*
Nepal	No personal data protection law is available at present.
Singapore	*The Personal Data Protection Act of 2012 (No.26 of 2012)*. The 2020 revised version does not involve cross-border data transmission.

Country/Region	Name
Korea	*Personal Information Protection Act*
Egypt	*Personal Data Protection Law No.151 of 2020*
Ethiopia	There is no effective data protection law, and only the payment guidance rules have localization requirements.
South Africa	*The Protection of Personal Information Act*
Nigeria	*Nigerian Data Protection Regulation 2019*
Algeria	*Law No. 18-07 of 2018*
Zambia	*Data Protection Act No. 3 of 2021*
Libya	Currently, there is no data protection law or regulation in Libya.
Uganda	*Data Protection and Privacy Act No. 9 of 2019*
Angola	*Data Protection Law*
Morocco	*Law No. 09-08 on Personal Information Protection*
United Arab Emirates	There is no privacy protection law in the United Arab Emirates. Section 13 of the *Law on Information and Communication Technology in Healthcare* specifies local storage requirements. In 2007, Dubai International Financial Centre (DIFC) enacted the *Data Protection Law*, and revised it in 2020. *Data Protection Law (DIFC Law No.5 of 2020)*
Hong Kong Special Administrative Region (SAR)	*Personal Data (Privacy) Ordinance* (No regulations on cross-border data flows)
China	*Cybersecurity Law of the People's Republic of China*
	Data Security Law of the People's Republic of China
	Personal Information Protection Law of the People's Republic of China
	Measures for Cybersecurity Review
	Outbound Data Transfer Security Assessment Measures (Draft)
	Data Security Management Measures (Draft)
	Security Assessment Guidelines for Outbound Information Security Technology Data Transfer (Draft)
	Security Assessment Measures for Outbound Personal Information and Critical Data Transfer (Draft)
	Security Assessment Measures for Outbound Personal Information Transfer (Draft)

Appendix 6: List of Global Management and Control Requirements for Cross-Border Data Flows

Country/Region	Name	Interpretation of Relevant Regulations/Key Points
China	*Cybersecurity Law of the People's Republic of China*	The personal information and important data collected and generated by critical information infrastructure operators during their operations within the territory of the People's Republic of China shall be stored within the territory. If it is truly necessary to provide the data overseas for business purposes, security assessment shall be conducted in accordance with the measures formulated by the Cyberspace Administration of China and other relevant departments under the State Council.
	Security Assessment Measures for Outbound Personal Information and Critical Data Transfer (Draft)	Personal information and important data collected and generated by network operators during their operations within the territory of the People's Republic of China shall be stored within the territory. If it is truly necessary to provide services overseas for business purposes, security assessment shall be conducted in accordance with the Measures.
	Data Security Law of the People's Republic of China	In addition to the general data security protection obligations, the enhanced protection obligations are specified for processors of important data. 1. Processors of important data shall designate a responsible data security person, establish a data security organization, and fulfill responsibilities for data security protection. 2. Processors of important data shall conduct periodic risk assessments during their data processing activities as required, and submit risk assessment reports to the relevant government agencies. The risk assessment reports shall include the type and quantity of important data managed by the organization, the situation of data collection, storage, processing, and use, and the data security risks and countermeasures.
	Information Security Technology — Guideline for Identification of Critical Data (Draft)	A complete definition of important data is proposed for the first time (based on the functions of data and possible impacts caused by damage to the data, important data are divided into the following categories: national economy operation, safety protection, natural resources and environment, health, sensitive technologies, users, and government secrets). The types and ranges of important data of 28 industries are listed. In the definition of important data, the criteria for determining important data are provided. Nine scenarios are specified in accordance with the possible consequences caused by unauthorized data disclosure and loss, abuse, tampering or destruction, convergence, integration, and analysis of data.
	Guidelines for Identification of Critical Data of Basic Telecommunications Service Providers	Definition of important data, and the principles, rules, and workflow of important data in the basic telecommunication services are stipulated.
Germany	*Telecommunications Act*	Regulations on local storage of original data are stipulated.
India	*National E-Commerce Policy*	A legal and technical framework will be created to impose restrictions on cross-border data flows in the following scenarios: (1) Data collected by IoT devices installed in public places. (2) Data generated by Indian users from various sources, including e-commerce platforms, social media, and search engines. However, there are some exceptions in which cross-border flows are allowed. For example, technical data in cloud computing services do not involve personal or community data.

Country/Region	Name	Interpretation of Relevant Regulations/Key Points
	Unified License Agreement	According to the Agreement, the following contents shall not be transmitted to any place other than India: 1. Any accounting information related to the subscribers (except international roaming/bills) (Note: This requirement does not restrict the disclosure of financial information in accordance with legal requirements). 2. User information (except foreign subscribers or IPLC subscribers who use the Indian operator network during roaming).
	Draft Rules on E-Pharmacy	The pilot policy against cross-border data flows has been implemented in the e-pharmacy industry.
	National Data Sharing and Accessibility Policy	All data collected through the use of public funds shall be stored within India.
Indonesia	*Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions*	Public electronic system operators must place their electronic systems and data (including government, energy, transportation, finance, medical care, IT and communications, defense, and other strategic data) in Indonesia. Unless otherwise specified by the companies, private electronic system operators may place their electronic systems and data in or outside Indonesia. However, private electronic system operators must allow government agencies to "supervise" through access to electronic systems and data for monitoring and law enforcement.
Vietnam	*Decree on the Management, Provision, and Use of Internet Services and Online Information*	Information collection websites, social networking websites, mobile communication network service providers, and online game service providers are required to set up at least one server in Vietnam. In addition, the *Cybersecurity Law* requires that enterprises providing Internet services and online additional services shall store the following data: (1) information data that they collect, use, analyze, and process, (2) personal and service user relationship data, and (3) data created by Vietnamese users.
South Korea	*Regulations on Supervision of Electronic Financial Transactions*	Data localization measures are applicable to the financial field. The regulations prohibit financial institutions in South Korea from transmitting any identifiable information across borders, and require them to install servers and disaster recovery facilities in South Korea. Only information processing systems that impose limited security and reliability impacts on electronic financial transactions and may therefore be designated as "non-critical" for this purpose can be established abroad.
	Regulations on Financial Institutions' Outsourcing of Data Processing Business and IT Facilities	Specific restrictions are applicable to data processing outsourcing in the financial field. Financial companies in South Korea must report to the Financial Service Commission (FSS) about specific issues specified in the laws and regulations on outsourcing data processing, regardless of whether such data processing takes place in South Korea or under foreign jurisdiction.

Country/Region	Name	Interpretation of Relevant Regulations/Key Points
the U.S.	List of Controlled Unclassified Information	1. In accordance with applicable laws, regulations, and government policies, information under protection or dissemination control is divided into the following categories: For Official Use Only (FOUO) Law Enforcement Sensitive (LES) Unclassified Controlled Nuclear Information (DoD UCNI) Sensitive But Unclassified Information (DoS SBUI) DEA Sensitive Information Foreign Government Information Distribution Statements on Technical Documents 2. The management of controlled unclassified information includes the following requirements: The organizations that create or process unclassified information shall take protective and control measures to protect the CUI from unauthorized access. Whether laws, regulations, or government policies should include communication control shall be determined based on specific instructions and a reference in the CUI registration form shall be provided. When protection measures are no longer needed, the CUI control and the control of the relevant authorities over information dissemination should be cancelled as soon as possible.
Russia	*Sovereign Internet Law*	1. The main responsible parties for the stable operation of the Internet in Russia are telecom operators and the owners of technical communication networks, network traffic exchange points, and Autonomous System Numbers (ASNs). 2. Roskomnadzor (RKN) performs centralized communication network management functions by determining routing policies and coordinating telecom operators, responsible parties, and their connections. 3. The obligations of the responsible party include: participating in routine network drills to stabilize the Russian network and installing technical equipment to prevent threats to the stability, security, and integrity of the Internet operations in Russia.
Turkey	/	The Information and Communication Technology (ICT) Authority has released two decisions to regulate the embedded SIM technologies that cause sensation in the country. In particular, the localization requirements for SIM cards of the electronic call system are to prevent the permanent roaming of vehicles. The first decision is to standardize the electronic call service in vehicles; and the second decision is to standardize the remote programmable eSIM technology.
Algeria	/	Through legislation, Algeria requires e-commerce operators to provide services from data centers in Algeria.

Appendix 7: Contact Information of Major Global Supervisory Authorities

Country/Region	Supervisory Authority	Official Website	Contact Information	Communication Item
China	Cyberspace Administration of China/Office of the Central Cyberspace Affairs Commission	*http://www.cac.gov.cn/*	Address: No.9 Chegongzhuang Street, Xicheng District, Beijing Tel: (010)68365570	1. Procedures and enforcement details related to security assessment and security-related certification. 2. Equal protection standards agreement, and the applicability of the internal SCCs of the group. 3. Determination of CII operators and personal information processors processing a certain amount of data.
France	National Cybersecurity Agency of France	*https://www.ssi.gouv.fr/*	Email: communication@ssi.gouv.fr	Data controller registration.
Italy	Intelligence System for the Security of the Republic	*https://www.sicurezzanazionale.gov.it*	Email: info@sicurezzanazionale.gov.it	
Poland	Digital Affairs Department	*https://www.gov.pl/*	Email: mc@mc.gov.pl Fax: +48228294850	
the UK	Information Commissioner's Office	*https://ico.org.uk/*	Tel: 0303 123 1113 Fax: 01625 524510	Release of the *International Data Transfer Agreement and Guidance.*
Malaysia	National Cyber Security Agency	*https://www.nacsa.gov.my/*	Address: Level LG&G, West Wing, Perdana Putra Building, Federal Government Administrative Center, Putrajaya, Malaysia.	1. The release of the white list. 2. China's progress of obtaining adequacy decision under the GDPR. 3. Registration of data controller/database.
	Malaysian Communications and Multimedia Commission	*https://www.mcmc.gov.my/en/home*	Tel: 03-80008000 Fax: 03-89115183 Email: webmaster@kkmm.gov.my	
India	Central Information Committee	*http://www.cic.gov.in/*	Fax: 26186536 Tel: 011-26183053 Email: fdesk-cic@gov.in	1. The effectiveness of drafts. 2. Approval procedures for SCCs or internal plans by the group.
Egypt	Ministry of Communications and Information	*https://www.mcit.gov.eg/*	Tel: (+202) 35341300	1. Report the implementation of cross-border data transmission compliance to regulatory authorities.

Country/Region	Supervisory Authority	Official Website	Contact Information	Communication Item
	Technology			2. Obtain approval from the supervisory authorities for cross-border transmission.
Algeria	Ministry of Posts and Telecommunications	*https://www.mpt.gov.dz/en*	Email: contact@mpttn.gov.dz Tel: +213(0)21 711 220 Fax: +13(0)21 730 047	1. Report the legislation status of the data receiving country and the implementation of compliance requirements for cross-border data flows of the company to the regulatory authority, and prove that the equal protection requirements are met. 2. Obtain approval from the supervisory authorities for cross-border data transmission.
Angola	Ministry of Telecommunications and Information Technology of Angola	*https://www.missionangola.ch/*	Address: Rue de Lausanne 80, Genève, 1202, Suisse Tel: 41 22 732 30 60	1. Determine whether China can be recognized as a country with an appropriate level of protection after its *Personal Information Protection Law* came into force. 2. Apply for evaluation or institutional approval in accordance with China's certification situation.
Russia	Federal Service for Supervision of Communications, Information Technology, and Mass Media	*http://www.rsoc.ru/*	Address: 7, BLDG 2, Kitaigorodsky Proezd, Moscow, 109995, Russia	1. Report before the start of data processing activities. 2. China's progress of obtaining adequacy decision under the GDPR.
Ukraine	National Network Security Coordination Center	*https://zakon.rada.gov.ua/laws/show/2163-19*	Temporary unavailable (website inaccessible)	1. The release of the white list. 2. China's progress of obtaining adequacy decision under the GDPR.
Nigeria	Computer Emergency Response Team	*https://www.cert.gov.ng/*	Mailbox: info@cert.gov.ng Tel: +234 905 555 4499	
Dubai DIFC	Dubai International Financial Center	*https://www.dfsa.ae*	/	Publication of SCCs.

Country/Region	Supervisory Authority	Official Website	Contact Information	Communication Item
Turkey	National Cyber Security Committee	*www.udhb.gov.tr*	/	Data controller registration.
Uganda	National Information Technology Authority	*https://www.nita.go.ug*	Tel: +256-417-801038 Email: info@nita.go.ug	
Angola	Ministry of Telecommunications, Information Technology and Media	*https://minttics.gov.ao/*	Tel: +244 222 210 740 Mailbox: geral@minttics.gov.ao	
Colombia	Superintendence of Industry and Commerce, Ministry of Telecommunications, Information Technology and Social Communication	*https://mintic.gov.co/portal/inicio/*	/	Database registration.

Appendix 8: European Control Mechanisms for Cross-Border Data Flows

(1) SCCs

The SCCs are model contractual clauses "pre-approved" by the European Commission. Under the GDPR, contractual clauses ensuring appropriate data protection safeguards can be used as a basis for data transmission from the EU to third countries.

On June 4, 2021, the European Commission published modernized SCCs under the GDPR for the transmission of data from controllers or processors in the EU/EEA (or otherwise subject to the GDPR) to controllers or processors outside the EU/EEA (not subject to the GDPR). One of the files in the following link applies to data commission processing activities between data controllers and data processors, the other applies to the transmission of personal information to third countries.

[Access and Download] *https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en*

(2) Countries with Adequacy Decision

An adequacy decision means that only when the protection level of personal data in the third country meets the requirements of the EU can the personal data of the EU member states be transferred across borders. According to the GDPR, whether a third country provides "adequate" data protection depends on the completeness and implementation of the third country's legal system related to personal data protection.

Currently, the countries with adequacy decision include: Andorra, Argentina, Canada (only commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay, and South Korea.

[Access and Download] *https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en*

(3) BCRs

The BCRs are legal means to provide adequate protection for personal data exported from the EU to other countries that have not been confirmed by the EU to meet adequate protection. If a multinational enterprise or group has the BCRs recognized by the data management authorities of the EU member states, it can directly conduct cross-border data transmission within the group without additional approval.

The BCRs can only be implemented after they are formulated and approved by the data management agencies in the major EU member countries.

So far, the European Commission and the data management authorities of member states have listed companies authorized for BCRs:

[Access and Download] *https://edpb.europa.eu/our-work-tools/accountability-tools/bcr_en*

Appendix 9 Law Enforcement and Jurisdiction Cases of Cross-Border Data Flows

- **Spanish Data Protection Authority fined Vodafone EUR 8.15 million for violating data protection laws.**

In March 2021, the Spanish Data Protection Authority fined a total of EUR 8.15 million on Vodafone and its service providers for multiple and repeated violations of the GDPR and the national laws of Spain, including a fine of EUR 2 million for its service providers' transmission of personal data to countries that do not meet the European data protection requirements.

- **Norwegian Data Protection Authority imposed a fine on Ferde for illegal transmission of image data to China.**

In May 2021, the Norwegian Data Protection Authority decided to fine Ferde with NOK 5 million. As investigated, Ferde did not conduct risk assessment before manual processing of more than 12 million license plates and images, and lacked an appropriate legal basis for the data transfer to China between 2017 and 2019. As a result, Ferde was fined for violating Article 28, Article 33, and Article 44 of the GDPR.

- **Japan Personal Information Protection Commission investigated Line Corporation over access to Japanese user data by its Chinese affiliate.**

In March 2021, the Japan Personal Information Protection Commission investigated Line Corporation (hereinafter referred to as "Line"), a messaging application provider. According to the investigation, the Japanese user data was accessed by a Chinese affiliate of Line, which enabled engineers of the affiliate to view the personal information stored in Japan from August 2018 to February 2021. The Commission conducted an onsite inspection after requiring Line to submit an incident report. The investigators visited Line and its parent company, Z Holdings Corporation (4689) in accordance with the *Act on the Protection of Personal Information*, and indicated that the inspection was "intended to determine whether (Line's supervision of the affiliate and its access to data) comply with the law." According to Line, it had terminated the development, maintenance and operation of its dialogue system in China.

- **The French CNIL fined Google EUR 50 million for violations of the GDPR.**

In January 2019, Google was fined EUR 50 million by the Commission on Information Technology and Liberties (CNIL) of France. Google was fined as it violated the transparency and information communication obligations under the GDPR in the cross-border data operation process.

References

Alibaba Data Security Research Institute. (2019). *Research report on global data cross-border flow policy and China strategy*.

China Development Institute. (2020). *Cross-border data flow: Global situation and the countermeasures for China*.

European Commission. (2021, June 4). *Standard contractual clauses for international transfers*. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en

European Commission. (n.d.). *Adequacy decisions: how the EU determines if a non-EU country has an adequate level of data protection.* https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#:~:text=How%20the%20EU%20determines%20if,adequate%20level%20of%20data%20protection.&text=The%20European%20Commission%20has%20the,adequate%20level%20of%20data%20protection.

European Commission. (2021, June 18). *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data-Version 2.0.* https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en

United Nations Conference on Trade and Development. (2021). *Digital Economy Report 2021*. https://unctad.org/webflyer/digital-economy-report-2021

Xu, D. (2020). Legal guarantee for dual-way compliance of enterprises subject to regulations of transborder data flow. *Oriental Law*.

Zhu, C. (2019). Market, state, and the restructuring of international trade and economic rules system. *Foreign Affairs Review. (05)*.

合规创造价值

Compliance Creates Value

Editors-in-Chief: Gao Ruixin, Shen Yanru, Fang Yuan, Huang Hao, He Zhicong, Wang Chen, Liu Tianya, Yang Yuxin, Xu Min, Xiao Tengfei, Huang Hui'e, Marco Costantini, Alberto Lezcano Hormeño

Editors: Zhou Yuxin, Wang Zhiyu, Ding Pei, Wei Andi, Mei Aoting, Song Weiqiang, Chen Lisheng, Wen Hualong, Zhao Zhihai, Li Lin, Chi Yifei, Hui Zhaoshuai, Qu Shenwei, Long Hao, Chen Weite, Chen Zhengwei, Lin Suming, Hu Zhiqiang, Deng Yuanyuan, Yue Yanhong, Lu Kexing, Lin Jun, Zhang Liang, Zhang Zhe, Yang Liu