深圳数据交易所
SHENZHEN DATA EXCHANGE

ASIAN BUSINESS LAW INSTITUTE

China-Singapore Joint Data Compliance Guide

Practical Handbook

Disclaimer

Important Notice: This document is provided solely as a general informational guide and does not constitute legal or other professional advice. In the event of any conflict or inconsistency between the Chinese and English versions, the Chinese text shall prevail for the China Chapter, and the English text shall prevail for the Singapore Chapter.

China-Singapore Joint Data Compliance Guide: Practical Handbook (hereinafter, the "Guide") are a non-profit collaborative project jointly led by the Shenzhen Data Exchange and the Asian Business Law Institute (ABLI), and prepared with the support of volunteer expert contributors. The purpose of the Guide is to provide general reference information and guidance for individuals and organizations engaged in business activities in China and Singapore, or otherwise interested in data compliance and protection.

The contents of the Guide are based on publicly available information and the contributors' understanding of the relevant laws and regulations as of the date of publication. The editors and contributors have made reasonable efforts to ensure the accuracy, completeness, and timeliness of the information contained herein. Nevertheless, laws and regulations in the field of data privacy and compliance are complex, subject to frequent change, and open to varying interpretations. Accordingly, the Guide may not cover all relevant details and may not fully reflect the most recent legal developments, regulatory requirements, or practical changes.

The Guide do not constitute, and should not be relied upon as, legal, accounting, investment, or other professional advice of any kind. The information herein is not a substitute for professional tax, accounting, legal, or other advice tailored to specific circumstances. Readers should consult qualified professional advisers and provide them with all relevant facts before making any decision or taking any action related to data compliance.

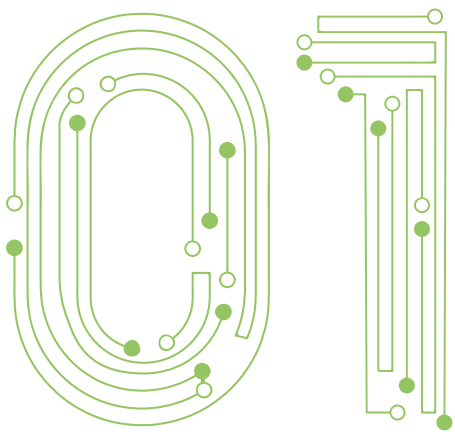
The editors and contributors make no express or implied representations or warranties

as to the completeness, accuracy, or timeliness of the information contained in the Guide, including, without limitation, any warranties of functionality, merchantability, or fitness for a particular purpose. The editors and contributors disclaim any liability for errors or omissions, or for any actions taken or not taken, or any consequences arising from reliance on any part of the Guide.

The use of the Guide is subject to the following conditions:

- The Guide are provided solely for informational reference and shall not be used for any commercial purpose.
- Any reproduction or dissemination of the Guide, in whole or in part, must clearly indicate the source and acknowledge the non-profit collaborative nature of the project.
- The editors reserve the right to amend, update, or withdraw the Guide at any time without prior notice.
- By accessing, reading, or using the Guide, you acknowledge that you have read, understood, and agreed to all terms of this Disclaimer.

China Chapter



Foreword

In today's world, the digital economy is flourishing, and data has become the core engine driving economic growth and social progress. Consequently, the cross-border flow of data is now an established trend. Building upon the development of the "International Data Hub" and the China-Singapore (Shenzhen) Smart City Initiative, both nations have achieved significant outcomes in areas such as data export and the mutual recognition of digital identities. The entry into force of the Regional Comprehensive Economic Partnership (RCEP) in 2023 and the establishment of the China-Singapore Digital Policy Dialogue mechanism have further accelerated digital trade and data cooperation between the two countries. However, while facilitating business operations, the cross-border flow of data also presents challenges related to personal information protection, the disclosure of commercial secrets, and risks to national security.

China has established a scientific and efficient regulatory system centered on the Cybersecurity Law of the People's Republic of China, the Data Security Law of the People's Republic of China, and the Personal Information Protection Law of the People's Republic of China, complemented by regulations such as the Provisions on Promoting and Regulating Cross-Border Data Flow. Singapore, meanwhile, has solidified its position as an Asia-Pacific data hub based on its Personal Data Protection Act. The legal systems of the two countries feature both synergies and differences, placing higher compliance demands on enterprises. To properly manage the compliance risks associated with cross-border data flows for businesses expanding overseas, Shenzhen is further advancing the spirit of the Implementation Plan for the Comprehensive Pilot Reform of Shenzhen as a Pilot Demonstration Area for Socialism with Chinese Characteristics (2020-2025). The city is exploring efficient, convenient, and secure mechanisms for cross-border data flow by building a "1231" service system (one action plan, two major free trade zones, three cross-border data service platforms, and one association). By leveraging the advantages of the Qianhai and Hetao platforms and integrating the innovative practices of the Shenzhen Data Exchange,

Shenzhen is exploring a negative list system for cross-border data. It is also carrying out initiatives such as "Regional Outbound Data Transfer Security Assessment," "Personal Information Protection Certification," and the "filing of standard contracts for the export of personal information." These efforts aim to provide one-stop data cross-border compliance services for enterprises in need, creating a Shenzhen model that connects with Hong Kong and Macau and links to the global stage.

Against this backdrop, the Shenzhen Data Exchange and the Asian Business Law Institute in Singapore have jointly compiled the China-Singapore Joint Data Compliance Guide: Practical Handbook. This initiative aims to provide enterprises in both countries with a systematic and actionable regulatory framework for cross-border data flow, helping them accelerate their integration into the global digital economy on a compliant basis and effectively mitigate the data compliance risks encountered during overseas expansion. Grounded in a systematic comparison of the legal frameworks of China and Singapore and tailored to the practical needs of businesses, these guidelines comprehensively address key points at three levels: entity compliance, data compliance, and cross-border circulation compliance. This includes data classification and grading, identification of important data, personal information protection, and industry-specific data management. Supplemented by typical case studies on data export compliance for foreign-invested enterprises, the Guide serve as a practical operational manual. By helping companies accurately seize policy opportunities and avoid potential legal risks, this guide will further deepen and solidify China-Singapore data cooperation, contributing to the development of an open, inclusive, fair, and secure global digital economy governance framework.

Editorial Committee

Guiding Organizations

Shenzhen Municipal Service and Data Administration

Shenzhen Municipal Bureau of Justice

The Authority of Qianhai Shenzhen-Hong Kong Modern Service Industry Cooperation Zone of Shenzhen

Shenzhen Law Society

Supporting Organization

Network Data Security Compliance Laboratory (Shenzhen Qianhai)

Editor-in-Chief

Wang Qinglan, General Manager, Compliance Department, Shenzhen Data Exchange

Deputy Editors-in-Chief

Hu Jingzhuo, Data Compliance Manager, Shenzhen Data Exchange

Meng Jie, Partner, Global Law Office (Beijing)

Wang Yi, Partner, Global Law Office (Shenzhen)

Contributing Authors (in chapter order)

Wang Qinglan, General Manager, Compliance Department, Shenzhen Data Exchange

Zhang Yi, Partner, Fangda Partners (Shanghai)

Li Huihui, Counsel, Fangda Partners (Beijing)

Huang Jiajie, Partner, Tianda & Gonghe Law Firm (Beijing)

Ma Kaiyang, Attorney, V&T Law Firm

Li Rui, Partner, Zhong Lun Law Firm

Pu Yuhan, Attorney, Zhong Lun Law Firm

Xu Chen, Former Attorney, Zhong Lun Law Firm

Duan Zhichao, Partner, Han Kun Law Offices (Beijing)

Wang Yuting, Counsel, Han Kun Law Offices (Beijing)

Meng Jie, Partner, Global Law Office (Beijing)

Lin Yi, Counsel, Global Law Office (Chengdu)

Wang Yi, Partner, Global Law Office (Shenzhen)

Liu Jiayi, Associate, Global Law Office (Shenzhen)

Shi Jinyuan, Partner, Simmons & Simmons (Hong Kong)

Lai Yuchen , Simmons & Simmons (Hong Kong)

Lai Yanyu , Formerly of Simmons & Simmons

Wu Han, Partner, King & Wood Mallesons (Beijing)

Yao Minlü, Attorney, King & Wood Mallesons (Beijing)

Editors

Chen Yiqian, Data Compliance Manager, Shenzhen Data Exchange

Hu Minzhe, Data Compliance Manager, Shenzhen Data Exchange

Acknowledgments

Sincere thanks to experts Yang Yuxin, Hong Yanqing, Chen Meng, Mai Lijuan, Xie

Chen yang, and Zhang Yanan for their support in preparing the Guide.

Catalogue

Chapter I Overview and User Guide※

I. Introduction: The Context of China–Singapore Digital Cooperation and the Value of the Guide

In the wave of the global digital economy, data has surpassed traditional factors of production to become the core engine driving economic growth, technological innovation, and social development. Its cross-border flow, as the lifeblood of the digital economy, has become increasingly vital. Against this backdrop, in 2023 China and Singapore elevated their bilateral relationship to an “All-Round, High-Quality, and Forward-Looking Partnership,” charting a course for deeper cooperation across multiple fields. Among these, digital economy cooperation—particularly in the area of cross-border data flows—stands out as one of the most dynamic and forward-looking components.

Since 2013, China has been Singapore’s largest trading partner, while Singapore has consistently ranked as China’s largest source of new foreign investment. This strong economic foundation provides a solid basis for cooperation in the digital domain. Both countries share broad common interests and enormous potential in promoting global trade facilitation, advancing innovation in financial services, and jointly building the “Digital Silk Road.” Efficient and secure data flows are the key to realizing these shared goals.

(i) The Practical Basis of China–Singapore Data Cooperation and Enterprise Needs

China–Singapore cooperation in cross-border data flows has gone far beyond conceptual discussions. Through high-level dialogue mechanisms and flagship

※ Author of this Chapter,Wang Qinglan, Ph.D. in Law, Postdoctoral Fellow in Computer Science and Technology. Currently serves as Director and General Manager of the Compliance Department at the Shenzhen Data Exchange. She is also a Council Member of Shenzhen Law Society, Executive Vice President of the Research Society on Foreign-Related Rule of Law of Shenzhen Law Society, and Vice President of the Shenzhen Association for the Promotion of Data Compliance and Cross-Border Data Flows.

projects, the two sides have translated strategic consensus into tangible outcomes. These efforts are wide-ranging, with strong demonstrative effects, and fully attest to the central role of data flows in driving the development of the regional digital economy.

At the strategic level, the two countries have established a high-level dialogue platform to systematically advance digital cooperation. On 27 June 2024, the inaugural “China–Singapore Digital Policy Dialogue (DPD)” was successfully held in Beijing, marking a new phase of institutionalized and structured cooperation in the digital domain. This mechanism not only provides strong policy guidance and safeguards for specific projects, but also reflects both parties’ strategic resolve to jointly build an open, secure, and trusted digital ecosystem.

At the practical level, cooperation has flourished across multiple fronts, with particularly fruitful outcomes in smart cities and emerging industry ecosystems. Since the launch of the Singapore–Shenzhen Smart City Initiative (SCI) in 2019, the two sides have rolled out numerous projects in fields such as international data connectivity, cross-border trade, and smart industrial parks. At the fourth SCI Joint Steering Council meeting in December 2023, 14 new cooperation projects were added, and the China–Singapore Qianhai Smart City Innovation Demonstration Park was inaugurated. These city-level projects explore cross-border data applications across diverse scenarios and have accumulated valuable experience for scaling up data flows.

Such practices, while advancing the implementation of China–Singapore digital cooperation, have also enabled enterprises to appreciate the distinctive features of the two countries’ data governance frameworks. China adheres to the principle of “balancing security and development,” safeguarding data security while actively promoting orderly flows. Singapore, meanwhile, has relied on a market-oriented approach to build a flexible compliance framework. Both systems are highly aligned in their core objectives.

As cooperation scenarios continue to expand, enterprises engaged in high-frequency data flows in cross-border operations and trade increasingly need to grasp China’s

regulatory requirements in areas such as data classification and grading, cross-border filings, and security assessments. These rules not only provide strong safeguards for data security, but also chart a clear path for enterprises to operate in compliance. Accordingly, a set of guidelines that systematically interpret the features of both countries' governance systems and clarify key compliance requirements will enable enterprises to better understand the scientific and facilitative nature of China's compliance framework. To achieve this, however, it is essential first to understand the development trajectory and opening direction of China's data compliance system—topics that will be addressed in the following sections.

(ii) Evolution and Opening Trends of China's Data Compliance Framework

China's digital governance framework is anchored in the "three pillars" of the *Cybersecurity Law of the People's Republic of China* (hereinafter, *"Cybersecurity Law*"), the *Data Security Law of the People's Republic of China* (hereinafter, "*Data Security Law*"), and the *Personal Information Protection Law of the People's Republic of China* (hereinafter, "*PIPL*"). Together, these laws establish a top-level framework that integrates development and security, with data classification and grading as its foundation. Building on this, the *Provisions on Promoting and Regulating Cross-Border Data Flows* ("Provisions on Cross-Border Data Flows"), the *Measures for Security Assessment of Outbound Data Transfers*, and the *Measures on the Standard Contract for the Outbound Transfer of Personal Information*, among others, collectively form a comprehensive regulatory regime. These measures clarify rules on data classification and grading, cross-border exemptions, security assessment mechanisms, standard contract filings, and personal information protection certifications. Combined with negative lists and positive operational guidelines in free trade zones, they continuously advance the standardization and facilitation of cross-border data flows.

China's data compliance system is constantly evolving and being optimized. In recent years, policy adjustments have accelerated significantly, sending a clear signal of openness and development. This not only provides enterprises operating in China with

clearer compliance guidance but also underscores China's proactive engagement in global digital governance. The 2024 *Provisions on Cross-Border Data Flows* are particularly pivotal: while firmly safeguarding national security and large-scale personal information protection, they substantially simplify procedures for routine, low-risk business scenarios involving cross-border data transfers. This reflects China's confidence and openness in data governance and marks a significant step toward promoting the orderly and free flow of data under the premise of security.

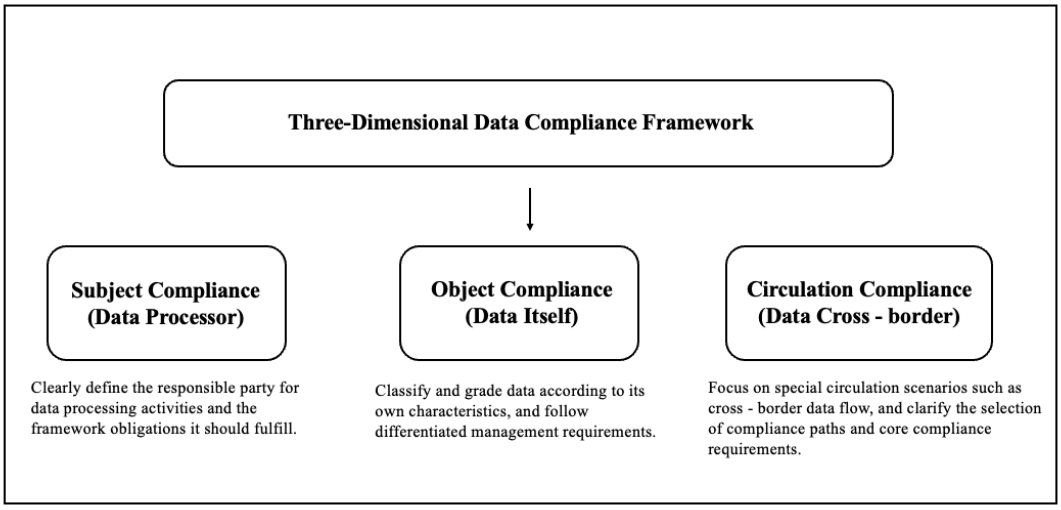
The *Provisions on Cross-Border Data Flows* directly address enterprise concerns and achieve several breakthrough innovations: first, they specify exemptions for outbound transfers of personal information in common economic activities such as "concluding or performing a contract to which the individual is a party," "human resources management," and "emergency situations," thereby significantly reducing the compliance costs of daily operations; second, they refine the rules for identifying "important data," providing that if data has not been notified or publicly designated as "important data" by the relevant authorities or regions, data processors are not required to declare it for outbound data transfer security assessment, thereby resolving uncertainties faced by enterprises in data classification and grading; third, they establish a "negative list" mechanism in pilot free trade zones, authorizing regions to independently define the scope of regulation and creating institutional space for higher-level opening-up; fourth, they lower the regulatory threshold for outbound transfers of personal information, providing greater convenience for small- and medium-scale data flows.

To build a practical compliance guide aligned with the legal systems of both countries and to support enterprises in conducting cooperation efficiently and in compliance, the Shenzhen Data Exchange and the Asian Business Law Institute (ABLI) jointly launched this project. Based on the legal systems of China and Singapore, and taking into account practical needs and the contributors' professional experience, the Guide assist enterprises in accurately understanding regulatory policies and institutional norms in both countries across three dimensions: subject compliance, object compliance, and

compliance in cross-border flows. They systematically set out compliance scenarios in business practice. In the following sections, to help readers better grasp the internal logic and practical pathways of China's data compliance system, we will begin with its core framework and provide a detailed explanation of the compliance architecture of "subject–object–flow."

II. China's Practical Framework and Compliance Logic for Data Governance

To assist readers—particularly business practitioners from different jurisdictions—in quickly and systematically understanding the internal logic of China's data compliance framework, these Guidelines distill from legal provisions and practical experience a three-dimensional framework of "Subject–Object–Flow." This framework deconstructs complex compliance requirements into three interlinked elements, forming a clear logical chain of "Who processes the data (Subject) – What data is being processed (Object) – How the data flows across borders (Flow)." It should be noted that this framework is not a formally codified system under Chinese law. Rather, it is a methodology derived from the core requirements of China's data protection laws and regulations, combined with practical compliance experience, intended to provide enterprises with a clear and operational compliance pathway. These three dimensions are interrelated and progressive: together they cover the critical nodes of the entire data processing lifecycle while reflecting China's governance philosophy of "classification and grading, security and controllability," thereby enabling enterprises to accurately identify and implement their compliance obligations.



Through this framework, enterprises can systematically examine their data processing activities: first, by clarifying their responsibilities and obligations as the “Subject”; second, by identifying the types and risk levels of the “Object” being processed; and finally, when data “Flows” (particularly across borders), by selecting the appropriate compliance pathway. This structured approach helps enterprises avoid compliance blind spots and establish a comprehensive and dynamic data compliance management system.

(i) Subject Compliance: Core Obligations of Data Processors

Subject compliance focuses on the data processor itself (such as enterprises or institutions) and requires the establishment and improvement of internal management systems. These obligations can be summarized under three main modules—“framework building – ex-ante prevention and control – ex-post response”—to ensure that compliance efforts are structured and that risks remain manageable.

Type of Obligation	Core Content	Purpose and Explanation
Framework	**Organizational structure** (e.g., legally appointing a data security officer and a	Lays the foundation for compliance by

Type of Obligation	Core Content	Purpose and Explanation
Building	personal information protection officer); **institutional development** (e.g., formulating a master plan for data security management, establishing a data classification and grading system, and preparing emergency response plans); **personnel management** (e.g., conducting compliance training, carrying out background checks for key positions).	clarifying “who is responsible and according to what rules,” ensuring that compliance responsibilities are assigned to specific departments and individuals.
Ex-Ante Prevention and Control	**Data classification and grading** (identifying general, important, and core data); **management of external partners** (assessing external partners’ data compliance and security capabilities); **risk assessment** (conducting impact assessments before high-risk personal information or important data processing activities).	Proactively identifies and assesses risks before data processing activities begin, thereby reducing compliance vulnerabilities at the source and avoiding a purely reactive approach.
Ex-Post Response	**Security incident response** (e.g., activating an emergency plan for data breaches); **handling and reporting** (taking remedial measures and, as required, reporting to regulatory	Ensures that once a risk event occurs, enterprises can respond quickly, effectively minimize

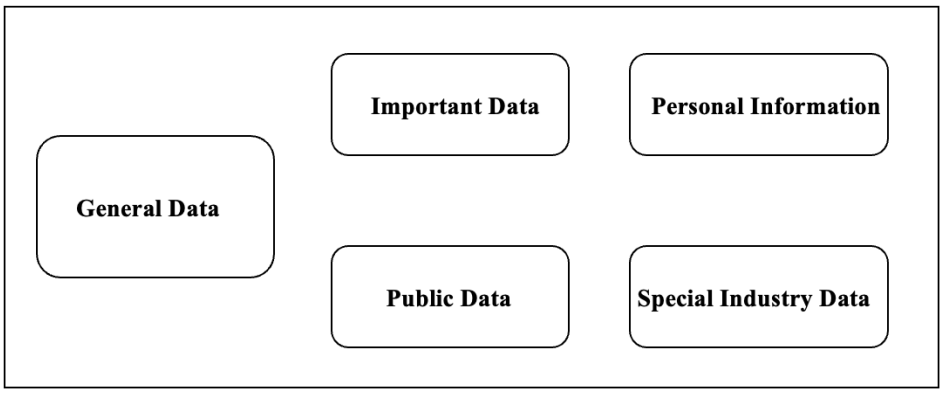
Type of Obligation	Core Content	Purpose and Explanation
	authorities and notifying affected individuals).	losses, and fulfill statutory reporting and notification obligations so as to reduce negative impacts to the lowest possible level.

(ii) Object Compliance: Special Requirements for Different Types of Data

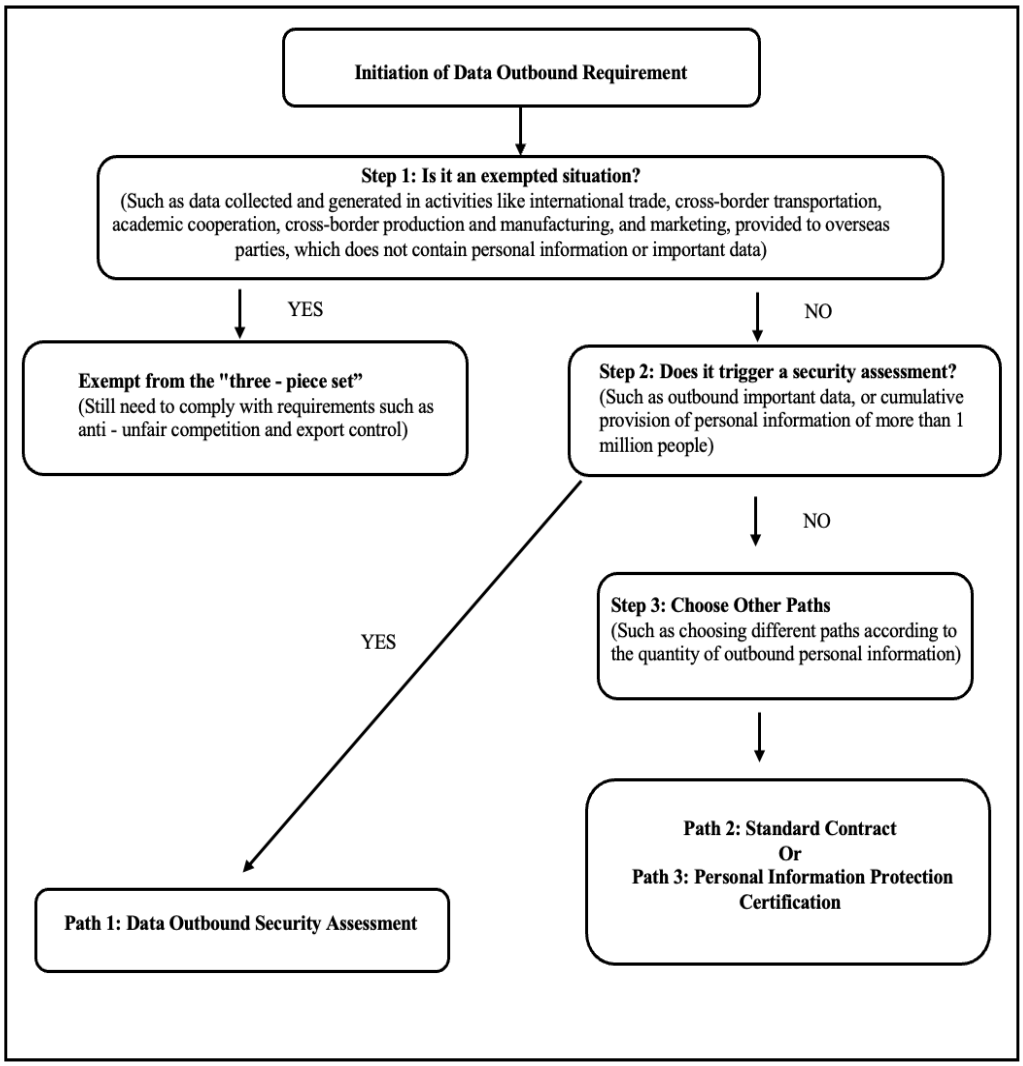
Object compliance focuses on the data itself, with the core principles of “classification and grading, differentiated management, and overlapping obligations.” China’s data governance framework classifies data from the dual perspectives of national security and data utilization. It first establishes the general compliance requirements applicable to all data, and then specifies additional obligations for data with special attributes (such as important data, personal information, public data, and sector-specific data). Enterprises must first accurately identify the type of data they process and then match it with the appropriate compliance obligations—for example, public data must comply with open-sharing rules; personal information requires the safeguarding of data subject rights; important data must comply with requirements such as domestic storage and outbound data transfer security assessment; and industry-specific data must satisfy additional sectoral requirements.

It is particularly important to note that the same dataset may carry multiple attributes. For instance, large-scale patient medical records held by a hospital constitute personal information containing sensitive details, may also be deemed important data, and at the same time qualify as both public data and sector-specific medical data. In such cases, compliance obligations must be “applied cumulatively,” meaning enterprises are required to meet all relevant regulatory requirements concurrently to ensure

comprehensive and gap-free compliance.



Cross-border data flows are the top priority in China's data compliance regulatory framework. The core rules can be summarized as "compliance pathways + conditional review." Before providing data abroad, enterprises must assess factors such as the type, volume, and sensitivity of the data, and then determine and select a legally prescribed compliance pathway.



To maximize the practical value of these Guidelines, we recommend that readers make use of the following tools and tips in their reading and application.

III. Guidelines for Use and Practical Tools

(i) Content Index Table

These Guidelines are designed with a “problem-oriented” approach. Depending on your specific needs, you can use the table below to quickly locate the most relevant chapters for focused reading.

Your Need	Recommended Chapter	Summary of Core Content
Want to know **which authorities are responsible for data regulation in China?**	Chapter II: Regulatory System and Departmental Responsibilities	Division of responsibilities and regulatory focus of the CAC, MIIT, MPS, SAMR, and other authorities.
Need to **build an overall data compliance management framework for your enterprise**?	Chapter III: Compliance Requirements for Data Processing Entities	Framework obligations such as organizational structure, institutional development, risk assessment, and incident response.
How to handle **different types** of data in business operations?	Chapter IV: Compliance Standards for Data Objects	Classification and grading standards and differentiated compliance requirements for various types of data.
Need to **transfer data outside of China**?	Chapter V: Compliance Pathways for Cross-Border Data Flows	Three main pathways—security assessment, standard contracts, and protection certification—as well as detailed exemptions.
Want to reference **best practices from leading enterprises**?	Chapter VI: Guidelines on Good Compliance Practices	Case studies of foreign-invested enterprises on personal information protection, outbound data transfers, and employee management.
Need to resolve specific	Chapter VII: Frequently	High-frequency issues such as outbound

Your Need	Recommended Chapter	Summary of Core Content
compliance questions?	Asked Questions	data filing, exercise of personal information rights, and identification of important data, with official regulatory explanations and practical guidance.
Need template tools for support?	Appendix II: Compliance Templates and Checklists	Ready-to-use tools such as a PIA report template, outbound data transfer risk self-assessment checklist, standard contract guidance, and a framework for incident response plans.

(ii) Usage Tips

Comprehensive Assessment: When handling specific issues—especially those involving cross-border data flows—it is necessary to consider the chapters on “Subject Compliance,” “Object Compliance,” and “Flow Compliance” together in order to make a comprehensive judgment.

Make Good Use of the Appendices: The appendices to these Guidelines provide a “Glossary of Terms,” “Frequently Asked Questions,” and “Compliance Templates and Checklists” that can be directly downloaded and used. These tools can effectively help enterprises implement compliance requirements more efficiently.

Dynamic Monitoring: Laws and regulations in the field of data compliance are frequently updated. The contents of these Guidelines are current as of August 2025. Enterprises are advised to maintain continuous attention to legislative and enforcement developments to ensure the timeliness of their compliance work.

Chapter II Regulatory System and Departmental Responsibilities※

What is the first step toward data compliance in China? The answer lies in understanding who regulates data. Before delving into specific regulatory rules, it is essential to introduce the key regulatory authorities responsible for data protection in China. China's data governance and enforcement landscape is primarily shaped by the following authorities: the Cyberspace Administration, the Ministry of Industry and Information Technology (MIIT), public security authorities and market regulation authorities. In addition, sector-specific regulators may exercise statutory supervisory powers within their respective industries over data protection matters. Understanding the roles of these regulators helps businesses operating in China identify the proper points of contact and avoid compliance missteps due to misunderstandings about jurisdiction.

I. Cyberspace Administration of China (CAC)

Pursuant to Article 8 of the *Cybersecurity Law*, Articles 6 and 31 of the *Data Security Law*, and Articles 60 and 62 of the *PIPL*, the Cyberspace Administration of China (CAC) acts as the central coordinating body for cybersecurity, data security, and personal information protection. In addition to drafting and issuing supporting rules under key data protection laws, the CAC leads both macro-level supervision—such as national cybersecurity policy enforcement—and micro-level enforcement, including the regulation of privacy practices in mobile apps.

At the **macro level**, the CAC oversees enforcement actions against enterprises that fail to fulfill their data security obligations—such as those resulting in system intrusions or data breaches. In serious cases involving national security, the CAC is empowered

※ **Authors of this Chapter**: **Zhang Yi**, Partner, Fangda Partners (Shanghai); Certified Information Privacy Professional/Europe (CIPP/E), Certified Information Privacy Professional/Asia (CIPP/A), Certified Information Privacy Manager (CIPM), and Fellow of Information Privacy (FIP), International Association of Privacy Professionals (IAPP).**Li** Huihui, Counsel, Fangda Partners (Beijing). **Contributors:** Wang Yi, Duan Zhichao, Liu Jiayi, Wang Yuting, Shi Jinyuan, Lai Yanyu, Lai Yuchen.

to initiate cybersecurity reviews in accordance with applicable laws.[1] It also plays a coordinating role in matters such as the protection of critical information infrastructure (CII) and network product vulnerability management.

With respect to **cross-border data transfers**, the CAC is responsible for establishing key rules—including the Measures for Security Assessment of Data Exports and the Standard Contract Mechanism—and for supervising the assessment and filing procedures required for outbound data transfers. In the area of **personal information protection**, the CAC leads the development of relevant standards and regulatory mechanisms, with the goal of building a nationwide ecosystem for third-party privacy services and certification.

At the **micro level**, the CAC and its local counterparts have actively enforced app compliance requirements in recent years. Enforcement activities have included technical inspections of apps, third-party SDKs, and mini-programs, resulting in public notices and takedowns for violations such as failure to disclose data processing rules, unauthorized personal information collection, and lack of account deletion functions. The CAC also focuses on real-world scenarios—such as compulsory identity collection through QR codes or abuse of facial recognition—and has launched targeted enforcement campaigns through public hearings, inspections, and administrative penalties.

II. Ministry of Industry and Information Technology (MIIT)

The MIIT and its local communications bureaus are also key regulatory authorities in the field of data protection. They are responsible for supervising data processing and security activities within the industrial and information technology sectors. Their main responsibilities include: supervising the data processing activities and the implementation of data security safeguards by data processors in the industrial and

[1] Article 16 of the Measures for Cybersecurity Review provides that: Where a member entity of the cybersecurity review working mechanism deems that a network product, service, or data processing activity affects or may affect national security, the Cybersecurity Review Office shall, in accordance with the prescribed procedures, submit the matter for approval by the Central Cyberspace Affairs Commission. Upon approval, a review shall be conducted in accordance with these Measures.

information technology sectors; promoting the development and utilization of data and the establishment of relevant data security standards; formulating standards and specifications for data classification and grading, and guiding the implementation of classification and grading management; and conducting inspections on the fulfillment of data security responsibilities and management measures by relevant data processors, as well as imposing administrative penalties for violations of data security regulations.

Like the CAC, the MIIT is also deeply involved in micro-level enforcement, particularly in relation to mobile apps. As one of the primary regulators targeting unlawful or excessive personal data collection by apps, the MIIT has—by the time of this publication—issued public notices against 45 batches of non-compliant apps.

As the regulator for the telecommunications sector, the MIIT also enforces standards against user experience violations—such as forced redirection, non-closable pop-up windows, or unauthorized automatic launching—and has issued compliance requirements for all parties in the app ecosystem, including developers, SDK providers, and app stores.[2]

Since 2023, the MIIT has taken on responsibility for app and mini-program registration.[3] All apps and mini-programs made publicly available in China must be filed with the MIIT via their respective network access service providers or platform operators prior to launch.

III. Public Security Authorities

In the field of data protection, public security authorities focus more on data protection matters within the context of cybersecurity and on law enforcement related to criminal activities. Their primary responsibilities include supervising, inspecting, and guiding the

[2] For example, in its special enforcement actions in 2021 and 2023, the MIIT detailed specific compliance requirements for mobile applications (Apps). These are set out respectively in the *Notice of the Ministry of Industry and Information Technology on Launching the Perception Enhancement Campaign for Information and Communication Services* (2021) and the *Notice of the Ministry of Industry and Information Technology on Further Improving the Service Capabilities of Mobile Internet Applications* (2023).

[3] See the Notice of the Ministry of Industry and Information Technology on Carrying Out the Filing of Mobile Internet Applications.

implementation of the multi-level cybersecurity protection system (MLPS); conducting security inspections of internet service providers and connected entities; combating illegal and criminal activities involving the exploitation of vulnerabilities in network products; investigating violations such as unlawful processing of personal information and acts endangering cybersecurity; and enhancing security safeguards for critical information infrastructure (CII) to prevent and combat criminal activities targeting or exploiting CII. In addition, the Public Security authorities also play an important practical role in the field of personal information protection. For example, when a personal information processor reports a security incident in accordance with Article 57 of the *PIPL*, in practice it is typically the Public Security authorities that are responsible for receiving such reports and handling the related cases in accordance with the law.

For example, in the implementation of the MLPS, the public security authorities, as the competent regulatory body, conduct both routine visits and annual inspections to examine whether enterprises have properly fulfilled their obligations under the MLPS. This includes reviewing the adequacy of data protection measures, such as whether data is stored in encrypted form, whether appropriate access controls are in place, and whether tools to prevent data leakage have been deployed. In practice, when a data breach occurs, the public security authorities may, depending on the severity of the incident, initiate what is referred to as a “dual-track investigation”, meaning that both the suspected perpetrators of the data breach and the enterprise involved will be investigated to determine whether there was a failure to fulfill data security protection obligations.

IV. Market Regulation Authorities

Market regulation authorities are primarily responsible for overseeing data protection from the perspectives of consumer rights protection, regulation of online transactions, as well as fair competition and anti-monopoly enforcement.

Based on past enforcement practices, these authorities have placed particular emphasis on the unlawful collection and external provision of personal information, especially in sectors such as real estate leasing and sales, small loans and finance, education and training, insurance brokerage, beauty and fitness, home renovation, travel and accommodation, express delivery services, and telemarketing.

In addition, market regulation authorities also enforce data-related rules to ensure fair market competition. For instance, in September 2024, the Shanghai Municipal Administration for Market Regulation issued an administrative penalty decision against a financial information technology company. The company was found to have a dominant market position in a specific segment of the bond voice brokerage real-time trading data market and had engaged in conduct such as refusal to deal and the imposition of unreasonable trading conditions, which constituted an abuse of market dominance. This case has been referred to as “China’s first data-related anti-monopoly enforcement case.”

Beyond administrative enforcement, the State Administration for Market Regulation (SAMR) is also involved in the development of certification schemes related to personal information and data protection. Enterprises applying for data security management certification or personal information protection certification for cross-border transfers must comply with the certification rules and requirements issued by SAMR.

V. Industry Regulators and Other Authorities

As data protection has increasingly become a focal point of public and industry attention in recent years, regulators in various sectors—being most familiar with the operational practices and data handling characteristics within their respective industries—often formulate data security management measures within their respective areas of responsibility. In specific circumstances, they also perform their data protection duties in order to advance regulatory oversight in this field.

The following are the main laws, regulations, and regulatory requirements related to

data protection that have been issued by the State Council and various sectoral regulators (sometimes jointly with the Cyberspace Administration).

Below are key laws, regulations, and regulatory requirements related to data protection issued by industry regulators (or jointly with the CAC).

Issuing Authority	Title of Regulation
State Council	*Regulations on the Administration of Human Genetic Resources*
State Council	*Regulations on the Administration of Public Security Video and Image Information Systems*
Cyberspace Administration of China, National Development and Reform Commission, Ministry of Industry and Information Technology, Ministry of Public Security, Ministry of Transport	*Provisions on the Administration of Automotive Data Security (for Trial Implementation)*
People's Bank of China	*Measures for the Administration of Credit Reporting Business*
National Financial Regulatory Administration	*Measures for the Administration of Data Security of Banking and Insurance Institutions*
Ministry of Finance, Cyberspace Administration of China	*Interim Measures for the Administration of Data Security of Accounting Firms*
Ministry of Industry and	*Interim Measures for the Administration of Data Security in the Field of Industry and Information*

Information Technology	*Technology*
Ministry of Natural Resources	*Measures for the Administration of Data Security in the Field of Natural Resources* *Notice on Strengthening the Security Administration of Surveying and Mapping Geographic Information Related to Intelligent Connected Vehicles*
National Health Commission, National Administration of Traditional Chinese Medicine, National Disease Control and Prevention Administration	*Measures for the Cybersecurity Administration of Medical and Healthcare Institutions*

The National Data Administration, as the body responsible for coordinating the planning and implementation of the digital economy, society, and “Digital China” strategy, and for implementing the national big data strategy, has not yet directly undertaken regulatory enforcement actions related to data protection. However, it plays an active leading role in promoting legislation and property rights clarification over data elements, guiding the development of the data element market, and coordinating the integration, sharing, and utilization of data resources, as well as advancing the planning and construction of digital infrastructure.

Moreover, although not a typical law enforcement agency, consumer associations are legally authorized to file public interest litigation against conduct that infringes upon the lawful rights and interests of a large number of consumers in relation to personal information.[4] In practice, several provincial-level consumer associations have already

[4] Article 47 of the *Law of the People's Republic of China on the Protection of Consumer Rights and Interests* stipulates that, where the lawful rights and interests of a large number of consumers are infringed upon, the China Consumers Association and the consumer associations established in provinces, autonomous regions, and municipalities directly under the central government may file a lawsuit with the people’s court.

taken such actions to safeguard consumers' rights and interests through public interest litigation in the field of personal information protection.

VI. National Data Security Coordination Mechanism

To address the complex challenges of data security governance that span multiple domains and administrative levels, the central national security leadership body has established the National Data Security Coordination Mechanism. As the core national-level governance mechanism for data security under Article 5 of the *Data Security Law*, its establishment and operation embody the holistic view of national security and serve as an important institutional arrangement for balancing data security and development. From a governance perspective, data security is characterized by its wide coverage across sectors, the systemic transmission of risks, and the immediacy of emergency response. By contrast, individual departments face inherent constraints, such as limited regulatory scope, independent division of powers and responsibilities, and procedural requirements for cross-departmental collaboration. The coordination mechanism provides institutional safeguards for systematic risk governance by establishing a normalized, cross-departmental and cross-sector framework for unified coordination.

The core responsibilities of the coordination mechanism span three dimensions: At the institutional level, pursuant to the *Regulations on Network Data Security Management* (hereinafter, *Network Data Regulations*), it coordinates relevant departments in formulating catalogues of important data and standards for identifying core data, thereby providing a fundamental institutional basis for classified and graded data protection. For example, in key areas such as industry and natural resources, it guides sectoral regulators in delineating the scope of data protection priorities with precision (see the *Administrative Measures for Data Security in the Industrial and Information Technology Sector* and the *Administrative Measures for Data Security in the Field of Natural Resources*).

At the risk prevention and control level, it leads the establishment of a unified system

for data security risk assessment, information sharing, and monitoring and early warning. It strengthens interdepartmental emergency response capabilities for major data security incidents, strictly preventing the spread of systemic risks.

At the security review level, it organizes and implements national data security reviews, strictly scrutinizing data processing activities that affect or may affect national security. It is also responsible for risk assessment and overall coordination in key areas such as the sharing of core data.

Chapter III Compliance Requirements for Data Processing Entities※

With the promulgation and implementation of the three fundamental data protection laws—the *Cybersecurity Law*, the *Data Security Law*, and the *PIPL*—together with their supporting regulations and implementation measures (such as the *Network Data Regulations* and the *Measures for Compliance Audits of Personal Information Protection* (hereinafter, *PIPL Audit Measures*), China's data protection regulatory authorities have continuously strengthened their enforcement activities. Data compliance governance has thus become one of the core compliance tasks for enterprises.

A sound data compliance system not only guides employees to follow data protection rules in daily business practices—thereby avoiding violations caused by insufficient compliance awareness and reducing compliance risks for enterprises—but also serves as strong evidence that an enterprise lacks subjective fault when unlawful data processing activities occur. This provides necessary support for distinguishing and allocating liability between the enterprise and the individual violator. Building a data compliance system and embedding data protection into brand value creation also bring substantial benefits to enterprise operations.

I. Organizational Structure

China's current data protection laws and regulations impose requirements on the organizational structure for corporate data protection across multiple legal instruments, reflecting the legislative approach of classified management and graded protection. For example, the *Cybersecurity Law* requires network operators to designate a **"person in charge of cybersecurity"** (Article 21), and requires critical information

※ **Authors of this Chapter Zhang Yi**, Partner, Fangda Partners (Shanghai); Certified Information Privacy Professional/Europe (CIPP/E), Certified Information Privacy Professional/Asia (CIPP/A), Certified Information Privacy Manager (CIPM), and Fellow of Information Privacy (FIP), International Association of Privacy Professionals (IAPP). **Li Huihui**, Counsel, Fangda Partners (Beijing). **Contributors:** Wang Yi, Duan Zhichao, Ma Kaiyang, Liu Jiayi, Wang Yuting.

infrastructure operators ("CIIOs") to establish a **"dedicated security management body and designate persons in charge of security management"** (Article 34). The *Data Security Law* requires important data processors to designate a **"person in charge of data security and establish a management body"** (Article 27).[5] The *PIPL* requires personal information processors that process personal information in volumes meeting thresholds set by the national cyberspace authority to designate a **"person in charge of personal information protection"** (Article 52). The *Network Data Regulations* stipulate that processors handling the personal information of more than 10 million individuals, as well as important data processors, must designate a "person in charge of network data security and establish a management body" (Articles 28 and 30). The *Measures for Compliance Audits of Personal Information Protection* require processors handling the personal information of more than 1 million individuals to designate a "person in charge of personal information protection" (Article 12). The *Provisions on the Cyber Protection of Children's Personal Information* require network operators to designate a **"dedicated person"** responsible for the protection of children's personal information (Article 8).

In practice, many enterprises have already established dedicated data protection teams or appointed dedicated data protection officers in order to meet the requirements of data protection laws and regulations. Since data protection teams generally need to possess specialized expertise in personal information protection, in most enterprises the responsibilities of the data protection department are not assumed by the information security or network security departments. The former focuses more on compliance governance and privacy protection across the full lifecycle of data (especially personal information), whereas the latter mainly addresses network security maintenance and more technically oriented aspects of general data security protection. The responsibilities of the data protection department typically include establishing and implementing personal information protection policies and

[5] Important data is a concept unique to China's data protection legal framework. It refers to data in specific sectors, concerning specific groups, or relating to particular regions, or data that reaches a certain level of precision or scale, which—if tampered with, damaged, leaked, or unlawfully accessed or used—may directly endanger national security, economic operations, social stability, or public health and safety.

procedures, conducting compliance and risk assessments of products and services, providing data protection consulting and training, handling data subject rights requests and complaints, and responding to data security incidents.

II. Policy Development and Personnel Management

With certain exceptions, most of China's current data protection laws and regulations do not provide detailed requirements on the internal rules and operational procedures that enterprises must establish. Instead, they emphasize broad and general obligations.. For example, the *Data Security Law* merely requires data processors to "establish and improve full-process data security management systems" (Article 27); the *PIPL* uses only the general phrasing "formulate internal management systems and operating procedures" (Article 51). This legislative approach, while leaving enterprises with flexibility in designing their systems, also requires a higher degree of autonomy and initiative from enterprises in identifying and prioritizing the establishment of key internal policies in compliance practice.

In practice, companies typically consider the following when developing data protection frameworks: (1) To ensure systematic and standardized policy development, enterprises should first issue overarching and guiding policy documents—such as a "General Policy on Data Protection" or equivalent—as the foundation for subsequent detailed rules and procedures. (2)Legal and regulatory requirements that explicitly call for policy development should be prioritized. These include, for example, full-process data security management systems, mechanisms for receiving and handling data subject rights requests, security incident response plans, important data management standards, and data classification and grading mechanisms. The absence of such policy may be deemed non-compliance during regulatory inspections or incident response, and thus they should be assigned high priority. (3) For multinational enterprises, tailoring internal compliance systems to local legal requirements is already a widely recognized best practice. For foreign-invested enterprises operating in China, although group-wide compliance systems may exist, the specific features of China's data protection laws make it advisable to "localize" policy by creating China-specific

chapters within global policies or adjusting relevant procedures. For example, security incident response plans should incorporate mechanisms for reporting to Chinese regulators and notifying affected individuals, and personal information protection impact assessment (PIPIA) processes should be adapted to China's legal requirements. (4) For critical data protection processes requiring coordination across multiple business departments—such as internal and external data transfer management, outbound data transfer self-assessment, and monitoring mechanisms—codifying these processes into formal written rules enhances enforceability, strengthens employee compliance awareness, and facilitates uniform implementation within the enterprise.

Once rules and procedures are in place, enterprises should ensure internal enforcement through training, communications, performance assessments, and disciplinary or incentive measures. It is advisable to clearly incorporate employee obligations to comply with data protection policies in employment contracts, employee handbooks, onboarding or regular training materials, and maintain signed records to serve as compliance evidence. Special management obligations should also be observed. For instance, the *Cybersecurity Law* requires CIIOs to conduct security background checks on personnel in critical roles (Article 34), and the *Network Data Regulations* require similar checks for those handling certain types and scales of important data (Article 30).

III. Data Classification and Grading

Similar to policy development requirements, China's data protection laws and regulations generally adopt a purpose- or outcome-oriented regulatory model for data security management, supplemented with examples of security measures as references.[6] This legislative approach reflects a regulatory philosophy of aligning

[6] For example, Article 21 of the *CLS* requires network operators to "implement measures such as data classification, important data backup, and encryption"; Article 42 mandates that network operators "shall adopt technical and other necessary measures to ensure the security of the personal information they collect, and prevent information leakage, damage, or loss." Article 27 of the *Data Security Law* requires data processors to "take appropriate technical and other necessary measures to safeguard data security." Article 51 of the *PIPL* stipulates that personal information processors must "implement classified management of personal information" and "adopt appropriate security technical measures such as

security measures with data security risks, allowing enterprises to select appropriate safeguards according to business scale, data volume, and sensitivity, thereby avoiding unnecessary compliance costs arising from over-regulation.

Within this risk-matching framework, enterprises must first clarify the protection requirements for different types and sensitivities of data. Through classification and grading, legal requirements can be effectively linked with business practices, providing the foundation for differentiated security strategies and ensuring that measures are precisely matched to risks. China's classification and grading system is built upon a multilayered set of legal instruments, forming a systematic regulatory framework and guidance. Specifically: the *Cybersecurity Law* first introduced the concept of "important data," laying the foundation for graded protection; the *Data Security Law* explicitly requires the establishment of a data classification and grading protection system and designates data relating to national security and the national economy as "core data," subject to stricter management; the *PIPL* promotes refinement of the classification system through differentiated requirements for different categories of personal information; the *Measures for Cybersecurity Review* incorporate risks associated with "core data" and "important data" into the scope of national security review; and the *Network Data Regulations* further define the connotation of important data and provide a dedicated chapter on important data security management.

In conducting classification and grading, enterprises should follow the GB/T 43697-2024 *Data Security Technology – Rules for Data Classification and Grading* (hereinafter, *"Classification and Grading Rules"*), *which serve as a core reference. These Rules articulate five basic principles—scientific and practical, clear boundaries, higher standards for higher risks, integration of overall and specific perspectives, and dynamic updates—thus providing enterprises with a clear operational framework.*

For classification, enterprises may refine categories according to the logic of "industry sector – business scope – business attribute": first, identify the broader sector (e.g.,

encryption and de-identification" to "prevent unauthorized access as well as the leakage, tampering, or loss of personal information."

industry, finance, telecommunications); then refine into specific segments based on business models and processes; and finally, determine subcategories according to the actual business attributes of the data. This enables the creation of classification rules tailored to industry characteristics. In practical internal operations, classification can be organized along business lines and internal functions[7], with the goal of anchoring corresponding sectoral regulatory requirements and assigning internal accountability, so that data security management can be carried out under a “dedicated person, dedicated responsibility” model.

For grading, enterprises should consider the importance of data to the economy and society, as well as the potential harms caused by leakage or misuse, and categorize data into three levels: core data, important data, and general data. The specific process typically involves: identifying the grading object; assessing key factors (such as data domain, scale, and accuracy); analyzing the scope and degree of potential impact; and reaching a comprehensive evaluation of the level. This ensures that grading outcomes accurately reflect data security risks, thereby providing a solid basis for formulating differentiated protection measures.

Based on classification and grading, enterprises must then align with the specific security measures enumerated in relevant laws and regulations, as well as the level requirements applicable to their information systems (such as the *GB/T 22239-2019 Information Security Technology – Basic Requirements for Cybersecurity Classified Protection*). Enterprises are also encouraged to draw on other international standards for information and data security protection (such as *ISO/IEC 27001 Information Security Management Systems* and *ISO/IEC 27701 Privacy Information Management Systems*), to select the necessary safeguards and apply differentiated protections according to the type and level of data. Common data security measures include (static and dynamic) data encryption and masking, access control and permission management, data backup and recovery, traffic monitoring and anomaly detection, and

[7] For example, based on business lines and functional departments, enterprises can typically categorize data into customer (user) data, research and development (R&D) data, system operations and maintenance data, financial data, human resources data, and other business management data.

log auditing and monitoring.

IV. Management of External Partners

In real-world operations, data processing often involves multiple collaborating parties. These may be independent controllers, joint controllers, or processors operating under a data processing delegation. The *PIPL* expressly requires that, in scenarios involving the entrusted processing of personal information, the personal information processor and the entrusted party must agree on the specific matters of entrusted processing. When providing personal information to external parties, the processor must inform the individual of the recipient's name, contact details, purpose of processing, method of processing, and the types of personal information involved, and must obtain the individual's separate consent.

Building on the PIPL, the *Network Data Regulations* further refine compliance requirements in scenarios involving multi-party data cooperation. Under the Network Data Regulations, whenever an enterprise provides personal information or important data to other data processors, or entrusts them with its processing, it must specify the details of processing through contractual arrangements and supervise the recipient's performance of its obligations.

In practice, when cooperating with third parties in arrangements involving data interactions, enterprises generally set out the rights and obligations of both parties either by including a data processing chapter in the main cooperation agreement or by drafting a standalone data processing agreement. To fulfill the supervision obligation, companies typically reserve audit or similar rights, such as requiring the partner to provide documents proving contract compliance. For high-risk or legally sensitive collaborations, enterprises are advised to conduct due diligence on partners—e.g., reviewing negative media, validating security qualifications, requiring disclosure of data sources, inspecting privacy policies and consent forms, and requesting signed compliance undertakings.

V. Risk Assessment Mechanisms

Key risk assessment mechanisms under Chinese law include: Personal Information Protection Impact Assessments (PIPIA) under the *PIPL* (Article 55), Important Data Risk Assessments under the *Data Security Law* (Article 30) and the *Network Data Regulations* on (Articles 31 and 33), and export-related assessments under data transfer mechanisms (e.g., security assessments and standard contract filings).[8]

Under the *PIPL*, personal information processors must conduct PIPIA before engaging in high-impact processing activities.[9] As this often involves collaboration among business, legal, and security teams, many multinational firms deploy automated tools to support the process. It is worth noting that certain privacy assessment tools and frameworks used by enterprises are primarily designed on the basis of the GDPR. When using such tools, enterprises should localize and adapt them in accordance with the requirements and standards of Chinese law (for example, Articles 55 and 56 of the *PIPL*, and the *GB/T 39335-2020 Information Security Technology – Guidelines for Personal Information Security Impact Assessment*) to ensure the completeness of both the triggering scenarios and the assessment content.

Under the *Network Data Regulations* , important data risk assessments fall into two

[8] According to Articles 6 and 8 of the *Measures for Security Assessment of Cross-Border Data Transfer*, when applying for a security assessment of data export, a Self-Assessment Report on the Risks of Cross-Border Data Transfer must be submitted. This report should primarily assess the risks that the outbound data transfer may pose to national security, public interests, and the lawful rights and interests of individuals or organizations.
According to Article 5 of the *Measures on Standard Contracts for the Outbound Transfer of Personal Information*, a Personal Information Protection Impact Assessment must be conducted by personal information processors prior to providing personal information to overseas recipients.

[9] According to Article 55 of the *PIPL*, such processing activities primarily include the handling of sensitive personal information; the use of personal information for automated decision-making; the entrustment of personal information processing to third parties, provision of personal information to other processors, or public disclosure of personal information; cross-border provision of personal information; and other personal information processing activities that may have a significant impact on individuals' rights and interests.

types: activity-triggered assessments[10] and annual activity assessments.[11] At present, the industrial and telecommunications sectors have issued specific risk assessment rules and guidelines: the *Detailed Rules for the Implementation of Data Security Risk Assessment in the Industrial and Information Technology Sector (Trial)* and the *YD/T 3956-2024 Data Security Risk Assessment Specifications in the Telecommunications Sector*. With the gradual advancement and deepening of important data identification work across industries and sectors, further clarification and operational guidance on such risk assessments will continue to be developed and improved.

In practice, many enterprises struggle to distinguish when and how each assessment is triggered. A summary comparison table follows to clarify key differences.

[10] Article 31 of the *NDSM Regulation*: Before providing, entrusting, or jointly processing important data, the processor of such data shall conduct a risk assessment, except where such processing is necessary for performing statutory duties or legal obligations.
The risk assessment shall focus on the following aspects:(1) Whether the purposes, methods, scope, etc., of providing, entrusting, jointly processing network data and of the recipient's processing activities are lawful, legitimate, and necessary; (2) The risks that the provided, entrusted, or jointly processed network data may be tampered with, damaged, leaked, or illegally acquired or used, and the potential impact on national security, public interest, or the lawful rights and interests of individuals or organizations; (3) The integrity and legal compliance of the network data recipient; (4) Whether the relevant contracts concluded or to be concluded with the data recipient can effectively bind the recipient to fulfill network data security protection obligations; (5) Whether the technical and managerial measures taken or to be taken can effectively prevent the network data from being tampered with, damaged, leaked, or illegally acquired or used; (6) Other evaluation matters as prescribed by competent authorities.

[11] Article 33: Processors of important data shall conduct a risk assessment of their network data processing activities annually, and submit a risk assessment report to the competent authorities at the provincial level or above. The relevant authorities shall promptly share the report with the cyberspace administration and public security organs at the same level.
The risk assessment report shall include the following contents: (1) Basic information of the network data processor, information about the network data security management organization, and the name and contact details of the network data security officer; (2) The purpose, type, quantity, method, scope, storage period, and storage location of the important data processed, and the status of network data processing activities, excluding the content of the network data itself; (3) The network data security management system and its implementation, as well as the effectiveness of technical and other necessary measures such as encryption, backup, labeling, access control, and security certification; (4) Identified network data security risks, security incidents that occurred, and response measures taken; (5) The risk assessment results of providing, entrusting, or jointly processing important data; (6) Cross-border transfer of network data; (7) Other report contents as required by competent authorities.
Large-scale network platform service providers that process important data shall include, in addition to the above, a detailed explanation of key business and supply chain network data security situations in their risk assessment reports.

Type of Assessment	Personal Information Protection Impact Assessment	Important Data Risk Assessment	Data Cross-border Security Assessment
Legal Basis	Article 55、56 of *PIPL*	Article 31、33 of *Network Data Regulations*	Article 37 of *Cybersecurity Law*，Article 38 of *PIPL*，*Measures for Security Assessment for Outbound Data Transfer*，*Provisions on Cross-Border Data Flows*
Triggering Circumstances	Ex-Ante Assessment • Processing of sensitive personal information • Automated decision-making using personal information • Entrusting others to process personal information, providing personal information to other processors,	Ex-Ante Assessment • Conducted before providing, entrusting, or jointly processing important data. Annual Assessment • Conducted on a yearly basis, with the annual risk assessment report required to be submitted to the competent authorities at or above the provincial level.	Ex-Ante Assessment • Providing important data overseas • CIIOs providing personal information overseas (except in cases of exemption) • Non-CIIOs cumulatively providing personal information of over 1 million individuals (excluding sensitive personal information) or over 10,000 individuals' sensitive personal

Type of Assessment	Personal Information Protection Impact Assessment	Important Data Risk Assessment	Data Cross-border Security Assessment
	or making personal information public • Providing personal information to overseas parties • Other personal information processing activities that may significantly affect individual rights and interests		information since January 1 of the year (except in cases of exemption)
Implementing Entity	Personal Information Processor	Important Data Processor	Data Processor
Assessment Focus	• Whether the purpose and method of personal information processing are legal, legitimate, and necessary	• Legality, Legitimacy, and necessity of the purpose, method, and scope of providing, entrusting, or jointly processing network data, and how the recipient will process it	•Legality, Legitimacy, and necessity of the purpose, scope, and method of data export • Impact of the data security protection policies, laws, and cybersecurity

Type of Assessment	Personal Information Protection Impact Assessment	Important Data Risk Assessment	Data Cross-border Security Assessment
	• Impacts on individual rights and security risks • Whether the protective measures are lawful, effective, and commensurate with the risk level	• Risks of tampering, destruction, leakage, or illegal access/use of data, and risks to national security, public interests, or lawful rights of individuals and organizations • Integrity and compliance of the data recipient • Whether contractual clauses effectively bind the data recipient to fulfill security obligations • Effectiveness of technical and management measures to prevent risks • Other assessment items as required by competent authorities	environment of the recipient country/region on outbound data security; whether the recipient's protection level meets China’s laws and mandatory standards • Scope, type, sensitivity, and volume of exported data; risks of tampering, destruction, leakage, loss, transfer, or illegal access/use during and after export • Whether data security and personal information rights can be fully and effectively protected • Whether the legal documents with the overseas recipient fully specify security

Type of Assessment	Personal Information Protection Impact Assessment	Important Data Risk Assessment	Data Cross-border Security Assessment
			responsibilities and obligations • Compliance with Chinese laws, regulations, and departmental rules • Other matters deemed necessary by the CAC
Formal Requirements	For transfers under Standard Contract, the assessment report must be prepared based on CAC's official template For other cases, refer to recommended national standard GB/T 39335-2020 *Information Security Technology – Guidelines for Personal*	Referring to the *Detailed Rules for the Implementation of Data Security Risk Assessment in the Industrial and Information Technology Sector (Trial)*, a risk assessment report should include: the basic information of the data processor; the basic information of the assessment team; the categories and quantities of important data; the circumstances	Must be strictly prepared in accordance with the *Guidelines for the Application for Security Assessment for Outbound Data Transfer*

Type of Assessment	Personal Information Protection Impact Assessment	Important Data Risk Assessment	Data Cross-border Security Assessment
	Information Security Impact Assessment	of the data processing activities carried out; the environment for data security risk assessment; as well as analysis of data processing activities, compliance assessment, security risk analysis, assessment conclusions, and proposed mitigation measures.	

VI. Security Incident Response and Handling

The *Data Security Law*, the *PIPL*, and the *Network Data Regulations* each set forth clear requirements for responding to and handling data (including personal information) security incidents.[12] These provisions generally require enterprises to immediately activate contingency plans upon the occurrence of a security incident, take measures to prevent further harm and eliminate security risks, report to the competent authorities as required, and determine whether affected individuals should be notified based on the severity of the incident.[13]

[12] Article 20 of *Data Security Law*, Article 57 of *PIPL*, and Article 11 of *NDSM Regulation*.
[13] For example, Article 57 of the *PIPL* permits enterprises to refrain from notifying individuals if effective

The *Administrative Measures for Cybersecurity Incident Reporting (Draft for Comment)*, released in 2023 but not yet formally enacted or effective, further define the scope, classification, and requirements for responding to and handling cybersecurity incidents. According to the draft, a “cybersecurity incident” refers to an event that, due to human factors, software/hardware defects or failures, or natural disasters, causes harm to networks, information systems, or the data within them, and has a negative impact on society. This definition makes it clear that cybersecurity incidents encompass data security incidents, and responses to the latter must also follow the relevant rules. Under this draft regulation, when a cybersecurity incident occurs and it is classified as relatively major, major, or particularly major (e.g., involving the leakage of personal information of over 1 million individuals, or the leak or theft of important data that poses a significant threat to national security and social stability), network operators must report it within 1 hour using the “Cybersecurity Incident Information Reporting Form”.[14]

Regulators such as the CAC, Public Security authorities, and the MIIT have each established security incident reporting obligations within the scope of their respective responsibilities in the fields of cybersecurity or data protection, thereby providing enterprises with multi-level guidance for handling data security incidents. As each authority has different functional priorities, enterprises should, when a security incident occurs, carefully assess the nature and type of the incident and accurately fulfill the corresponding reporting obligations so that regulators can obtain timely information.In practice, enterprises are advised to pay close attention to whether the locality where the security incident occurs has introduced a coordination mechanism for

---

measures have been taken to avoid harm caused by the leakage, alteration, or loss of personal information. However, if the regulatory authorities determine that such incidents may still result in harm, they retain the authority to require the enterprise to notify the affected individuals.

[14] According to Article 5 of the *Measures for the Reporting and Management of Cybersecurity Incidents (Draft for Comments)*, an incident report shall at minimum include the following:
(1) The name of the affected entity and basic information about the facilities, systems, or platforms involved in the incident; (2) The time and location of the incident’s detection or occurrence, the type of incident, the impact and damage already caused, and measures taken along with their effectiveness. For ransomware attacks, the report shall also include the ransom amount, payment method, and payment date; (3) The anticipated development of the incident and the potential further impact and damage; (4) Preliminary analysis of the cause of the incident; (5) Clues required for further investigation and analysis, including potential attacker information, attack paths, existing vulnerabilities, etc.; (6) Proposed response measures and requests for assistance; (7) Information on the preservation of the incident scene; (8) Other information that should be reported.

cybersecurity incident reporting, in order to ensure that reporting obligations are fulfilled promptly. Moreover, although multinational corporations often have internal contingency plans for information security incidents, such plans frequently focus on internal alerts, responses, and mitigation measures, while lacking clear guidance on external obligations such as regulatory reporting and notification to affected data subjects. Enterprises are therefore encouraged to incorporate the following considerations when developing or updating their incident response protocols:

Tiered Reporting Mechanism: In accordance with provisions such as the *Emergency Plan for Data Security Incidents in the Industrial and Information Technology Sector (Trial)*, classify data security incidents based on their severity (e.g., particularly major, major, relatively major, general), and report to the competent authorities within the required timeframe when legal conditions are met.

Notification Requirements for Personal Information Subjects: If a security incident involves personal information and causes harm to individuals, the affected personal information subjects must be notified within the prescribed timeframe. Although such a requirement is reflected in most data protection legislation globally, special attention should be paid to the specific provisions of each jurisdiction regarding the notification timeframe, content, and other details. Under Chinese regulations, the notification generally should include the following:

- Basic information about the incident (e.g., types of personal information involved, cause of the incident);
- Risk level and potential adverse consequences;
- Remedial measures already taken;
- Recommendations for affected individuals to mitigate risks;
- Contact details of the enterprise for follow-up communication.

Enterprises should align their emergency response protocols with both Chinese regulations and relevant regulatory requirements in Singapore, to ensure compliant and effective handling of data security incidents.

Chapter IV. Compliance Management Standards for Data Subject Matter※

To ensure data compliance when conducting business in China, it is essential to understand the basic logic behind China's data governance framework. The Chinese data governance system classifies data from two perspectives: from a national security standpoint, data is divided into core data, important data, and general data based on its level of sensitivity. This classification system originates from the *Data Security Law* and is intended to strengthen the protection of data related to national security through tiered management. From the perspective of data utilization, the *20 Measures on Data* distinguishes data into personal information, public data, and enterprise data, based on the ownership and purposes of the data utilization, thereby promoting the reasonable circulation and efficient use of data elements on the basis of safeguarding security.

The foregoing classification system reflects China's policy orientation in data governance: on the one hand, through tiered management, it enhances the protection of core data and important data, and prevents risks to national security; on the other hand, through classified management, it seeks to balance the relationship between data security and the circulation of data elements.

Moreover, industries with unique characteristics must comply with sector-specific data management rules. The following sections provide a brief overview of China's data classification and grading logic and explain compliance requirements for important data, personal information, public data, general data, and sector-specific data.

※ The authors of this chapter are Huang Jiajie, Partner at Beijing East & Concord Partners; Ma Kaiyang, Lawyer at V&T (Shenzhen) Law Firm; Li Rui, Partner at Zhong Lun Law Firm; Duan Zhichao, Partner at Beijing Han Kun Law Offices; Meng Jie, Partner at Beijing Global Law Office; Pu Yihan, Lawyer at Zhong Lun Law Firm; Xu Chen, Former Lawyer at Zhong Lun Law Firm; Wang Yuting, Consultant at Beijing Han Kun Law Offices; Lin Yi, Consultant at Beijing Global Law Office (Chengdu). Wang Yi, Zhang Yi, Shi Jingyuan, Liu Jiayi, Li Huihui, Lai Yanyu, and Lai Yuchen also contributed.

I. Common Requirements for General Data※

Why is it necessary to pay attention to the common compliance management requirements for general data?

In practice, there exists a widespread compliance blind spot in the management practices of enterprises (particularly those that do not provide services directly to end-consumers at the C-end): so long as data does not involve personal information or important data, it is generally assumed that there are no statutory or regulatory compliance obligations with respect to other "general data," and that the arbitrary management and use of such data entails no compliance risks.

However, the use of general data by enterprises must comply with the regulatory requirements set forth in the *Cybersecurity Law*, the *Data Security Law*, and other applicable laws and regulations. In addition, with the official promulgation of the *Network Data Regulations* on August 30, 2024, Chapter II "General Provisions" expressly sets forth the compliance principles and baseline requirements that enterprises shall comply with when processing general data. Although the compliance management of general data is not as stringent as that applicable to important data and personal information, enterprises are nevertheless required to implement requirements across multiple dimensions, including data classification and grading, lawfulness of processing, security throughout the entire data lifecycle, risk prevention and control, and institutional safeguards.

(i) Definition of General Data

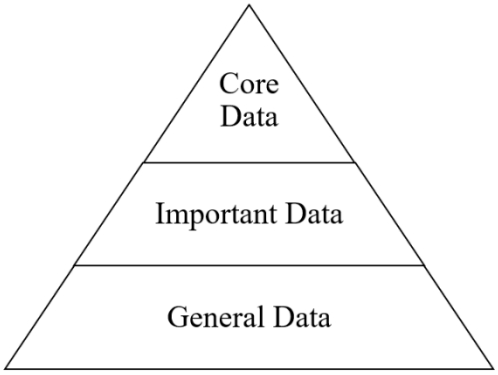
With respect to the definition of general data, according to the provisions of the national standard *Data Classification and Grading Rules,* general data refers to data other than

※ The author of this chapter, Lawyer Huang Jiajie, is Partner at Beijing East & Concord Partners, with a dual professional background in Chinese and U.S. law. She serves as a compliance advisor to numerous central state-owned enterprises, state-owned enterprises, listed companies, and leading industry enterprises, and is dedicated to the fields of compliance and risk governance, as well as data and cybersecurity. She has been recognized as an Emerging Foreign-related Lawyer of Guangdong Province, a compliance expert of the Shenzhen Committee of the China Council for the Promotion of International Trade, and a corporate compliance expert for the rule-of-law business environment of Shenzhen. She has undertaken multiple government research projects in Shenzhen's pioneering rule-of-law initiatives and compliance pilot programs.

core data and important data.

Impact Object	Degree of Impact		
	Severe Harm	Significant Harm	General Harm
National Security	Core Data	Core Data	Important Data
Economic Operation	Core Data	Important Data	General Data
Social Order	Core Data	Important Data	General Data
Public Interest	Core Data	Important Data	General Data
Organizational Rights and Interests, Personal Rights and Interests	General Data	General Data	General Data
Note: If large - scale personal or organizational rights and interests are affected, the impact object may include not only personal rights and interests or organizational rights and interests, but also may impact national security, economic operation, social order or public interest.			

(Source: Table 1 - Rules Table for Determining Data Levels in *Data Classification and Grading Rules*)The scope of general data is extensive. Apart from core data and important data, the majority of data that ordinary enterprises come into contact with and use in the course of their daily operations and management may generally be classified as “general data” (including personal information). The diagram below provides an intuitive reflection of the scope of general data, serving as a reference and aid for enterprise understanding.



(ii) Common Types of General Data

Given that personal information and public data have been discussed in detail in other sections of this chapter, this section focuses on **other types of general data**, namely internal enterprise data that does not involve national security, public interests, or significant social impacts. The following list of data types is compiled based on industry practices **for reference only**. Enterprises should note that: the nature of the same data may change depending on the usage scenario (for example, production logs in the manufacturing industry are general data, but may be upgraded to important data if they involve critical infrastructure); some data may involve multiple classification dimensions simultaneously (for example, customer service recordings belong to "operation and management data", and if they contain personal information, the requirements of the PIPL must also be applied).

(iii) Key Compliance Requirements for General Data

The use and processing of general data shall, in general, comply with the basic requirements and provisions of the *Data Security Law*. Given that the data used and processed by enterprises at present are mainly network electronic data, enterprises still need to focus on the key provisions and compliance requirements under the *Cybersecurity Law* and the *Network Data Regulations*. The compliance management requirements that enterprises should carry out for general data under the above laws and regulations are summarized according to the key control points as follows:

1. **General Principle: Legality and Compliance**

Enterprises shall adopt legal and proper methods when collecting general data, and shall not engage in illegal processing activities such as stealing or obtaining general data through other illegal means, illegally selling or illegally providing general data to others.

In addition, enterprises shall not provide programs or tools specifically used for the illegal activities mentioned in the preceding paragraph; if they know that others are engaged in the illegal activities mentioned in the preceding paragraph, they shall not provide technical support such as Internet access, server hosting, network storage, or communication transmission, or provide help such as advertising promotion or payment and settlement.

Enterprises shall conduct compliance assessments of partners and business operations, including: establishing a comprehensive data governance system, strictly prevent participation in any operations that violate data security laws and regulations, and focus on monitoring illegal acts such as illegal acquisition, transaction, or disclosure of data resources; simultaneously conduct due diligence on partners, and systematically terminate collaborative cooperation such as network infrastructure services, cloud computing resource supply, data storage space leasing, opening of information transmission channels, digital marketing support, and docking of financial payment interfaces for market entities with credit flaws or abnormal operations.

2. Cybersecurity and Technical Measures

Article 21 of the *Cybersecurity Law* stipulates that network operators shall fulfill relevant security protection obligations in accordance with the requirements of the cybersecurity grading protection system.

According to the definition of “network” in the *Cybersecurity Law*, it refers to a system composed of computers or other information terminals and related equipment that collects, stores, transmits, exchanges, and processes information in accordance with certain rules and procedures.

In practice, many enterprises simply construe “network” as limited to website operation,

app operation, or other direct online business systems. However, the scope of “network operators” includes those engaged in the Internet, private networks, cloud computing platforms/systems, the Internet of Things, industrial control systems, mobile Internet technology systems, etc. (excluding personal or family - used networks). Specifically, if an enterprise’s business includes cloud platforms, Internet of Things systems, SaaS systems (Software as a Service), or other products or services with networking functions, it should be regarded as a “network operator” and is required to comply with relevant cybersecurity compliance requirements.

Enterprises that carry out data processing activities through information networks such as the Internet shall fulfill data security protection obligations on the basis of the cybersecurity grading protection system. Specifically, enterprises need to strengthen network data security protection, establish and improve network data security management systems, adopt technical measures such as encryption, backup, access control, and security authentication, as well as other necessary measures to protect network data from tampering, damage, leakage, illegal acquisition, or illegal use. They shall handle network data security incidents, prevent illegal and criminal activities targeting or using network data, and assume the main responsibility for the security of the network data they process.

3. Risk Prevention and Control as well as Emergency Response

When conducting data processing activities, enterprises shall strengthen risk monitoring. If risks such as data security defects and vulnerabilities are found, they shall immediately take remedial measures and fulfill the reporting obligations.

Firstly, enterprises shall establish a dynamic risk monitoring mechanism covering the entire life cycle of data processing. By combining the deployment of automated audit tools with manual inspections, they can promptly identify security risks such as abnormal data storage and API interface vulnerabilities, and establish a closed-loop mechanism for risk repair.

Secondly, it is recommended that enterprises establish a hierarchical disposal mechanism for security incidents. For example, for primary risks (such as single-point system vulnerabilities), the technical team shall complete patch upgrades within 48 hours and retain repair logs; for intermediate risks (such as partial data leakage), immediately activate the business continuity plan and simultaneously assess the scope of impact; for advanced risks (such as large-scale data tampering), a cross-departmental emergency response team shall be formed within 30 minutes, implement system fusing and report to the decision-making level.

Thirdly, establish a dual notification and reporting mechanism, whereby security incidents are notified and reported to both users and regulators. On the user side, differentiated notifications and announcements might be adopted according to data types (for personal information, it shall be delivered via registered email/SMS within 72 hours after confirming the leakage); on the regulatory side, in accordance with the requirements of Article 42 of the *Cybersecurity Law*, enterprises shall submit a structured incident report through the provincial regulatory platform (including the type/quantity of affected data, measures taken, contact information, etc.).

4. Cooperation and Third-Party Risk Management

For general data, enterprises also face cooperation scenarios such as providing data to external parties and entrusting others to process data. For example, an enterprise may outsource some functional modules in its R&D system for R&D, testing, operation and maintenance, after - sales service and other work.

In practice, contracts between enterprises and third parties are most often in the form of “Entrusted Development Agreements”, which contain general intellectual property clauses, confidentiality clauses and other contents, but there are few provisions on rights and obligations in terms of data security, or contain only broad and general clauses (e.g., “the parties shall comply with relevant requirements on data security and cybersecurity”). Although the current laws and regulations do not directly stipulate the contractual data compliance clauses for general data, in order to reduce the risks of

enterprises in data flow, it is suggested that enterprises refer to the requirements for the provisions of contractual clauses on “providing to external parties and entrusting processing” in the *PIPL* and the *Network Data Regulations*, and add data security clauses in the cooperation agreements including, inter alia, the following principal provisions:

Data Processing Status	**Specific indicators such as the type and quantity of data being processed**
	Purpose, method and scope of processing
	Without consent, data must not be accessed, obtained, retained, used, disclosed, or provided to others, and must not be subjected to correlation analysis.
	Data processing (return/destruction) after the contract ends
Security Management Obligations	Compliance management measures and guarantees provided within the enterprise
Acceptance of supervision	Agree to accept inquiries and inspections from the data source regarding data processing activities, and accept supervision/audit
Liability for Breach of Contract	Liability for breach in the event of non-compliance with contractual stipulations concerning data processing

5. Data Assets and Transactions

As the data type with the largest proportion in an enterprise’s production and operation, general data is also the main target for enterprises considering initiating data assetization and data transactions. Currently, general data (excluding personal

information) is reflected in a variety of product types in the data element market. The following are three examples of product forms:

Industry Forecast and Analysis Products	**Such products, based on big data analysis, can provide users with information such as industry trends, market competition patterns, and consumer behavior analysis. Take the real estate big data monitoring system as an example. It may assist numerous real estate enterprises or other industries involved in the real estate market (such as the financial sector) in conducting big data-driven decision-making and monitoring.**
Risk Early Warning Model Products	Risk early warning models usually refer to risk assessment models built using machine learning technology, which help enterprises identify, analyze and warn risks for specific users or subjects. For example, they can assess the credit status of specific enterprises. Risk early warning models are widely used in fields such as finance, credit and credit investigation.
IoT Data Services	IoT data services are an emerging field at present. Both medical enterprises and communication technology and manufacturing enterprises have seen changes in their demand for the IoT. Enterprises usually connect devices to the cloud and then to the company's internal system network platform to support the entire IoT business form. The IoT involves device sensing data services, cloud platforms, and company internal platforms, and the relevant data consists of internal data of individual users and enterprise users.

While enterprises are initiating data assetization and data transactions, they must also strictly conduct compliance reviews on the compliance of general data in accordance with relevant laws and regulations. Taking the Shenzhen local standard *DB4403/T564—2024 Specifications for Compliance Assessment of Data Transactions* as an example, the compliance requirements for data subjects involve conducting compliance reviews from the dimensions of legality, security, integrity, and rights and interests.

II. Important Data※

(i) Relevant Identification and Assessment of Important Data

As previously mentioned, when Singaporean companies based in China acquire and process data, they should first classify the data in accordance with relevant laws and regulations of China. The process generally includes: determining the scope of data to be classified, identifying classification elements, and conducting a data security impact analysis, in order to ultimately identify and assess whether the data involves core data or important data. However, as industry-specific catalogues of important data are still being formulated successively, certain ambiguities remain in the practical application of relevant identification standards. Against this backdrop, local regulations and industry guidelines serve as a strong supplement and reference in the process of identifying and assessing important data, thereby assisting enterprises in more accurately understanding and performing their data compliance obligations.

1. Methods for Identifying Important Data

Specifically, any of the following criteria would indicate that the data in question should be classified as important data:

(1) Data that, once leaked, tampered with, damaged, or illegally obtained, used, or shared, could pose general risks to national security, economic operations, social order, or the public interest[15];

(2) Data that directly relates to specific domains, populations, or regions and concerns national security, economic operations, social stability, or public

※ The author of this chapter is Kaiyang Ma, Lead of the International Committee and Hong Kong Representative of V&T Law Firm. He is qualified to practice law in China and New York State, USA. He serves as a council member of the Information and Communication Law Research Society of Guangdong Law Society and a council member of the Digital Law Research Society of Shenzhen Law Society. He acts as a compliance advisor for several leading industry companies and AI data companies. His accolades include LEGALONE "Blue Ribbon 15: Cross-Border Dispute Resolution", LEGALBAND "China Legal Profession Outstanding Young Talents 30", LEGAL ONE "Stella Novo 30", Guangdong Province Foreign-Related Lawyer Rising Talent, and Shenzhen Outstanding Young Lawyer.

[15] The specific considerations for national security, economic operations, social order, and public interest can be found in Appendix E and Appendix G of the *Data Classification and Grading Rules*.

health and safety;

(3) Data that reaches a certain level of precision, scale, depth, or importance and directly affects national security, economic operations, social stability, or public health and safety;

(4) Data identified as important by competent industry regulators through evaluation.

Upon completion of data-item level identification using the criteria above, if the object of classification is a dataset or derived data, enterprises must further determine the classification level by applying the “strictest applies” and “combined point-and-scope” principles:

（1） If the classification object is a dataset, the dataset’s classification level should, by default, be the highest level among its constituent data items, in line with the “strictest applies” principle. Additionally, the classification level should be adjusted as necessary based on classification elements (e.g. data volume).

（2） If the classification object is derived data (including de-identified data, labeled data, statistical data, and integrated data), its level should be determined based on the classification of the original data and the added influence of processing factors such as data depth, in terms of risks posed to national security, economic operations, social order, public interest, organizational interests, and individual rights.

2. Identification Guidelines Issued by Local Authorities

Meanwhile, several local authorities have issued identification guidelines, providing Singaporean companies that based in China with practical references when classifying and assessing important data. Tianjin, Beijing, Hainan, Shanghai, Zhejiang, and other regions have successively formulated and issued negative lists for cross-border data transfer within pilot free trade zones, covering seventeen sectors including

automobiles, pharmaceuticals, retail, civil aviation, reinsurance, deep-sea industries, and seed industries, with the aim of providing a clearer compliance pathway and creating more favorable conditions for the cross-border flow of relevant data[16].

3. Industry-Specific Identification Guidelines

In addition to general or regional rules, regulators in specific industries have developed detailed classification and grading standards tailored to their sectors. Below are examples from the financial, healthcare, and technology sectors.

(1) Financial Sector

On December 28, 2024, China's National Financial Regulatory Administration issued the Measures for Data Security Management of Banking and Insurance Institutions, which outlines requirements for data governance, classification and grading, technical protection, personal information protection, and risk monitoring.

On September 23, 2020, the People's Bank of China issued the Guidelines for Financial Data Security Grading (JR/T 0197-2020), which provides detailed guidance on: (1) Objectives, principles, and scope of financial data grading; (2) Grading elements, rules, and procedures; (3) Criteria for identifying important data. This guideline is a recommended industry standard.

On August 6, 2023, the People's Bank of China issued the *Guidelines for Classification and Grading of Data Security Risks in the Securities and Futures Industry* (GB/T 42775-2023), which is a recommended national standard. It covers: (1) Safeguards for data classification and grading in the securities and futures sectors; (2) Principles, key points, and methods for classification and grading; (3) Solutions to key issues in data classification and grading.

(2) Healthcare Sector

On July 1, 2021, China's State Administration for Market Regulation and the

[16] WeChat Official Account "Compliance Xiaodaoke" "Following the Release of Negative Lists for Data Exports in China's Free Trade Zones, How Will This Impact Enterprise's Management of Important Data?"

Standardization Administration jointly implemented the *Guidelines for Health and Medical Data Security in Information Security Technology* (GB/T 39725-2020). This guideline provides detailed provisions on data security objectives, classification frameworks, usage and disclosure principles, security measures, and typical scenarios (e.g. physician access to patient data, patient inquiries).

(3) Technology Sector

On January 24, 2025, the State Administration for Market Regulation and the Standardization Administration jointly released the *Guidelines for the Security Classification and Grading of Scientific Data*, a recommended national standard that provides comprehensive rules for the classification and grading of scientific data and relevant principles.

4. Dynamic Evaluation and Adjustment Mechanism

In the context of accelerating digitalization and intensifying global competition, the identification and management of important data is not a static task, but rather a systematic undertaking that must dynamically adapt to technological iteration, business expansion, and regulatory evolution. As data classification and grading standards continue to be refined, enterprises are required to establish a closed-loop "identification–assessment–adjustment" mechanism to address complex challenges such as cross-border data flows and the application of emerging technologies. This should be accomplished through regular updates of data classification and grading, dynamic monitoring of risk scenarios, and flexible optimization of protective strategies. When there are changes in the business attributes, importance, or potential harm of the data, the classification level of the data subject must be dynamically updated.

Once important data has been initially identified, enterprises should promptly initiate dynamic evaluation and adjustment procedures in response to the following common scenarios:

（1） Changes in data scale render the original security classification no longer applicable;

（2） While the content of the data remains unchanged, significant changes occur in its timeliness, scale, application scenarios, or processing methods;

（3） Direct merging of multiple original datasets causes the original classification to no longer apply to the merged dataset;

（4） A newly formed dataset is created by partially combining elements from different datasets, making the original classification level unsuitable for the new dataset;

（5） The aggregation and integration of different data types results in a new data category, thereby invalidating the previous classification levels;

（6） The data is subjected to desensitization, key field deletion, or has undergone de-identification or anonymization processing;

（7） A data security incident occurs, leading to a change in the sensitivity of the data;

（8） Reclassification is mandated by national or industry regulators, rendering the original classification obsolete;

（9） Other circumstances arise that necessitate changes to the data’s security classification level.

(ii) Obligation for Managing Important Data

1. Adoption of Technical and Other Necessary Measures

As a network data processor handling important data, an enterprise must implement encryption, backup, access control, security authentication, and other technical and necessary measures to protect network data.

In addition, both the *Cybersecurity Law* and the *Network Data Regulations* impose general security protection obligations on all network operators and network data processors. These general provisions are not reiterated here.

2. Specific Security Obligations for Processors of Important Data

Beyond the general requirements, enterprises identified as network data processors of important data must undertake the following security obligations:

(1) Identification and Reporting of Important Data

Enterprises must identify and report important data to the relevant authorities. The reporting requirements across industries and regions are broadly similar—with respect to targets, content, and procedures. Representative examples are as follows:

Automotive Sector: The Cyberspace Administration of Guangdong Province has explicitly required that automotive data processors registered in Guangdong and engaged in important data processing activities must submit the *Annual Report on Automotive Data Security Management* and a *Risk Assessment Report*, as well as complete the *Information Form for Automotive Data Processors Engaged in Important Data Processing Activities*. Enterprises may submit these materials either in hard copy or electronically to the Guangdong Cyberspace Administration. In addition to the Guangdong authority, the Beijing Cyberspace Administration, the Beijing Municipal Bureau of Economy and Information Technology, and the Beijing Communications Administration have jointly organized the submission of the 2024 *Beijing Automotive Data Security Management Reports* and other relevant documentation.

Shanghai*:* Since 2023, the Shanghai Communications Administration has organized pilot enterprises to carry out identification and filing of important data catalogs in accordance with relevant industrial data classification and grading guidelines. During this period, expert panels from the city's Data Security Working Committee reviewed the submitted important data through two rounds of evaluation and provided guidance via assessment summaries, public training sessions, and on-site interviews to help enterprises complete data classification, identification, and protection tasks.

(2) Appointment of a Network Data Security Officer and Establishment of a Security Management Body

Under Article 30 of the *Network Data Regulations*, a network data processor of important data shall appoint a network data security officer and a network data security management body. Enterprises must designate a network data security officer who possesses professional knowledge and relevant management experience in network data security. This individual must be a member of the enterprise's senior management and authorized to report directly to regulatory authorities.

The network data security management body must fulfill the following responsibilities:

- Develop and implement internal policies, operational protocols, and emergency response plans for network data security;
- Regularly organize risk monitoring, assessments, incident response drills, and awareness training to promptly address risks and incidents;
- Handle complaints and reports related to network data security.

If the enterprise processes important data of specific types or scales as defined by regulatory authorities, it must also conduct security background checks on the data security officer and key personnel and strengthen their training. Public security and national security agencies may be requested to assist in background checks.

(3) Risk Assessment Obligations

As an important data processor, an enterprise must fulfill risk assessment obligations in the following circumstances:

- Before providing, commissioning, or jointly processing important data, a risk assessment must be conducted.
- Enterprises must conduct an annual risk assessment of their network data processing activities and submit the report to the competent authority at or above the provincial level.

The content of risk assessments and the structure of the risk assessment reports are specified in Articles 31 and 33 of the *Network Data Regulations*. In addition to these requirements, enterprises must also follow industry-specific rules and formats when

conducting assessments.

Continuing with the example of the automotive industry risk assessment report in Guangdong Province, the report primarily covers the following aspects:

Overview of Automotive Data Security Risk Assessment: this section includes the objectives and scope of the assessment, as well as a summary of the assessment conclusions.

- Basic Information: This section provides general information about the entity, the business scenarios involving data processing, relevant information systems, and details regarding the types, volumes, scope, storage location and duration, and usage of important data. It also includes a description of data processing activities and whether the data is provided to third parties.
- Identification of Automotive Data Security Risks: Risks are identified across the entire data lifecycle, including collection, storage, usage, processing, transmission, provision, disclosure, deletion, and cross-border transfer. Risk points are identified in accordance with relevant regulatory requirements, such as the *Provisions on Automotive Data Security Management (Trial)* and related standards.
- Analysis and Evaluation of Automotive Data Security Risks: Based on the identified risk points, the report assesses the overall data security risk level by considering both the potential severity of harm and the likelihood of security incidents occurring.
- Assessment Summary and Risk Mitigation Measures: This section describes the security measures implemented to address identified risks, evaluates the effectiveness of these measures, and provides a final summary of the assessment outcomes.

Additionally, in accordance with the requirement in *Network Data Regulations,* for large-scale network platform service providers handling important data, the report must also include detailed information about the security of critical business and supply chain data.

(4) When circumstances such as mergers, splits, dissolution, or bankruptcy occur and may affect the security of important data, the enterprise must take necessary protective measures and report the data disposal plan to the relevant competent authority at or above the provincial level. The report must include the name and contact details of the receiving party. If the competent authority is unclear, the report should be submitted to the provincial-level coordination mechanism for data security.

(5) When enterprises provide or entrust important data processing to other network data processors, they must enter into agreements that specify the purpose, methods, scope, and data protection obligations. Enterprises must also supervise the recipient's compliance and ensure that records of important data and personal information processing are retained for at least three years.

III. Personal Information※

As a special category of data, personal information not only concerns data security, but also involves broader legal issues such as the rights to personality and privacy of natural persons. Therefore, the overall requirements for its protection and compliance are more refined, and law enforcement in practice is also the most active. For enterprises, personal information protection runs through all aspects of internal management and external business operations, including but not limited to customer personal information protection, employee personal information protection, and protection of personal information of contacts of upstream and downstream business partners. For enterprises whose business model targets the consumer end and/or those that treat personal information as a key production element (such as cross-border e-commerce, artificial intelligence, pharmaceutical research and development, etc.), it is also necessary to comprehensively consider the applicable personal information protection requirements and the actual situation of information system

※ The authors of this chapter are Li Rui, Partner at Zhong Lun Law Firm, who provides legal services on cybersecurity and data compliance in China for numerous domestic and international enterprises, with extensive experience in cutting-edge areas such as cross-border data transfer, artificial intelligence, and digital transformation, and whose practice covers cybersecurity and data compliance issues arising in multiple contexts including daily operations, investment and financing, and regulatory investigations; Pu Yuhan, a lawyer at Zhong Lun Law Firm; and Xu Chen, a former lawyer at Zhong Lun Law Firm.

architecture, so as to seek a better balance between compliance risk management and business development.

(i) Overview and Introduction

From a legislative perspective, China's personal information protection requirements are primarily based on the compliance framework established under the *PIPL*, while also being subject to the general data security obligations provided under other laws and regulations such as the *Civil Code*, the *Cybersecurity Law*, and the *Data Security Law*. On top of this foundation, regulatory authorities have issued guiding documents during the course of enforcement to clarify and refine certain compliance requirements, which carry strong instructive value — for example, the *Measures for the Determination of Illegal and Non-Compliant Acts of App Collecting and Using Personal Information*. A series of national and industry standards also play an important role within China's personal information protection regulatory framework and serve as key references for enterprises in carrying out compliance work.

The *PIPL* and relevant regulations establish multiple fundamental principles and core mechanisms for personal information protection, similar to those under the *GDPR*. They set out requirements for full-lifecycle protection and regulate important aspects such as the protection of data subjects' rights and responses to personal information security incidents. In addition, under relevant legal requirements, personal information processors must build a sound internal compliance system, including organizational structures, policies, and key compliance tools.

Taking into account the regulatory framework and compliance requirements mentioned above, this chapter will first clarify certain key concepts relevant to determining when China's personal information protection obligations are triggered. It will then explain the fundamental principles underlying personal information protection, analyze the compliance requirements across each stage of the personal information lifecycle, and summarize the additional protection obligations applicable to two special categories of

personal information. Finally, the chapter will introduce key compliance measures for enterprises to implement under the personal information protection regime.

（ii）Assessment and Determination on the Triggering of Personal Information Protection Obligations

1. Definition of Personal Information and Related Key Concepts

According to the *PIPL*, personal information refers to all kinds of information, recorded electronically or otherwise, that relates to identified or identifiable natural persons. Information that has been anonymized — meaning it has been processed in such a way that it can no longer be used to identify a specific natural person and cannot be restored — is not regarded as personal information.

When determining whether they are subject to personal information protection requirements, enterprises should first assess whether their business processes involve the handling of personal information, based on the definitions above. For more detailed definitions of the terms “personal information” and “anonymization,” please refer to Appendix 1: Terminology.

2. Extraterritorial Effect of China’s Personal Information Protection Requirements

According to Article 3, Paragraph 2 of the *PIPL*, if an enterprise located outside China processes personal information of individuals located inside China, and such activities are for the purpose of providing products or services to individuals in China, analyzing or assessing their behavior, or under other circumstances provided by laws or administrative regulations, then the *PIPL* also applies to such activities. Thus, similar to the *GDPR*, the *PIPL* has extraterritorial effect. For personal information processors (i.e., enterprises) meeting the conditions of Article 3 of the *PIPL*, the law applies even if they are located outside China.

(iii) Personal Information Protection Requirements

Under China's legislative and regulatory framework for personal information protection, personal information processors must first have a legitimate basis for processing personal information. In addition, they must implement targeted personal information protection measures at each stage of the personal information lifecycle. An introduction to the legal bases for processing personal information is provided in Section 3.1 below. The various stages of the lifecycle and the corresponding compliance requirements are discussed in Section 3.2.

1. Legal Bases for Processing Personal Information

First, the processing of personal information must be grounded in one of the seven legal bases explicitly set out in Article 13 of the *PIPL*. In commercial practice, the most commonly relied upon legal basis is obtaining informed consent from the personal information subject (hereinafter, the *notice-and-consent mechanism*), whereby the enterprise must inform the individual of its intended personal information collection activities and obtain their consent. For the specific practices related to this mechanism, see Section 3.2, Subsection (1) of this chapter.

It is particularly important to note that in scenarios that may have a greater impact on the rights and interests of personal information subjects, the personal information processor must obtain the individual's **separate consent** (e.g., through a separate pop-up window or checkbox selection by the user). Such scenarios include:

a. Processing of sensitive personal information;
b. Provision of personal information to parties outside of China;
c. Provision of personal information to other personal information processors;
d. Public disclosure of personal information;
e. Use of personal images or identification information collected through image capturing or identification devices installed in public places for purposes other than maintaining public safety;
f. Other circumstances requiring separate consent as stipulated by laws or

administrative regulations.

According to Article 13 of the *PIPL*, in addition to the notice-and-consent mechanism, the other legitimate bases for processing personal information include:

a. Where necessary for the conclusion or performance of a contract to which the individual is a party, or for human resources management in accordance with lawfully established employment rules or lawfully concluded collective contracts;

b. Where necessary for fulfilling statutory duties or obligations;

c. Where necessary for responding to public health emergencies or protecting the life, health, or property of natural persons in emergency situations;

d. Where personal information is processed to carry out news reporting or public supervision in the public interest, within a reasonable scope;

e. Where the personal information has been lawfully and publicly disclosed by the personal information subject themselves or through other lawful means, and is processed within a reasonable scope;

f. Other circumstances as provided by laws and regulations.

2. Full Lifecycle Protection Requirements for Personal Information

The lifecycle of personal information includes various stages such as collection, storage, processing and use, entrusted processing, sharing, transfer, public disclosure, and deletion.

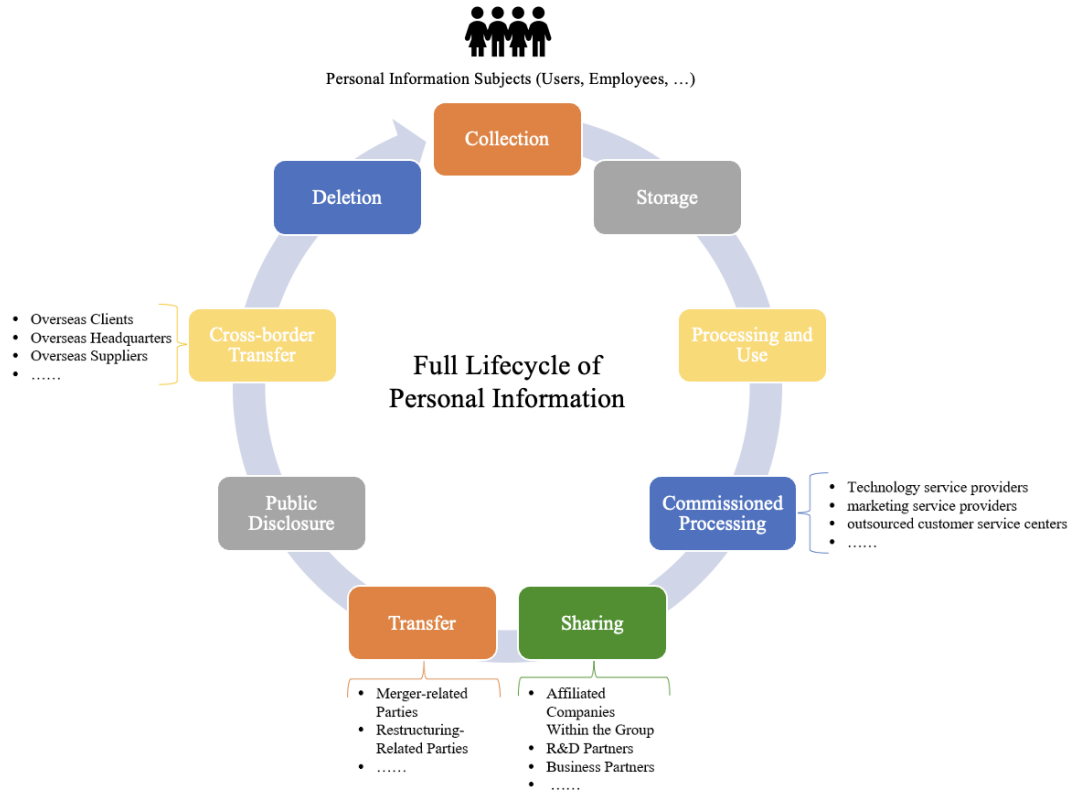


Figure: Stages of the Personal Information Lifecycle

As a general requirement, during the process of protecting personal information throughout its lifecycle, enterprises must first implement the following key principles set forth in the *PIPL*:

a. Legality, Legitimacy, and Necessity Principle: Personal information must not be processed through misleading, fraudulent, coercive, or other improper means;
b. Purpose Limitation Principle: The processing of personal information must have a clear and reasonable purpose and be directly related to that purpose. The method of processing should minimize any impact on the rights and interests of individuals;
c. Data Minimization Principle: The collection of personal information must be limited to the minimum scope necessary to achieve the processing purpose. Over-collection is prohibited;
d. Transparency Principle: The processing of personal information must follow the principles of openness and transparency. Enterprises must publicly disclose their rules for handling personal information and explicitly state the purposes, methods,

and scope of such processing;

e. Accuracy and Integrity Principle: Enterprises must ensure the quality of personal information during processing to avoid adverse effects on individuals caused by inaccurate or incomplete information.

Sections 3. below, we will, on the basis that personal information processors rely on the notice-and-consent mechanism as their lawful basis, introduce the specific compliance obligations enterprises must fulfill at each stage of the personal information lifecycle.

3. Full Life-Cycle Compliance Obligations of Personal Information

(1) Collection of Personal Information

As previously noted, the notice-and-consent mechanism is the most commonly invoked legal basis in commercial practice. To implement this mechanism, enterprises must clearly inform personal information subjects of the types and purposes of the personal information being collected, the rules governing its processing (including but not limited to the data storage location, retention period, the enterprise's data security capabilities, and whether the data will be shared, transferred, or publicly disclosed), ensuring that individuals give their authorization voluntarily and explicitly based on informed consent. If minors' personal information is collected, special requirements related to the notice-and-consent mechanism outlined in Section 3.3 of this chapter must also be observed.

It is also important to note that an individual's consent must be specific and clear. It cannot be obtained through default settings, pre-checked boxes, or other ambiguous methods that fail to reflect the true intent of the personal information subject (e.g., a pop-up interface where "Agree" or similar buttons are automatically selected by the system).

In practice, enterprises often collect personal information not only directly but also indirectly from third parties during their operations. Depending on the collection method, the approach to ensuring compliance with the notice-and-consent mechanism varies

slightly:

a) Direct Collection of Personal Information

Direct collection refers to information obtained by enterprises directly from personal information subjects. In internet-based scenarios, privacy policies displayed on user interfaces are the most commonly used method to implement the notice-and-consent mechanism.

Generally, a privacy policy should include the personal information processor's basic information, the purposes and business functions for which personal information is collected and used, the rules of processing (such as the method of collection and retention period), and any arrangements for sharing, transferring, or outsourcing personal information processing. It should also include the method for notifying users of changes to the policy. The information disclosed in the privacy policy must be truthful, accurate, and complete, and presented in clear and understandable language. According to the *Network Data Regulations*, enterprises must also establish and disclose a "Personal Information Collection List" and a "List of Shared Personal Information with Third Parties" to accompany the privacy policy.

b) Indirect Collection of Personal Information

Indirect collection refers to situations where enterprises obtain information through third-party channels rather than directly from personal information subjects. In such cases, enterprises must ensure that the third party providing the personal information has fulfilled the necessary legal obligations for lawful collection—this includes obtaining the personal information subject's consent and informing them of the purposes and scope of data sharing.

(2) Storage and Deletion of Personal Information

a) Requirements for the Duration of Personal Information Storage

According to Article 19 of the *PIPL*, personal information shall not be retained indefinitely. The retention period must be the shortest duration necessary to achieve

the purpose of processing. Once the retention period has expired, enterprises must delete or anonymize the personal information, unless otherwise required by laws or regulations.

b) Security Requirements for Personal Information Storage: Technical and Organizational Measures

Ensuring security during the storage period is also a key aspect of compliance. Enterprises should adopt technical measures such as encryption and de-identification for stored personal information, and consider establishing sound access control policies aligned with the internal organizational structure to prevent unauthorized or hierarchical access, thereby reducing the risk of data breaches.

(3) Processing and Use of Personal Information

In daily business operations, enterprises may process personal information in various ways to extract commercial and practical value, such as analyzing user tags, building user profiles, or conducting automated decision-making. When processing and using personal information, enterprises should follow general principles and adopt targeted risk control measures for scenarios that significantly affect individuals' rights and interests. Below is a summary of the general compliance requirements for processing and two typical use cases:

a) General Requirements for Processing and Using Personal Information

In general, when using personal information, enterprises must strictly adhere to the scope of authorization granted by the personal information subject. If the intended use exceeds the originally authorized scope, new consent from the personal information subject must be obtained.

b) Compliance Requirements for Typical Processing and Use Scenarios

- User Profiling and Tagging

When using personal information to generate user tags and profiles, enterprises must avoid including keywords related to illegal or harmful content in users' interests or using

such labels for content recommendations. Enterprises must also avoid setting discriminatory or biased user tags or creating rules that result in unfair treatment of certain users. Moreover, descriptions of personal traits in user profiles must not contain obscene, pornographic, gambling-related, superstitious, violent, or terror-related content, or any content discriminatory against ethnicity, race, religion, disability, or illness.

- Automated Decision-Making

When conducting automated decision-making using personal information, enterprises must ensure transparency and fairness in the decision-making process and outcomes. They must not implement unreasonable differential treatment in transaction prices or other conditions. Where automated decision-making is used to push information or conduct commercial marketing, enterprises must provide users with an option that is not based on their personal characteristics, or offer a convenient opt-out mechanism. If automated decision-making produces decisions that have a significant impact on individual's rights and interests, the individual shall have the right to request an explanation from the personal information processor, and shall have the right to refuse a decision made solely by means of automated decision-making. In addition, pursuant to Article 55 of the *PIPL*, where personal information is used for automated decision-making, the personal information processor shall conduct a personal information protection impact assessment in advance and keep records of the processing activities. For an introduction to personal information protection impact assessments, please refer to Section 5, "Personal Information Protection Impact Assessment", below.

(4) Entrusted Processing, Sharing, Transfer, and Public Disclosure of Personal Information

a) Entrusted Processing of Personal Information

Under the *PIPL*, entrusted processing refers to situations where a personal information processor entrusts part of the personal information processing activities to a trustee (similar to the "Data Intermediary" under the Singapore Personal Data Protection Act)

for further processing. For a more detailed definition, please refer to [Appendix 1: Glossary] of this guide. The trustee must strictly follow the instructions of the personal information processor and has no authority to determine the purposes or methods of processing personal information.

When a personal information processor entrusts a third party to process personal information, it shall conduct a personal information protection impact assessment beforehand and agree with the trustee on matters such as the purpose, duration, method of processing, categories of personal information, protection measures, and the rights and obligations of both parties. The personal information processor shall also supervise the processing activities of the trustee. The trustee, in turn, must strictly comply with relevant requirements.

b) Sharing of Personal Information

Personal information sharing refers to the act of a personal information processor providing the personal information it holds to another personal information processor. In the context of sharing, the recipient shall use the data for the agreed-upon purpose but can independently determine the purpose and method for the subsequent processing of personal information.

When an enterprise shares personal information with another processor, it must conduct a personal information protection impact assessment in advance and inform the individual in the consent documentation of the recipient’s name or identity, contact information, purpose and method of processing, and the categories of personal information involved. The enterprise must obtain the individual’s separate consent. To better implement compliance and protection requirements, the parties shall also sign a data processing agreement to define their respective responsibilities and obligations.

c) Transfer of Personal Information

According to relevant national standards, if an enterprise needs to transfer personal information due to reasons such as merger, division, dissolution, or bankruptcy, it shall inform the individuals of the relevant circumstances and ensure that the new personal

information processor continues to fulfill equivalent obligations.

d) Public Disclosure of Personal Information

As a general principle, enterprises should not publicly disclose the personal information they process. If public disclosure of any personal information is authorized by law or otherwise reasonably necessary, the enterprise must conduct a personal information protection impact assessment in advance, inform the individual of the purpose and type of the personal information to be disclosed, obtain the individual's separate consent, and record and retain documentation of the disclosure. Biometric information, results derived from sensitive personal information, and similar data must not be publicly disclosed.

4. Protection Requirements for Special Categories of Personal Information

(1) Personal Information of Minors

According to the *PIPL*, personal information of minors under the age of 14 is classified as sensitive personal information and is therefore subject to heightened protection requirements. In addition, the protection of minors' personal information must comply with relevant provisions of other laws and regulations, such as the *Regulations on the Protection of Minors in Cyberspace*.

Before collecting personal information of minors under the age of 14, the consent of the minor's parents or other legal guardians must be obtained, and specific rules for the processing of such personal information must be formulated. Other protection requirements for minors also include that enterprises shall, either on their own or by engaging a professional institution, conduct annual audits of their compliance in processing minors' personal information and promptly report the audit results to the Cyberspace Administration and other relevant authorities.

(2) Personal Information of Deceased Individuals

According to Article 49 of the *PIPL*, after a natural person dies, his or her close relatives have the right, for the purpose of protecting their own lawful and legitimate interests,

to access, copy, correct, or delete the deceased person's relevant personal information, unless the deceased had made other arrangements during their lifetime.

5. Protection of Personal Information Subjects' Rights

(1) Rights of Personal Information Subjects

Responding to the rights of personal information subjects is a key aspect of personal information protection and compliance efforts. Enterprises must ensure that the channels for exercising such rights are effective and accessible. According to the *PIPL*, personal information subjects are entitled to the following rights:

a) Right of Access

Personal information subjects have the right to consult and duplicate their personal information from personal information processors, except where laws or administrative regulations require confidentiality, or where access and copying would interfere with the lawful performance of duties by government authorities.

b) Right to Rectification

Personal information subjects have the right to request the correction or supplementation of their personal information. Personal information processors must verify such information and make timely corrections or additions.

c) Right to Deletion

In any of the following circumstances, enterprises must proactively delete personal information. If they fail to do so, the personal information subject has the right to request deletion:

- The processing purpose has been fulfilled, cannot be fulfilled, or is no longer necessary to fulfill;
- The enterprise has ceased providing the product or service, or the retention period has expired;

- The individual has withdrawn consent;
- The processing of personal information violates laws, administrative regulations, or contractual agreements;
- Other circumstances as prescribed by laws and administrative regulations.

If the legally mandated retention period has not expired, or if deletion is technically difficult to implement, the enterprise must cease processing the personal information beyond storage and must implement necessary security measures.

d) Right to Explanation

Personal information subjects have the right to request an explanation of the enterprise's rules for handling their personal information.

e) Right to Data Portability

Personal information subjects have the right to request that their personal information be transferred to a personal information processor of their choice. For data portability requests that meet the following conditions, the enterprise must provide means for the designated recipient to access and obtain the relevant personal information:

- The identity of the requesting individual can be verified;
- The information requested for transfer was provided based on consent or collected pursuant to a contract;
    - The transfer is technically feasible;
    - The transfer does not infringe upon the lawful rights and interests of others.

f) Right to Withdraw Consent

Where personal information is processed based on consent, the data subject has the right to withdraw such consent. The enterprise must provide a convenient mechanism for withdrawing consent and may not refuse to provide products or services solely

because the individual has not consented or has withdrawn consent—unless the processing of personal information is necessary for the provision of such products or services.

(2) Response to Personal Information Subjects' Requests

When a personal information subject exercises their rights, the enterprise shall respond promptly after verifying the identity of the subject. According to the Methods for the Recognition of Illegal Use and Collection of Personal Information by Apps jointly issued by the national cyberspace administration and other departments, it is appropriate for App product operators to respond to personal information subjects' requests to exercise their rights within 15 working days from the date of receiving the request and to provide feedback. If it cannot respond within this timeframe, the personal information processor shall contact the user in advance and explain the situation and estimated feedback time.

In principle, no fees should be charged for reasonable requests. However, for repeated requests made within a short period, the enterprise may charge a reasonable fee based on actual costs incurred.

6. Personal Information Protection Impact Assessment

The Personal Information Protection Impact Assessment (hereinafter, the PIPIA) is a key compliance mechanism explicitly stipulated in Article 55 of the *PIPL*. It refers to the process of evaluating the legality and compliance of specific personal information processing activities, assessing the risks such activities pose to the legitimate rights and interests of personal information subjects, and evaluating the effectiveness of protection measures taken.

(1) Scenarios That Trigger a Personal Information Protection Impact Assessment

According to Article 55 of the *PIPL*, enterprises shall conduct a PIPIA in advance under any of the following circumstances, and consider adjusting and improving compliance measures based on the assessment results:

- Processing sensitive personal information;
- Using personal information for automated decision-making;
- Entrusting others to process personal information, providing personal information to third parties, or publicly disclosing personal information;
- Providing personal information overseas;
- Other personal information processing activities that have a significant impact on personal rights and interests.

(2) Key Elements of a Personal Information Protection Impact Assessment

According to Article 56 of the *PIPL*, the assessment shall include whether the purpose and method of processing personal information are lawful, legitimate, and necessary; the impact on personal rights and the potential security risks; and whether the protection measures are lawful, effective, and commensurate with the level of risk.

7. Personal Information Protection Compliance Audit

The compliance audit for personal information protection is a legal obligation stipulated by the *PIPL*. It refers to the supervision activity that reviews and evaluates whether a personal information processor complies with laws and administrative regulations in its personal information processing activities. Key requirements can be referenced from the *PIPL Audit Measures*. Generally, enterprises shall proactively conduct regular audits (“enterprise-initiated audits”), but personal information protection authorities may also require audits initiated by designated regulators (“authority-initiated audits”) under specific circumstances. Key scenarios, frequency, and audit points are summarized below.

(1) Enterprise-Initiated Audit

According to the *PIPL Audit Measures*, enterprises that process the personal information of more than 10 million individuals shall conduct at least one personal information protection compliance audit every two years. Other enterprises may

determine the frequency of such audits based on their own circumstances. Additionally, enterprises processing personal information of more than 1 million individuals shall appoint a personal information protection officer responsible for compliance audits.

(2) Authority-Initiated Audit

Article 5 of the *PIPL Audit Measures* provides that in one of the following circumstances, the national cyberspace administration and other relevant regulators ("protection authorities") may require enterprises to entrust professional institutions to conduct compliance audits of their personal information processing activities:

- Where personal information processing activities are found to pose significant risks to personal rights or have severe deficiencies in security measures;
- Where the processing activities may harm the rights and interests of a large number of individuals;
- Where a personal information security incident occurs, resulting in the leakage, tampering, loss, or destruction of personal information of more than 1 million individuals, or sensitive personal information of more than 100,000 individuals.

(3) Key Audit Point

Whether the audit is conducted by the enterprise itself or by a professional institution at the request of regulators, it shall follow the guidelines in the Annex "*Personal Information Protection Compliance Audit Guide*" of the *PIPL Audit Measures*. This includes, but is not limited to: the lawful basis of personal information processing activities; the completeness and accuracy of personal information processing rules; the compliance and protection measures for entrusted processing and sharing of personal information; whether the rights of personal information subjects are guaranteed; whether internal management systems and operating procedures are in place.

8. Handling of Personal Information Security Incidents

Personal information security incidents are often hidden, sudden, and diverse in nature. According to Article 51 of the *PIPL*, enterprises shall formulate and implement emergency response plans for personal information security incidents and conduct regular drills. In the event of an incident, enterprises shall respond and manage it immediately in accordance with the emergency plan.

(1) Emergency Response Plan and Drills

Enterprises shall assess and forecast the personal information security risks they face based on their business practices, and formulate a comprehensive, effective, and executable emergency response plan for security incidents. Enterprises shall also provide training to relevant personnel on the emergency plan and regularly conduct drills.

(2) Emergency Response and Incident Handling

In the event of a personal information security incident, the enterprise shall promptly investigate the impact, scope, and potential harm in accordance with the emergency plan and procedures; analyze and determine the cause of the incident; and propose countermeasures to prevent further damage.

The enterprise shall also establish notification channels, and in accordance with relevant regulations, promptly notify both regulatory authorities and affected individuals after the incident occurs. In addition, the enterprise shall take appropriate measures to minimize losses and mitigate any risks or harm caused by the incident.

9. External Supervisory Body for Personal Information Protection

Pursuant to Article 58 of the *PIPL*, personal information processors that provide important internet platform services, have a large number of users, and engage in complex types of business shall perform the following obligations:

(1) Establish and improve a compliance system for personal information protection in accordance with national provisions, and establish an

independent body mainly composed of external members to supervise the status of personal information protection;

(2) Adhere to the principles of openness, fairness, and impartiality, formulate platform rules, and specify the norms for personal information processing and the obligations of personal information protection for product or service providers within the platform;

(3) Cease to provide services to product or service providers within the platform that seriously violate laws and administrative regulations in the processing of personal information;

(4) Regularly publish personal information protection social responsibility reports and accept public supervision.

At present, the supporting provisions concerning the "independent body mainly composed of external members" are still in the process of being formulated. With respect to specific matters such as the qualifications for appointment of external members of such body, nomination and removal procedures, performance requirements, candidate selection and tenure, and supervisory responsibilities, enterprises may refer to the relevant content of *National Standard GB/T 45404—2025 Information Security Technology—Requirements for the Internal Personal Information Protection Supervisory Body of Large Internet Enterprises*.

IV. Public Data※

(i) Policy Background for the Development and Utilization of Public Data

In China, government departments and enterprises/institutions performing public management or public service functions are highly numerous. In the course of fulfilling their public duties or providing services, these entities collect and generate vast

※ The authors of this chapter are Duan Zhichao, Partner at Beijing Han Kun Law Offices, who has long specialized in data compliance and cross-border transfers, is well-versed in both domestic and foreign regulatory frameworks, and serves numerous leading multinational enterprises and technology companies; and Wang Yuting, Consultant at Beijinh Han Kun Law Offices.

amounts of data. Such data often covers various aspects of economic and social life, characterized by large scale, high quality, significant potential value, strong multiplier effects, and pronounced public attributes. It plays a crucial role in data circulation, contributing substantially to enhancing governance capabilities, optimizing the allocation of public resources, and safeguarding public services. Therefore, how to unlock the value of data held by public entities and fully leverage its role as a production factor has always been a key issue in the development of the digital economy.

As early as 2015, the *Guidelines on Actively Promoting the "Internet Plus" Initiative* and the *Action Outline for Promoting Big Data Development* already recognized the importance of public data in the context of big data development. Subsequently, the state introduced numerous policy documents to encourage and guide the development and utilization of public data. Among these, the most significant are the *20 Measures on Data* and the *Opinions on Accelerating the Development and Utilization of Public Data Resources* (hereinafter, *Development and Utilization Opinions*).

In 2022, the *20 Measures on Data*, as the first national-level document establishing foundational data systems, not only clarified the definition of public data and formally categorized it as one of the three major types of data elements but also introduced, for the first time, mechanisms for public data authorization, sharing, and development.

In 2024, the *Development and Utilization Opinions* proposed 17 specific measures to accelerate the development and utilization of public data, identifying three primary approaches: sharing, open access, and authorized operation. As the first central-level policy document to systematically address the development and utilization of public data resources, it serves as a guiding framework in this field.

(ii) Definition and Identification of Public Data

1. Definition at the National Level

The concept of “public data” first emerged as an independent concept in national laws and regulations in the *Cybersecurity Law*. However, this law only reflects the legislators’ affirmative attitude towards the opening up of public data resources and does not specifically define the concept of public data. Similarly, the *E-commerce Law* only mentions this concept without providing a specific definition.

In the early days, national - level legislation did not clearly distinguish between government data and public data, and the use of the above - mentioned two concepts was often interrelated and even interchangeable. For example, in 2021, the *Data Security Law* dedicated a special chapter to the security and opening up of government data. Although it does not directly define the concept of government data, from the literal interpretation of Article 38[17] it can be understood that government data refers to the data collected and used by state organs for the need of performing their statutory duties. In addition, Article 43[18] also broadens the scope of government data, making it possible for the concept of government data to be in line with that of public data, and clarifies that the data processed by organizations with public affairs management functions in the performance of their duties shall be subject to the provisions of this special chapter. Similarly, in the *Guidelines for the Construction of a “National Integrated Government Big Data System”* issued by the General Office of the State Council in 2022, public data is still used as a broad - sense concept of government data. This confusion in the concepts of government data and public data continued until the release of the *20 Measures on Data*.

The *20 Measures on Data* for the first time defines public data at the national level as **“data generated in the process of government departments at all levels, Party organizations, and enterprises and institutions performing their duties**

[17] Article 38 of the Data Security Law: “When state organs need to collect or use data to perform their statutory duties, they shall do so within the scope of their statutory duties and in accordance with the conditions and procedures stipulated by laws and administrative regulations. They shall, in accordance with the law, keep confidential the data such as personal privacy, personal information, trade secrets, and confidential business information that they come to know in the course of performing their duties, and shall not disclose or illegally provide such data to others.”

[18] Article 43 of the Data Security Law: “The provisions of this chapter shall apply to the data processing activities carried out by organizations authorized by laws and regulations to perform public affairs management functions for the purpose of fulfilling their statutory duties.”

according to law or providing public services”, officially including government data within the scope of public data and clarifying that enterprises and institutions are also among the main bodies.

On December 30, 2024, Article 15 of the *Explanation of Commonly - Used Terms in the Data Field (First Batch)*[19] announced by the National Data Bureau adopted this definition, hoping to further unify the society’s understanding of the definition of public data.

2. Definition at the Local Level

Against the backdrop of top-level policies supporting the development and utilization of public data, various provinces and cities across the country, such as Beijing, Shanghai, and Guangdong, have successively issued a large number of laws and regulations focusing on exploring and promoting the development and utilization of public data, among which definitions of public data are also provided. Generally speaking, localities basically define public data through the element model of "subject" + "behavior". While he elements of conduct are all stipulated as, “in the process of performing public affairs management duties or providing public services in accordance with the law”, the elements of subject vary slightly depending on local circumstances. As the State elevates definitions and developmental directions relating to public data from the policy level to the legal level, the definition of public data has ultimately been unified. At the level of subject elements, most local regulations regard state organs and organizations authorized to undertake public functions as the subjects of public data. However, local regulations, in turn, take into account the specific circumstances of local enterprises and organizations and therefore establish differentiated requirements. on whether public institutions and enterprise organizations providing public services are included in the scope of subjects. For example, Beijing does not include public institutions and public service organizations in the scope of

[19] Article 15 of the Explanation of Commonly - Used Terms in the Data Field (First Batch): “Public data refers to data generated in the process of government departments at all levels, Party organizations, and enterprises and institutions performing their duties according to law or providing public services”

subjects[20]. Shanghai adopts a specific enumeration method, clearly identifying public institutions and organizations providing basic public services such as water supply and electricity supply as the subjects of public data[21]. Jiangsu directly and generally stipulates that enterprises and public institutions with public service functions are all subjects of public data[22].

3. Methods for Identifying Public Data

From the review of definitions in the aforementioned policies and regulations, it can be concluded that the core elements for identifying public data are two criteria: "subject" and "conduct". Since the conduct element is relatively fixed, enterprises should focus on the subject element during specific identification. The broadest scope of such subjects includes administrative organs, public institutions, public function organizations, and public service organizations. Since each region has refined and adjusted the subject elements in accordance with local characteristics and circumstances, enterprises must likewise make determinations on a case-by-case basis with specific reference to local laws and regulations, so as to achieve accurate identification.

- During the identification process, the nature of the subject should first be verified. If the subject does not fall within the scope of subjects specified in local regulations, the data in question should be excluded from public data.

---

[20] Article 2 of the Measures for the Administration of Authorized Operation of Beijing Public Data Zones (Trial): “The term 'public data' as used in these Measures refers to various types of data processed by state organs at all levels in this municipality and organizations legally authorized to have the function of managing public affairs in the process of performing their duties and providing public services.”

[21] Article 3 of the Detailed Rules for the Implementation of Public Data Opening in Shanghai: “The term 'public data' as used in these Rules refers to data collected and generated by state organs, public institutions, organizations legally authorized to have the function of managing public affairs, and organizations providing public services such as water supply, electricity supply, gas supply, and public transportation (hereinafter collectively referred to as public management and service institutions) in the process of performing public management and service duties.”

[22] Article 2 of the Measures for the Administration of Public Data in Jiangsu Province: “The term ‘public data’ as used in these Measures refers to records of information with public use value in electronic or other forms, which are collected and generated by administrative organs at all levels, organizations authorized by laws and regulations to have the function of managing public affairs, and public enterprises and institutions (hereinafter collectively referred to as public management and service institutions) for the performance of statutory duties and the provision of public services.”

- If the nature of the subject is in compliance, the nature of the conduct shall then be determined. This involves a comprehensive assessment of factors such as whether the scenario in which the data is generated falls within the scope of the subject's performance of duties (e.g., daily office work, external services, law enforcement and supervision) and whether the conduct is legally authorized.
- Finally, it is necessary to check the public data catalog published by the local competent authority. This is because there may be cases where certain types of data, despite not meeting the subject or conduct elements, are explicitly included in a local public data catalog. For example, the public data published by Wuxi City includes "general overview of secondary private hospitals"[23]. Private hospitals generally do not fall under the category of administrative organs, or enterprises, public institutions, and social organizations that perform public management and service functions as stipulated in the *Measures for the Administration of Public Data in Wuxi City*. Nevertheless, the data generated by them is still included in the public data catalog.

(iii) Sharing and Opening of Public Data

As mentioned earlier, Article 2 of the *Development and Utilization Opinions* specifies three ways to develop and utilize public data, including sharing, opening, and authorized operation. Although these three methods differ in terms of applicable objects, implementing entities, and application scenarios, they are essentially practical explorations in China to achieve efficient supply of data resources and release of value by innovating the paths for developing and utilizing public data on the basis of strictly ensuring data security. Accurately recognizing and deeply understanding these three methods, as well as earnestly paying attention to and strictly abiding by the compliance points involved, are crucial for enterprises to effectively, legally, and fully explore and utilize the value of public data.

[23] See Wuxi Public Data Open Platform.

1. Public Data Sharing

Public data sharing is an important way for government departments at all levels and regions to break down data barriers and conduct data exchange. As early as 2016, the *Interim Measures for the Administration of Government Information Resource Sharing* put forward the principle for government data that “sharing is the norm, and non - sharing is the exception”. Up to now, public data sharing remains an important approach for the development and utilization of public data, which can improve the internal collaborative supervision capacity of the government and ultimately enhance the level of public services.

Public data sharing relies on government departments to compile public data catalogs and take the lead in collecting and sharing relevant data. Taking the working mechanism of public data sharing in Shanghai as an example, according to the *Shanghai Measures for the Implementation of Public Data Sharing (Trial)*, the departments responsible for public data sharing mainly include the General Office of the Municipal Government, the Municipal Big Data Center, municipal - level responsible departments, and district - level public data competent departments. A top - down departmental responsibility system has been established, with key tasks including compiling, collecting, and sharing public data catalogs. The realization of the sharing mechanism depends on the big data resource platform. Other administrative departments at all levels in various regions that need to use shared data must submit an application on this platform and make a commitment on their needs. Subsequent use must be limited to the scope of the commitment and must not be applied to other scenarios or purposes.

2. Opening of Public Data

Different from public data sharing, public data opening mainly targets enterprises and the public, with the goal of safeguarding their right to access and utilize public data. Therefore, its positive significance to enterprises is more direct.

In general, the key scope of public data opening covers data related to public security, people's livelihood security, and enterprise public credit information, etc. According to the degree of sensitivity, local regulations usually classify public data opening into three categories: non - open, conditionally open, and unconditionally open. The subject responsible for opening public data can determine the opening attribute in accordance with the relevant rules for classification and grading of public data.

Taking the *Interim Measures for the Opening of Public Data in Guangdong Province* as an example, non - open public data mainly includes data involving state secrets, data whose opening would affect national and social security, and data that would infringe on trade secrets, personal privacy, intellectual property rights, etc. Conditionally open data mainly includes data involving trade secrets and personal privacy for which the data subject has consented to opening, data whose unconditional opening would affect the operational efficiency of public data processing, data with significant economic benefits but potential security risks, and data other than those falling under the category of non-open data and the category of conditionally open data shall be classified as unconditionally open data..

In terms of the opening mechanism, public data holders, in accordance with laws and regulations, compile a public data opening list within the scope of the local public data catalog and enter public data into the data opening platform. For unconditionally open public data, enterprises and the public can inquire, obtain, and utilize the opened public data through methods specified by laws and regulations such as data download and interface calls. For conditionally open public data, enterprises and the public need to submit an application, obtain approval, and sign a data utilization agreement with the data opening subject before they can access and use it.

In addition, for public data that has not yet been opened, enterprises and the public can also put forward data needs to relevant government units through the data opening platform. For example, on the Shenzhen Municipal Government Data Opening

Platform, users can submit personalized public data opening needs by filling in the content of data needs and application scenarios[24].

3. Compliance Points for Enterprises Participating in Public Data Sharing and Opening

(1) Desensitization and Declassification of Data Intended for Disclosure

State - owned enterprises involved in providing public services, when accessing data involving state secrets, trade secrets, or personal information, must conduct declassification and desensitization in accordance with the law or obtain the consent of relevant rights holders before opening or processing such data. Other enterprises that obtain public data resources involving such data must also comply with the regulations on the protection of trade secrets and personal information.

Taking personal information protection as an example, there have been cases in practice where reprinting public judgments containing personal information was deemed an infringement of personal rights. In the case of Yi v. a company in Suzhou, Jiangsu Province regarding infringement of personal information rights[25], the defendant was an enterprise providing access to judicial documents, and all the judicial document information on its operating website was reprinted from legally public information on China Judgments Online. However, the plaintiff claimed that such reprinting constituted secondary disclosure of his personal information without his consent, infringing on his right to personal information. The court held that in this case, the subject of personal information has the right to control the dissemination of his legally public personal information; enterprises' reprocessing of publicly available personal information must not violate his freedom of choice; and the personal rights of the subject of personal information in controlling information dissemination take precedence over the potential property rights generated by the circulation of legally

[24] See the Collection Form for Public Data Opening Needs and Application Scenarios on the Shenzhen Municipal Government Data Opening Platform.
[25] See Civil Judgment (2019) Su 05 Civil Final No. 4745 of the Intermediate People's Court of Suzhou City, Jiangsu Province.

public personal information. Finally, the court ruled that the defendant enterprise should delete the relevant judgments and compensate the plaintiff 8,000 yuan for economic losses.

(2) Obtaining Public Data Through Legal Means

In the process of obtaining public data, current local regulations only put forward the principle requirement that the legitimate rights and interests of the state, society, and other subjects must not be harmed. Article 32 of the *Implementation Rules for the Opening of Public Data in Shanghai* explicitly prohibits enterprises from obtaining public data by illegal means, infringing on the legitimate rights and interests of others such as trade secrets and personal privacy, or developing and utilizing public data in other illegal or irregular ways[26].

It is particularly important to note that for unconditionally open public data, enterprises cannot obtain it in any way they like. They need to specifically refer to local regulations on public data opening and the provisions of public data opening platforms to avoid improper use of automated tools such as web crawlers.

For example, Article 22 of the Interim Measures for the Opening of Public Data in Guangdong Province stipulates legal ways for enterprises to obtain public data, including data download, data access through interface calls, obtaining result data through algorithm models on the data opening platform, data transmission via storage media, and other ways specified by laws, regulations, and rules. The provisions do not include automated means such as web crawlers, which many enterprises often use in practice. Although China's laws and regulations do not completely prohibit web crawling activities across the board, laws and regulations such as the *Anti - Unfair Competition Law*, the *Cybersecurity Law*, the *Network Data Regulations*, and the

[26] Article 32 of the Implementation Rules for the Opening of Public Data in Shanghai: “(1) Violating the management system of the opening platform; (2) Obtaining public data by illegal means; (3) Infringing on the legitimate rights and interests of others such as trade secrets and personal privacy; (4) Using public data beyond the application scenarios restricted by the data utilization agreement; (5) Other acts violating laws, regulations, rules, and data utilization agreements.”

Criminal Law impose restrictions on such activities. For instance, Article 18 of the *Network Data Regulations* requires network data processors to assess the impact of automated tools on network services. Enterprises must carefully consider the compliance risks that may arise from the use of such automated means, such as unfair competition, administrative penalties, or even being convicted of crimes such as illegal intrusion into computer information systems or illegal acquisition of computer information system data.

(3) Taking Necessary Measures to Ensure Data Quality

In the process of developing and utilizing public data, enterprises cannot neglect their duty of care within a reasonable scope simply because of the public nature of public data. Failure to ensure the accuracy and timeliness of the public data used will not only reduce the efficiency of public data development and utilization but also may lead to the risk of infringement. In particular, when public data involves major negative and sensitive information that may affect the rights and interests of others, it should be verified to ensure the accuracy of the public data being developed and utilized.

For example, in the case of commercial defamation and unfair competition between Suzhou Langdong Network Technology Co., Ltd. and Zhejiang Ant Small and Micro Financial Services Group Co., Ltd., etc., the defendant failed to verify the timeliness of the enterprise liquidation information obtained from the National Enterprise Credit Information Publicity System. It repeatedly pushed incorrect notifications about the plaintiff's liquidation change information to users on its website platform, causing the public to mistake the plaintiff's historical liquidation information for the real - time information of 2019, which caused damage to the plaintiff's business reputation. The court held that this constituted unfair competition and ordered the defendant to compensate the plaintiff for losses and reasonable expenses totaling 600,000 yuan[27].

[27] See Civil Judgment (2020) Zhe 01 Civil Final No. 4847 of the Intermediate People's Court of Hangzhou City, Zhejiang Province.

4. Authorized Operation of Public Data

As the third approach to development and utilization, authorized operation generally refers to activities where professional operating institutions, based on authorization, develop and utilize non-original public data to provide data products and services to market entities. Its purpose is to bring in social professional forces for processing and utilizing data resources, thereby fully releasing the value of data resources. Compared with the sharing and opening of public data, authorized operation started relatively late. It emerged as a supplementary channel on the basis of sharing and opening to address the idle value of some highly sensitive and high-value public data.

Since 2025, building on the *Development and Utilization Opinions*, the state has issued the *Implementation Specifications for Authorized Operation of Public Data Resources (Trial)* (hereinafter, the *Implementation Specifications*), the *Interim Measures for the Registration and Administration of Public Data Resources*, and the *Notice on Establishing a Price Formation Mechanism for Authorized Operation of Public Data Resources*. These form a "1 + 3" policy and regulatory system, providing a legal basis for efficient and compliant authorized operation of public data.

(1) Overview of Public Data Authorized Operation

a) Participating Entities

Three main entities are involved in the authorized operation of public data, namely the authorizing entity, the implementing institution, and the operating institution.

With regard to the authorizing entity, the *Implementation Specifications* stipulate that its scope mainly includes local people’s governments at or above the county level and national industry competent departments. In addition, Article 25 of the supplementary provisions states that central Party and mass organizations, local Party committees at or above the county level, and public utility enterprises such as water supply, gas

supply, heating, power supply, and public transportation may refer to the applicable provisions.

According to the *Implementation Specifications*, the implementing institution refers to a unit determined by local people's governments at or above the county level or national industry competent departments that is specifically responsible for carrying out authorized operation activities. Its responsibilities mainly include formulating implementation plans, fairly selecting operating institutions, signing authorized operation agreements, and conducting internal control audits on operating institutions.

The operating institution refers to a legal person organization that obtains authorization in accordance with the *Implementation Specifications* and specifically develops and operates public data resources. In other words, private enterprises usually participate in the authorized operation of public data as operating institutions.

b) Authorization Model

The *Development and Utilization Opinions* summarizes the authorization models, which are generally divided into the overall authorization model, the sector-specific authorization model, and the scenario-based authorization model[28].

- The overall authorization model refers to the one-to-one authorization or comprehensive authorization model. Under the overall planning of local data authorities, cross-departmental public data resources are authorized as a whole

[28] Development and Utilization Opinions, Article 2, Item 3: "(3) Encourage exploration of authorized operation of public data. Implement the requirements of the structural separation system of data property rights, and explore the establishment of a classified and hierarchical authorization mechanism for public data. Strengthen the overall management of authorized operation, clarify data management agencies, explore the inclusion of authorized operation in the decision-making scope of 'three major and one large', clarify authorization conditions, operation models, operation periods, exit mechanisms, and safety management responsibilities. In light of actual circumstances, **adopt models such as overall authorization, sector-specific authorization, and scenario-based authorization** to authorize qualified operating agencies to carry out the development of public data resources, product operations, and technical services. Data management agencies shall perform their industry supervision duties and guide and supervise operating agencies to operate in accordance with laws and regulations. Operating agencies shall implement authorization requirements, standardize operation behaviors, provide services fairly to the market, and strictly prohibit unauthorized use of data beyond the scope. Accelerate the formation of a clear power and responsibility, and a coordinated central-provincial authorized operation pattern. Formulate regulations on the management of authorized operation of public data resources in a timely manner."

to operating agencies for development and utilization. The authorized operation of public data in Chengdu is such a model[29];

- The sector-specific authorization model refers to one-to-N authorization by industry or field. According to the data characteristics and application needs of different industries or fields, operating agencies with industry attributes are selected to develop application scenarios in specific fields. A typical example is the authorization model specified in the *Measures for the Administration of Authorized Operation of Beijing Public Data Zones (Trial)*[30];

- The scenario-based authorization model means that, according to specific needs, different operating agencies carry out the development and utilization of resources in accordance with the principle of “one scenario, one application, one approval”. Typical development and application scenarios under this authorization model include road signal optimization and credit risk early warning in practice[31].

It should be noted that these three authorization models are not completely independent. Various regions often flexibly establish operation systems by combining the advantages of different models. For example, Nanjing and Jinan have adopted a parallel development model of overall authorization and sector-specific authorization in order to achieve good collaborative effects[32].

c) Data Circulation Link

From the perspective of the circulation link, a typical authorized operation mode is as follows: the authorizing entity collects and gathers generated public data, and may

[29] Introduction on the official website of Chengdu Public Data Operation Service Platform.
[30] Measures for the Administration of Authorized Operation of Beijing Public Data Zones (Trial), Article 3, Paragraph 1: “The term 'public data zones’ as mentioned in these Measures refers to the general term for various thematic data areas built to promote multi-source integration of public data and socialized development and utilization, and release the value of data elements for major fields, key regions, or specific scenarios, which are generally divided into field-based, region-based, and comprehensive basic types.”
[31] See Meng Qingguo, Wang Youkui, Wang Lida: *Open Utilization and Authorized Operation of Public Data - Connotation, Model and Mechanism Methods*, published in Chinese Public Administration, Issue 9, 2024.
[32] See “Insights into the Development of Public Data Authorized Operation (2024)” by the Big Data Technology Standard Promotion Committee.

carry out data cleaning through the local data authorized operation platform. Subsequently, the implementing agency formulates a public data resource authorized operation implementation plan in accordance with regulations, and selects an operating agency through public bidding and other methods in accordance with the plan. After review, an authorized operation agreement is signed with the selected operating agency, so that the operating agency can process and transform public data into public data products and services, list them on local data trading centers, and finally circulate them to data trading counterparts.

(2) Compliance Key Points for Enterprises Participating in Authorized Operation

The *Development and Utilization Opinions* clearly states that the authorized operation of public data shall be included in the decision-making scope of "three major and one large"[33], which not only reflects the country's emphasis on authorized operation of public data, but also indicates that such operation may affect national data security and public interests. Therefore, all relevant entities must ensure legality and compliance throughout the process to safeguard data security and personal information security. Chapter II of the *Implementation Specifications* also sets out similar provisions on the basic requirements for authorized operation, with additional emphasis that monopoly behaviors shall not be conducted in authorized operation activities[34].

As mentioned earlier, private entities usually participate in public data authorized operation as operating agencies. For operating agencies, their obligations mainly include: meeting the qualifications of operating entities; registering public data products or services; disclosing lists of public data products and services, and relevant information to accept social supervision; assuming the main responsibility for data

[33] Three major and one large refers to decision-making on major issues, appointment and removal of important cadres, decision-making on major project investments, and use of large amounts of funds.
[34] Implementation Specifications, Article 6, Paragraph 1: "In carrying out authorized operation activities, no abuse of administrative power or market dominance shall be allowed to eliminate or restrict competition, and no monopoly behaviors shall be engaged in by taking advantage of data, algorithms, technology, capital advantages, etc."

security; ensuring data security through management and technical measures; and strengthening financial management related to public data.

Therefore, based on the basic requirements of the *Implementation Specifications* and the aforementioned obligations, the following compliance key points should be noted:

(3) Fulfilling Personal Information Protection Obligations

Since public data may involve personal information, operating agencies must pay attention to complying with relevant regulatory requirements for personal information protection and fulfill compliance obligations when conducting development and utilization. For details, please refer to “(1) Desensitization and declassification of data to be made public” in “3.3 Compliance Key Points for Enterprises Participating in Public Data Sharing and Opening” of the previous text.

(4) Implementing Data Security Protection Requirements

Firstly, during the agreement signing stage, according to the *Implementation Specifications*, an enterprise must possess the data security capabilities specified in the implementation plan to be selected as an operating agency. Therefore, if an enterprise intends to participate in authorized operation, it must ensure that it has basic data security capabilities.

In the operation and management stage, operating agencies shall fulfill data security protection obligations such as strengthening internal control management, ensuring that they always maintain relevant data security capabilities, implementing data security and personal information protection requirements, as well as risk monitoring and emergency response measures in accordance with relevant laws and regulations and the provisions of the operation agreement. Moreover, they must use public data resources within the authorized scope and strictly prevent and control data security risks in links such as data processing, operation, and services.

Finally, it should be emphasized that Paragraph 2 of Article 21 of the *Implementation Specifications* requires operating agencies to assume the main responsibility for data security. This responsibility is an active compliance responsibility, requiring operating agencies to fully carry out more comprehensive and thorough compliance self-certification work. In addition, since the implementing agency has the right to supervise and audit the operating agency, operating agencies must also implement data security protection measures to smoothly cooperate with relevant audit work.

(5) Avoiding Suspicions of Monopolistic Operation

The *Implementation Specifications* specifically address the risk of monopoly in public data operation, stating that “operating agencies shall carry out business within the authorized scope in accordance with the agreement and shall not directly or indirectly redevelop relevant public data products and services”.

The core purpose of this provision is to prevent operating agencies from abusing the public data resources they obtain, restricting other market entities from participating in the development and utilization of public data, thereby avoiding the formation of market monopoly. Therefore, to prevent the risk of monopoly, enterprises must ensure that during the operation of public data, they do not hinder market competition through technical barriers, exclusive agreements, restrictions on redevelopment, or other means, and maintain market fairness and openness.

5. Future Outlook for the Development and Utilization of Public Data

With the continuous improvement of unified national policies and systems as well as local specific legal norms, China has gradually addressed the previous issues of lacking unified specialized regulations and specific supporting implementation standards. The development and utilization of public data have officially entered a new stage of “having rules to follow, regulations to abide by, and evidence to check”. However, it should be noted that since the relevant systems for public data sharing, development, authorized operation, and information disclosure mechanisms are still in

the initial construction stage, specific details and implementation standards remain to be further refined. In the next step, localities and industries will plan implementation paths, form local implementation plans according to actual conditions, and explore a standardized full-process regulatory system.

In addition, although various localities have actively carried out many specific practical explorations in the development and utilization of public data, but at present the application scenarios are relatively concentrated in fields such as finance, medical care, and transportation. The types of public data products are not rich enough, and the development and utilization are faced with difficulties such as “holding data but not knowing how to use it” and “wanting to use data but not being able to find it”. Future work will further optimize the judgment and response to the application needs of public data and establish sound supply and demand docking channels. In addition, the National Data Bureau will coordinate to promote breakthroughs in key fields first, create a number of influential projects, and form replicable and promotable development and utilization models.

In conclusion, sharing, development, and authorized operation have effectively promoted the development and utilization of public data resources, thereby advancing the construction of the data element market. In the future, the relevant explorations of local departments will be further deepened, and with the introduction of more professional, flexible, and diverse social forces from enterprises, the value potential of public data will be further released.

6. Policy and Regulation Index

Scope of Validity	Name of the Regulation	Announcement Time	Effective Date
National	Guiding Opinions of the State Council on Actively Promoting the "Internet +" Action	2015.7.1	2015.7.1

Scope of Validity	Name of the Regulation	Announcement Time	Effective Date
	Action Plan for Promoting the Development of Big Data	2015.8.31	2015.8.31
	Interim Measures for the Management of Government Information Resources Sharing	2016.9.5	2016.9.5
	Guidelines for the Construction of a National Integrated Government Big Data System	2022.9.13	2022.9.13
	Opinions on Building a Data Foundation System to Better Give Play to the Role of Data Elements	2022.12.2	2022.12.2
	Opinions of the General Office of the Communist Party of China Central Committee and the General Office of the State Council on Accelerating the Development and Utilization of Public Data Resources	2024.9.21	2024.9.21
	Explanation of Commonly - Used Nouns in the Data Field (the First Batch)	2024.12.30	2024.12.30
	Implementation Specifications for the Authorized Operation of Public Data Resources (Trial)	2025.1.8	2025.3.1
	Interim Measures for the Registration and Management of Public Data Resources	2025.1.8	2025.3.1
	Notice on Establishing a Price -	2025.1.16	2025.3.1

Scope of Validity	Name of the Regulation	Announcement Time	Effective Date
	Formation Mechanism for the Authorized Operation of Public Data Resources		
Beijing	Measures for the Administration of Authorized Operation of Beijing Public Data Zones (Trial)	2023.12.5	2023.12.5
Shanghai	Implementation Rules for the Opening of Public Data in Shanghai	2022.12.31	2022.12.31
	Interim Measures for the Sharing of Public Data in Shanghai	2023.3.2	2023.3.2
Jiangsu	Measures for the Management of Public Data in Jiangsu Province	2021.12.18	2022.2.1
	Measures for the Management of Public Data in Wuxi City	2020.2.26	2020.5.2
Guangdong	Interim Measures for the Opening of Public Data in Guangdong Province	2022.11.30	2022.11.30

V. Special Industry Data

At present, China has established a data compliance legal framework centered on the *Cybersecurity Law*, the *Data Security Law*, and the *PIPL*, which sets forth basic systems such as full-life-cycle data management, classification and grading, and risk assessment. Due to the national security attributes, public interest relevance, and sensitivity inherent in data of certain specialized industries, such data shall be subject to specific compliance obligations under the unified legislative framework.

The compliance governance of special industry data has significant spillover effects. For example, surveying and mapping geographic information data, as a digital

mapping of national sovereignty, its accuracy and security affect national security; meteorological data, as a core resource for public safety, is closely related to the public welfare needs of ensuring disaster prevention and mitigation; financial data constitutes the digital foundation of the financial system, and its compliance is directly related to financial stability and the credibility of financial institutions; e-commerce marketing data involves the protection of consumers' rights and interests and the order of fair market competition. In addition, medical and health data is subject to dual supervision by industry competent authorities and data competent authorities because it is related to citizens' right to life and health; industrial manufacturing data is related to industrial competitiveness and the security of critical infrastructure, and needs to be managed throughout the whole process in accordance with the *Measures for the Administration of Data Security in the Industrial and Information Technology Sector (Trial)*; emergency management data, as a form of support for public safety emergency response, requires the establishment of specific rules for data collection, sharing and use under the framework of the *Emergency Response Law of the People's Republic of China* (hereinafter, the *Emergency Response Law*).

The compliance needs of the above typical industries not only reflect the common requirements of the basic laws and regulations on data compliance, but also highlight the necessity of differentiated supervision. Since surveying and mapping geographic information, meteorological data, financial credit reference data, and e-commerce marketing data correspond to the four dimensions of national security, public safety, financial security, and consumer safety respectively, the following will focus on the above four types of special industry data to provide guidance for data compliance management of relevant enterprises.

(i) Surveying, Mapping and Geographic Information Data

1. Definition of Surveying, Mapping and Geographic Information Data

Surveying and Mapping Law of the People's Republic of China (hereinafter, the *Surveying and Mapping Law*) does not clearly define surveying, mapping and

geographic information data. It only stipulates in Article 2 that surveying and mapping activities refer to “activities such as measuring, collecting and expressing the shape, size, spatial position and attributes of natural geographical elements or surface artificial facilities, as well as processing and providing the obtained data, information and results”. With the rapid development of intelligent connected vehicles, the Ministry of Natural Resources issued the *Notice on Promoting the Development of Intelligent Connected Vehicles and Safeguarding the Security of Surveying, Mapping and Geographic Information* (hereinafter, the *2022 Notice*) in 2022 and the *Notice on Strengthening the Management of Surveying, Mapping and Geographic Information Security Related to Intelligent Connected Vehicles* (hereinafter, the *2024 Notice*) in 2024. The *2022 Notice* first clearly states that “surveying, mapping and geographic information data” includes “spatial coordinates, images, point clouds and their attribute information of vehicles and surrounding road facilities, etc.”. The *2024 Notice* further refines real - scene image data (including environmental perception data such as videos and images) and expands to road topology data, highlighting the regulatory needs for dynamic data in intelligent connected scenarios.

2. Subject Access for Data Processing Activities

(1) Qualification Levels

China implements an administrative licensing system for entities engaged in surveying and mapping activities. Surveying and mapping entities must obtain corresponding surveying and mapping qualifications before carrying out such activities. According to Article 27 of the *Surveying and Mapping Law*, entities engaged in surveying and mapping activities shall meet the corresponding conditions and obtain a surveying and mapping qualification certificate in accordance with the law before engaging in surveying and mapping activities.

The professional categories of surveying and mapping qualifications include geodetic surveying, aerial photogrammetry, photogrammetry and remote sensing, engineering surveying, marine surveying and mapping, boundary and real estate surveying and

mapping, geographic information system engineering, cartography, electronic navigation map production, and internet map services. The *Measures for the Administration of Surveying and Mapping Qualifications* and the *Classification and Grading Standards for Surveying and Mapping Qualifications* issued by the Ministry of Natural Resources have reduced the types and levels of qualifications, integrating the surveying and mapping qualification levels from four levels to two levels: Class A and Class B.

Class A surveying and mapping qualifications are applicable nationwide and are approved by the Ministry of Natural Resources; Class B surveying and mapping qualifications are limited in business scope and region and are approved by provincial competent authorities, such as engaging in electronic navigation map production within the autonomous driving areas designated by relevant government departments. In addition, Article 2 of the *2024 Notice* strengthens the qualification requirements for intelligent connected vehicle scenarios, clarifying that links such as data collection, storage, and transmission must be undertaken by entities with surveying and mapping qualifications such as electronic navigation map production. Article 5 further stipulates that geographic information data used for navigation-related activities, as well as map production and updating, shall be directly transmitted to entities with surveying and mapping qualifications for electronic navigation electronic map production for management, and unqualified enterprises are not allowed to access such data.

(2) Subject Types

In accordance with the *Interim Measures for the Administration of Surveying and Mapping in China by Foreign Organizations or Individuals,* foreign investment access follows the principle of “limited opening”. Foreign organizations or individuals must carry out surveying and mapping activities within China in the form of joint ventures or cooperative ventures, and are not allowed to engage in key businesses such as navigation electronic map compilation, geodesy, marine surveying and mapping, aerial photogrammetry, and surveying and mapping of administrative boundary lines. If a

foreign organization or individual needs to conduct one-off surveying and mapping activities, it is not required to establish a joint venture or cooperative enterprise, but it must be approved by the Ministry of Natural Resources in conjunction with the military surveying and mapping authority, and must be carried out jointly with surveying and mapping personnel from relevant Chinese departments and units. Meanwhile, the *2022 Notice* also stipulates that domestic-funded enterprises must obtain corresponding surveying and mapping qualifications in accordance with the law or entrust units with corresponding surveying and mapping qualifications to carry out relevant surveying and mapping activities.

(3) Special Compliance Requirements for Data Processing Activities

a) Localized Storage

According to Article 5 of the *2024 Notice*, geographic information data shall be stored locally within the territory of China and shall not be directly transmitted to overseas servers; in addition, the storage devices, networks, cloud services, etc. used by enterprises must comply with the relevant national security and confidentiality requirements.

b) Cross-border Transmission

If the relevant data falls within the scope specified in Item b)and Item e)[35] of Appendix G to *Data Classification and Grading Rules*, or belongs to “geographic information of important sensitive areas”, “external vehicle video and image data containing facial information, license plate information, etc.”, and “other data that may endanger national security, public interests, or the legitimate rights and interests of individuals or organizations” [36] as specified in the *Provisions on the Administration of Automobile*

[35] Data that can be used by other countries or organizations to launch military strikes against China, or reflect China’s strategic reserve, emergency mobilization, combat capabilities, such as geographic data meeting certain accuracy indicators or data related to the production capacity and reserves of strategic materials.

[36] Data reflecting the physical security protection of key targets and important places or the location of undisclosed geographic targets, which can be used by terrorists and criminals to carry out sabotage, such as data describing the construction drawings, internal structure, and security situation of key security units, important production enterprises, and national important assets (such as railways and oil pipelines).

Data Security (Trial), it may be identified as important data. Relevant enterprises shall, in accordance with the requirements of laws and regulations such as the *Measures of Cross-Border Data Transfer Security Assessment* and the *Provisions on Cross-Border Data Flows*, with reference to the publicly released catalog of important data in the industry and the notification of important data by surveying and mapping authorities. Meanwhile, when applying to provide geographic information data to overseas parties, they must strictly go through the approval procedures for external provision or map review, and implement relevant provisions such as security assessment of cross-border data transfers.

(4) Compliance Obligations for Classified Surveying and Mapping Data

According to the provisions of the *Catalogue of State Secrets in Surveying, Mapping and Geographic Information Management Work* attached to the *Regulations on the Scope of State Secrets in Surveying, Mapping and Geographic Information Management Work*, measured results such as 3D models, point clouds, oblique images, real-scene images, and electronic navigation maps that have a horizontal accuracy better than or equal to 10 meters (outside military restricted zones) or a relative measurement accuracy of ground object height better than or equal to 5%, with a continuous coverage area exceeding 25 square kilometers, are identified as state secrets.

In addition, with reference to Article 34 of the *Surveying and Mapping Law* and Article 18 of the *Regulations on the Administration of Surveying and Mapping Achievements of the People's Republic of China*, enterprises are not allowed to provide classified surveying and mapping results to overseas parties without authorization. Before providing such data to overseas parties, they shall, in accordance with the approval procedures specified by the State Council and the Central Military Commission, submit an application for approval to the surveying and mapping administrative department of the State Council or the surveying and mapping administrative department of the relevant provincial government, autonomous region, or municipality directly under the

Central Government. Prior to approval, the surveying and mapping administrative department shall seek opinions from the relevant military departments.

（ii）Meteorological Data

1. Definition and Classification of Data

According to Article 3 of the *Measures for the Administration of Meteorological Data (Trial)*, meteorological data refers to numbers, texts, symbols, pictures, audio and video, etc. in the fields of atmospheric and space weather science and technology obtained through observation and monitoring, investigation, collection and exchange, scientific research, experimental development, production analysis, authorization management, and other means. Moreover, according to different data generation methods, meteorological data can be divided into raw dataand product data[37]. This dichotomy provides a basic framework for enterprises' compliance management. Since raw data directly reflects natural phenomena, the collection link needs to be focused on for control; since product data contains processing and analysis contents, its use scenarios and compliance requirements are more abundant.

2. Special Compliance Obligations in the Data Processing Process

(1) Data Collection

According to the provisions of Chapter III of the *Meteorological Law*, a strict access system is implemented for meteorological data collection. Meteorological data collection/meteorological data detection must be carried out by meteorological stations with corresponding qualifications and should comply with the national unified meteorological technical standards, specifications, and procedures. If an enterprise intends to collect meteorological data by establishing a station, it should obtain a valid license for special meteorological technical equipment [38] and file it with the

[37] Raw data refers to the original records obtained in the process of observation and monitoring, investigation, scientific research, and experimental development, as well as the data that has not been processed obtained through format change, quality control, data interpolation, unit conversion, measurement transformation, statistical calculation, compilation, etc.

[38] Refer to Article 5 of the Measures for the Administration of the Use License of Special Meteorological

meteorological competent authority[39], and shall not arbitrarily establish meteorological detection stations (points) in national defense and military facilities, military - sensitive areas, areas that have not yet been opened to the outside world, and other areas involving national security. If an enterprise obtains meteorological data through the sharing method of the meteorological competent authority and its subordinate units or enterprises, according to the provisions of Chapter II of the *Measures for the Administration of Meteorological Data Sharing Services and Security (Trial)*, the enterprise should accept security supervision and management, and sign a cooperation agreement involving data sharing services.

(2) Data Storage

For meteorological data obtained from meteorological authorities at all levels through sharing, enterprises shall comply with the requirements of Article 14 of the *Measures for the Administration of Meteorological Data Sharing*, restricting such data to internal use. When distributing the data, it can be stored on a local area network (LAN) exclusively for the unit's own use, but must not be connected to wide area networks (WANs) or the Internet. Relevant enterprises shall establish sound and strict data access and storage systems, clarify the usage rights of various internal departments and personnel regarding meteorological data, and conduct regular inspections and maintenance of the LAN's network architecture and security protection measures to prevent data leakage caused by network configuration errors or external attacks.

(3) Data Usage

Regarding various types of meteorological data, Article 20 of the *Measures for the Administration of Meteorological Data (Trial)* prohibits any unit or individual from disclosing the obtained meteorological data to the public in the form of forwarding, transferring, selling, etc., or using it for purposes other than meteorological services and scientific research and development without permission. Meanwhile, in

Technical Equipment

[39] Refer to Article 15 of the Measures for the Administration of Meteorological Information Services

accordance with Article 31 of the *Measures for the Administration of Meteorological Data Sharing Services and Security (Trial)* and Chapter III of the *Measures for the Administration of Meteorological Data Sharing*, enterprises that obtain meteorological data through sharing shall use the meteorological data legally, implement the security guarantee measures agreed in the meteorological data service agreement. Such enterprises shall not use the data beyond the scope agreed in the meteorological data service agreement without permission or mine meteorological data for the purpose of obtaining state secrets, commercial secrets or personal privacy, and shall not endanger the safety of public meteorological services. In addition, enterprises only have limited and non-exclusive right to use meteorological data, and shall not transfer the meteorological data obtained from meteorological authorities at all levels, whether for consideration or free of charge. Relevant enterprises must strictly abide by the above provisions when their business operations involve meteorological data.

(4) Data export

According to Article 5 of the *Measures for the Administration of Foreign-related Meteorological Detection and Data*, any organization or individual is strictly prohibited from providing meteorological data to unapproved foreign organizations or individuals, and shall not provide meteorological data involving state secrets to foreign organizations or individuals in any manner. Therefore, when enterprises establish cooperative relations with overseas entities involving cross-border transmission of meteorological data, they shall go through strict approval and verification procedures to ensure that the receiving party has obtained approval, so as to ensure compliant operation. With reference to Article 17 of the *Implementation Rules for the Meteorological Department to Keep State Secrets*, the cross-border transmission of meteorological data shall go through hierarchical approval procedures according to different confidentiality levels, as shown in the following table:

Level	Approval Requirements

Top secret	Submitted by the host unit to the provincial (autonomous region, municipality directly under the Central Government) meteorological bureau or the National Meteorological Administration, reviewed by the relevant functional institutions of the National Meteorological Administration, examined and approved by the Security Committee of the National Meteorological Administration, and filed with the National Security Bureau.
Confidential	Submitted by the host unit to the provincial (autonomous region, municipality directly under the Central Government) meteorological bureau or the National Meteorological Administration, reviewed by the relevant functional institutions of the National Meteorological Administration, examined and approved by the Security Committee of the National Meteorological Administration, and filed with the National Security Bureau.
Internal	Submitted by the host unit to the provincial (autonomous region, municipality directly under the Central Government) meteorological bureau or the relevant functional institutions of the National Meteorological Administration for examination and approval.
Public	To be resolved through consultation between the host unit and the prefectural (municipal), county meteorological bureaus or the division-level units of the National Meteorological Administration and provincial (autonomous region, municipality directly under the Central Government) meteorological bureaus.

Furthermore, if the meteorological data provided to overseas organizations or individuals falls into the category of important data, the obligation of security

assessment shall also be fulfilled. It should be reminded to enterprises that the *China (Tianjin) Pilot Free Trade Zone Data Export Management List (Negative List) (2024 Edition)* specifies that for providing various meteorological monitoring data and disaster prevention data serving military, national defense scientific research, and high-tech fields to overseas organizations or individuals[40], except for data publicly released by meteorological and other relevant departments, the obligation of data security assessment shall be fulfilled. Therefore, it is recommended that enterprises in the free trade zone pay close attention to the latest negative lists issued in their respective free trade zones, establish a dynamic tracking mechanism for the lists, and keep abreast of the key points of policy changes. Before carrying out cross-border transmission of meteorological data, they should check the data to be transmitted one by one according to the negative list to determine whether it falls into the restricted scope.

It is worth noting that the China Meteorological Administration stated on February 18, 2025 that it will continue to strengthen cooperation with the National Data Administration, accelerate the introduction of basic data systems such as meteorological data authorization operation and compliance management, so as to provide guarantees for the use and circulation of meteorological data. It is recommended that enterprises pay close attention to the dynamics of policy changes, so as to formulate compliance plans and effectively prevent potential data compliance risks.

(iii) Financial Credit Reference Data

1. Definition of Data

Financial data is the foundation for financial institutions to carry out business, provide services, and conduct daily operations and management, covering multiple fields such

[40] Such as meteorological support data for major events, data of important sensitive areas, data on climate change response and crop yield forecasting, Fengyun satellite L0-level data and telemetry data, radar base data, ground operation point data of weather modification, historical meteorological archives and derivative data, meteorological government service data, and key information infrastructure data of meteorology, etc.

as banking, insurance, securities, and credit reference[41]. Among them, personal financial information is the personal information obtained, processed, and stored by financial institutions through channels such as providing financial products and services. In addition, focusing on the credit investigation field, according to the *Measures for the Administration of Credit Investigation Business*, credit information is defined as "basic information, lending information, other relevant information that is legally collected to provide services for financial and other activities and used to identify and judge the credit status of enterprises and individuals, as well as analysis and evaluation information formed based on the aforesaid information". Due to the sensitivity and particularity of financial credit investigation data, its compliance management is not only related to the protection of personal privacy, but also directly affects the stability of the financial market and the reputation of financial institutions.

2. Special Compliance Obligations in Data Processing

(1) Data Collection

According to the provisions of *Financial Data Security - Specification for Data Lifecycle Security(JR/T0223-2021)* , financial data collection by financial institutions includes two methods: collection from external institutions and collection from personal financial information subjects. Specifically:

First, when collecting data from external institutions, financial institutions shall clarify the rights and obligations of both parties and the specific content of collection through contracts or agreements, ensure that the collection is authorized by the data subject, and avoid legal risks caused by unauthorized data collection. Before data collection, a data security impact assessment shall be conducted, and logs of the data collection process shall be recorded to ensure the security of the collection process and the traceability of data sources. At the same time, financial institutions shall take necessary

[41] According to the *Guidelines for Classification of Financial Data Security (JR/T 0197－2020)* (hereinafter referred to as the "***Guidelines for Data Security Classification***") issued by the People's Bank of China, financial data refers to "various types of data required or generated by financial institutions in conducting financial business, providing financial services, and daily operation and management". Personal financial information refers to "personal information obtained, processed, and stored by financial institutions through providing financial products and services or other channels."

technical measures and security control measures to ensure the compliance, integrity, and authenticity of the data. For the collection of highly sensitive data, financial institutions shall meet stricter encryption requirements to prevent data leakage or tampering during transmission and storage.

Second, when collecting data from personal financial information subjects, in addition to meeting the abovementioned technical measures and encryption requirements, financial institutions shall not collect data beyond the scope authorized by subjects. When institutions stop providing financial products or services, they shall cease data collection and analytical application activities to avoid unnecessary interference to users and data risks.

In addition, focusing on the credit investigation industry, regarding the collection of credit information, Article 14 of the *Regulations on the Administration of the Credit Investigation Industry* requires credit investigation institutions to obtain the explicit consent of the information subject in advance before collecting personal credit information. Meanwhile, credit investigation institutions are prohibited from collecting personal information such as religious beliefs, genes, fingerprints, blood types, disease and medical history, as well as other personal information that is prohibited from being collected by laws and administrative regulations. For certain sensitive information, such as personal income, deposits, securities, commercial insurance, real estate information, and tax payment amount information, collection can only be permitted after clearly informing the information subject of the possible adverse consequences of providing such information and obtaining their written consent.

(2) Data Sharing

In practice, to improve the efficiency and quality of financial services and help financial institutions more effectively identify risks and assess customers' credit status, the sharing of financial data is relatively common. It should be reminded to financial institutions that for external sharing of financial data, in addition to meeting the general requirements of the *PIPL*, necessary security control measures shall also be

implemented. For example, conducting regular security audits on shared data, establishing emergency response mechanisms, and for the sharing of financial data at specific sensitive levels, encryption processing shall be carried out.

In addition, Article 29 of the *Measures for the Administration of the Credit Investigation Industry* stipulates that institutions engaged in credit business shall obtain the written consent of the information subject in advance before providing credit information to the financial credit information basic database or other subjects. It can be seen that since credit business involves important issues such as financial risks and fund security, the "written consent" here, on the one hand, allows the information subject to treat the authorization of their credit information more cautiously, and on the other hand, facilitates institutions engaged in credit business to provide clear authorization basis in subsequent possible legal disputes and other situations.

(3) Data Export

Given that financial data often contains customers' sensitive information and industry - critical data, enterprises should particularly consider factors such as the type and sensitivity of the data to be exported, and meet the corresponding compliance requirements for data export.

First, for the export of important data in the financial industry, according to the explanation in Appendix C of the *Guidelines for Data Security Classification*, important data in the financial field includes macro characteristic data, derivative characteristic data obtained from massive information aggregation, data during the decision - making and law enforcement process of industry regulatory authorities, and information on network security vulnerabilities of critical information infrastructure, etc. In accordance with the requirements of the *Measures for Security Assessment of Cross-Border Data Transfers*, the *New Cross - border Regulations* and other relevant provisions, if the relevant departments or regions inform or publicly release the data as important data, data processors shall fulfill the obligation of security assessment for cross-border data transfers. It is worth noting that for the financial industry, if the relevant data belongs to

Level 5 data generated within China[42], it can only be stored domestically and is prohibited from being exported.

Second, for the export of personal financial data, combined with the provisions of the *Guidelines for Data Security Classification*[43] and the *Technical Specification for the Protection of Personal Financial Information (JR/T0171 - 2020)*[44] , personal financial information collected and generated domestically shall, in principle, be stored, processed and analyzed domestically. If it is really necessary to provide it to overseas parties, relevant enterprises shall obtain the explicit consent of the subject of personal financial information, conduct security assessment for cross-border transfer, and supervise overseas institutions to fulfill their data protection obligations.

Among them, for the special category of personal credit information, in accordance with the requirements of the *Regulations on the Administration of the Credit Reference*

[42] Important data, usually mainly used for key business of large or extra - large financial institutions and important core node institutions in the financial transaction process. It is generally open to specific personnel and only accessed or used by those who must know it; if the data security is damaged, it will affect national security or cause serious impact on public rights and interests.

[43] Article 7.1.3 (d): Personal financial information collected and generated in the process of providing financial products or services within the People's Republic of China shall be stored, processed and analyzed domestically. If it is really necessary to provide personal financial information to overseas institutions (including head offices, parent companies, branches, subsidiaries and other affiliated institutions necessary for completing the business) due to business needs, the security assessment for the cross-border transfer of personal financial information shall be carried out in accordance with the measures and standards formulated by relevant national and industry departments to ensure that the data security protection capability of overseas institutions meets the security requirements of relevant national and industry departments and financial institutions; Agreements shall be signed with overseas institutions and on - site inspections shall be conducted to clarify and supervise overseas institutions to effectively fulfill their responsibilities and obligations such as keeping personal financial information confidential, deleting data and assisting in case investigation.

[44] Paragraph 1 of Article 7 of the *Technical Specification for the Protection of Personal Financial Information* stipulates that personal financial information collected and generated in the process of providing financial products or services within the territory shall be stored, processed and analyzed within the territory. If it is really necessary to provide it to overseas institutions (including head offices, parent companies, branches, subsidiaries and other affiliated institutions necessary for completing the business) due to business needs, the specific requirements are as follows: ① It shall comply with national laws, regulations and relevant provisions of industry competent departments; ② It shall obtain the explicit consent of the subject of personal financial information; ③ The security assessment for the outbound transfer of personal financial information shall be carried out in accordance with the measures and standards formulated by relevant national and industry departments to ensure that the data security protection capability of overseas institutions meets the security requirements of relevant national and industry departments and financial institutions; ④ Agreements shall be signed with overseas institutions and on - site inspections shall be conducted to clarify and supervise overseas institutions to effectively fulfill their responsibilities and obligations such as keeping personal financial information confidential, deleting data and assisting in case investigation.

Industry [45]and the Measures for the Administration of Credit Investigation Services[46], the collation, storage and processing of information collected by credit reference institutions within China shall, in principle, also be stored domestically; if credit reference institutions provide enterprise credit information inquiry products and services to overseas information users, they shall conduct necessary reviews on the identity of information users and the purpose of using credit information to ensure that the credit information is used for cross - border trade.

(iv) E-commerce Marketing Data

1. Laws and Regulations in the E-commerce Field

In the field of e-commerce, data compliance supervision presents a three-dimensional governance system of "upper-level laws + special regulations + industry norms". The *E-commerce Law* clarifies the obligations of e-commerce operators to protect consumers' personal information at the macro level; the *Measures for the Supervision and Administration of Online Transactions* focuses on online transaction scenarios and refines the principles of data collection; the *Interim Provisions on Regulating Promotional Activities*, *Measures for the Administration of Internet Live-streaming Marketing Information Content Services (Draft for Comment)*, and *Measures for the Administration of Internet Advertising* put forward corresponding compliance requirements for operators from the perspectives of promotion, live-streaming marketing, and advertising. It is worth noting that although the current legislation does not clearly define "e-commerce marketing data", combined with the definition of e-

[45] Article 24: The collation, storage and processing of information collected by credit reference institutions within China shall be carried out within China. Credit reference institutions that provide information to overseas organizations or individuals shall comply with laws, administrative regulations and relevant provisions of the credit reference industry supervision and administration department of the State Council.
[46] Article 39: Credit reference institutions that carry out credit reference business and related activities within the People's Republic of China shall store the collected enterprise credit information and personal credit information within the People's Republic of China. Article 40: Credit reference institutions that provide personal credit information to overseas parties shall comply with the provisions of laws and regulations. Credit reference institutions that provide enterprise credit information inquiry products and services to overseas information users shall conduct necessary reviews on the identity of information users and the purpose of using credit information to ensure that the credit information is used for reasonable purposes such as cross - border trade and investment and financing, and shall not endanger national security.

commerce in the *E-commerce Law*[47] , such data usually includes various types of data collected, generated, and used by e-commerce enterprises in selling goods, providing services, and carrying out marketing activities through information networks, such as consumers' basic information, consumption behavior data, transaction data, commodity and service data, platform management data, and advertising placement data.

2. Compliance Key Points for Data Processing in E-commerce Marketing Scenarios

(1) Data Collection

First, in accordance with the requirements of Article 23 of the *E-commerce Law* and Article 17 of the *PIPL*, when collecting consumers' data, e-commerce enterprises must clearly and understandably inform consumers of the purposes, methods, scope of collection, as well as the use and sharing of the data. Specific requirements include:

a. Providing detailed user agreements and privacy policies for users to actively check and consent during registration, and avoiding embedding authorization clauses in lengthy agreements;

b. For the collection of sensitive personal information and the invocation of terminal permissions, using prominent methods such as pop-up windows and independent pages for separate notification;

c. Establishing a dynamic notification mechanism, and re-obtaining user consent when the purpose of data use changes.

Second, due to the wide range of sources of e-commerce marketing data, when enterprises obtain data from third-party partners, they must review whether the third party's data collection and use comply with laws and regulations, sign legally valid data

[47] Article 2 of the *E-commerce Law*: E-commerce refers to business activities of selling goods or providing services through information networks such as the Internet.

sharing agreements, clarify the data rights and obligations of both parties, and prevent legal risks caused by data source issues.

(2) Data Storage

Due to the large number of transactions involving goods/services in the e-commerce industry, e-commerce platforms bear compliance supervision obligations. Therefore, to ensure the traceability of e-commerce transactions/marketing activities and deal with possible disputes, damage to consumers' rights and interests, or investigations by regulatory authorities, the *E-commerce Law* and *Measures for the Supervision and Administration of Online Transactions* clearly stipulate the storage period of relevant data. For example, information on goods and services, as well as transaction information, shall be retained for no less than three years from the date of completion of the transaction; information on the identity of operators within the platform shall be retained for no less than three years from the date of their withdrawal from the platform; and all historical versions of the platform's service agreements and transaction rules shall be retained for three years prior to the effective date of the revised versions. E-commerce platforms should pay attention to the above retention period requirements and retain key information, which not only helps the platform in the compliance supervision of merchants, but also enables them to provide accurate data to regulatory authorities in subsequent matters involving merchant qualification review and transaction behavior traceability.

a) User Right Exercise

Due to the large number of transactions involving goods/services in the e-commerce industry, e-commerce platforms bear compliance supervision obligations. Therefore, to ensure the traceability of e-commerce transactions/marketing activities and deal with possible disputes, damage to consumers' rights and interests, or investigations by regulatory authorities, the *E-commerce Law* and *Measures for the Supervision and Administration of Online Transactions* clearly stipulate the storage period of relevant data. For example, information on goods and services, as well as transaction

information, shall be stored for no less than three years from the date of completion of the transaction; information on the identity of operators within the platform shall be stored for no less than three years from the date of their withdrawal from the platform; all historical versions of platform service agreements and transaction rules shall retain the versions three years prior to the effective date of the revised versions. E-commerce platforms should pay attention to the above storage period requirements and retain key information, which not only helps the platform in the compliance supervision of merchants, but also enables them to provide accurate data basis to regulatory authorities in subsequent matters involving merchant qualification review and transaction behavior traceability.

b) Data Export

To balance the convenience and security of data flow, Article 5 of the *Provisions on Promoting and Regulating Cross-Border Data Flows* stipulates that when a data processor provides an individual's personal information across borders for the conclusion or performance of a contract in which the individual is a party, it falls within the scope of being exempt from declaring a security assessment, concluding a standard contract, or obtaining protection certification. It also lists typical business scenarios such as cross-border shopping, cross-border delivery, cross-border remittance, and cross-border payment. In the e-commerce industry, transaction activities are frequent and mostly revolve around the sale of goods or services. For example, in cross-border shopping, when a consumer places an order to purchase overseas goods and enters into a sales contract with an overseas merchant or e-commerce platform, the e-commerce platform needs to provide the consumer's personal information such as name, delivery address, and contact information to the overseas merchant or logistics carrier across borders to complete the transaction. Therefore, the cross-border data activities of relevant enterprises are likely to fall into this exemption scenario.

In practice, relevant enterprises should first determine whether the exported data is "necessary for the conclusion or performance of a contract in which the individual is a

party". If it falls within the scope of exemption, there is no need to fulfill additional export requirements; if not, they need to determine whether it belongs to sensitive personal information or important data based on the data volume and sensitivity, so as to choose the corresponding compliant export path.

(v) Human Genetic Resource Information

1. Definition of Data

According to Article 85 of the *Biosecurity Law of the People's Republic of China* (hereinafter, the *Biosecurity Law*) and Article 2 of the *Regulations on the Administration of Human Genetic Resources of the People's Republic of China* (hereinafter, the *Human Genetic Resources Regulations*), human genetic resource information refers to data and other information materials generated by using human genetic resource materials. The *Implementation Rules of the Regulations on the Administration of Human Genetic Resources* (hereinafter, the *Implementation Rules*) further clarify that the human genetic resource information referred to in Article 2 of the *Human Genetic Resources Regulations* includes information materials such as human gene and genome data generated by using human genetic resource materials; it does not include clinical data, imaging data, protein data, and metabolic data.

In addition, according to relevant guidelines of the National Health Commission (hereinafter, the NHC)[48], human genetic resource information includes nucleic acid sequence information such as human genes, genomes, transcriptomes, and epigenomes, as well as information materials related to diseases associated therewith, excluding simple clinical data, imaging data, protein data, metabolic data, etc.

Human genetic resource information and human genetic resource materials both belong to human genetic resources, and their collection, preservation, utilization, and provision to foreign parties are subject to a series of special restrictions.

[48] See the Application Guidelines on the Human Genetic Resources Service System of NHC: https://zwfw.nhc.gov.cn/bsp/rlyczyfwxt/202405/t20240517_2758.html

2. Special Compliance Obligations in Data Processing

(1) General Requirements for Data Collection, Storage, Processing and Utilization and Provision to Foreign Parties

The collection, preservation, utilization, and provision of human genetic resources to foreign parties must comply with the following special requirements[49] :

- Foreign organizations, individuals, and institutions established or actually controlled by them (hereinafter, the foreign-related entities) are prohibited from collecting or preserving China's human genetic resources within the territory of China, and from providing China's human genetic resources to overseas parties.
- The collection, preservation, utilization, and provision of China's human genetic resources to foreign parties must not endanger the public health, national security, or public interests of China.
- The collection, preservation, utilization, and provision of China's human genetic resources to foreign parties shall comply with ethical principles and undergo ethical review in accordance with relevant national regulations.
- The collection, preservation, utilization, and provision of China's human genetic resources to foreign parties shall respect the right to privacy of the providers of human genetic resources, obtain their prior informed consent, and protect their legitimate rights and interests.
    - Among them, for the collection of China's human genetic resources, the provider of human genetic resources shall be informed in advance of the purpose and use of the collection, possible impacts on health, measures for protecting personal privacy, and their rights to voluntarily participate and unconditionally withdraw at any time, and written consent shall be obtained from the provider. When informing the provider of relevant information, it must

[49] Articles 7 to 10 and Article 12 of the *Human Genetic Resources Regulations*

be comprehensive, complete, true, and accurate, without concealment, misleading, or deception.

- The collection, preservation, utilization, and provision of China's human genetic resources to foreign parties shall comply with technical specifications formulated by the competent health department of the State Council.
- The trading of human genetic resources is prohibited (the legal provision or use of human genetic resources for scientific research with payment or receipt of reasonable cost expenses shall not be regarded as trading).

(2) Administrative Licensing or Filing Requirements for Collection, Preservation, and International Cooperation

Due to the high sensitivity of human genetic resources, in specific circumstances, their collection, preservation, and international cooperation are subject to special administrative licensing or filing requirements[50]:

- For the collection of China's important genetic pedigrees, human genetic resources from specific regions, or human genetic resources of the types and quantities specified by the competent health department of the State Council, specific conditions must be met and approval must be obtained from the competent health department of the State Council.
- For the preservation of China's human genetic resources and the provision of a basic platform for scientific research, specific conditions must be met and approval must be obtained from the competent health department of the State Council.
- Administrative licensing for international scientific research cooperation and filing for international cooperative clinical trials shall be applied for jointly by the Chinese and foreign entities. All cooperating parties shall commit to the authenticity, accuracy, and completeness of the information in the application materials.

[50] Articles 11, 14, 22 of the *Human Genetic Resources Regulations*; Chapter IV, Sections 1 and 2 of the *Implementation Rules*

- To apply for administrative licensing for international scientific research cooperation involving human genetic resources, ethical review in the respective countries (regions) of both cooperating parties must be obtained. If a foreign entity is truly unable to provide ethical review certification materials from its country (region), it may submit materials certifying that the foreign entity recognizes the ethical review opinions of the Chinese entity.
- For international cooperative clinical trials using China's human genetic resources in clinical medical and health institutions to obtain marketing authorization for relevant drugs and medical devices in China, which do not involve the outbound transfer of human genetic resource materials and meet specific conditions, approval is not required, but filing must be completed.

(3) Requirements for Providing China's Human Genetic Resource Information to Foreign Parties

As mentioned above, foreign-related entities are subject to strict restrictions on the collection, preservation, and provision of China's human genetic resources to foreign parties. However, in scientific research and commercial practices, Singaporean universities, research institutions, and biomedical enterprises have legitimate needs to utilize human genetic resources in legal research and development activities. Such needs can be met through cooperation with Chinese research institutions, universities, medical institutions, and enterprises (hereinafter, the Chinese entities)[51]in compliance with China's laws and regulations.

Except for the administrative licensing and filing requirements for international cooperation as mentioned above, Chinese entities must also pay attention to the following specific requirements for providing human genetic resource information to foreign parties[52]:

[51] According to Article 11 of the *Implementation Rules*, domestic-funded and controlled institutions in Hong Kong and Macao are regarded as Chinese entities.
[52] Article 57 of the *Biosecurity Law*, Article 28 of the *Human Genetic Resources Regulations*, and Chapter IV, Section 3 of the *Implementation Rules*

- When providing or opening access to human genetic resource information to foreign-related entities, the Chinese information owner shall file a record with the competent health department of the State Council and submit an information backup. However, during the implementation of internationally cooperative scientific research projects that have obtained administrative licensing or internationally cooperative clinical trials that have completed filing, if a Chinese entity provides human genetic resource information generated from the cooperation to a foreign-related entity and the international cooperation agreement has stipulated that the information can be used by both cooperating parties, separate filing and submission of an information backup are not required.
- Providing or opening access to human genetic resource information to foreign-related entities must not endanger China's public health, national security, or public interests; if it may affect China's public health, national security, or public interests, it shall undergo a security review organized by the competent health department of the State Council. Circumstances requiring security review include: (1) human genetic resource information of important genetic pedigrees; (2) human genetic resource information of specific regions; (3) exome sequencing and genome sequencing information resources involving more than 500 cases; (4) other circumstances that may affect China's public health, national security, or public interests.

Chapter V: Compliance Paths for Cross-Border Data Flow※

Since China first proposed provisions on cross-border data flow in the *Cybersecurity Law* in 2016, it has continuously improved the rules for data flow in relevant laws and regulations. On the basis of the three laws, the *Cybersecurity Law*, the *Data Security Law*, and the *PIPL*, the Cyberspace Administration of China has successively issued relevant regulations specifically for cross-border data flow from 2022 to 2024, including the *Measures for the Security Assessment of Data Exports*, the *Measures for the Standard Contract for the Export of Personal Information*, and the *New Regulations on Cross-Border Flow*,[53] building a cross-border data flow compliance system with Chinese characteristics.

I. Path Selection for Outbound Data Flow

(i) Completing data export security assessment declarations, personal information export standard contract filings, personal information protection certifications, etc., in accordance with applicable compliance paths

Data Export Security Assessment

The data export security assessment is only for a few data export scenarios, applicable to CIIOs, export activities involving important data, and export activities involving a large number of personal information subjects. According to the official disclosure of the Cyberspace Administration of China, as of December 2024, the Cyberspace Administration of China had completed a total of 285 security assessment projects, of which 27 security assessment projects failed the assessment, accounting for less than

---

※ Chapter authors: **Wang Yi**, Partner at Beijing Global Law Firm (Shenzhen Office); **Shi Jingyuan**, Partner at Hong Kong Sirmans Law Firm; **Liu Jiayi**, Associate at Beijing Global Law Firm (Shenzhen Office); **Lai Yuchen**, Sirmans Law Firm;
Lai Yanyu, former associate, Sirmans Law Firm; **Meng Jie**, **Ma Kaiyang**, and **Lin Yi** also contributed.

[53] According to Article 13 of theProvisions on Cross-Border Data Flows, if there is any inconsistency with the Data Cross-border Security Assessment Measures and the Personal Information Cross-border Standard Contract Measures, theProvisions on Cross-Border Data Flows shall prevail.

10% of the total.[54]

The security assessment includes four major stages: internal material preparation by the enterprise, formal review by the provincial cyberspace administration, substantive review by the national cyberspace administration, and re-evaluation (if necessary). If an enterprise triggers the security assessment requirement, it needs to reserve sufficient time to prepare the application materials and communicate with the regulatory authorities to avoid adverse effects on its business operations.

The Cyberspace Administration of China has successively issued three versions of the *Guidelines for Declaring Security Assessment of Data Exports*, which provide detailed instructions on the specific procedures and material requirements, and has opened a special consultation telephone line to answer questions for enterprises. In practice, we have noticed that the following two aspects are the focus of regulatory attention, and enterprises should pay special attention to them.

First is the legality of personal information export, that is, whether there is an appropriate legal basis. According to the declaration guidelines, the Cyberspace Administration of China requires the declaring unit to provide a description of the implementation of Article 39 of the *PIPL* and supporting materials in the materials, including the obligation to inform and obtain separate personal consent (except for exceptions). Therefore, enterprises should strictly review whether their privacy policies, etc., meet the disclosure requirements of Article 39 of the *PIPL*, whether they have complete records of the separate personal consent obtained, and whether the scope, purpose, and method of data export agreed to by the individual are consistent with the declared matters. If the aforementioned conditions are not met, the privacy policy should be revised in a timely manner, valid separate consent should be obtained, and the records should be properly kept. In practice, it is not only necessary to pay attention to the formal requirements of the compliance path, but more importantly, to the construction of the prerequisite legal basis. For example, some enterprises did not

[54] Article 2 of the Critical Information Infrastructure Security Protection Regulations

discover that they had not yet obtained the valid consent of the relevant individuals for personal information export activities until they declared a security assessment or filed a standard contract, which brought unnecessary twists and turns to the overall compliance work. In addition, it is worth special attention for multinational enterprises that obtaining separate personal consent or having other legal bases is a prerequisite for legally providing personal information overseas, and it is a parallel legal requirement with completing the compliance path, and they cannot replace each other. This is also different from the regulatory requirements of other countries and regions such as Singapore.

Second is the necessity of data export. The principles of purpose limitation and data minimization are basic principles upheld by data privacy laws in all countries and should run through the entire life cycle of data processing activities. This means that in enterprise operation activities, some cross-border data flows that are only out of habit and are dispensable should be avoided, and data export should be limited to the necessary scope. It is particularly noteworthy that enterprises must explain the necessity of data export field by field in the declaration materials for security assessment, which also requires that a relatively strict standard be adopted when conducting internal necessity reviews to avoid being questioned by the regulatory authorities. A common challenge faced by multinational enterprises is that with the popularization of cloud infrastructure and SaaS services, a large number of internal enterprise management systems are uniformly deployed at the group level, making cross-border data flow inevitable. In response to this situation, the business necessity of the data export activity (such as cost, implementation of unified group management, etc.) and data security measures such as access control should be fully explained in the declaration materials to obtain the understanding and recognition of the regulatory authorities.

In addition, enterprises applying for security assessment should pay attention to the validity period of the assessment result. The validity period of the result of passing the data export security assessment is 3 years, calculated from the date the assessment

result is issued. When the validity period expires, and it is necessary to continue to carry out data export activities and there is no situation that requires re-declaration of the data export security assessment, the data processor can, within 60 working days before the validity period expires, apply to the national cyberspace administration through the local provincial cyberspace administration to extend the validity period of the assessment result. With the approval of the national cyberspace administration, the validity period of the assessment result can be extended for 3 years.[55]

During the validity period of the assessment result, if any of the following circumstances occur, the data processor should re-declare the security assessment: the purpose, method, scope, type of data provided overseas and the purpose and method of processing data by the overseas recipient change, affecting the security of the exported data, or extending the overseas storage period of personal information and important data; the data security protection policies and regulations and network security environment of the country or region where the overseas recipient is located change, as well as other force majeure situations, changes in the actual control of the data processor or overseas recipient, changes in the legal documents between the data processor and the overseas recipient, etc., affecting the security of the exported data; other circumstances affecting the security of the exported data occur.[56]

Enterprises should pay close attention to the approaching expiration of the assessment result's validity period and the triggering conditions for re-declaration, and prepare to apply for an extension or re-declare in advance to avoid business interruptions or other adverse effects.

Personal Information Export Standard Contract

Cross-border data flow standard contractual clauses are a data export guarantee measure recognized in many countries and regions and are widely used in the daily practice of multinational enterprises. China's standard contract has drawn some useful

[55] Article 9 of theProvisions on Cross-Border Data Flows

[56] Article 14 of the Data Cross-border Security Assessment Measures

experience from the EU's standard contractual clauses (hereinafter referred to as "SCCs"), and also has some unique features. We will briefly compare and explain them in the table below (not an exhaustive list) with China's personal data export standard contract, the EU's SCCs, and the ASEAN Model Contractual Clauses for Cross Border Data Transfers ("MCCs"), which are recognized and encouraged for use by Singapore.

	China Personal Information Export Standard Contract	**SCCs**	**MCCs**
Fixed Form	The standard contract and SCCs are fixed-form contract clauses, only allowing the contracting parties to make limited modifications to the contract content (e.g., adding supplementary security measures in an appendix that do not conflict with the main contract clauses).		The MCCs are recommended model clauses recognized by many ASEAN countries including Singapore. Enterprises may adopt and modify them as appropriate (but must not conflict with ASEAN's data protection principles).
Priority Application	In case of conflict between other relevant contracts and the standard		No mandatory application effect.

	contract/SCCs, the standard contract/SCCs shall prevail. For example, affiliated entities of a multinational enterprise may have entered into a multi-party data transfer agreement (hereinafter referred to as "IGDTA") involving multiple countries and regions, and incorporated the standard contract and SCCs as appendices to the IGDTA. In this case, if there is a conflict between the main text of the IGDTA and the appendices, the standard contract (for data transferred out of China) and the SCCs (for data transferred out of the European Economic Area) should prevail respectively.	It needs to be explicitly agreed in the MCCs which text shall prevail in case of conflict.
Impact Assessment	When adopting the standard contract and SCCs as the compliance path for data export, it is necessary to conduct a personal information protection impact assessment and a transfer impact assessment (hereinafter referred to as "TIA") respectively in accordance with the requirements of Chinese and EU laws, but the assessment contents are different.	It is not explicitly required that a TIA must be completed for the cross-border data transfer scenario.

Scope of Application	Non-CIIOs that cumulatively provide personal information of more than 100,000 but less than 1 million individuals (excluding sensitive personal information) or sensitive personal information of less than 10,000 individuals overseas since January 1 of the current year.	The destination country or region has not obtained the EU's "adequacy decision", regardless of the type of data exporter or the scale of data export.	Voluntary application, can be used as one of the ways to prove that the overseas recipient can provide equivalent protection standards.
Role Modules	The standard contract does not apply different modules depending on the roles of the data exporter and recipient, but some clauses distinguish the obligations based on the role of the data recipient	Different modules apply depending on the different roles of the data exporter and recipient (data controller or data processor), with 4 different	Different modules apply depending on the different roles of the data recipient (data controller or data processor), with 2 different modules.

	(personal information processor or trustee).	modules.	
Filing Requirements	The personal information processor shall, within 10 working days from the effective date of the standard contract, file it with the local provincial cyberspace administration.	No filing requirement. But the contracting parties should record the TIA in writing and provide it to the supervisory authority upon request.	Voluntary mechanism, no filing requirement.
Applicable Law and Dispute Resolution	Chinese law applies. The contracting parties may choose to resolve disputes through litigation in a Chinese court or arbitration by an arbitration institution in a member state of the *New York*	In different role modules, the contracting parties may choose the applicable law and to resolve disputes through litigation in the courts of a specific	The parties may agree on the applicable law and dispute resolution mechanism themselves.

	Convention.	country.	

The standard contract compliance path mainly includes two stages: internal preparation (conducting assessments, negotiating contracts) and submitting for filing. A difficult point in the preparation process is assessing the impact of the personal information protection policies and regulations of the country or region where the overseas recipient is located on the performance of the standard contract. It is necessary to seek internal or external professionals familiar with overseas policies and laws to carry out specific work. It is recommended that enterprises objectively assess the foreseeable risks brought by overseas policies and regulations, and whether the protective measures adopted can effectively mitigate these risks, in order to successfully complete the filing.

During the validity period of the standard contract, if any of the following circumstances occur, the personal information processor should re-conduct a personal information protection impact assessment, supplement or re-conclude the standard contract, and perform the corresponding filing procedures: the purpose, scope, type, sensitivity, method, or storage location of the personal information provided overseas, or the purpose and method of processing personal information by the overseas recipient changes, or the overseas storage period of personal information is extended; the personal information protection policies and regulations of the country or region where the overseas recipient is located change, etc., which may affect the rights and interests of personal information; other circumstances that may affect the rights and interests of personal information.

As of December 2024, the cyberspace administration had completed a total of 1,071 standard contract filings.[57]

[57] Data source: December 31, 2024, National Data Administration press conference text on promoting high-quality development of data industry and enterprise data resource development and utilization: http://www.news.cn/energy/rdzt/sjyszb/index.html

Personal Information Protection Certification

Personal Information Protection Certification (hereinafter referred to as "PIP Certification") is one of the three export compliance paths stipulated in the *PIPL*, but its application in practice is relatively rare at present. According to the information disclosed by the China Cybersecurity Review Technology and Certification Center, as of November 2024, the center, as the supporting unit for PIP Certification, had received a total of 104 intention applications for PIP Certification and issued 7 personal information protection certification certificates.[58]

In January 2025, the Cyberspace Administration of China issued the *Measures for the Personal Information Protection Certification for the Export of Personal Information (Draft for Comment)* (hereinafter referred to as the *"Certification Measures"*). With the subsequent promulgation of these measures, it is expected to provide clearer guidance for the market and promote the wider implementation of PIP Certification.

According to the *New Regulations on Cross-Border Flow* and the Certification Measures, the applicable conditions for PIP Certification are the same as for the standard contract, that is, non-CIIOs that cumulatively provide personal information of more than 100,000 but less than 1 million individuals (excluding sensitive personal information) or sensitive personal information of less than 10,000 individuals overseas since January 1 of the current year. In addition, personal information processors that process domestic personal information overseas and meet the provisions of Article 3, Paragraph 2 of the *PIPL* can also carry out personal information export activities by obtaining PIP Certification.[59]

The key contents to be assessed for PIP Certification include: the legality, propriety, and necessity of the purpose, scope, and method of personal information export; the impact of the personal information protection policies, laws, and network and data

[58] Data source: November 28, 2024, China Cybersecurity Review Certification and Market Supervision Big Data Center news: https://www.isccc.gov.cn/xwdt/tpxw/11/910689.shtml

[59] Articles 4 and 5 of the Personal Information Cross-border Personal Information Protection Certification Measures (Draft for Comments)

security environment of the country or region where the overseas personal information processor and overseas recipient are located on the security of the exported personal information; whether the personal information protection level of the overseas personal information processor and overseas recipient meets the provisions of the laws and administrative regulations of the People's Republic of China and the requirements of mandatory national standards; whether the legally binding agreement concluded between the personal information processor and the overseas recipient stipulates the obligations of personal information protection; whether the organizational structure, management system, and technical measures of the personal information processor and overseas recipient can fully and effectively guarantee data security and personal information rights and interests; other matters that the professional certification body believes need to be assessed according to the relevant standards for personal information protection certification.[60]

Compared with the standard contract, PIP Certification has the characteristics of market-oriented and socialized services. The state will also promote international exchanges and cooperation in PIP Certification activities and promote the mutual recognition of PIP Certification with other countries, regions, and international organizations. At present, Singapore recognizes "designated certification" as a guarantee measure for cross-border data flow, and "designated certification" includes certification under the two systems of "APEC Cross-Border Privacy Rules" (referred to as "APEC CBPR") and "APEC Privacy Recognition for Processors" (referred to as "APEC PRP").

Circumstances for Exemption from the Three Compliance Paths

The promulgation of the *New Regulations on Cross-Border Flow* in 2024 has exempted data export activities in some specific scenarios from the requirements of the above three compliance paths. We classify and summarize the different exemption conditions

[60] Article 10 of the Personal Information Cross-border Personal Information Protection Certification Measures (Draft for Comments)

as follows.

Small-scale, non-sensitive personal information export: Non-CIIOs that cumulatively provide personal information of less than 100,000 individuals (excluding sensitive personal information) overseas since January 1 of the current year are exempt from declaring a security assessment, concluding a standard contract, and passing PIP Certification.[61] This exemption is particularly important for small and medium-sized enterprises and B-end business enterprises.

Exemptions based on specific business scenarios, including:

- **Necessary for the performance of a contract**: For the conclusion or performance of a contract to which the individual is a party, such as cross-border shopping, cross-border delivery, cross-border remittance, cross-border payment, cross-border account opening, flight and hotel reservations, visa processing, and examination services, where it is indeed necessary to provide personal information overseas, it is exempt from declaring a security assessment, concluding a standard contract, and passing PIP Certification.[62] This exemption is particularly beneficial to C-end enterprises in the aforementioned business fields. Before the implementation of the *New Regulations on Cross-Border Flow*, such enterprises were likely to trigger the security assessment requirement because their user scale reached the million level, but the implementation of the new regulations has greatly reduced their compliance burden.
- **Necessary for cross-border human resources management**: For the implementation of cross-border human resources management in accordance with lawfully formulated labor rules and regulations and lawfully concluded collective contracts, where it is indeed necessary to provide employee personal information overseas, it is exempt from declaring a security assessment, concluding a standard contract, and passing PIP Certification.[63] This exemption

[61] Item (4) of Article 5 of the Provisions on Cross-Border Data Flows
[62] Item (1) of Article 5 of the Provisions on Cross-Border Data Flows
[63] Item (2) of Article 5 of the Provisions on Cross-Border Data Flows

is particularly beneficial to multinational enterprises, but it should be noted that "lawfully formulated labor rules and regulations" has its specific meaning under labor laws and regulations. In addition to the content of the rules and regulations must comply with the provisions of our country's laws, the formulation of the rules and regulations should also meet the procedural requirements stipulated by law, such as completing the democratic consultation procedure.

- **Necessary to respond to emergencies**: In an emergency, to protect the life, health, and property safety of natural persons, where it is indeed necessary to provide personal information overseas, it is exempt from declaring a security assessment, concluding a standard contract, and passing PIP Certification.[64]

When applying the above exemptions based on specific business scenarios, enterprises should pay special attention to the prerequisite of "indeed necessary". Simply being related to the business scenario, but not constituting a necessity for the performance of a contract, the implementation of human resources management, or responding to an emergency, does not meet the requirement of "indeed necessary".

Personal information "in transit": If a data processor transmits personal information collected and generated overseas to the territory for processing and then provides it overseas, and no domestic personal information or important data is introduced during the processing, it is exempt from declaring a security assessment, concluding a standard contract, and passing PIP Certification.[65] For example, a Chinese subsidiary of a multinational enterprise group that provides data processing services for its overseas affiliates, and no domestic personal information or important data is introduced in the process, will benefit from this exemption.

Data outside the negative list of a free trade zone: A free trade zone may, under the framework of the national data classification and grading protection system, formulate its own list of data that needs to be included in the management scope of security

[64] Article 4 of the Provisions on Cross-Border Data Flows

[65] Article 4 of the *Provisions on Cross-Border Data Flows*

assessment, standard contract, and PIP Certification (referred to as the *"negative list"*). If a data processor in the zone provides data outside the negative list overseas, it may be exempt from declaring a security assessment, concluding a standard contract, and passing PIP Certification.[66] As of August 2025, the free trade zones (ports) of Tianjin, Beijing, Shanghai, Hainan, Zhejiang, Guangxi, and Jiangsu have successively issued their 2024 or 2025 version of the negative list, involving industries such as automobiles, medicine/medical, retail, civil aviation, artificial intelligence, reinsurance, international shipping, catering and accommodation, deep sea, aerospace, seed industry, tourism, duty-free retail, e-commerce (business-to-business), clearing and settlement, geographic information and meteorological services, enterprise credit information services, live-streaming cross-border e-commerce, and overseas audio and video production and dissemination.

It needs to be particularly emphasized that the above new regulations only exempt the three compliance paths of security assessment, standard contract, and PIP Certification, but do not exempt the legality requirements for data export (obtaining separate consent or having other legal bases), personal information protection impact assessment, or important data risk assessment.

II. Requirements for Data Processors in Outbound Data Flow

Within our country, the subject of data export may be a data processor, a trustee data processor, or it may involve multiple data processors and multiple trustee data processors jointly completing the data export activity. The specifics need to be further judged based on the data export scenario and whether the exporting subject has the right to independently determine the purpose of data processing. For the relevant requirements for data processors in outbound data flow, as described in the third part of this guide on subject compliance, they will not be repeated here.

III. Localization Data Storage Requirements

[66] Article 6 of the Provisions on Cross-Border Data Flows

Whether data processors or trustee data processors have an obligation to store data locally in China is also of great concern to the market.

Based on the importance of the information systems operated by the data processor and the industry in which it is located, it may be subject to different data localization storage requirements. From the perspective of rules generally applicable to all industries, Article 37 of the *Cybersecurity Law* stipulates that personal information and important data collected and generated by CIIOs during their operations in the People's Republic of China should be stored domestically. If it is indeed necessary to provide it overseas due to business needs, a security assessment should be conducted in accordance with the measures formulated by the national cyberspace administration in conjunction with the relevant departments of the State Council. Article 40 of the *PIPL* further clarifies that CIIOs and personal information processors that process personal information up to the amount specified by the national cyberspace administration should store the personal information collected and generated in the People's Republic of China domestically. If it is indeed necessary to provide it overseas, it should pass the security assessment organized by the national cyberspace administration.

Whether an enterprise is identified as a CIIO is key to determining whether it bears the obligation of data localization storage. Critical Information Infrastructure (hereinafter referred to as "CII") refers to important network facilities, information systems, etc., in important industries and fields such as public communication and information services, energy, transportation, water conservancy, finance, public services, e-government, and national defense science and industry, as well as others that, once damaged, lose their function, or have their data leaked, may seriously endanger national security, the national economy and people's livelihood, and the public interest.[67] The identification of CIIOs is the responsibility of the relevant competent and supervisory departments. The identification results will be notified to the relevant CIIOs and reported to the public security department of the State Council.[68] Once notified and identified as a CIIO, the

[67] Article 2 of the Critical Information Infrastructure Security Protection Regulations
[68] Article 10 of the Critical Information Infrastructure Security Protection Regulations

relevant enterprise should earnestly fulfill the obligation of data localization storage.

The Cyberspace Administration of China has not yet issued a quantitative threshold for the localization storage of personal information. In addition, industries such as finance, credit reporting, insurance, medical and health, and ride-hailing have also faced or are facing specific requirements for data localization storage or information system localization (some can be referred to in Chapter III, Section (VI)). It is worth noting that some industry regulations or normative documents promulgated before the *Cybersecurity Law* and the *PIPL* are undergoing adjustments to adapt to the superior laws, which also reduces the compliance burden of relevant enterprises.

For example, the *Notice of the People's Bank of China on Banking Financial Institutions Doing a Good Job in the Protection of Personal Financial Information*, issued in 2011, explicitly stipulated in Article 6 that the storage, processing, and analysis of personal financial information collected in China should be carried out in China. Unless otherwise provided by laws and regulations and the People's Bank of China, banking financial institutions shall not provide domestic personal financial information overseas. This notice was formally repealed by the People's Bank of China in 2023. The *Measures for the Data Security Management in the Business Fields of the People's Bank of China*, promulgated on May 1, 2025, and implemented from June 30, stipulates that if a data processor needs to provide data overseas for business or other needs, and the circumstances stipulated by the national cyberspace administration exist, it shall strictly abide by its relevant provisions. If laws, administrative regulations, and relevant provisions of the People's Bank of China have domestic storage requirements, the business data should also be stored in the People's Republic of China at the same time.[69]

It should be noted that the requirement of data localization storage is not equivalent to a ban on export. As mentioned above, if there is a real business need and the applicable prerequisites are met, relevant enterprises can still achieve compliant data

[69] Article 24 of the People's Bank of China Business Field Data Security Management Measures

export.

(i) Requirements for Overseas Recipients in Outbound Data Flow

Before receiving data from mainland China, local enterprises in Singapore should provide the Chinese exporting entity with information such as their industry, data demand content, and data purpose to ensure that the data demand is true, legal, and reasonable, and consistent with their industry and business needs.

Local enterprises in Singapore should use the data legally and compliantly in accordance with the purpose, scenario, and method of use stipulated in the cross-border data agreement signed with the Chinese enterprise, and in accordance with the purpose, scope, and restrictions of the authorized use of the data.

Content Restrictions on Outbound Data Flow

To comply with the requirements of our country's PIPL and other relevant laws and regulations, the content of cross-border data flow should not have the following circumstances:

- May endanger national security or public interest;
- May infringe on the legitimate rights and interests of third parties;
- Contains personal information obtained without legal authorization or data that can identify specific natural persons without the help of other data;
- Contains public data that has not been legally disclosed or opened;
- Other circumstances where circulation is prohibited by domestic and foreign laws and regulations.

For example, satellite and its carrier radio remote control and telemetry encoding and encryption technology algorithms, unmanned aerial vehicle flight control system algorithms, key algorithms of our country's geographic information systems, and topographic and geographic coordinate data with a scale > 1:1,000,000 in our country's

geographic information systems are all included in the *Catalogue of Technologies Prohibited or Restricted from Export by China*. According to Article 2 of the *Export Control Law of the People's Republic of China*, technical data and other data related to export-controlled items are also regarded as export-controlled items and are subject to the relevant provisions on export control.

The records of processing relevant personal information and important data should be kept for at least three years.

(ii) Compliance Requirements for Cross-Border Transfer of Important Data

Because important data involves core areas such as national security and public interest, its cross-border flow must follow stricter rules: data export must pass a security assessment, and important data collected and generated by CIIOs during their domestic operations should in principle be stored locally and matched with technical measures such as encryption and access control. In addition, for the export of important data by data processors in free trade zones that have issued negative lists, the compliance path needs to be adapted to dynamic policies such as the free trade zone's negative list.

(iii) Security Assessment for the Export of Important Data

According to the Measures for the Security Assessment of Data Exports and the New Regulations on Cross-Border Flow, a data processor that provides important data overseas should declare a data export security assessment to the national cyberspace administration through the local provincial cyberspace administration. The security assessment for the export of important data by an enterprise can be roughly divided into the following steps:

- Pre-declaration self-assessment of data export risks;[70]
- Conclusion of legal documents;

[70] See Article 5 of the Data Cross-border Security Assessment Measures

- Data export security assessment;[71]
- Fulfillment of obligations after completing the data export security assessment, including: the provision of important data overseas should be consistent with the purpose of data export and other conditions specified at the time of assessment, and an application to extend the validity period of the assessment result should be made before its expiration.

Given the frequent data exchanges between Chinese and Singaporean enterprises, if it is necessary to provide important data overseas, Singaporean enterprises can fulfill their various obligations according to the following guidelines:

Conclude legal documents with the overseas recipient, clearly stipulating the data security protection responsibilities and obligations. The legal documents must include the following content:

- The purpose, method, and scope of the data export, and the purpose and method of processing the data by the overseas recipient;
- The storage location and duration of the data overseas, and the measures for handling the exported data after the storage period expires, the agreed purpose is achieved, or the legal documents are terminated;
- Binding requirements for the overseas recipient to re-transfer the exported data to other organizations or individuals;
- The security measures that the overseas recipient should take when its actual control or business scope changes substantially, or when the data security protection policies, regulations, and network security environment of the country or region where it is located change, or when other force majeure situations occur, making it difficult to guarantee data security;
- Remedial measures, liability for breach of contract, and dispute resolution

[71] See Article 8 of the Data Cross-border Security Assessment Measures

methods for violating the data security protection obligations stipulated in the legal documents;

- Requirements for proper emergency response and ways and means for individuals to protect their personal information rights and interests when the exported data is tampered with, destroyed, leaked, lost, transferred, or illegally obtained or used.

Conduct a self-assessment of data export risks, with specific content including:

- The legality, propriety, and necessity of the purpose, scope, and method of the data export and the processing of data by the overseas recipient;
- The scale, scope, type, and sensitivity of the exported data, and the risks that the data export may bring to national security, public interest, and the legitimate rights and interests of individuals or organizations;
- The responsibilities and obligations undertaken by the overseas recipient, and whether the management and technical measures and capabilities to perform the responsibilities and obligations can guarantee the security of the exported data;
- The risks of the data being tampered with, destroyed, leaked, lost, transferred, or illegally obtained or used during and after the export, and whether the channels for protecting personal information rights and interests are smooth;
- Whether the data export-related contracts or other legally effective documents (hereinafter collectively referred to as legal documents) to be concluded with the overseas recipient have fully stipulated the data security protection responsibilities and obligations;
- Other matters that may affect the security of data export.

Submit the following materials to the provincial cyberspace administration to declare a data export security assessment:

No.	Material Name	Requirement	Remarks
1	Scanned copy of the Unified Social Credit Identifier certificate	Stamped with official seal	
2	Scanned copy of the legal representative's ID card	Stamped with official seal	
3	Scanned copy of the agent's ID card	Stamped with official seal	
4	Power of attorney from the agent	Stamped with official seal	
5	Data export security assessment declaration form		Fill in using Chinese
6	Copy of the data export-related contract or other legally effective documents to be concluded with the overseas recipient		Highlight, underline, or otherwise mark the relevant contract clauses for data export. The legal document shall be based on the Chinese version. If there is only a non-Chinese version, an accurate Chinese translation must be

			submitted at the same time.
7	Data export risk self-assessment report		Write in Chinese
8	Other relevant supporting materials		
(Source: Appendix 1 "Requirements for Data Export Security Assessment Declaration Materials" of the "Guidelines for Declaring Security Assessment of Data Exports (Third Edition)")			

When an enterprise applies for a data export security assessment, there are two ways to submit the application materials:

- Submit the application materials through the data export declaration system, the system website is https://sjcj.cac.gov.cn;
- If the enterprise is a critical information infrastructure operator or it is not suitable for other reasons to declare a data export security assessment through the data export declaration system, it shall adopt an offline method to declare the data export security assessment to the national cyberspace administration through the local provincial cyberspace administration. The declaration method is to deliver written application materials with an electronic version of the materials. The written application materials need to be bound into a volume.

Fulfill the obligations after completing the data export security assessment, including: the provision of important data overseas should be consistent with the purpose of data export and other conditions specified at the time of assessment, and an application to extend the validity period of the assessment result should be made before its expiration. If any of the following circumstances occur, the enterprise needs to re-

declare the assessment:

- The purpose, method, scope, or type of data provided overseas, or the purpose and method of processing data by the overseas recipient changes, affecting the security of the exported data, or extending the overseas storage period of personal information and important data;
- The data security protection policies and regulations and network security environment of the country or region where the overseas recipient is located change, as well as other force majeure situations, changes in the actual control of the data processor or overseas recipient, changes in the legal documents between the data processor and the overseas recipient, etc., affecting the security of the exported data;
- Other circumstances affecting the security of the exported data occur.

Article 6 of the New Regulations on Cross-Border Flow clearly stipulates that free trade zones can formulate their own data lists that need to be included in the data export security assessment (hereinafter referred to as the "negative list"). If the exported data belongs to the industries and fields listed in the negative list, but is not included in the negative list, the data processor registered in the free trade zone may be exempt from the data export security assessment. This provision is a major highlight of the New Regulations on Cross-Border Flow. When enterprises identify important data in related fields, they only need to check whether the data belongs to the important data specified in the list. If it does not, there is no need to conduct a data export security assessment.

As mentioned earlier, the Shanghai Free Trade Zone, the Beijing Free Trade Zone, the Tianjin Free trade Zone, and other free trade zones have all formulated their own negative lists within their respective free trade zones, which can provide reference and convenience for enterprises to identify important data and declare security assessments. Taking the Shanghai Free Trade Zone as an example, the negative list of this zone lists the negative lists of important data in two fields: the reinsurance field and the international shipping field, and details the scene name, data sub-category,

and basic characteristics and description of the data. Among them, the four data sub-categories under the personal insurance reinsurance scenario and the property insurance reinsurance scenario in the reinsurance field are all important data:

- Underwriting, claims, and other related data that may affect national security;
- Relevant data involving some sensitive and special units and their individuals;
- Relevant data that may have a serious impact on economic operation, social stability, etc., after being made public;
- Important data as assessed and determined by the competent (supervisory) department of the industry or field.

In other words, in the reinsurance field, data under the personal insurance reinsurance scenario and the property insurance reinsurance scenario that does not belong to the above four data sub-categories does not need to be identified as important data, and there is no need to apply for a security assessment when exporting the data.

(iv) Compliance Steps for Cross-Border Data Flow for Multinational Corporations

At present, China's data cross-border supervision system is composed of different laws, administrative regulations, departmental rules, local regulations, and standard specifications, building a three-dimensional framework of full-process supervision and precise exemption. In this section, we will provide step-by-step action guidelines based on the practice of cross-border data flow of multinational enterprises.

1. Data Export Scenarios

As mentioned earlier, China's data cross-border supervision reflects the characteristic of being commensurate with risks. Enterprises may be subject to different compliance requirements due to factors such as the importance of their information systems and data, the scale of data export, scenarios, and sensitivity. Therefore, the prerequisite for achieving compliant export is to sort out and inventory data export activities in order to identify the corresponding compliance obligations.

We recommend establishing a three-dimensional matrix of business scenarios–information systems–data types to clearly and intuitively reflect data export activities. Taking a certain automobile manufacturing enterprise as an example (the table below is only a simple example, the mapping table in practice is usually far more complex).

Business Scenario	**Information System / Whether identified as CII**	**Data Type / Whether it contains important data, sensitive personal information**	**Personal Information Subject Type / Whether consent for export has been obtained**	**Overseas Recipient and Location**
Global R&D	CAD collaboration platform / No	Vehicle test data (including geographic location) / No	N/A	German Headquarters
Supply Chain Management	ERP system / No	Supplier contact information / No	Supplier contact / Yes	Singapore Asia-Pacific Center
Customer Service	CRM system / No	Car owner identity information,	Individual car owner / Yes	US Cloud Service Provider

		maintenance records / Contains sensitive personal information		

2. Identification and Path of Data Export Compliance Responsibility

Based on the detailed information of the data export activities that have been sorted out, the enterprise should identify the applicable legal requirements, data export, and compliance responsibilities and paths. In this process, we recommend that enterprises check the compliance requirements in a certain order to accurately locate the applicable legal requirements and ensure that nothing is repeated or missed.

1. **Identify special data supervision requirements**: Does the exported data contain specially restricted data types such as human genetic resources information or data related to export-controlled items? What are the corresponding special supervision measures?
2. **Identify whether any information system is identified as CII**: If so, all non-exempt personal information export activities should be declared for security assessment. If there is no CII, the number of personal information subjects involved in non-exempt data export activities should be counted (note deduplication), and the applicable compliance path should be identified according to the quantitative threshold in the *New Regulations on Cross-Border Flow*.
3. **Identify whether important data export is involved**: Has the region and industry where the company is located announced an important data catalogue? If so, has the company completed the identification and declaration of important data? Does the exported data contain important data?

4. **Identify the compliance path for personal information export**:

   - Identify applicable exemption conditions for compliance paths—identify the application of the following exemption conditions one by one and keep written records of the basis for judgment.

     - Is there a situation of personal information "in transit" processing? For example, a Chinese subsidiary provides data processing services for overseas data for an overseas affiliated company.

     - Is there a situation where it is indeed necessary to provide personal information overseas for the purpose of concluding or performing a contract to which the individual is a party? Note that this exemption is only applicable to specific business fields, including cross-border shopping (such as cross-border e-commerce), cross-border delivery, cross-border remittance, cross-border payment, cross-border account opening (such as cross-border wealth management connect account opening in the Guangdong-Hong Kong-Macao Greater Bay Area), flight and hotel reservations, visa processing, and examination services.

     - Is there a situation where it is indeed necessary to provide employee personal information overseas for the implementation of human resources management? Does the company already have lawfully formulated labor rules and regulations?

     - Is there a situation where it is indeed necessary to provide personal information overseas to protect the life, health, and property safety of natural persons in an emergency?

     - Is the company established in a free trade zone? Has the free trade zone issued a negative list for data export, and is it applicable to the company's data export scenario?

Quantity	**Over 1 million general personal information**	**100,000 to 1 million general personal information**	**Less than 100,000 general personal information**	**No general personal information**
Over 10,000 sensitive personal information	Security Assessment	Security Assessment	Security Assessment	Security Assessment
Less than 10,000 sensitive personal information	Security Assessment	Standard Contract or PIP Certification	Standard Contract or PIP Certification	Standard Contract or PIP Certification
No sensitive personal information	Security Assessment	Standard Contract or PIP Certification	Exempt	Exempt
(Note: Enterprises in free trade zones are subject to the provisions in the issued negative lists)				

3. Internal Assessment and Preparation of Compliance Legal Documents

After identifying the applicable compliance path, the company should start to carry out internal assessment and prepare relevant legal documents, including the standard contract or other agreements with the overseas recipient, assessment reports, declaration forms, and supporting documents to prove the company's data protection

capabilities.

For the high-frequency scenario of intra-group data sharing common in multinational enterprises, full consideration should also be given to:

- If the human resources management exemption is applicable, supporting materials such as labor contracts and collective contracts need to be retained, and the scope of transmission is limited to the information necessary for "implementing cross-border human resources management in accordance with lawfully formulated labor rules and regulations and lawfully concluded collective contracts."
- If multiple domestic subsidiaries belong to the same group company and the data export business scenarios are similar, the group company can act as the declaring entity to declare the data export security assessment or file the personal information export standard contract on a consolidated basis to improve the efficiency of export compliance work.
- The national cyberspace administration is promoting the introduction of relevant management measures for personal information export protection certification to guide third-party professional certification bodies to certify personal information export activities. If either the domestic enterprise or the overseas recipient passes the certification, the enterprise can carry out personal information export activities within the scope of the certification. For multinational groups that have passed the certification, they can carry out personal information export activities within the group without having to separately sign personal information export standard contracts with subsidiaries in various countries.

The preparation of internal assessment and compliance legal documents often involves coordination across departments and entities. It is recommended that the enterprise internally clarifies the lead and supporting departments and plans a clear work cycle to avoid adverse effects on the business due to delays in completing compliance actions.

For compliance gaps found during the internal assessment process, rectification should be arranged as soon as possible. Common risk points include:

- The privacy policy does not cover all personal information subjects involved in data export activities. For example, the company only has a privacy policy for customers, which cannot cover employees, job applicants, suppliers, etc.
- The privacy policy has not been updated for a long time, and its specific content is inconsistent with the actual data export activities. For example, with business development, the company's data export activities have added data types and overseas recipients compared to two years ago, but the privacy policy still uses the version from two years ago.
- No separate consent from individuals has been obtained and there is no other applicable legal basis. For example, only the consent of the personal data subject for general data processing activities has been obtained, but no separate consent for data export has been obtained through ticking, pop-up windows, etc.
- Data access rights are set too broadly, leading to unnecessary export activities. For example, after the data of the Chinese subsidiary is uploaded to the global system, the corresponding business departments of all overseas affiliates can view the data, but in fact, only the overseas headquarters and specific directly responsible personnel have the need and necessity to view the data.

Objectively speaking, very few enterprises can get a "perfect score" in the internal assessment. Enterprises should face up to the problems found in the assessment, truthfully disclose compliance gaps, rectification measures, and results in the assessment report, and ensure that they submit true, complete, and accurate information to regulatory authorities and certification bodies in the process of implementing the compliance path.

For high-frequency data export scenarios of multinational enterprises, such as the internal transmission of employee personal information within a multinational enterprise group, if the human resources management exemption is applicable,

supporting materials such as labor contracts and collective contracts need to be retained, and the scope of transmission is limited to data directly related to the employee's performance of duties (such as salary, position information). For multinational enterprises, special attention should also be paid to details such as terminology when converting internal assessment documents into declaration and filing materials. For example, when describing security measures, internal data protection mechanisms, data types and fields, etc., try to use the standard terminology in Chinese laws, regulations, standards, and guidelines. When translating foreign language documents, ensure accuracy to avoid delays in subsequent regulatory review due to such details. For internal organizational structure or business information, internal system documents, etc., that are not highly relevant to data export activities, it is also necessary to pay attention to screening and confidential handling in the declaration and filing materials.

Declaration and Filing

At present, both the national and provincial cyberspace administrations have opened consultation channels for data export security assessment declarations and personal information export standard contract filings. We recommend that enterprises actively engage in pre-communication with the cyberspace administration when preparing for declaration and filing, and fully seek regulatory opinions on difficult or uncertain issues to improve the pass rate and efficiency of formal declaration and filing.

When submitting declaration and filing materials, it should be ensured that the requirements regarding the form and content of the materials are strictly met. Timely response and close cooperation should be given to the material correction requirements proposed by the cyberspace administration.

In addition, if multiple domestic subsidiaries belong to the same group company and the data export business scenarios are similar, the group company can act as the declaring entity to declare the data export security assessment or file the personal information export standard contract on a consolidated basis to improve the efficiency

of data export work. In addition, the Cyberspace Administration of China is promoting the introduction of relevant management measures for personal information export protection certification to guide third-party professional certification bodies to certify personal information export activities. If either the domestic enterprise or the overseas recipient passes the certification, the enterprise can carry out personal information export activities within the scope of the certification. For multinational groups that have passed the certification, they can carry out personal information export activities within the group without having to separately sign personal information export standard contracts with subsidiaries in various countries.

Internal Compliance Management After Export

The cross-border data flow of multinational enterprises is in a state of dynamic change. Expanding new businesses, new markets, and introducing new suppliers may all cause substantial changes in data export activities. At the same time, changes in policies and regulations in different countries and regions may also have an impact on cross-border data flow.

Completing the gap rectification and going through the compliance path only means that the data export compliance management has achieved phased results, but it does not mean that one can rest easy from now on. We recommend that enterprises implement a series of "post-event management" measures to ensure continuous compliance. Matters that should be paid attention to include but are not limited to:

- **Changes in applicable compliance obligations**: It is recommended to pay close attention to the important data catalogues, negative lists, etc., subsequently issued by various regions and departments, and assess the possible impact on the company's business.
- **Validity period of the compliance path**: Pay attention to the validity period of the security assessment results and PIP certification, as well as the term of the standard contract, set up expiration reminders, and timely arrange for applications for extension of validity, re-declaration, conclusion and filing, certification, and

other work.

- **Major changes in export activities caused by business development**: For example, adding new overseas recipients or the original recipient changing the purpose and method of processing data, adding new types of data export, adding new destination countries or regions for data export, extending the overseas storage period, and a significant increase in the number of individuals involved in data export activities. Enterprises should assess the impact of these changes and assess whether it is necessary to re-declare a security assessment, or to supplement or re-conclude the standard contract.
- **Changes in overseas data protection policies and regulations**: It is necessary to timely assess whether such changes may affect data security or the rights and interests of personal information subjects.
- **Applicable periodic reporting requirements**: For example, the annual risk assessment and submission requirements for important data processors, the annual data security risk assessment report requirements for banking and insurance institutions under the *Measures for the Data Security Management of Banking and Insurance Institutions*, and the annual data security management situation submission requirements for automotive data processors under the *Provisions on the Management of Automotive Data Security (for Trial Implementation)*.
- **Continuous implementation of data export security guarantee mechanisms**: For example, clearly defining the data protection responsibilities of the overseas recipient in the data export contract; providing a "data export circuit breaker mechanism", such as emergency recall measures when the overseas recipient violates the agreement; and providing remedies for data subjects when a personal information leakage risk occurs.

The compliance management of cross-border data flow is both a necessary requirement for the global operation of enterprises and a basic capability for

participating in international digital economy cooperation. The current supervision system built by China both strictly adheres to the bottom line of data security and improves policy adaptability through institutional innovations such as the negative list of free trade zones. Enterprises need to deeply understand this supervision logic: on the premise of ensuring national security and the rights and interests of data subjects, promote the orderly flow and value release of data elements. When Singaporean enterprises invested or newly established in our country, or cooperative enterprises, carry out the cross-border flow activities of the above-mentioned subject data, they should pay attention to referring to the above-mentioned flow compliance requirements to complete the compliance work.

(v) Penalties for Non-compliant Data Export

According to Article 66 of the *Cybersecurity Law*, if a CIIO violates the regulations by storing network data overseas or providing network data overseas, the relevant competent department shall order it to make corrections, give a warning, confiscate the illegal gains, and impose a fine of not less than 50,000 yuan and not more than 500,000 yuan, and may order it to suspend relevant business, stop business for rectification, close the website, or revoke the relevant business license or business license; a fine of not less than 10,000 yuan and not more than 100,000 yuan shall be imposed on the directly responsible person in charge and other directly responsible personnel.

According to Article 46 of the *Data Security Law*, if important data is provided overseas in violation of regulations, the relevant competent department shall order correction, give a warning, and may impose a fine of not less than 100,000 yuan and not more than 1 million yuan. A fine of not less than 10,000 yuan and not more than 100,000 yuan may be imposed on the directly responsible person in charge and other directly responsible personnel. If the circumstances are serious, a fine of not less than 1 million yuan and not more than 10 million yuan shall be imposed, and it may be ordered to suspend relevant business, stop business for rectification, or revoke the relevant business license or business license. A fine of not less than 100,000 yuan and not

more than 1 million yuan shall be imposed on the directly responsible person in charge and other directly responsible personnel.

According to Article 66 of the *PIPL*, if personal information is processed in violation of regulations, or if the prescribed personal information protection obligations are not fulfilled when processing personal information, it may face an order to make corrections, a warning, confiscation of illegal gains, and for applications that illegally process personal information, an order to suspend or terminate the provision of services. If it refuses to make corrections, a fine of not more than 1 million yuan shall be imposed. A fine of not less than 10,000 yuan and not more than 100,000 yuan shall be imposed on the directly responsible person in charge and other directly responsible personnel. For the aforementioned illegal acts, a fine of not more than 50 million yuan or not more than 5% of the previous year's turnover may also be imposed, and it may be ordered to suspend relevant business or stop business for rectification, and the relevant competent department shall be notified to revoke the relevant business license or business license. A fine of not less than 100,000 yuan and not more than 1 million yuan shall be imposed on the directly responsible person in charge and other directly responsible personnel, and it may be decided to prohibit them from serving as directors, supervisors, senior managers, and personal information protection officers of relevant enterprises for a certain period of time.

The *Measures for the Security Assessment of Data Exports* does not propose additional penalties, but stipulates that violations of these measures shall be dealt with in accordance with the *Cybersecurity Law*, *Data Security Law*, *PIPL*, and other laws and regulations. If a crime is constituted, criminal responsibility shall be pursued in accordance with the law.

(vi) Dispute Resolution for Data Export

Article 9(4) of the Standard Contract for the Export of Personal Information (hereinafter referred to as the "Standard Contract") attached to the Measures for the Standard Contract for the Export of Personal Information stipulates that disputes arising between

the personal information processor and the overseas recipient due to the "Standard Contract" can be resolved through arbitration or litigation.

First, if arbitration is chosen, the two parties can only choose a specific arbitration institution in mainland China (such as the China International Economic and Trade Arbitration Commission, the China Maritime Arbitration Commission, the Beijing International Arbitration Center, or the Shanghai International Arbitration Center) or an arbitration institution in a member state/region of the *Convention on the Recognition and Enforcement of Foreign Arbitral Awards* (*New York Convention*). It is worth noting that at present, the Shanghai Arbitration Commission and the Wuhan Arbitration Commission in our country have respectively issued the *Guidelines for Data Arbitration* and the *Arbitration Rules for Data Disputes*. It is recommended that if the Wuhan Arbitration Commission is chosen as the dispute resolution institution, the *Arbitration Rules for Data Disputes* can also be included in the dispute resolution agreement[72]. Furthermore, the *"Standard Contract"* excludes the application of cross-type arbitration clauses (i.e., jurisdiction of the arbitration institution where the arbitration applicant or respondent is located) and hybrid arbitration clauses (i.e., the arbitration institution conducts arbitration according to arbitration rules that do not belong to that arbitration institution), which further compresses the negotiation and consultation space for personal information processors and overseas recipients.

In addition, the location of the arbitration institution does not affect the choice of the place of arbitration (i.e., "arbitration in XX"). Even if an arbitration institution in mainland China is agreed upon, the place of arbitration can be agreed to be overseas. The choice of the place of arbitration will affect the governing law of the arbitration procedure and the nationality of the arbitral award.

---

[72] Article 4 of the Wuhan Arbitration Commission (Wuhan International Arbitration Center) Data Dispute Arbitration Rules: (1) For data dispute cases accepted by this Commission, if the parties agree to apply these rules, these rules shall apply. (2) If these rules are inconsistent with the Wuhan Arbitration Commission (Wuhan International Arbitration Center) Arbitration Rules, these rules shall apply; if these rules do not provide for it, the Wuhan Arbitration Commission (Wuhan International Arbitration Center) Arbitration Rules shall apply. (3) If the parties agree to modify certain contents of these rules, their agreement shall prevail, unless the agreement cannot be implemented or conflicts with mandatory legal provisions.

Second, if litigation is chosen, the two parties can only agree that a court with jurisdiction in mainland China has jurisdiction, and cannot choose a foreign court.

Considering the institutional obstacles in the recognition/enforcement of judgments of mainland Chinese courts outside the territory, it is recommended to choose arbitration, so that the recognition and enforcement of future arbitral awards will be guaranteed by the institutional framework of the New York Convention.

Chapter VI: Good Compliance Practice Guidelines※

Case 1: Personal Information Protection Management System of a Foreign-Invested Enterprise

In global operations, foreign-invested enterprises face differences and challenges from privacy regulations in various countries and regions. When integrating global privacy systems with the requirements of China's *PIPL*, it is crucial to formulate a set of scientific, reasonable, and feasible local Standard Operating Procedures (SOPs) for personal information protection in China.

The privacy protection team of a global enterprise first conducted an in-depth analysis of the company's global privacy system and China's relevant laws and regulations on personal information protection. They carefully sorted out the requirements at each stage—collection, storage, use, processing, transmission, provision, public disclosure, and deletion of personal information—to identify similarities and differences. For example, the global privacy system focuses more on privacy protection norms at the principle level, while China's *PIPL* has detailed regulations on the content of consent notification and the methods for obtaining consent. Through precise benchmarking, the content that needed to be prioritized for improvement and strengthening in the SOP was clarified, ensuring it not only conforms to the globally unified privacy management framework but also fully meets the requirements of Chinese law.

After clarifying the specific requirements, the company's privacy protection team built the SOP framework, including its purpose, scope of application, definitions, roles and responsibilities, basic principles, full lifecycle compliance requirements, training requirements, special process requirements, and monitoring and audit processes. Specifically, the special process requirements include App compliance processes, data export processes, and personal information security incident response processes. For

---

※ Chapter authors:
Wu Han, Partner, Compliance Department at King & Wood Mallesons **Yao Minlv**, Lawyer at King & Wood Mallesons.
Maggie Meng and Lin Yi of Beijing Global Law Office also contributed.

instance, for special processes like the App compliance guide, the company formed a professional App compliance working group. During the App functional requirement stage, the privacy protection team would deeply discuss the specific personal information needs with the business and IT teams. For example, when the business needed to develop a health monitoring App, the privacy protection team would discuss the necessity of collecting user health data field by field with the business team and how to obtain user consent in the most reasonable way. The IT team would provide suggestions from the perspective of implementation feasibility. Before the App function went live, the privacy protection team would conduct multiple rounds of real-world testing, simulating various usage scenarios to check whether the personal information processing activities were legal, proper, and necessary. For example, in the user registration process, they would check for the presence of separate consent and whether the notification content met the relevant requirements of the *PIPL*.

After the SOP was formulated, to ensure that all employees understood and executed it, the company carried out comprehensive training and publicity activities. It organized offline centralized training, inviting internal compliance personnel and external experts to give lectures. At the same time, it continuously promoted the importance of personal information protection and the key points of the SOP through internal emails, bulletin boards, and other channels. In addition, the company would regularly review the implementation of the SOP. Through internal audits and other methods, it checked the compliance of various departments in the process of personal information processing. Problems found were promptly rectified, and the review results were linked to employee evaluations to strengthen the execution of the system.

Case 2: Data Export Compliance Management Rules for a Foreign-Invested Enterprise

Regarding the practical experience of data export compliance management in foreign-invested enterprises, by constructing a standardized, full-process data export compliance management system that is closely aligned with the data export regulatory process, a comprehensive, closed-loop assessment and supervision process covering

pre-event, in-event, and post-event stages is formed. This ensures that data export compliance obligations are effectively implemented in every department, every business, every system, and for every employee. Specifically:

First, strengthen data export compliance obligations and consolidate primary responsibility. The company deeply understands that employee compliance awareness is the first line of defense for data export compliance. Therefore, it vigorously strengthens daily training and publicity for data export compliance work. It has expanded from a personal information protection promotion day to a promotion week and a promotion season, using novel training methods such as games, videos, and comics, combined with a full-process construction of knowledge-based education and assessment, interpretation of process specifications, and learning and assessment rewards. This fully mobilizes employees' enthusiasm for participating in training, transforming from passive knowledge infusion to active improvement of compliance awareness and capabilities, helping employees establish a good concept of data export compliance.

Second, form a cross-departmental data export compliance working group. The company has integrated resources from multiple departments to establish a data export management committee that spans compliance, security, IT, business, legal, and other departments. The committee members have rich professional knowledge, covering multiple fields such as personal information protection assessment and data security assessment. In daily work, the compliance team takes the lead in the main work of data export compliance, ensuring that all business activities comply with regulatory requirements. When encountering complex export compliance assessments, it fully integrates internal and external resource advantages, such as inviting external experts to provide professional opinions and exchanging experiences with other enterprises in the industry to ensure the accuracy and authority of the assessment results.

Third, integrate the company's privacy impact assessment and security risk assessment processes. At the data export demand stage, it is clearly required that the

demanding party must carry out an internal data export risk self-assessment, covering both privacy and security assessments. The privacy assessment focuses on the impact of data export on the rights and interests of personal information subjects, while the security assessment focuses on the security guarantee measures during the data transmission process. Only after passing a strict internal assessment and confirming that the risks are controllable can the relevant work of data export be further promoted, controlling data security risks from the source.

Fourth, carry out fine-grained management of data export scenarios, building data export scenarios from multiple dimensions such as business model, export purpose, data type, and data processor. Based on factors such as the risk level, business importance, and industry prevalence of different data export scenarios, targeted compliance plans are formulated. For example, for exports involving human genetic resources information, considering its sensitivity and importance, a more stringent data export plan is formulated. For employee data export, after judging whether it falls under the situation of "indeed necessary to provide employee personal information overseas for the implementation of cross-border human resources management in accordance with lawfully formulated labor rules and regulations and lawfully concluded collective contracts" based on the relevant conditions of the *New Regulations on Cross-Border Flow*, a simplified plan is adopted to achieve a compliance balance. Tools are used to provide a systematic and structured view of the data export scenario system, enabling management to clearly understand the overall situation of the company's data export and providing a complete and unified management perspective and a powerful handle for the company's data export management.

Fifth, establish a long-term supervision and management process for data export. For data export activities that have passed the data export security assessment or completed the personal information export standard contract filing, a dedicated tracking form is used to record key information such as the scale, fields, and recipients of the data export, achieving tracking of the export activities. At the same time, internal audits are conducted regularly to comprehensively review data export activities to

ensure that compliance requirements are continuously implemented. Once a statutory change occurs, such as an increase in data types, exceeding the expected export scale, a change in the purpose of personal information processing, or a change in the data security protection policies and regulations and network security environment of the country or region where the overseas recipient is located, the data export security assessment is promptly re-declared or the personal information export standard contract filing is completed again, according to the risk level of the change.

Case 3: Construction of a Personal Information Protection Impact Assessment System for a Foreign-Invested Enterprise

In the context of globalized operations, data compliance is a key element for the stable development of foreign-invested enterprises. From a professional legal compliance perspective, foreign-invested enterprises are generally committed to building a unified personal information protection standard and policy framework on a global scale. The core of this system lies in implementing the principles of personal information impact minimization and purpose limitation, as well as effectively protecting the rights of data subjects.

Typically, when foreign-invested enterprises conduct business in China, they will closely integrate with the localized needs of the Chinese market and make detailed adjustments and improvements to the globally unified standards. For example, in view of the separate consent requirement for sensitive personal information in our country's *PIPL*, enterprises will, in conjunction with China's data classification and grading requirements, formulate applicable internal enterprise classification standards and processing procedures. In this way, they not only meet global compliance requirements but also effectively fulfill our country's local legal obligations. This model of deeply integrating global unified standards with localization, with the *PIPL* at its core while also referencing internationally accepted standards such as the EU's *General Data Protection Regulation*, ensures the consistency of the enterprise's data processing activities on a global scale and its compliance in the Chinese market, effectively avoiding legal risks.

At the specific operational level, the enterprise conducts comprehensive and in-depth prior assessments of personal information processing activities in its external business and daily operations. The enterprise integrates the concept of privacy by design throughout the entire lifecycle of products and services, considering privacy protection from the planning stage. During the development process, privacy tools are used to formulate a "Personal Information Impact Assessment Checklist" in a Q&A format. Through a detailed analysis of the feedback from the checklist, and by comprehensively using manual and automated means, potential risks are accurately identified, effectively improving the standardization, judgment accuracy, and overall efficiency of the security impact assessment. In special usage scenarios involving sensitive personal information such as face recognition, location tracking, and specific identities, a professional assessment of the sensitivity of the personal information is conducted in advance, the personal information is classified and graded, and response measures are formulated in advance to reduce risks.

The enterprise relies on its global multi-level personal information protection organizational structure to clarify the responsibilities and authorities at each level and to coordinate personal information protection work on a global scale. Each business department has a dedicated data protection liaison responsible for personal information protection work in daily business. The data protection liaison not only ensures that business processes comply with compliance requirements but also needs to promptly report problems and make suggestions to the group's privacy compliance office and management, thereby achieving standardized assessment and normalized operation of the entire process of personal information from collection, storage, use, and sharing to deletion.

It is also worth mentioning that the enterprise regards the security assessment system for personal information processing activities as a dynamic development and continuous improvement process. It attaches great importance to regularly reviewing and optimizing the assessment system, and timely adjusting the assessment standards and operating procedures according to the updates of laws and regulations,

the actual needs of business development, and the continuous advancement of technology, so that the enterprise's data compliance work can always adapt to the changes in the internal and external environment and maintain a leading position in the ever-changing legal and business environment.

Case 4: A Foreign-Invested Enterprise's Compliance Self-Inspection Strategy for Personal Information Processing Activities in Business Operations

For foreign-invested enterprises processing personal information, formulating an effective data compliance self-inspection strategy and plan is not only a basic prerequisite for their legal operation but also the key to protecting personal information security and the long-term development of the enterprise. Therefore, some foreign-invested enterprises have currently built a self-inspection system that runs through the entire lifecycle of personal information processing.

Specifically, according to the process of personal information processing, in the collection stage, they strictly review whether the collection purpose is clear and reasonable, whether the collection method is legal and open, and whether the collection scope adheres to the principle of minimum necessity. Taking the basic "user registration" process in external business as an example, only information directly related to the provision of services, such as name and contact information, is collected, and excessive collection is resolutely prohibited, ensuring the compliance of personal information from the source. In the storage stage, they focus on assessing the security of data storage and formulate inspection plans on whether technical means such as encryption and access control are adopted to prevent data leakage and illegal access. For potentially sensitive personal information such as ID card numbers and bank card numbers, high-strength encryption algorithms are used to ensure the confidentiality and integrity of the data during storage. In the use stage, they strictly verify whether data use is within the scope of authorization to prevent unauthorized sharing, transfer, or abuse. If data is provided to third-party partners, the enterprise will obtain the user's explicit consent in advance and sign a detailed data processing agreement to clarify

the rights and obligations of both parties, ensuring the compliance and security of data flow.

While ensuring the above self-inspection process, the company will simultaneously formulate a self-inspection plan and regularly conduct comprehensive data compliance audits, such as conducting at least one internal audit annually based on the overall business situation, to ensure that all data processing activities strictly follow national laws and regulations and the enterprise's internal rules and regulations. It matches this with a cross-departmental professional self-inspection team, with members from legal, information security, data management, and other different business lines. They examine the legality of data processing activities from different perspectives, detect the security and stability of data systems, and re-verify the accuracy, completeness, and consistency of data. Through multi-departmental collaboration, they achieve a comprehensive investigation and effective control of data compliance risks.

In addition, during the self-inspection process, the company also simultaneously establishes its own risk warning mechanism, for example, by using advanced technical tools to improve the efficiency and accuracy of data compliance self-inspection. For example, by using data discovery tools to automatically identify various types of personal information stored in the system, count the type, quantity, and distribution of data, and quickly locate potential compliance risk points. This allows for the timely discovery and identification of potential data security hazards and compliance risks. Once a warning is triggered, an emergency response procedure is immediately activated, and relevant departments are notified to take effective measures to reduce risk losses. It implements a normalized self-inspection mechanism and uses technical means to empower self-inspection work to establish a closed loop of risk warning and rectification.

Case 5: A Foreign-Invested Enterprise's Compliance Management Plan for Internal Employee Personal Information

In the globalized business environment, foreign-invested enterprises play an important

role in the international market with their extensive business layout. However, their unique operating structure also brings many complex challenges to the protection of employee personal information, which far exceed those faced by ordinary domestic enterprises. Many foreign-invested enterprises have a large number of branches around the world, a relatively large number of employees, and are involved in business activities such as global employee recruitment, personal performance evaluation, salary plan design, and personal resume management. These activities cover the entire lifecycle of employee management (recruitment, onboarding, training, salary and performance management, and departure), which contains a large amount of personal information and even sensitive personal information, making the information processing work relatively complex.

In the face of these challenges, a certain foreign-invested enterprise has adopted a series of strict and detailed measures. In the human resources management process, it has formulated targeted informed consent forms for the characteristics of different stages. In the recruitment and onboarding stages, the enterprise strictly defines the boundaries of personal information processing and explains in plain language to employees the purpose, method, scope, and duration of collecting, using, storing, and sharing their personal information at each stage. For example, when collecting employee onboarding materials, the informed consent form will clearly list the specific contents required, such as academic certificates, ID card copies, and emergency contact information, to ensure that employees fully understand the purpose of providing this information. On this basis, the employee's consent or separate consent is obtained (refer to the requirements for "separate consent" in the "Personal Information" section of Chapter III of this guide).

To ensure that employees fully understand and sign the informed consent form, the enterprise makes full use of various online and offline channels. For example, online, a special informed consent signing module is set up in the employee onboarding system. Employees must read and click to agree before they can continue to complete the subsequent onboarding process. Offline, during new employee training,

professional personnel are arranged to explain the content of the informed consent form and guide employees to sign the paper documents on site. In addition, once the enterprise makes a major adjustment to the way it processes personal information, it will promptly update the informed consent form and seek the employee's consent again, thereby fully protecting the employee's right to know and right to choose.

In the field of employee benefits, the enterprise cooperates frequently with various suppliers such as insurance providers, health management service providers, and e-commerce service providers. To effectively ensure the security of employee personal information in the interaction with suppliers, the enterprise will sign a detailed data security protection agreement with the supplier. The agreement will accurately define the scope and purpose of the supplier's use of employee personal information, strictly limiting them to using the information only for the specific business required to provide services. For example, when cooperating with an insurance provider, it is only allowed to use employees' basic information, health status, and other personal information within the scope of business such as calculating employee insurance premiums and processing claims. At the same time, suppliers are required to adopt data security protection measures that are as strict as those of the enterprise, including encrypted storage, access control, and regular security audits. The agreement also makes clear provisions on the liabilities and compensation for personal information leakage. If a supplier has a data leakage incident, it must immediately notify the enterprise and bear the corresponding legal responsibility and compensation for losses. The enterprise will also regularly inspect and evaluate the data security status of the supplier. Once a problem is found, the supplier is immediately required to make corrections, thereby comprehensively ensuring the security of employee personal information.

Case 6: A Foreign-Invested Enterprise's Emergency Response System for Network Data Security Incidents

Foreign-invested enterprises typically rely on a globally unified Security Operation Center (SOC) to be responsible for 24/7 detection of all activities on endpoints, servers, databases, network applications, websites, and other systems, and for the prevention,

analysis, and response to network and data security incidents. China's *Cybersecurity Law* , *Data Security Law*, and *PIPL* all require enterprises to formulate emergency response plans for security incidents, strengthen risk monitoring, and have proposed the obligation to report to relevant regulatory athorities. This undoubtedly brings many challenges to the coordination and communication between the global security operation center and the local team in China.

To effectively respond to these challenges, a multinational company has actively built a network data security incident emergency response process. This process covers key contents such as internal responsibilities, incident discovery, incident information collection, internal incident notification process, incident handling process, incident grading standards, and incident reporting requirements, and is equipped with a series of practical templates, such as the "Network Security Incident Information Report Form" and the "Personal Information Subject Notification Form".

In clarifying internal responsibilities, the company focuses on clarifying the key responsibilities of the data protection officer and information security officer in China in network data security incidents. The data protection officer mainly proceeds from the perspective of personal information protection, supervises the compliance of data processing activities throughout the entire process, and ensures that the rights and interests of personal information subjects can be effectively protected when a security incident occurs, for example, by sending notifications to the affected personal information subjects in a timely and accurate manner, informing them of the details of the incident and the possible impact. The information security officer focuses on the technical level, quickly judges the technical risk points after an incident occurs, and resolutely takes effective response measures, and assists the data protection officer in collecting relevant technical background and materials.

In terms of incident grading standards, the company fully refers to China's current laws and regulations and designs grading standards from both qualitative and quantitative dimensions. Qualitatively, it considers the impact of the incident on national security, social order, economic construction, and public interest. Quantitatively, it evaluates

based on indicators such as the amount of data leaked and the scale of affected users. At the same time, it fully combines the particularity of its own industry, giving extra risk consideration and a higher security level rating to information involving important sensitive data (such as medical and health data, financial transaction data) and key protected populations (such as minors, the elderly).

The company is committed to building an efficient communication channel between the local team and the global security operation center and has formulated a special communication specification. This specification clarifies the detailed process and content requirements for reporting security incident information within the company. It sets different reporting time limits, levels, and specific requirements for security incidents of different risk levels. For example, for low-risk security incidents, the information security officer needs to briefly report the incident situation to the data governance committee by email within 8 hours of discovery. For high-risk security incidents, it must be reported urgently through dual channels of telephone and instant messaging tools within 15 minutes, followed by a detailed written report.

Finally, the company regularly organizes emergency drills, simulating different types and levels of security incidents, to test the feasibility and effectiveness of the emergency response plan and to discover potential problems in a timely manner. The drills comprehensively involve the local team, the global security operation center, and other relevant departments such as legal and public relations. For example, in one drill, it was found that there was incomplete information transmission in the communication link, which led to deviations in the execution of response measures. In response to such problems, the emergency response plan and communication process were quickly optimized to further clarify the format, key points of content, and confirmation mechanism for information transmission, ensuring the accurate and complete transmission of information.

Data Protection and Compliance Guidelines: Frequently Asked Questions※[73]

1. What are the contact details for data export consultation and reporting?

A: (1) Data export security assessment declaration: 010-55627135, sjcj@cac.gov.cn; (2) Personal information export standard contract filing: 010-55627565, bzht@cac.gov.cn; (3) Personal information protection certification application: 010-82261100, data@isccc.gov.cn

For contact details (office address, telephone number) of provincial-level cyberspace administrations that handle data export security assessment declarations and personal information export standard contract filings, please refer to the official websites and WeChat public accounts of the internet information offices of each province, autonomous region, municipality, and the Xinjiang Production and Construction Corps, as well as the data governance section of the official website of the Cyberspace Administration of China (https://www.cac.gov.cn).

2. When a personal information processor in our country calculates the amount of personal information exported, should de-identified personal information in the data be considered personal information and included in the count?

A: Yes, it should. According to the definitions of anonymization and de-identification in Article 73 of the *PIPL,*[74] anonymization is the process whereby personal information is processed so that a specific natural person cannot be identified and the information cannot be restored. De-identification is the process whereby personal information is

---

[73] Chapter authors are **Wang Yi**, a partner at Beijing Global Law Office (Shenzhen);
Li Rui, a partner at Zhong Lun Law Firm;
Wu Han, a partner at King & Wood Mallesons in Beijing;
Liu Jiayi, a senior associate at Beijing Global Law Office (Shenzhen);
Pu Yuhan, a lawyer at Zhong Lun Law Firm;
Xu Chen, a former lawyer at Zhong Lun Law Firm; and
Yao Minlv, a lawyer at King & Wood Mallesons in Beijing.

[74] Article 73 of the Personal Information Protection Law: (3) De-identification refers to the process of processing personal information so that it cannot identify a specific natural person without the help of additional information. (4) Anonymization refers to the process of processing personal information so that it cannot identify a specific natural person and cannot be restored..

processed so that a specific natural person cannot be identified without the aid of additional information. The difference between anonymization and de-identification is that de-identified information can still identify a specific natural person with the help of other information, while anonymized information cannot be restored or re-identified to a specific natural person even with the help of other information. Therefore, in Article 4 of the *PIPL*, only anonymized information is excluded from the scope of personal information,[75] while de-identified information is still considered personal information.

3. What is the validity period of a data export security assessment result? Can an extension be applied for?

A: The *New Regulations on Cross-Border Flow* extend the validity period of a data export security assessment result from 2 years as stipulated in the *Measures for the Security Assessment of Data Exports* to 3 years, calculated from the date the assessment result is issued. At the same time, it adds a provision allowing data processors to apply for an extension of the validity period of the assessment result. When the validity period expires, and it is necessary to continue data export activities and no circumstances requiring a re-declaration of the data export security assessment have occurred, the data processor may, within 60 working days before the validity period expires, apply to the national cyberspace administration through the local provincial cyberspace administration to extend the validity period of the assessment result. With the approval of the national cyberspace administration, the validity period of the assessment result can be extended for 3 years.

4. Can the "Standard Contract for the Export of Personal Information" and its appendices be left blank? What matters can be agreed upon in the blank pages of Appendix II?

A: The main text of the "Standard Contract" and the content that should be filled in Appendix I should not be left blank. Appendix II can be filled in according to needs; if

[75] Article 4 of the Personal Information Protection Law: Personal information is all kinds of information recorded electronically or in other ways related to identified or identifiable natural persons, excluding anonymized information.

there are no special matters to be supplemented, it can be left blank. Appendix II of the "Standard Contract" can stipulate clauses that the two parties need to supplement outside the template of the "Standard Contract" but do not conflict with it. For example: the validity period of the "Standard Contract"; if it is used as a legal document for security assessment, it is also recommended to supplement, in accordance with the requirements of Article 9(4) of the *Assessment Measures*, the security measures that the overseas recipient should take when its actual control or business scope changes substantially, or when other force majeure situations occur that make it difficult to guarantee data security; clearly agree on the data law roles, data processing relationships, etc., of both parties; and, without affecting the assumption of external responsibility, agree on the internal allocation of responsibility between the two parties.

5. What is sensitive personal information?

A: Sensitive personal information is personal information that, once leaked or illegally used, is likely to cause harm to the personal dignity of a natural person or endanger their personal or property safety. This includes information such as biometrics, religious beliefs, specific identities, medical and health information, financial accounts, and location tracking, as well as the personal information of minors under the age of fourteen.

In practice, when an enterprise wants to determine whether the information it processes involves "sensitive personal information," it can make a comprehensive judgment based on the degree of impact of such information on the rights and interests of the data subject, while also referring to examples such as the table in the national standard GB/T 45574-2025 Data Security Technology - Security Requirements for Processing Sensitive Personal Information.

6. What is automated decision-making?

A: According to the PIPL, automated decision-making refers to the activity of automatically analyzing and evaluating an individual's behavioral habits, interests, hobbies, or economic, health, and credit status through computer programs, and

making decisions based on this analysis. Automated decision-making has the advantages of high accuracy and efficiency. Common application scenarios for automated decision-making include preliminary assessment for bank credit approval, personalized content recommendation on platforms, intelligent resume screening, and personalized pushing of commercial marketing information.

From an implementation perspective, automated decision-making usually includes two links:

- **Feature generation**, for example, building user profiles. Specifically, a personal information processor collects, aggregates, and analyzes specific personal information (such as age, gender, behavioral preferences, etc.) to analyze or predict the personal characteristics of a specific natural person in aspects such as occupation, economy, health, education, personal preferences, credit, and behavior, forming their personal characteristic model.
- **Making decisions using the results of feature generation**. The decision can be made entirely by a computer program based on the generated personal characteristic information, or it can be completed by a computer program assisting a human.

7. Do enterprises that process the personal information of fewer than 10 million people need to conduct a personal information protection compliance audit?

A: Regarding the frequency of conducting personal information protection compliance audits, according to the *Measures for the Management of Personal Information Protection Compliance Audits*, personal information processors that process the personal information of more than 10 million people should conduct a personal information protection compliance audit at least once every two years. According to Article 54 of the *PIPL*, all personal information processors should conduct regular compliance audits. Therefore, although the *Audit Management Measures* do not explicitly stipulate the audit frequency for personal information processors that process the personal information of fewer than 10 million people, according to the

Cybersecurity Standard Practice Guide—Personal Information Protection Compliance Audit Requirements issued by the National Information Security Standardization Technical Committee, personal information processors that process the personal information of more than 1 million but not more than 10 million people should reasonably determine the frequency of compliance audits based on personal information compliance risks, the amount of personal information processed, and business scale, and conduct a personal information protection compliance audit at least once every three or four years. Personal information processors that process the personal information of no more than 1 million people should conduct a personal information protection compliance audit at least once every 5 years.

8. Will a personal information processor that indirectly collects personal information be held jointly liable with the original data provider if the provider lacks a legal basis for data processing?

A: Indirect collection of personal information refers to obtaining personal information indirectly through channels such as sharing, transfer, and collection of public information, rather than directly from the personal information subject. Common scenarios in practice include a logistics company obtaining consumer order-related personal information from an e-commerce platform for shipping; an insurance company obtaining medical records from a medical institution for underwriting and claims processing.

In the main text of the guide, we have clarified the key compliance requirements for indirect collection of personal information. It is important to note that the entity that indirectly collects personal information may also be held jointly liable with the original data provider for reasons such as the provider not having a legal basis for data processing. For example, a data processor that fails to exercise a reasonably prudent review obligation regarding the source of the data may bear responsibility. A typical representative case is the first sound rights infringement case in the country. In this case, the plaintiff was a voice actor who had commissioned the second defendant to record audio products (hereinafter "audio"). The second defendant later provided the

audio to the third defendant, allowing the third defendant to use it for commercial and/or non-commercial purposes. The third defendant used the audio as material for AI processing to generate the text-to-speech product involved in the case and sold it on a third-party platform. After the product was sold, it was called by the first defendant in the form of an application programming interface and used in its own product. The plaintiff believed that all the defendants involved above had infringed on the plaintiff's sound rights and filed a lawsuit. The court, after hearing the case, held that the text-to-speech product involved in the case, which was developed using the plaintiff's personal voice, had a high degree of consistency with the plaintiff's timbre, tone, and speaking style, so the plaintiff's sound rights extended to the AI voice involved in the case. Secondly, since the second defendant's provision of audio to the third defendant was not with the plaintiff's informed consent, both companies constituted an infringement of the plaintiff's sound rights and should bear compensation liability totaling 250,000 yuan. This case illustrates that if the data source of the original data provider is illegal, or if the use exceeds the authorization, the enterprise that subsequently obtains the data indirectly through third-party procurement or other means may also bear responsibility.

However, if the personal information processor has fulfilled its reasonably prudent obligation to review the legality of the data source, it may be exempted from related liability. In practice, there are various ways to fulfill this review obligation, including contractual agreements, sample verification, etc. For example, when the aforementioned logistics company obtains consumer order information from an e-commerce platform for shipping, it can, through contractual agreement, clarify that the e-commerce platform's processing of data must have a legal basis. As another example, when an insurance company obtains medical records from a medical institution, it can verify whether the medical institution has obtained the patient's consent to share the data-related records. These measures can effectively reduce the risk of being held jointly liable with the data provider for indirectly collecting data.

9. In the context of cross-border human resources data management, how

should the exemption from conducting a data export security assessment, concluding a standard personal information export contract, or obtaining personal information protection certification be understood and applied?

A: According to Article 5 of the *New Regulations on Cross-Border Flow*, if an enterprise wishes to claim exemption from obligations related to the export of personal information in the context of human resources, including conducting a data export security assessment, concluding a standard personal information export contract, or obtaining personal information protection certification, it must ensure that the following conditions are met:

- It has lawfully formulated labor rules and regulations or a lawfully signed collective contract.
    - Labor rules and regulations are corporate rules and regulations that protect the labor rights enjoyed by workers and the labor obligations they need to fulfill. They involve matters directly related to the vital interests of workers, such as labor remuneration, working hours, rest and leave, labor safety and health, insurance and benefits, employee training, labor discipline, and labor quota management. A collective contract is a written agreement signed between an employer and the employees of the unit through collective negotiation on matters such as labor remuneration, working hours, rest and leave, labor safety and health, vocational training, and insurance and benefits, in accordance with the provisions of laws, regulations, and rules.
- It is necessary for the implementation of cross-border human resources management.
    - Currently, there are no clear provisions or interpretations at the legal level as to what data is necessary for data export activities related to human resources management. In practice, this issue will depend more on the enterprise's own determination and explanation of "necessity" on a case-by-case basis. In this regard, it is recommended that when claiming exemption from data export

obligations in the context of human resources, the enterprise should specify the specific reasons for data export in the labor rules and regulations or collective contract in advance, and explain the relevant rationality and necessity.

- It is limited to the personal information of employees who have signed a labor contract with the enterprise.
    - The term "employee" here should be interpreted narrowly, referring only to employees who have signed a labor contract with the enterprise and established a legal labor relationship, not including third-party outsourced employees and candidates and interns participating in the enterprise's recruitment process.

10. How should personal information protection obligations in internet advertising and marketing be understood?

A: Unlike traditional advertising, internet advertising often relies on programmatic advertising technology with targeted delivery effects. Therefore, it usually involves matching user information collected from user terminals with the needs of advertisers, and advertisers combine it with their own user personal information for analysis to generate user profiles. As it involves the analysis and processing of user personal information, relevant laws and regulations such as the *PIPL* have put forward corresponding personal information protection obligations for the participants in this business model. The company should, in combination with the business model in practice, set up a user interface for users to conveniently exercise their personal rights, and inform users of the corresponding content required by laws and regulations in external texts such as the privacy policy.

- Obligation to Inform and Obtain Consent

  In different business models, the company needs to fulfill its corresponding obligation to inform and obtain consent according to its actual role in the data processing relationship. Generally speaking, disclosing the processing purpose,

method, duration, scope, and other relevant information about data processing activities through a front-end privacy policy where user personal information is collected is a relatively common way to fulfill the obligation to inform in practice, in order to reach the scope of personal information subjects as completely as possible. In practice, the company needs to comprehensively sort out the scope of personal information fields used to provide advertising services, and consider the possible changes in the scope of personal information processing due to changes in business partners or business development methods, and finally disclose it in a clear and easy-to-understand way in the privacy policy. In addition, the company also needs to reasonably decide on the disclosure method and scope of data flow situations based on its own data processing role and the customer contact methods in the actual business development process.

- Obligations Related to Automated Decision-Making and Personalized Recommendation

  In practice, the front-end channel that directly contacts the user needs to provide the user with the function of turning off personalized advertising or not using personal tags to push ads. It also needs to ensure that the option to turn off personalized advertising is easy to find and simple to operate, avoiding setting complex steps or hidden options. Usually, convenient options can be provided in the privacy settings of the website, App, or mini-program, or in the settings menu of the application, allowing users to choose to opt out of personalized advertising. Once the user chooses to opt out of personalized advertising, the company should ensure that the system respects this choice and no longer uses personal information to push ads. In addition, if feasible, the company can provide technical support to help users solve problems they may encounter when turning off personalized advertising.

11. What does a relatively complete cybersecurity and data compliance system mainly include?

A: Building a corporate cybersecurity and data compliance system can: 1) meet the

compliance requirements under current laws and regulations and reduce legal risks from a systemic level; 2) fully protect users' personal information; 3) promptly discover and resolve existing cybersecurity vulnerabilities and avoid security incidents such as data breaches; 4) gain brand reputation and market competitive advantages, etc. As for the overall system framework, it can be built from three dimensions in combination with the enterprise's own management practices.

- Level 1 Document: Series of Management Policies on Cybersecurity and Data Compliance

  The level 1 document proceeds from the overall corporate level, provides guidance for the establishment and operation of the company's cybersecurity and data compliance management system, provides strategic planning directions for content such as cybersecurity, data security, and personal information security, and clarifies the relevant institutions and responsibilities.

- Level 2 Document: Series of Category Divisions for Cybersecurity and Data Compliance

  The level 2 document mainly considers and further divides the categories of cybersecurity and data compliance, which can specifically include but are not limited to: information security management system category, information security management organization category, personnel security management category, asset management category, access control category, password and key category, physical and environmental category, data security category, network security category, system operation category, system development category, supplier management category, information security incident category, laws and regulations, etc.

- Level 3 Document: Specific Provisions on Cybersecurity and Data Compliance

  The level 3 document is mainly aimed at implementing the specific provisions on cybersecurity and data compliance in the current laws and regulations to fully meet the compliance requirements, including but not limited to: regulations on the management of information system operating permissions, data classification and

grading system, emergency response plan for information security incidents, regulations on the security management of the full data lifecycle, regulations on the management of the full personal information lifecycle, personal information protection impact assessment system, data export security assessment system, etc.

12. Once an enterprise has a data breach or other security incident, what obligations or responsibilities does it need to fulfill or bear?

A: A data breach is a destruction of the data itself, resulting in the loss of the data's secure state. Laws and regulations such as the *PIPL* stipulate the notification obligation after a data breach or other security incident occurs. When an enterprise has a data breach incident, it should, in accordance with relevant laws and regulations and internal policy requirements, promptly send notifications and reports to affected users, regulatory agencies, and other relevant parties. Its main purpose is to protect the personal information and data security of users, ensuring that affected users can promptly understand the situation of the breach incident and take necessary measures to reduce losses and risks. At the same time, reporting to regulatory agencies helps the supervisory agencies to promptly understand the situation of the data breach incident and strengthen supervision and accountability. Generally, it usually includes the following content:

- **Notification objects:** including affected users, regulatory agencies, and other relevant parties.
- **Notification content:** including the basic situation of the breach incident, the cause, the scope of impact, response measures, contact information, etc.
- **Notification method:** notification can be made by email, text message, telephone, letter, etc.
- **Notification time:** after a data breach incident is discovered, a notification should be sent to the relevant parties within a reasonable time.

- **Reporting requirements:** requirements for reporting to regulatory agencies, including the time, content, and method of reporting.

Data breach notification is actually a separate obligation, independent of the data security guarantee obligation. No party in data governance should regard a "data breach" itself as an illegal act, otherwise the data breach notification system would lose its meaning and would not be feasible to implement. In practice, the following four situations may occur: first, the data breach notification obligation is fulfilled, and the data security guarantee obligation is also fulfilled, in which case no relevant legal liability is borne; second, the data breach notification obligation is fulfilled, but the data security guarantee obligation is not fulfilled, in which case no legal liability for failure to notify of the breach arises, but legal liability for failure to fulfill the data security guarantee obligation must be borne; third, the data breach notification obligation is not fulfilled, but the data security guarantee obligation is fulfilled, in which case no legal liability for the data security guarantee obligation is borne, but legal liability for failure to notify must be borne; fourth, neither the data breach notification obligation nor the data security guarantee obligation is fulfilled, in which case both the legal liability for failure to notify and the legal liability for failure to fulfill the data security guarantee obligation must be borne.

Annex 1: Glossary※[76][77]

Data: Refers to any record of information in electronic or other forms. Data is referred to from different perspectives as raw data, derived data, data resources, data products and services, data assets, data elements, etc.

Raw Data: Refers to data that is initially generated or collected from the source and has not been processed.

Personal Information: Refers to various kinds of information related to identified or identifiable natural persons recorded by electronic or other means.[78]

Personal Information Subject: Refers to the natural person identified by or associated with the personal information.[79]

Sensitive Personal Information: Refers to personal information that, once leaked or illegally used, is likely to cause harm to the personal dignity of a natural person or endanger their personal or property safety, including information such as biometrics, religious beliefs, specific identities, medical and health information, financial accounts, and location tracking, as well as the personal information of minors under the age of fourteen.[80]

Anonymization: Refers to the process whereby personal information is processed so that a specific natural person cannot be identified and the information cannot be restored.[81]

---

[76] Chapter authors:
Wang Yi, a certified data transaction compliance officer with 12 years of practice focusing on data compliance, and **Liu Jiayi**, a senior associate at Beijing Global Law Office (Shenzhen).

[77] Items 1-2, 15-19, 23-26 come from the first batch of Common Terms in Data Field issued by National Data Administration on December 30, 2024; Items 27-38 come from the second batch (draft for comments) of Common Terms in Data Field issued on January 23, 2025; Items 20-22 come from Shenzhen local standard Data Transaction Compliance Assessment Specification (DB4403/T 564-2024); sources of other definitions are detailed in corresponding footnotes.

[78] See Article 4 of the PIPL.

[79] From Item (4) of Article 1 of the Personal Information Cross-border Standard Contract (Second Edition) template.

[80] See Article 28 of the PIPL.

[81] See Article 72 of the PIPL

De-identification: Refers to the process whereby personal information is processed so that a specific natural person cannot be identified without the aid of additional information.[82]

Important Data: Refers to data in specific fields, for specific groups, in specific regions, or that reaches a certain level of precision and scale, which, once tampered with, destroyed, leaked, or illegally acquired or used, may directly endanger national security, economic operation, social stability, or public health and safety.[83]

Core Data: Refers to data related to national security, the lifeline of the national economy, important aspects of people's livelihood, and major public interests, which is subject to a more stringent management system.[84]

Data Classification and Grading: Refers to the classification and graded protection of data implemented by the state based on the importance of data in economic and social development, as well as the degree of harm to national security, public interest, or the legitimate rights and interests of individuals or organizations that would be caused if the data were tampered with, destroyed, leaked, or illegally acquired or used.[85]

Data Export: Refers to (a) a data processor transmitting data collected and generated during domestic operations to a destination outside the territory; (b) data collected and generated by a data processor is stored within the territory, and can be queried, retrieved, downloaded, or exported by institutions, organizations, or individuals outside the territory; or (c) other data processing activities that fall under the circumstances of Article 3, Paragraph 2 of the PIPL, such as processing the personal information of natural persons within the territory from a location outside the territory.[86]

Note: The circumstances of Article 3, Paragraph 2 of the PIPL include (a) for the

---

[82] See Article 72 of the PIPL

[83] See article 62 of the Network Data Regulations

[84] See Article 21 of the *Data Security Law*.

[85] See Article 21 of the *Data Security Law*.

[86] From the "Scope of Application" section of the Data Cross-border Security Assessment Application Guidelines (Second Edition)

purpose of providing products or services to natural persons within the territory; (b) to analyze or evaluate the behavior of natural persons within the territory; (c) other circumstances stipulated by laws and administrative regulations.

Overseas Recipient: Refers to an organization or individual outside the People's Republic of China that receives personal information from a personal information processor.[87]

Data Export Security Assessment: Refers to the data export security assessment that a data processor must declare if it provides data collected and generated during its operations within the People's Republic of China to a destination outside the territory under any of the following circumstances: (a) a critical information infrastructure operator provides personal information or important data overseas; (b) a data processor other than a critical information infrastructure operator provides important data overseas, or, since January 1 of the current year, has cumulatively provided the personal information of more than 1 million individuals (excluding sensitive personal information) or the sensitive personal information of more than 10,000 individuals overseas. If the circumstances stipulated in Articles 3, 4, 5, and 6 of the *New Regulations on Cross-Border Flow* apply, those provisions shall prevail. A data processor declaring a data export security assessment should submit the declaration materials through the data export declaration system at the website https://sjcj.cac.gov.cn. If a critical information infrastructure operator or other entity is not suitable for declaring a data export security assessment through the data export declaration system, it shall adopt an offline method to declare the data export security assessment to the national cyberspace administration through the local provincial cyberspace administration.[88]

Personal Information Standard Contract Filing: Refers to the filing that a personal

---

[87] From Item (2) of Article 1 of the Personal Information Cross-border Standard Contract (Second Edition) template

[88].From the "Scope of Application" and "Application Methods and Procedures" sections of the Data Cross-border Security Assessment Application Guidelines (Second Edition)

information processor must declare to the local provincial cyberspace administration if it provides personal information overseas by concluding a standard contract and concurrently meets the following conditions: (a) it is a data processor other than a critical information infrastructure operator; (b) since January 1 of the current year, it has cumulatively provided the personal information of more than 100,000 but less than 1 million individuals (excluding sensitive personal information) overseas; (c) since January 1 of the current year, it has cumulatively provided the sensitive personal information of less than 10,000 individuals overseas. If the circumstances stipulated in Articles 3, 4, 5, and 6 of the *New Regulations on Cross-Border Flow* apply, those provisions shall prevail. A personal information processor shall not, by means such as quantity splitting, provide personal information that should legally pass a security assessment for export overseas by concluding a standard contract. The personal information processor should, within 10 working days from the effective date of the standard contract, file it through the data export declaration system at the website https://sjcj.cac.gov.cn.[89]

Personal Information Export Personal Information Protection Certification: Refers to the personal information protection certification for the personal information export activities of a personal information processor conducted by a professional certification body legally established and approved by the State Administration for Market Regulation to have personal information protection certification qualifications. A personal information processor that provides personal information overseas through personal information export personal information protection certification must also meet the following conditions: (a) it is not a critical information infrastructure operator; (b) since January 1 of the current year, it has cumulatively provided the personal information of more than 100,000 but less than 1 million individuals (excluding sensitive personal information) or the sensitive personal information of less than 10,000 individuals overseas. The personal information provided overseas mentioned in the

[89] From the "Scope of Application" and "Filing Methods" sections of the Personal Information Cross-border Standard Contract Filing Guidelines (Second Edition)

preceding paragraph does not include important data.[90]

Critical Information Infrastructure Operator (CIIO): Refers to important network facilities, information systems, etc., in important industries and fields such as public communication and information services, energy, transportation, water conservancy, finance, public services, e-government, and national defense science and industry, as well as others that, once damaged, lose their function, or have their data leaked, may seriously endanger national security, the national economy and people's livelihood, and the public interest.[91]

Data Processing: Includes the collection, storage, use, processing, transmission, provision, and public disclosure of data.

Entrusted Processing: Refers to the network data processing activities carried out by an individual or organization entrusted by a network data processor in accordance with the agreed purpose and method.[92]

Data Processor: Refers to an individual or organization that independently determines the purpose and method of processing in data processing activities.

Trustee Data Processor: Refers to an individual or organization that is entrusted by others to process data.

Data Flow: Refers to the process of data moving between different subjects, including data opening, sharing, trading, and exchange.

Data Trading: Refers to the trading behavior between a data provider and a data demander, with data in a specific form as the subject matter and currency or other equivalents as the consideration.

Trading Subjects: Refers to the data seller, data buyer, and data merchant in data trading activities.

---

[90].From Articles 3 and 4 of the Personal Information Cross-border Personal Information Protection Certification Measures (Draft for Comments).

[91] From Article 2 of the Critical Information Infrastructure Security Protection Regulations

[92] Article 62 of the Network Data Regulations

Note: A data seller is a legal person or unincorporated organization that sells the subject matter of a transaction. A data buyer is a legal person or unincorporated organization that purchases the subject matter of a transaction. A data merchant is a corporate legal person that collects or maintains data from various legal sources, transforms it into a subject matter of transaction through aggregation, processing, analysis, etc., and sells or licenses it to a buyer; or, to facilitate and smoothly perform a transaction, provides services such as publishing and underwriting the subject matter of a transaction to the client, and conducts business in compliance.

Data Subject: Refers to the natural person identified or associated with personal information, various market entities that collect and process enterprise data in their production and operation activities, and party and government organs at all levels, enterprises, and public institutions that generate and process public data in the process of performing their duties or providing public services according to law.

Subject Matter of Transaction: Refers to the object of the transaction between a data seller or data merchant and a data buyer. The subject matter of a transaction includes data products, data services, data tools, etc.

Note: Data service refers to the service of data processing (collection, storage, use, processing, transmission, etc.) provided by a data seller or data merchant. Data tool refers to the hardware and software tools that can realize data services.

Data Governance: Refers to the process of improving the quality, security, and compliance of data, and promoting the effective use of data. It includes organizational data governance, industry data governance, and social data governance.

Data Security: Refers to ensuring that data is in a state of effective protection and legal use by taking necessary measures, as well as having the ability to guarantee a continuous secure state.

Public Data: Refers to data generated by party and government organs at all levels, enterprises, and public institutions in the process of performing their duties or providing public services according to law.

Blockchain: Is a new type of database software that integrates various technologies such as distributed networks, encryption technology, and smart contracts. It has characteristics such as decentralization, consensus-based trust, immutability, and traceability, and is mainly used to solve trust and security problems in the process of data flow.

Data Property Rights: Refers to the property rights enjoyed by a right holder over specific data, including the right to hold data, the right to use data, and the right to operate data.

Data Property Rights Registration: Refers to the act of a data property rights registration institution reviewing and recording the source, description, compliance, etc., of data according to unified rules, and issuing a registration certificate.

Right to Hold Data: Refers to the right of a right holder to hold legally obtained data by themselves or entrust others to hold it on their behalf, aiming to prevent others from illegally stealing, tampering with, leaking, or destroying the data held by the right holder.

Right to Use Data: Refers to the right of a right holder to use data to optimize production and operation, form derived data, etc., through processing, aggregation, analysis, and other methods. Generally speaking, the right to use is the right of a right holder to use data for internal use without providing it externally.

Right to Operate Data: Refers to the right of a right holder to provide data externally through transfer, license, capital contribution, or establishment of security, either for a fee or free of charge.

Derived Data: Refers to the data formed when a data processor, on the premise of protecting the legitimate rights and interests of all parties, uses professional knowledge, modeling analysis, key information extraction, and other methods to achieve substantial changes in the content, form, structure, etc., of the data for which it enjoys the right to use, thereby significantly increasing the value of the data.

Enterprise Data: Refers to data formed or legally obtained and held by an enterprise in the course of its production and operation.

Data Trading Institution: Refers to a professional institution that provides data trading services for multiple parties of data supply and demand.

On-exchange Data Trading: Refers to the act of data supply and demand parties reaching a data transaction through a data trading institution.

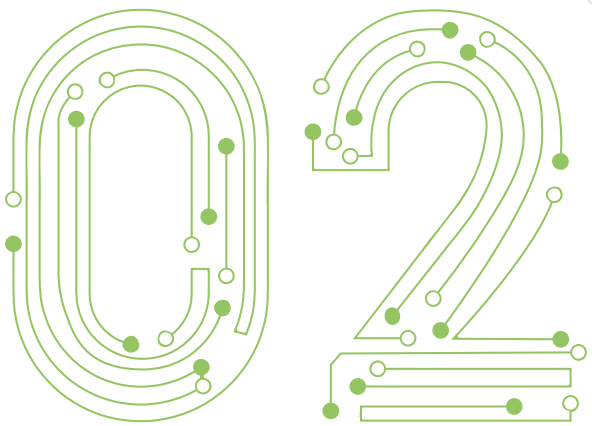
Off-exchange Data Trading: Refers to the act of data supply and demand parties reaching a data transaction without going through a data trading institution.

Data Matching: Refers to the act of helping data supply and demand parties to reach a data transaction.

Third-Party Professional Service Institutions: Professional organizations that, in order to promote the compliant and efficient conduct of data trading activities, provide third-party services such as data integration, data brokerage, compliance certification, security audits, data notarization, data insurance, data custody, asset valuation, dispute arbitration, risk assessment, and personnel training.

Third-Party Legal Service Institutions: Refers to legal persons or unincorporated organizations that assist in the orderly conduct of data trading activities, have obtained a practice license in accordance with the law, and provide legal services for data trading compliance assessment.

Singapore Chapter



Foreword

In today's interconnected digital world, data is not only a catalyst for innovation, but also a key driver of economic growth. As data continues to transform industries and markets, it has played an increasingly vital role in reshaping business models, boosting efficiency, and enhancing productivity across sectors. Singapore recognises the significance of data in this new era, and we welcome the collaboration between the Asian Business Law Institute and the Shenzhen Data Exchange.

This Joint Guide, an initiative between the Asian Business Law Institute based in Singapore, and the Shenzhen Data Exchange, provides an overview of the data protection laws and regulations governing both jurisdictions. It is designed to support businesses operating in China and Singapore, or engaging with, China-based and Singapore-based entities. By distilling the essential elements of the data protection regime into an easy-to-understand format, this guide serves as a practical resource for companies to better understand the regulatory requirements of each jurisdiction, and hence, be able to operate confidently in both jurisdictions.

We hope to foster greater collaboration between China and Singapore through platforms such as the Singapore-China Digital Policy Dialogue and the Singapore-China (Shenzhen) Smart City Initiative. We also hope to continue to work with valuable partners such as the Shenzhen Data Exchange, to encourage businesses to leverage data for innovation and growth, while ensuring the responsible use of data. We look forward to stronger cross-border partnerships and more seamless collaborations between China and Singapore in the digital age of tomorrow. Through key platforms including the Singapore-China Digital Policy Dialogue and the Singapore-China (Shenzhen) Smart City Initiative, we aim to strengthen bilateral collaboration between China and Singapore. In partnership with strategic institutions like the Shenzhen Data Exchange, we strive to promote data-driven innovation and growth while upholding responsible data governance practices. Looking ahead, we envision enhanced cross-border partnerships that will deepen digital cooperation between our two nations in the emerging digital era.

Authors

Benjamin Cheong (Partner and Deputy Head, Technology, Media and Telecoms, Rajah & Tann Singapore LLP)
Yu Peiyi (Senior Associate, Rajah & Tann Singapore LLP)
Wang Rui (Associate, Rajah & Tann Singapore LLP)
Megan Wong (Associate, Rajah & Tann Singapore LLP)
Pamela Low (Practice Trainee, Rajah & Tann Singapore LLP)
Nicholas Lim (Practice Trainee, Rajah & Tann Singapore LLP)
Darren Ong (Practice Trainee, Rajah & Tann Singapore LLP)
Qiyuan (Ivana) Fu
Weijun (Virgil) He

Table of Contents

1. Introduction

1.1. Purpose of the Guide

This guide aims to provide a practical guideline and illustration of the key principles and requirements of the Singapore data regulatory regime for Chinese companies that are conducting business or intend to expand their business in Singapore.

1.2. Overview of the Singapore Data Regulatory Regime

1.2.1. PDPA regime

The Singapore data protection regime is established by the Personal Data Protection Act 2012 ("**PDPA**")(accessible here), which is the primary data protection legislation in Singapore. The PDPA is further supplemented by subsidiary legislations including:

- the Personal Data Protection Regulations 2021 ("**PDPR**");
- the Personal Data Protection (Notification of Data Breaches) Regulations 2021;
- the Personal Data Protection (Composition of Offences) Regulations 2021;
- the Personal Data Protection (Do Not Call Registry) Regulations 2013;
- the Personal Data Protection (Enforcement) Regulations 2021; and
- the Personal Data Protection (Appeal) Regulations 2021.

The PDPA is administered and enforced by the Personal Data Protection Commission ("**PDPC**").

To provide more clarity to the PDPA, the PDPC has issued, and continuously issues from time to time, a series of advisory guidelines with respect to interpretation of the PDPA.

1.2.2. Other Legislation that Impact Data Protection

Other than the PDPA, there are other general legislation that impose data protection obligations on companies, such as:

- **Computer Misuse Act 1993.** Sets out the various offences involving the unauthorised use or access to computer materials and computer services.
- **Cybersecurity Act 2018.** Requires owners and operators of Critical Information Infrastructure to maintain cybersecurity of their computer systems and services and report cybersecurity incidents.

Further, there are some other sector-specific laws that impact data protection, such as:

- **Banking Act 1970**. Contains banking secrecy provisions to protect customer data.
- **Telecom and Media Competition Code 2022 (issued under the Telecommunications Act 1999).** Prohibits telecom operators from unauthorised use of End User Service Information.
- **Healthcare Services Act 2020.** Requires healthcare service licensees to securely retain medical records and protect the confidentiality of medical information.

The provisions of other written laws will prevail to the extent that they are inconsistent with the PDPA. See paragraph 2.2.11(d) below for further elaboration.

2. Understanding the PDPA framework

2.1. Scope and Applicability

All private sector organisations that collect, use and disclose personal data in Singapore must comply with the PDPA.

- **Who will be considered an "Organisation"?**

  "Organisations" are defined in the PDPA as "*any individual, company, association or body of persons, corporate or unincorporated, whether or not (a) formed or recognised under the law of Singapore; or (b) resident, or having an office or a place of business, in Singapore*" (Section 2 of the PDPA,).

  This means that the PDPA has extra-territorial effect and can apply to a foreign company even if it is not incorporated or registered in Singapore or does not have a physical presence in Singapore, so long as such foreign company carries out any collection, use, disclosure or other processing of personal data in Singapore.

- **What constitutes "Personal Data"?**

  Under the PDPA, "personal data" is defined as "*data, whether true or not, about an individual who can be identified (a) from that data; or (b) from that data and other information to which the organisation has or is likely to have access*" (PDPA, section 2).

  This means that data which on their own would allow the identification of an individual (such as name, NRIC number, fingerprints, bank account numbers, photographs, video footage) would constitute personal data.

  In addition, data which, when combined with other data would allow the identification of an individual (such as mobile phone number, addresses, gender, age), would also constitute personal data.

2.2. Key Principles of the PDPA

2.2.1. Consent

An organisation must obtain the consent of an individual before collecting, using or disclosing his/her personal data (PDPA, section 13), unless an exception to consent under the PDPA (please refer to Section 3.2 (Obtaining consent for processing and marketing) below) applies.

Please refer to Section 3.2 (Obtaining consent for processing and marketing) below for more detailed requirements with respect to consent to processing personal data under the PDPA.

2.2.2. Purpose limitation

Under the PDPA, an organisation may only collect, use or disclose personal data about an individual for purposes that a reasonable person would consider appropriate in the circumstances, and that the individual has been notified in accordance with the notification requirements under the PDPA (please refer to Section 2.2.3 (Notification) below) (PDPA, section 18).

If an organisation intends to use any personal data for any new purposes which had not been previously consented to by the data subject, it would need to obtain consent from the data subject again, unless otherwise required or permitted under applicable laws (Personal Data Protection Commission ("**PDPC**"), Advisory Guidelines on Key Concepts in the Personal Data

Protection Act ("**Guidelines**") (accessible here), paragraph 14.22).

2.2.3. Notification

Before collecting, using or disclosing Personal Data, the individual must be notified of the purposes for which the organisation intends to collect, use or disclose his/her Personal Data, unless an exception to consent applies (PDPA, section 20). The organisation must only collect, use or disclose personal data which is consistent with those purposes.

Notification of the purpose(s) for collection, use or disclosure of personal data should be given prior to the first collection of personal data from the individual.

The PDPA does not prescribe a specific form for the notification to be provided to individuals. As such, the notification may be provided to the individual in any manner and form so long as the individual is provided with the necessary information to understand the purposes for which his/her personal data is being collected, used or disclosed.

2.2.4. Access and correction

(a) Access

Upon request by an individual, the individual must be provided, as soon as reasonably possible, with information on (a) what personal data belonging to him/her is in the organisation's control as well as (b) how the organisation may have used or disclosed such personal data in the one (1) year preceding the date of the individual's request (PDPA, section 21).

The organisation must respond to an access request as soon as reasonably possible from the time the access request is received. If an organisation is unable to respond to an access request within 30 days after receiving the request, the organisation must inform the individual in writing within 30 days of the time by which it will be able to respond to the request.

Do note that an individual's right to access his/her personal data is not absolute, and the Fifth Schedule to the PDPA sets out various scenarios under which an organisation may or must refuse to comply with an access request. This includes circumstances where complying with an access request may:

- threaten the safety or physical or mental health of an individual other than the individual who made the request;
- cause immediate or grave harm to the safety or to the physical or mental health of the individual who made the request;
- be contrary to the national interest.

In the event that an organisation decides to reject the access request, it must notify the individual of the rejection. In case the individual wishes to challenge the organisation's rejection, a copy of the requested personal data must be preserved for at least 30 days after the request was rejected.

(b) Correction

Under the PDPA, an individual also has the right to submit a request for an organisation to correct an error or omission in the individual's personal data that is in the possession or under the control of the organisation (a "**correction request**"). Upon request by an individual, an organisation is required to consider whether the correction should be

made (PDPA, section 22).

An organisation is generally required to correct the personal data as soon as practicable from the time the correction request is made. If an organisation is unable to correct the personal data within 30 days from the time the request is made, the organisation must inform the individual in writing within 30 days of the time by which it will be able to correct the personal data.

- ***Correcting Personal Data***

  In cases where a correction request is accepted, the correction must be made as soon as practicable. The organisation may also be required to send the corrected personal data to every other organisation to which the personal data was disclosed to within a year before the date of the correction request, unless that other organisation does not need the corrected personal data for any legal or business purpose.

- ***Refusing to correct Personal Data***

  Under the PDPA, the correction of personal data can be refused if there are reasonable grounds for such a refusal.

  Besides this, there are certain statutorily provided classes of personal data or documents containing personal data which need not be corrected upon request.

  If an organisation is satisfied upon reasonable grounds that a correction should not be made (whether the organisation is responding to a correction request or has been notified of a correction made by another organisation), the organisation must annotate (i.e. make a note on) the personal data in its possession or under its control indicating the correction that was requested but not made. As good practice, the organisation may also wish to annotate the reasons and explain to the individual why it has decided that the correction should not be made.

2.2.5. Accuracy

Reasonable efforts must be taken to ensure that personal data collected by an organisation or on its behalf is accurate and complete if the personal data is likely to be used by the organisation to make a decision that affects the individual concerned, or disclosed by the organisation to another organisation (PDPA, section 23).

- ***Personal data provided directly by the individual***

  Organisations may presume that personal data provided directly by the individual concerned is accurate in most circumstances. When in doubt, organisations can consider requiring the individual to make a verbal or written declaration that the personal data provided is accurate and complete (Guidelines, paragraph 16.6).

- ***Personal data provided from a third-party source***

  In general, due consideration should be given when collecting personal data from a third party source instead of collecting such personal data directly from the individual himself. In that regard, it should be ensured that suitable warranties from the organisation's third party sources (that such third party sources had verified the accuracy and completeness of the personal data they are forwarding to the

organisation) should be obtained, and/or that further independent verification checks are conducted on the personal data provided by such third party sources (Guidelines, paragraph 16.7).

2.2.6. Protection

An organisation must protect personal data in its possession or under its control by putting in place appropriate technical and organisational measures to prevent (i) unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks and (ii) the loss of any storage medium or device on which personal data is stored (PDPA, section 24).

The PDPC has clarified in its Guidelines (at paragraph 17.2) that there is no 'one size fits all' solution for organisations to comply with the Protection Obligation and each organisation should consider adopting security arrangements that are reasonable and appropriate in the circumstances, taking into consideration factors such as:

(a) the nature of the personal data,

(b) the form in which the personal data has been collected (e.g. physical or electronic), and

(c) the possible impact to the individual concerned if an unauthorised person obtained, modified or disposed of the personal data.

2.2.7. Retention Limitation

An organisation's retention of personal data must cease, or the means by which the personal data can be associated with particular individuals must be removed (e.g. by anonymisation) as soon as it is reasonable to assume that the purpose for which the personal data was collected is no longer being served by retention of the personal data, and retention by the organisation is no longer necessary for any other legal or business purposes (PDPA, section 25).

Documents should be destroyed and/or disposed of after their respective retention periods. Alternatively, if there is a need to retain the documents and/or data for analytical purposes, steps must be taken to anonymise the documents and data. An organisation will be deemed to have ceased to retain documents containing personal data when it, its agents and its data intermediaries no longer have access to the documents and the personal data they contain (Guidelines, paragraph 18.10).

However, the destruction and disposal of documents in the normal course of business must be suspended in the event that the relevant documents are (i) related to any actual, potential or threatened litigation or regulatory request or investigation, or (ii) related to an on-going internal or external audit.

2.2.8. Transfer Limitation

The PDPA does not impose any data localisation requirements in relation to personal data. However, personal data may only be transferred to a country or territory outside Singapore in accordance with the relevant requirements prescribed under the PDPA, which include ensuring that the overseas recipient is bound by legally enforceable obligations to provide a standard of protection to the personal data so transferred that is comparable to the protection under the PDPA (PDPA, section 26).

For more information on requirements and recommended practices with respect to cross-border data transfer, please refer to Section 3.5 (Data Processing and Cross-Border Transfers)

below.

2.2.9. Accountability

An organisation is required to develop and implement policies and processes for data protection in compliance with the PDPA, including a process for responding to queries or complaints from members of the public or the PDPC. The organisation must make information about its data protection policies and procedures publicly available, which is typically done by publishing the organisation's privacy policy on its website (PDPA, section 12).

In addition, the organisation must appoint a Data Protection Officer ("**DPO**") to be responsible for ensuring the organisation's compliance with the PDPA. The DPO's business contact information must also be made publicly available (PDPA, section 11). For more information on Data Protection Officers, please refer to Section 3.1 (Data Protection Officer: Qualifications and Responsibilities) below.

2.2.10. Data Breach Notification

In the event an organisation has credible grounds to believe that a data breach has occurred, it must assess whether such data breach is notifiable, and notify the affected individuals and/or the PDPC where the data breach is assessed to be notifiable in accordance with the statutory timelines.

For more information on data breach notifications, please refer to Section 3.4 (Data Breach Management) below.

2.2.11. Scenarios not subject to any data protection obligations

Under the PDPA, the following 4 situations are excluded from compliance with any of the personal data protection obligations:

(a) Individual acting in a personal or domestic capacity

An individual acts in a personal capacity if he/she undertakes activities "for his/her own purposes" and not for another or on behalf of an organisation; and he/she acts in a domestic capacity when conducting activities that are "related to his/her home or family", such as making an application for school, purchasing insurance or opening a joint bank account using the personal data of a family member or setting up home access using biometric data (Guidelines, paragraphs 6.8 to 6.10).

(b) Employee acting in the course of his/her employment with an organisation

An employee acting in the course of his/her employment is excluded from the application of the data protection obligations, and any liability for his/her actions in a breach of the PDPA will be placed on the employer instead, no matter whether or not the employees' actions were done or engaged in with the employer's knowledge or approval (Guidelines, paragraphs 6.11 to 6.12).

It should be noted that as the PDPA defines an employee to include volunteers, individuals who undertake work without an expectation of payment may also fall under this exclusion (Guidelines, paragraph 6.11).

(c) Public agency or an organisation acting on its behalf

The PDPA defines a public agency to include (i) the Government, including any ministry,

department, agency, or organ of State; (ii) a tribunal appointed under any written law; or (iii) a statutory body specified by the Minister by notice in the Gazette (Personal Data Protection (Statutory Bodies) Notification 2013). Such public agencies are excluded from the data protection obligations under PDPA as there are separate legislations that are more suitable and efficient to govern their activities (PDPA, section 2).

However, organisations that provide services to public agencies may either have obligations under the PDPA as data controllers or as data intermediaries (Guidelines, paragraph 6.14).

(d) Other Written Law

The PDPA also stipulates that where any provision of the PDPA is inconsistent with any other written law of Singapore, the provisions of the other written law shall prevail (PDPA, section 6).

However, do note that this exception applies only to the extent of the inconsistency. The provision of the other written law will apply only to matters which are inconsistent between the two provisions. Other provisions of the PDPA which are not inconsistent with the other written law will continue to apply.

2.2.12. Scenarios exempted from certain data protection obligations only

There are also partial exclusions under the PDPA that are applicable in the following situations where only certain personal data obligations need to be complied with:

(a) Data Intermediaries

The PDPA recognises the important roles played by data intermediaries and the need to ensure they are able to function effectively; hence, it draws a distinction between organisations and data intermediaries.

- **What is a "Data Intermediary"?**

  Section 2 of the PDPA defines a data intermediary as "an organisation that processes personal data on behalf of another organisation". The term "processing" is defined in section 2 of the PDPA as "*the carrying out of any operation or set of operations in relation to the personal data, and includes any of the following: recording, holding, organisation, adaptation or alteration, retrieval, combination, transmission, and erasure or destruction*."

Under the PDPA, data intermediaries **that process personal data on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing** are only subject to the protection obligation, retention limitation obligation and data breach notification obligation.

On the other hand, section 4(3) of the PDPA provides that an organisation has the same obligations under the PDPA in respect of personal data processed on its behalf by a data intermediary as if the personal data were processed by the organisation itself. The PDPC in its Guidelines further clarifies that "*the organisation remains liable for any breach of the Data Protection Provisions for any processing by a data intermediary on its behalf and for its purposes*".

In this regard, the PDPC had stated in its Guidelines (at paragraphs 6.20 and 6.21) that:

(a) It is good practice for an organisation to undertake an appropriate level of due diligence to assure itself that the data intermediary is capable of complying with the PDPA.

(b) An organisation should make clear in its contract with the data intermediary the scope of work that the data intermediary is to perform on its behalf and for its purposes.

(b) Business contact information

In most situations, business contact information is not subject to the data protection obligations under the PDPA.

- **What is considered "Business Contact Information"?**

  Business contact information is defined in section 2 of the PDPA as "*an individual's name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the individual, not provided by the individual solely for his or her personal purposes*".

However, if an individual provides his/her work-related contact information solely for personal purposes, such information will not constitute business contact information and organisations would be required to comply with the data protection obligations in respect of such information.

(c) Exceptions in the Schedules of the PDPA

The PDPA also provides for exceptions and additional bases to obtaining consent for the collection, use and disclosure of Personal Data, and such exceptions can be found in the First and Second Schedules of the PDPA. Such exceptions include the following:

(i) If the personal data is already publicly available;

(ii) if the purpose of the collection, use or disclosure is clearly in the interests of the individual, and if consent cannot be obtained in a timely way;

(iii) if the collection, use or disclosure is necessary to respond to an emergency that threatens the life, health or safety of the individual or of another individual;

(iv) if the collection, use or disclosure is for the purpose of contacting the next-of-kin or a friend of any injured, ill or deceased individual; and

(v) if there are reasonable grounds to believe that the health or safety of the individual or another individual will be seriously affected and consent for the collection, use or disclosure of the data cannot be obtained in a timely way, provided that the organisation shall, as soon as may be practicable, notify the individual of the collection, use or disclosure and the purposes of the collection, use or disclosure.

The First and Second Schedules of the PDPA lay out a full list of the exceptions.

3. Key Compliance Obligations

3.1. Data Protection Officer: Qualifications and Responsibilities

As part of the Accountability obligation under the PDPA, any organisation processing personal data in Singapore is required to designate at least one individual to be responsible for ensuring that the organisation complies with the PDPA (PDPA, section 11). This individual is typically referred to as a Data Protection Officer ("**DPO**"). However, organisations should note that the designation of DPO does not relieve an organisation of any of its obligations under the PDPA, and the legal responsibility for complying with the PDPA remains with the organisation and is not transferred to the designated individual(s) (Guidelines, paragraph 21.3).

3.1.1. Responsibilities of the DPO

The DPO is responsible for ensuring the organisation's compliance with the PDPA. PDPC have further clarified that the DPO's responsibilities often include working with senior management and the organisation's business units to develop and implement appropriate data protection policies and practices for the organisation. In this regard, the DPO's job may cover a wide range of activities, which may include producing (or guiding the production of) a personal data inventory, conducting data protection impact assessments, monitoring and reporting data protection risks, providing internal training on data protection compliance, engaging with stakeholders on data protection matters and generally acting as the primary internal expert on data protection (Guidelines, paragraph 21.4).

3.1.2. Qualifications of the DPO

According to the Guidelines (at paragraph 21.5), individual(s) designated by an organisation as a DPO shall be:

(a) sufficiently skilled and knowledgeable; and

(b) amply empowered, to discharge their duties as a DPO, although they need not be an employee of the organisation.

In this regard, companies can support such individuals by training and/or certifying them on PDPA compliance, for example, sending them for the Practitioner Certificate for Personal Data Protection (Singapore) co-issued by the PDPC and the International Association for Privacy Professionals.

On the other hand, the appointed DPOs are also expected to engage in self-directed learning and upskilling. For instance, the DPOs may refer to the PDPC's DPO Competency Framework and Training Roadmap ("**Roadmap**") (DPO Competency Framework and Training Roadmap (accessible here)) to build core competencies and achieve certain proficiency levels. The Roadmap is intended as a self-help guide to complement the DPO's independent learning, by setting out trainings for key competencies in relevant courses such as data protection management, business risk management, cyber and data breach incident management, stakeholder management, audit and compliance and data governance.

Additionally, DPOs are also encouraged to develop non-data protection competencies to support key tasks such as managing people and organisation.

3.1.3. Publication of the DPO's business contact information

As the DPO will be the main point of contact for the public to reach out to the company in relation to data protection matters, the PDPA requires every organisation to make the business contact information of the DPO (or any other individual tasked with answering questions on

behalf of the organisation in relation to the collection, use or disclosure of personal data) publicly available (PDPA, section 11(5)).

Such requirement could be satisfied by registration of the DPO's information on BizFile+ for companies that are registered with ACRA (Guidelines, paragraph 21.7). Such requirement could also be satisfied by publishing the DPO's information in a readily accessible part of the organisation's official website (Guidelines, paragraph 21.7).

3.2. Obtaining Consent for Processing and Marketing

3.2.1. Consent for Collection, Use and/or Disclosure of Personal Data

(a) Express and Deemed Consent

Consent may be express or deemed. However, as far as possible, express consent should be obtained.

Express Consent

Express consent is where the individual actively communicates his/her consent. However, express consent need not be limited to written form and may be given verbally (i.e., where an individual verbally consents to such collection, use or disclosure). In such cases, organisations should keep a record of the verbal consent obtained by the individual as evidence of consent. Such records may be in the form of a voice recording or a follow-up e-mail / letter to the individual.

Deemed Consent

Deemed consent is when: (i) an individual does not actively indicate his/her consent but voluntarily provides his/her personal data; and (ii) it is reasonable under the circumstances that he/she would do so.

Under the umbrella of deemed consent, the PDPA also provides for three specific situations in which consent will be deemed.

(i) The first situation can be referred to as "*deemed consent by conduct*" (Guidelines, paragraph 12.20 and 12.21). This applies to situations where the individual voluntarily provides his/her personal data to the organisation. The purposes to which the data can be collected, used and/ or disclosed are limited to those that are objectively obvious and reasonably appropriate from the surrounding circumstances.

(ii) The second situation can be referred to as "*deemed consent by contractual necessity*" (Guidelines, paragraph 12.22). Where an individual provides personal data to an organisation with a view to entering into a contract with such organisation, the individual is deemed to consent to all downstream disclosure of the personal data to other organisations, provided that the disclosure is reasonably necessary for the conclusion of the contract.

In addition, where an individual provides personal data to an organisation and enters into a contract with such organisation, that individual is deemed to have consented to all downstream disclosure of the personal data to other organisations, including the downstream organisations collecting and using the personal data, provided that it is reasonably necessary:

- for the conclusion or performance of the contract between the

individual and the organisation; or

- for the conclusion or performance of a contract between the organisation and the downstream organisation which is entered into at the individual's request, or if a reasonable person would consider the contract to be in the individual's interest.

(iii) The third situation can be referred to as "*deemed consent by notification*" (Guidelines, paragraph 12.23). Here, an organisation obtains an individual's deemed consent if:

- Before collecting, using or disclosing the individual's personal data, the organisation has assessed that the proposed collection, use or disclosure is not likely to have an adverse effect on the individual. Where any adverse effects are identified, the organisation has taken steps to eliminate, reduce the likelihood of or mitigate them. If there are any residual adverse effects, the organisation must not rely on deemed consent by notification to collect, use or disclose personal data;

- The organisation has notified the individual of the purposes for the collection, use or disclosure of his/her personal data, and gave him/her a reasonable period of time to opt-out. Some considerations for determining the reasonableness of the opt-out period include: (i) the nature and frequency of interaction with the individual; and (ii) the communications and opt-out channels used.

  In its notification to the individual, the organisation should bring the individual's attention to: (i) the fact that the organisation intends to collect, use or disclose the personal data; (ii) the purpose of such collection, use or disclosure; and (iii) the manner for how the individual can opt-out, as well as the period of time to opt out; and

- The opt-out period has elapsed, and the individual did not opt-out.

It is important to note that deemed consent by notification cannot be used to obtain consent for certain prescribed purposes, including the purpose of sending direct marketing messages to individuals. If an organisation wishes to use the personal data of an individual for marketing purposes, it should obtain express consent from such an individual.

Furthermore, during the period that an organisation is collecting, using or disclosing personal data based on deemed consent by notification, it must retain a copy of its assessment of the potential adverse effects. Please refer to the Assessment Checklist for Deemed Consent by Notification ("**DC Checklist**") published by the PDPC here. The DC Checklist serves as a useful guide for organisations to assess whether: (i) they can rely on deemed consent by notification to collect, use or disclose personal data; and if so, (ii) the appropriateness of the notification to individuals and reasonableness of opt-out period. It is worth noting that the DC Checklist is not legally binding in nature and organisations are not mandated to use it. Generally, organisations should assess four main areas sequentially in the following order – (i) purpose,

(ii) appropriateness of notification and reasonableness of the mode and period of opt-out, (iii) any likely adverse effect on the individual, and (iv) the final decision outcome.

(b) Written or Verbal Consent

When organisations intend to collect, use or disclose personal data, individuals should be provided with the means to expressly indicate their consent. As a matter of best practice, consent should be obtained in writing or recorded in a manner that is accessible in case it is required for reference in the future. Where verbal consent is given, a record should be taken of the fact that consent was given, the purposes for which such consent was given as well as the date and time at which the verbal consent was given.

(c) Consent obtained as a result of false or misleading information

Consent will be invalid where it is given as a result of false or misleading information or obtained through deceptive or misleading practices.

(d) Obtaining Personal data from third parties

In many situations, personal data from parties other than the individual himself may be collected. In these situations, no such collection should be engaged in unless it is satisfactorily proven that the party providing the personal data has obtained the consent of the individual to disclose his/her personal data to the organisation that is collecting his/her personal data for the specified purpose(s) (Guidelines, paragraph 12.34).

(e) Persons validly acting on behalf of an individual

Consent may also be given by a person validly acting on behalf of an individual. Such individuals may be minors, deceased persons or persons who lack the mental capacity to give consent. In such situations, the consent of the person validly acting on behalf of the individual is no different from the consent of the individual himself/herself.

(f) Publicly Available Data

Publicly available data constitutes an exception to the requirement of consent for collection, use or disclosure. “Publicly available data” refers to data which any member of the public can obtain or access with few or no restrictions. Such data would include personal data which can be observed by reasonably expected means at a location or event that is open to the public at which the individual appears. In such situations, the personal data can be collected, used or disclosed without the individual’s consent.

(g) Legitimate Interests Exception

Personal data can be collected, used or disclosed by an organisation without the individual’s consent if it is in the legitimate interests of such organisation or any other person and the legitimate interests of the organisation or other person outweigh any adverse effect on the individual (PDPA, First Schedule Part 3).

“*Legitimate interests*” generally refer to any lawful interests of an organisation or other person (including other organisations). Examples of legitimate interests include

detecting or preventing illegal activities (e.g. fraud and money laundering), detecting or preventing threats to physical safety and security, ensuring IT and network security, or preventing the misuse of the organisation's services, and other necessary due diligence. It is worth noting that the PDPA clearly states that sending promotional or marketing messages to individuals does not constitute a legitimate interest.

Before collecting, using or disclosing personal data in reliance on the legitimate interests exception, an organisation must first:

(i) identify and be able to clearly articulate the situation or purpose that qualifies as a legitimate interest;

(ii) assess if there are any likely adverse effect to the individuals, and implement measures to eliminate, reduce the likelihood of or mitigate such effects. Please refer to the Assessment Checklist for Legitimate Interests Exception ("**LIE Checklist**") published by the PDPC here. As a brief overview, the LIE Checklist serves as a useful guide for organisations to assess whether they can rely on the legitimate interest exception. Notably, organisations may justify their reliance on the legitimate interest exception by demonstrating their compliance with the LIE Checklist. It is worth noting that the LIE Checklist is not legally binding in nature and organisations are not mandated to use it. Generally, organisations should assess four main areas sequentially in the following order – (i) purpose, (ii) appropriateness of notification and reasonableness of the mode and period of opt-out, (iii) any likely adverse effect on the individual, and (iv) the final decision outcome. In weighing the legitimate interests against any resulting adverse effects to an individual, organisations should note that this is not a merely quantitative exercise and that a proper evaluation of each response in this balancing test should be conducted. Meaning, even if the benefits of collection, use and/or disclosure numerically outweigh the adverse effects, this does not automatically imply that the organisation may rely on the legitimate interest exception;

(iii) ensure that the legitimate interest outweighs any adverse effect to the individual, if any; and

(iv) disclose its reliance on the legitimate interests exception to the relevant individuals, through any means that is reasonably effective, such as through the organisation's privacy policy.

(h) Business Improvement Exception

Under the exception provided in the PDPA, First Schedule Part 5, an organisation may use the personal data of individuals, without the need to obtain that individual's consent, for the following business improvement purposes:

(i) to improve, enhance or develop new goods or services provided by the organisation;

(ii) to improve, enhance, or develop new methods or processes for the operations of the organisation;

(iii) to learn about and understand the behaviour and preferences of individuals in relation to the goods and services provided by the organisation (i.e. customer preferences); and

(iv) to identify goods or services provided by the organisation that may be suitable for the individual, or personalising or customising any such goods or services for individuals.

Before an organisation can rely on this exception, the organisation will need to ensure that the business improvement purpose cannot reasonably be achieved using anonymised personal data only. The business improvement purpose should also be appropriate in the circumstances.

3.2.2. Withdrawal of Consent

An individual who has previously consented to the collection, use or disclosure of his/her personal data for notified purposes can withdraw his/her consent at any time upon giving reasonable notice. Once an organisation has received a notice to withdraw consent from an individual, the organisation should inform the individual concerned of the likely consequences of withdrawing his consent.

Although an individual may withdraw consent for the collection, use, or disclosure of his personal data, the PDPA does not require an organisation to delete or destroy the individual's personal data upon request. Organisations may retain personal data in their documents and records in accordance with the retention limitation obligation.

3.2.3. Obtaining Consent for Marketing Purpose

It is common for organisations to collect, use or disclose personal data for marketing purposes. However, organizations should note that when using personal data for such purposes, a separate and specific consent should be obtained from the individual whose personal data is to be used. Further, organisations should not require an individual to consent to the collection, use or disclosure of personal data about the individual beyond what is reasonable to provide the product or service to that individual, as a condition of providing a product or service.

3.3. Data Management Policies

Accountability requires organisations to demonstrate proper management and protection of Personal Data, including adapting legal requirements into policies and practices, and utilising monitoring mechanisms and controls to ensure that those policies and processes are effectively implemented (PDPC's Guide to Developing a Data Protection Management Programme

(accessible here), page 5). Such policies should be approved by the management, communicated to all relevant parties and reviewed regularly to ensure they remain relevant.

The policies will assist in providing clarity to internal stakeholders on the responsibilities and processes related to handling personal data in their day-to-day work. Additionally, they will also demonstrate accountability to external parties by informing them of the value the organisation places on data protection and how it will protect personal data in its care (PDPC's Guide to Developing a Data Protection Management Programme, page 15).

3.4. Data Breach Management

In the event an organisation has credible grounds to believe that a data breach has occurred (whether through self-discovery, alert from the public or notification by its data intermediary), the organisation must take reasonable and expeditious steps to assess whether such data breach is notifiable and, where it is assessed to be notifiable, notify the affected individuals and/or the PDPC in accordance with the statutory timelines ("**Data Breach Notification Obligations**") (PDPA, section 16C).

3.4.1. What constitutes a "Data Breach"?

Under the PDPA section 26A, "data breach" in relation to personal data means:

(a) the unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data; or

(b) the loss of any storage medium or device on which personal data is stored in circumstances where the unauthorised access, collection, use, disclosure, copying, modification or disposal of the personal data is likely to occur.

3.4.2. Duty to conduct assessment of data breach

Where an organisation has reason to believe that a data breach affecting personal data in its possession or under its control has occurred, the organisation must conduct, in a reasonable and expeditious manner, an assessment of whether the data breach is a notifiable data breach (PDPA, section 26C).

Any unreasonable delay in assessing a data breach will be a breach of the Data Breach Notification Obligations and may lead to enforcement action by the PDPC. While, in practice, there may be varying circumstances that would affect the time taken for the assessment, the PDPC has clarified that organisations should generally do so within 30 calendar days. If an organisation fails to so do, it would be prudent for the organisation to be prepared to provide the PDPC an explanation for the time taken to carry out the assessment (Guidelines, paragraph 20.4).

As a good practice, organisations should document the steps they have taken in assessing the data breach. This will also be helpful for the notification to the affected individual(s) and/or the PDPC if the data breach if assessed as notifiable.

Data breach within an organisation

A data breach that relates to the unauthorised access, collection, use, disclosure, copying or modification of personal data only within an organisation is deemed not to be a notifiable data breach (Guidelines, paragraph 20.6).

For example, where the HR department of an organisation mistakenly sends an email attachment containing personal data to another department within the same organisation that is not authorised to receive it, and the data breach is contained within the organisation, the data breach is not subject to the Data Breach Notification Obligation (Guidelines, paragraph 20.6).

Data breaches discovered by a data intermediary

Where a data intermediary has reason to believe that a data breach has occurred in relation to personal data that the data intermediary is processing on behalf of and for the purposes of another organisation, the data intermediary must notify that other organisation of the occurrence of the data breach without undue delay (PDPA, section 26C(3)).

In such situation, the data intermediary is not statutorily obligated to assess whether the data breach is notifiable as well as to notify affected individuals and/or the PDPC. However, the organisation engaging the data intermediary must conduct an assessment of whether the data breach is a notifiable data breach upon notification by the data intermediary, even if it enlists the help of a data intermediary to conduct the assessment of the data breach or to notify the affected individuals and/or the PDPC on its behalf (Guidelines, paragraph 20.8).

3.4.3. Duty to notify occurrence of notifiable data breach

(a) Notifiable data breach

Under the PDPA section 26B, a data breach would be notifiable:

- to both the PDPC and the affected individuals, if it is likely to result in significant harm to the affected individual(s), or
- to the PDPC, if it is of a significant scale.

(i) Significant harm to the affected individual(s)

According to the Personal Data Protection (Notification of Data Breaches) Regulations 2021 ("**Regulations**") (accessible here), a data breach relating to the following personal data is deemed to result in significant harm to the affect individual(s):

Individual's full name or alias or full national identification number in combination with any of the personal data as listed under the schedule of the Regulations, which includes the following categories of personal data (Regulations, Schedule; Guidelines, paragraph 20.15.) that are not publicly available and/or disclosed as required under any written law:

- Financial information which is not publicly disclosed;
- Identification of vulnerable individuals;
- Life, accident and health insurance information which is not publicly disclosed;
- Specified medical information;
- Information related to adoption matters;
- Private key used to authenticate or sign an electronic record or

transaction; and

- Individual's account identifier and data for access into the account (without individual's name, alias or full identification number).

(ii) Data Breach of Significant scale

A data breach involving personal data of not fewer than 500 individuals constitute a data breach of significant scale. Notification shall be made to the PDPC if an organisation is unable to determine the actual number of affected individuals in a data breach but has reason to believe that the number of affected individuals is at least 500 (Regulations, section 4; Guidelines, paragraph 20.21).

(b) Notification timeline

Under section 26D of the PDPA, where an organisation assesses that a data breach is notifiable, it must notify:

(i) the PDPC as soon as practicable, but in any case no later than 3 calendar days after the day the organisation makes that assessment; and

(ii) where required, each affected individual affected by the data breach as soon as practicable, at the same time or after notifying the PDPC.

(c) Information to be included in the notification

When notifying affected individuals and/or the PDPC of a notifiable data breach, an organisation shall provide relevant details of the data breach to the best of its knowledge and belief. Pursuant to the Guidelines (at paragraph 20.37), the notification should also include relevant information about the organisation's data breach management and remediation plans.

(i) Notification to the affected individuals

Notification to the affected individuals should be clear and easily understood, and include guidance on the steps affected individuals may take to protect themselves from the potential harm arising from the data breach (Guidelines, paragraph 20.42).

(d) Exceptions for the notification to the affected individuals

With respect to a data breach that is notifiable to the affected individual(s), an organisation is not required to notify the affected individuals if the organisation —

(i) takes any action, in accordance with any prescribed requirements, that renders it unlikely that the notifiable data breach will result in significant harm to the affected individual; or

(ii) had implemented, prior to the occurrence of the notifiable data breach, any technological measure that renders it unlikely that the notifiable data breach will result in significant harm to the affected individual.

However, organisations should note that, in such event, even though the notification to the affected individuals is not required, it is still required to notify the PDPC of the data breach.

3.5. Data Processing and Cross-Border Transfers

3.5.1. Requirements for transferring data outside of Singapore

The PDPA does not impose any data localisation requirements in relation to personal data. However, an organisation may only transfer personal data overseas if it has taken appropriate steps to ensure that the overseas recipient is bound by legally enforceable obligations to provide the transferred personal data with a standard of protection that is comparable to that under the PDPA (PDPA, section 26).

In this regard, section 11 of the PDPR provides that legally enforceable obligations may be imposed on the recipient under:

(a) any law;

(b) any contract that imposes a standard of protection that is comparable to that under the PDPA, and which specifies the countries and territories to which the personal data may be transferred under the contract;

(c) any binding corporate rules that require every recipient of the transferred personal data to provide a standard of protection for the transferred personal data that is comparable to that of the PDPA, and which specify (i) the recipients of the transferred personal data to which the binding corporate rules apply; (ii) the countries and territories to which the personal data may be transferred under the binding corporate rules; and (iii) the rights and obligations provided by the binding corporate rules; and

(d) any other legally binding instrument.

Further, if the recipient organisation holds a "specified certification" that is granted or recognised under the law of that country or territory to which the personal data is transferred, the recipient organisation is taken to be bound by such legally enforceable obligations (PDPR, section 12). Under the PDPR, "specified certification" refers to certifications under the Asia Pacific Economic Cooperation Cross Border Privacy Rules ("**APEC CBPR**") System, and the Asia Pacific Economic Cooperation Privacy Recognition for Processors ("**APEC PRP**") System (PDPR, section 12).

From a practical compliance standpoint, organisations may refer to the ASEAN Model Contractual Clauses ("**ASEAN MCCs**") as a legal basis for cross border data transfers to streamline such data transfers. The ASEAN MCCs are contractual terms which set out the parties' baseline responsibilities, required personal data protection measures, and related obligations that protects the data of data subjects. While the adoption of the ASEAN MCCs is voluntary, organisations may include these contractual terms in their binding legal agreement when transferring personal data to each other across borders to simplify the process of drafting data transfer agreements, reduce the need for extensive legal negotiations and minimise the risk of non-compliance with data protection regulations. Notably, the PDPC has stated that the ASEAN MCCs can be used to fulfil the organisation's Transfer Limitation Obligation under the PDPA (PDPC's Guidance for Use of ASEAN Model Contractual Clause in Singapore, paragraph 3). Additionally, the ASEAN MCCs may also be adapted (with suitable modifications

in accordance with the principles in the ASEAN Framework on Personal Data Protection or as required by any ASEAN member state's law) at the organisation's discretion when transferring data within the same country or to non-ASEAN member states. However, organisations are reminded that the ASEAN MCCs are only baseline in nature. In this regard, organisations should check and to the maximum extent possible, comply with any additional sector-specific or specific ASEAN member state guidance or requirements in relation to data transfers.

4. Enforcement and Penalties

The PDPC is the regulatory authority responsible for enforcing the PDPA in Singapore. The PDPC has the authority to investigate complaints and take enforcement actions against organisations that fail to comply with the PDPA.

4.1. Investigation powers of the PDPC

The PDPC may commence an investigation either upon receiving a complaint from an individual against an organisation or of its own motion (PDPA, section 50).

Where the PDPC receives a complaint or other information that indicates that an organisation has, or may have, contravened the PDPA, the PDPC will first consider whether the matter may be more appropriately resolved by resolving the underlying dispute between the complainant and the organisation (PDPC Advisory Guidelines on Enforcement of the Data Protection Provisions ("**Enforcement Guidelines**"), paragraph 16.2). In this regard, the PDPC has the power to refer the matter to mediation or other modes of alternative dispute resolution (PDPA, section 48G).

The PDPC may commence an investigation into the conduct of an organisation if the PDPC considers that an investigation is warranted, based on the information it has obtained (whether through a complaint or from any other source).

The PDPC's powers of investigation include:

(a) the power to require production of documents and information (PDPA, Ninth Schedule section 1);

(b) the power to require the attendance of persons, and to orally examine and take statements from them (PDPA, Ninth Schedule section 1A);

(c) the power to enter premises without a warrant (PDPA, Ninth Schedule section 2); and

(d) the power to enter premises with a warrant (PDPA, Ninth Schedule section 3).

All organisations and individuals are required to comply with any notice or other requirement imposed by the PDPC pursuant to its powers of investigations. Any individual who obstructs or impedes the PDPC in the exercise of its powers, knowingly or recklessly makes a false statement to the PDPC, or knowingly attempts to mislead the PDPC shall be guilty of an offence under the PDPA. Convicted individuals can be liable, for a fine not exceeding S$10,000 or imprisonment for a term not exceeding 12 months or both. Organisations that are found to have committed such an offence are liable for a fine not exceeding S$100,000 (PDPA, sections 51(3)(ba), 51(3)(bb) and 51(6).

4.2. Power to issue directions to secure compliance

The PDPC has the authority to issue directions to ensure that an organisation complies with the PDPA (PDPA, section 48I). The PDPC may give the organisation or individual (as the case may be) such directions as the PDPC thinks fit in the circumstances to ensure the organisation's compliance with that provision. Under section 48I of the PDPA, The PDPC may also order any or all of the following directions:

(a) a direction to stop collecting, using or disclosing personal data in contravention of the PDPA;

(b) a direction to destroy personal data collected in contravention of the PDPA; or

(c) a direction to comply with any direction of the PDPC under section 48H(2) of the PDPA on the PDPC's power to review.

In the event an organisation does not comply with a direction under section 48I of the PDPA, the PDPC is empowered under section 48M of the PDPA to enforce the direction by registering it in the Singapore District Court. A registered direction or written notice has the same force and effect for the purposes of enforcement as if it is an order obtained in the Singapore District Court. Legal proceedings may thus be taken on the registered direction to enforce the direction (PDPA, section 48M).

4.3. Financial Penalties

The PDPC may impose financial penalties of up to S$1 million or 10% of the organisation's annual turnover in Singapore (where their annual turnover in Singapore exceeds S$10 million), whichever is higher (PDPA, section 48J).

In determining the financial penalty to be imposed, the PDPC would consider harm caused and culpability of the organisation is in their infringement of the PDPA. The extent of harm caused will take into account factors like the number of affected individuals, categories of affected personal data and duration of the incident. Culpability refers to the organisation's conduct in the incident. The PDPC will also consider the nature of the specific breach of the PDPA and the organisation's overall compliance with the PDPA (Enforcement Guidelines, paragraph 27.4).

Other relevant factors that the PDPC will take into account include whether the organisations took action to mitigate the effects and consequences of the noncompliance, the timeliness and effectiveness of that action, and whether the organisation or person had previously failed to comply with the PDPA (Enforcement Guidelines, paragraph 27.4).

4.4. Voluntary Undertakings

The PDPC has the power to accept a written voluntary undertaking from the organisation or person concerned, instead of carrying out an investigation or issuing directions (PDPA, section 48L). Generally, the voluntary undertaking process is intended to allow organisations with good accountability practices and an effective remediation plan to be given a window of opportunity to implement their remediation plans. In appropriate cases, organisations may undertake to improve their data protection practices (Enforcement Guidelines, paragraph 25.3).

The provision of a voluntary undertaking by a person or organisation is subject to the PDPC's acceptance. For example, the PDPC may not accept a voluntary undertaking in circumstances including but not limited to where the person or organisation's non-compliance with the PDPA

is wilful or egregious (Enforcement Guidelines, paragraph 25.4).

Where an organisation or person fails to comply with any undertaking in a voluntary undertaking, the PDPC may give the organisation or person any direction that the PDPC thinks fit in the circumstances to ensure the compliance of the organisation or person with that undertaking (Enforcement Guidelines, paragraph 25.5).

5. Practical steps for Compliance

This section will identify some general challenges typically faced by small and large organisations in respect of PDPA compliance and highlight various existing initiatives in Singapore which can be leveraged by organisations.

An important note is that ***small and large organisations are subject to the same obligations under the PDPA***. However, the challenges they face in complying with the same might differ.

5.1. Challenges and Practical Solutions for Small Businesses

The challenges faced by smaller businesses primarily stem from them having limited resources and the numerous obligations imposed by the PDPA and related legislation. For instance, small organisations may not be fully aware of their obligations under the PDPA, as well as their organisation's business-critical data infrastructure and sources.

Practical solutions and initiatives by the Infocomm Media Development Authority ("**IMDA**") for small businesses include the following:

Appoint a Data Protection Officer and implement training

Every organisation, regardless of size, must appoint a DPO to oversee data protection responsibilities to ensure compliance with the PDPA (PDPA, section 11(3)). The DPO also serves as an important touch point to ensure that the business is complying with its obligations under the PDPA (please refer to Section 3.1 (DPO: Qualifications and Responsibilities) above).

The DPO can undergo training to better understand the organisation's obligations under the PDPA and transfer this knowledge to the rest of the organisation. The PDPC provides a DPO competency framework and training roadmap that can assist in the preparation of the DPO (please see here for more information on PDPC's DPO Competency Framework and Training Roadmap.).

Develop a Data Protection Policy

The business can and should create a clear and concise data protection policy that outlines how personal data is collected, used, disclosed, and protected and ensure that employees are trained on this policy. These are important in ensuring compliance with the business's Accountability Obligation (PDPA, section 12).

The business can obtain legal assistance in crafting a suitable and compliant Data Protection Policy. Otherwise, the PDPC has also produced numerous free-to-use guides and tools to assist organisations in their PDPA compliance and can be used as reference in the crafting the Data Protection Policy. Some examples include:

(a) the PDPC Guide to Developing a Data Protection Management Programme (please

see here);

(b) the PDPC Guide to Data Protection Impact Assessment (please see here); and

(c) the PDPA Assessment Tool for Organisations (please see here).

Implement Data Protection Measures

The company can adopt the following data protection measures that can also be provided for within the company's data protection policy:

(a) Data Minimisation: Collect only the personal data necessary for business purposes (PDPC Advisory Guidelines on the Personal Data Protection Act for Selected Topics ("**Guidelines for Selected Topics**"), paragraph 3.11).

(b) Access Controls: Restrict access to personal data to authorised personnel only, preventing unauthorised access and ensure that personal data is only used for legitimate purposes (Guidelines for Selected Topics, paragraph 3.16).

(c) Data Encryption: Use encryption to protect personal data during storage and transmission. Encryption adds an additional layer of security (Guidelines for Selected Topics, paragraph 3.7(d)).

Frameworks and Certifications: Data Protection Essentials Programme

Recognising the challenges specifically faced by smaller organisations, the IMDA has launched the Data Protection Essentials ("**DPE**") framework which provides a baseline standard of data protection that Small and Medium Enterprises ("**SMEs**") can use to safeguard their customers' personal data, build trust with their stakeholders and recover swiftly in the event of a data breach (please see here for more information about the DPE Programme.).

Besides helping SMEs comply with the PDPA by providing practical guidance, the DPE framework also grants its participants added benefits. Participants who fulfil all requirements will be recognised for their efforts by being listed on the IMDA website with use of the designated DPE logo; and in the event of a data breach, DPE certification would be considered a potential mitigating factor by the PDPC (please see here for more information on the benefits of the DPE Programme.).

To further assist SMEs in applying the DPE framework, IMDA offers free-to-use tools such as the "DPE Checklist" on their website to help users identify gaps in their existing data protection measures in relation to the DPE framework and provide practical recommendations on how to fill such gaps (please see here for the DPE Checklist.).

While the DPE framework provides a useful starting point for SMEs embarking on their journey toward compliance with the PDPA, it should not be viewed as an all-encompassing solution. Although the framework offers a structured pathway and practical tools to help SMEs establish a baseline of data protection and security practices, achieving sustained compliance and building a resilient data protection regime requires SMEs to take additional steps. They should eventually go beyond the foundational practices outlined in the DPE framework by developing customised, robust mechanisms tailored to address the unique risks, challenges, and operational complexities specific to their own businesses.

Upscaling programmes: Better Data Driven Business Programme

As SMEs grow and continue to improve their data protection practices, they may consider participating in additional programmes to further enhance their compliance and build credibility. These options may be viewed as practical milestones, similar to the DPE programme, that SMEs can achieve along their compliance journey. One such option is the Better Data Driven Business ("**BDDB**") programme developed by IMDA (Please see here for more information on the Better Data Driven Business Programme.).

In essence, the BDDB enables businesses to:

(a) Collect necessary data safely: Ensure data is gathered in compliance with relevant legal and security standards;

(b) Combine data across systems with adequate protections: Allow businesses to integrate and analyse data from various sources while maintaining security and privacy; and

(c) Share data externally with partners and suppliers safely: Ensure that any sharing of data with third parties is in line with the requirements of the PDPA.

5.2. Challenges and Practical Solutions for Large Corporations

While large corporations generally have more resources at their disposal, the volume of data and extent of compliance required of them is often correspondingly more. Further, large corporations may engage in more complex business activities such as multi-jurisdictional data trading and data processing, which would require added consideration of the data transfer and data intermediary management obligations. Overall, although subject to the same obligations, large corporations face their own set of compliance challenges which are distinct from small businesses.

Practical solutions and initiatives by the IMDA for large corporations include the following:

Conduct Regular Data Protection Audits

Perform regular audits to identify and address potential data protection risks. This includes reviewing data processing activities and ensuring compliance with the PDPA. Audits help organisations identify vulnerabilities and take corrective actions before issues escalate.

Establish Cross-Border Data Transfer Policies

Personal data must not be transferred to a country or territory outside Singapore except in accordance with the requirements prescribed under the PDPA, which include ensuring that the overseas recipient is bound by legally enforceable obligations to provide a standard of protection to the personal data so transferred that is comparable to the protection under the PDPA (PDPA, section 26).

Large organisations that deal with cross-border transfer of data both within the organisation and with other third parties, should develop policies and procedures for transferring personal data across borders, ensuring compliance with the PDPA and other relevant regulations. Cross-border data transfer policies should include mechanisms such as Binding Corporate Rules within the organisation or standard data transfer agreements or contractual clauses when dealing with third parties to ensure that personal data is protected when transferred

internationally (Guidelines, paragraph 19.5) (please refer to Section 3.5 (Data Processing and Cross-Border Transfers) above).

Free-to-use guides for dealing with data intermediaries

Due to the relatively larger volume of data typically handled in large organisations, it is not uncommon for these organisations to engage data intermediaries to support their compliance efforts. However, it is crucial to recognise that the organisation remains responsible for the personal data processed, even when it is handled by an intermediary. Under section 4(3) of the PDPA, the organisation is deemed to "have the same obligation under [the PDPA] in respect of personal data processed on its behalf and for its purposes by a data intermediary as if the personal data were processed by the organisation itself".

Large organisations can leverage the various free-to-use guides and tools made publicly available by the PDPC. One such guide which would be particularly relevant to larger organisations is the Guide to Managing Data Intermediaries ("**Data Intermediaries Guide**") (please see here for the Guide to Managing Data Intermediaries.). Broadly, the guide covers the following key areas: (1) Governance and Risk Assessment; (2) Policies and Practices; (3) Service Management; and (4) Exit Management.

Frameworks and Certifications: Data Protection Trustmark

An alternative way for larger organisations to achieve compliance is through participation in certification programmes such as the Data Protection Trustmark ("**DPTM**") offered by the IMDA. DPTM is a voluntary enterprise-wide certification that enables organisations to demonstrate their commitment to accountable data protection practices. Achieving the DPTM certification can enhance a business's competitive advantage and help build trust with customers and stakeholders (Please see here for more information on the DPTM.).

The DPTM Certification Checklist serves as a valuable set of practical guidelines for compliance (Please see here for the DPTM Certification Checklist.). Organisations can use this checklist to assess their readiness for applying the certification and to direct the enhancement of their compliance efforts. Broadly, the checklist is divided into four main principles: (1) Governance and Transparency; (2) Management of Personal Data; (3) Care of Personal Data; and (4) Individuals' Rights.

6. Specific Challenges for Chinese Companies

As Singapore continues to strengthen its position as a global business hub, a significant number of Chinese enterprises consider Singapore as the first stepstone of their global expansion roadmap. While seeking to expand their operations in Singapore, companies must be mindful of the challenges of compliance with local laws, including the PDPA. We have listed out below some typical issues that are commonly faced by Chinese companies.

(a) Cross-border Data Transfers

Cross-border data transfers are an integral part of operations for Chinese companies with Singapore subsidiaries, branches or overseas headquarters. Many Chinese companies may also centralise the management of their overseas data by employing cloud solutions in Singapore through their Singapore-based subsidiaries or branches.

Though the PDPA does not impose data localisation requirements in relation to personal data, it requires the transferring origination to demonstrate that the recipient jurisdiction

offers a comparable level of data protection or implementing strict safeguards, such as contractual clauses or corporate rules that ensure data protection. This can be particularly challenging when aligning with the different standards and regulations in China.

(b) Differences in Data Protection Standards

The variance in data protection standards between China and Singapore also poses a challenge for Chinese companies. These companies must elevate their data protection measures to meet the standards of both countries, which can involve significant adjustments to their existing policies, training, and operations.

Meanwhile, some foreign authorities may also demand extensive access data for investigations especially where state or public security is involved. As such, companies may be required to comply with regulators and law enforcement agencies' investigation procedures or requests for information in other jurisdictions, which may pose problems to compliance with the PDPA. With such access requests from foreign authorities, companies may find it difficult to fully comply with the PDPA obligations.

(c) Data Protection Officer Requirements

The PDPA mandates that every organisation shall appoint a DPO responsible for compliance of the PDPA. Chinese companies must ensure that their DPO is well-versed in Singapore's data protection laws and capable of bridging cultural and operational differences between Chinese and Singaporean practices. For Chinese companies just come to Singapore and are lack of competent candidate of DPO, an external DPO, such as a data protection lawyer in Singapore, could also be considered.

(d) Public Perception and Trust

Effective data management is critical not just for legal compliance but also for maintaining consumer trust. Failures in data protection can lead to public mistrust and reputational damage, which can adversely affect business operations. Chinese companies must prioritize robust data protection practices to build and maintain this trust in Singapore.

(e) Legitimate interests as a basis of processing data without consent

In Singapore, legitimate interests are a clearly defined alternative basis from consent for the collection, use and disclosure of personal data. China's data protection laws currently do not have anything similar to this legitimate interests basis. Chinese companies may therefore face challenges in complying with the detailed requirements under this legitimate interests basis, should they choose to rely on it rather than obtaining consent.

Appendices

6.1. Sample Checklists

(a) Adapted from the PDPA compliance checklist for organizations' data protection policies and practices (PDPC | PDPA Assessment Tool for Organisations)

No.	Point of compliance	Response
	Preliminary	
1	Does your organisation collect, use or disclose personal data? (This would be data like names, contact numbers, addresses of stakeholders such as employees, customers, contractors, donors, volunteers etc)	☐ Yes ☐ No
2	Is the collection, use or disclosure required or authorized under a written law other than the PDPA? (Some examples include the Telecommunications Act, Employment Act, Banking Act, Insurance Act, etc. If you are unsure, then kindly select "No".)	☐ Yes ☐ No
	Consent	
1	Your organisation obtains consent from individuals or relies on an exception to consent for the collection, use or disclosure of their personal data.	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
2	Your organisation notifies and seeks fresh consent from individuals to use their personal data for a new or different purpose.	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
3	Your organisation has channels for and responds to withdrawal of consent requests by individuals.	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
4	Your organisation ensures that the person providing consent on behalf of an individual is validly acting on behalf of that individual.	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
5	Your organisation ensures that third party sources which your organisation obtained personal data from, had obtained valid consent from individuals.	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
6	Your organisation has conducted the necessary assessments to utilise deemed consent to collect, use, or disclose personal data for a purpose.	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
7	Your organisation has put in place the necessary processes including conducting an assessment to utilise exceptions to collect, use, disclose personal data for a purpose.	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
	Purpose Limitation	
1	Your organisation only collects, uses or discloses personal data for reasonable purposes that individuals had been informed and had	☐ Implemented ☐ Partially implemented

	consented to.	☐ Not implemented ☐ Not applicable
Notification		
1	Your organisation informs individuals of the purposes for collecting, using or disclosing their personal data on or before collecting the data.	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
Access and correction		
1	Your organisation has the processes to preserve a complete and accurate copy of the personal data (for at least 30 calendar days) after rejecting an access request.	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
2	Your organisation has provided ways to allow access and correction requests to be made by individuals of their personal data in your custody.	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
3	Your organisation responds to access requests by individuals as soon as reasonably possible.	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
4	Your organisation informs the individual making the access request of any fees associated with processing the access request.	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
5	Your organisation responds to requests by individuals to correct their personal data as soon as practicable.	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
6	Your organisation informs the individual of the time needed to respond to an access or correction request.	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
7	Before responding to an access or correction request, your organisation exercises due diligence to verify the identity of the individual making the request or verify that the third party is legally authorised to act on the individual's behalf.	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
Accuracy		
1	Your organisation ensures that personal data collected from individuals is accurate and complete.	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
2	Your organisation ensures that personal data of individuals collected from a third-party source is accurate and complete.	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
Protection		
1	Your organisation has in place appropriate technical security measures to protect personal data in your organisation's possession or control.	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable

2	Your organisation has in place appropriate physical security measures to protect personal data in your organisation's possession or control.	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
3	Your organisation has in place appropriate administrative measures to protect personal data in your organisation's possession or control.	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
4	Your organisation conducts risk assessments to determine appropriate security measures to protect personal data in your organisation's possession or control.	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
5	Your organisation has measures in place to prevent the accidental disclosure of personal data.	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
6	Your organisation ensures that appointed information and communications technology ("ICT") service providers can provide adequate levels of protection and security to protect personal data in your organisation's possession or control.	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
7	Your organisation ensures that the ready-made software used can meet and provide adequate levels of security to protect personal data in your organisation's possession or control.	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
8	Your organisation ensures that third party organisations that processes personal data on your organisation's behalf, protects personal data in compliance with the PDPA.	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
Retention limitation		
1	Your organisation stops retaining personal data when it does not have legal or business reasons to do so.	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
2	Your organisation has defined the retention period and disposal requirements for third party service providers that process personal data on your organisation's behalf.	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
3	Your organisation has processes in place to dispose of personal data, including data held by third parties.	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
Transfer limitation		
1	Your organisation ensures that personal data is only transferred to organisations in overseas jurisdictions that have a comparable standard of data protection as the PDPA and PDPRs.	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
Accountability		
1	Your organisation has appointed a data protection officer (DPO) or office.	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable

2	Your organisation adopts accountability tools to assist organisations in demonstrating and practicing accountability.	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
3	Your organisation's DPO business contact information is made available to the public.	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
4	Your organisation has developed and implemented policies and practices to comply with the PDPA, including the development and implementation of a Data Protection Management Programme (DPMP).	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
5	Your organisation has policies and practices to respond to queries and complaints related to personal data protection.	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
6	Your organisation has clear reporting channels on personal data protection issues under the organisation.	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
7	Your organisation educates all staff on the organisation's personal data protection policies and practices.	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
Breach notification		
1	Your organisation has put in place measures to monitor for potential data breaches.	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
2	Your organisation has policies and practices to respond to data breaches	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
3	Your organisation has established a Data Breach Management Plan to respond to data breaches related to personal data protection	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
4	Your organisation runs regular breach simulation exercises to prepare to respond to data breaches in a prompt and effective manner.	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
Do Not Call regime		
1	Your organisation adheres to Do Not Call (DNC) requirements when sending telemarketing messages to Singapore telephone numbers.	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
2	Your organisation checks the Do Not Call (DNC) Registry before sending telemarketing messages.	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
3	Your organisation documents its checks with the DNC Registry.	☐ Implemented

		☐ Partially implemented ☐ Not implemented ☐ Not applicable
4	Your organisation has obtained and documented clear and unambiguous consent from individuals to send them telemarketing messages without checking the DNC Registry.	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
5	Your organisation ensures that third party service providers engaged for telemarketing activities, adhere to DNC requirements.	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
Internal compliance		
1	Your organisation has developed and implemented policies and practices to comply with the PDPA, including the creation of a Data Protection Management Programme (DPMP).	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
2	Your organisation educates all staff on its personal data protection policies and practices.	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
3	Your organisation regularly reviews and updates its data protection policies and monitors compliance.	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
4	Your organisation conducts risk and impact assessments to identify and address data protection risks.	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
5	Your organisation incorporates Data Protection by Design into products, services, systems, or processes.	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
Data Breach		
1	Your organisation has put in place measures to monitor for potential data breaches.	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
2	Your organisation has policies and practices to respond to data breaches (i.e. personnel roles, reporting timelines, and notification processes).	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable
3	Your organisation has established a Data Breach Management Plan to address breaches related to personal data protection.	☐ Implemented ☐ Partially implemented ☐ Not implemented ☐ Not applicable

6.2. Sample templates (e.g., sample consent forms or sample clauses)

(a) Sample Consent Clause for the Sending of Marketing Material (sampleclausesforobtainingandwithdrawingconsent8may2015.pdf)

(b) Guide on Data Protection Clauses for Agreements Relating to the Processing of Personal Data (Guide-on-Data-Protection-Clauses-for-Agreements-Relating-to-the-Processing-of-Personal-Data-1-Feb-2021.pdf)

(c) Sample clauses for employees and job applicants (Microsoft Word - Sample Clauses and Templates for Employees and Job Applicants - 171017)

Please see PDPC | Help and Resources for a full list of resources from the PDPC.