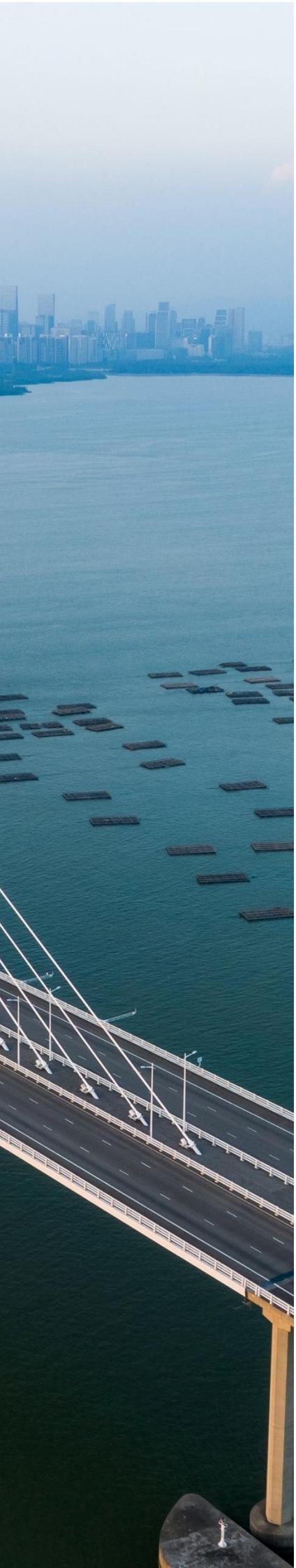
Enterprises in the GBA: Digitization opportunities, security challenges and response strategies

EY 安永
Building a better working world

Summary

The emergence and development of the Guangdong-Hong Kong-Macau Greater Bay Area (GBA) provide a major driving force for digitalization. Governments across the GBA have already released or will shortly release a series of measures to safeguard data security and to ensure compliance in the digitalization process, which provide strong support to data flow across governments and enterprises and across different enterprises in a cross-border data flow scenario. While enterprises enjoy the benefits of enabling policies and more data resources, they also face more data security challenges, including balancing business needs while coping with the different data security regulations of three regions, and responding to security safeguard challenges arising from the difference in network and other conditions across the three regions. To cope with the special challenges faced by digitization, enterprises should plan and set unified compliance standards and systems, build effective compliance capability in data security, improve data security management and defense capability. Only with effective security safeguard and compliance may enterprises sustain long-term development.



Contents

1 Digitalization is a core driver of GBA development

In February 2019, China's State Council formulated the *Outline Development Plan for the Guangdong-Hong Kong-Macao Greater Bay Area* ("Development Plan"), and it was stated that by 2035, the GBA should become an economic system with mode of development mainly supported by innovation. In addition to strategic targets, the Development Plan also listed a series of strategic initiatives mainly driven by digitalization, including:

Enhancing and upgrading information infrastructure

It was stated in the Development Plan that there will be a comprehensive planning for a new generation of information infrastructure to be based on Internet Protocol version 6 (IPv6), and based on this, the internet will be upgraded and transformed, and bandwidth capacity will be expanded. In driving the construction of city clusters in the GBA with wireless and fiber broadband, there is a need to set up unified standards, open data ports, push forward mutual recognition of digital signature certificates, and establish an interconnected application platform. Smart city development and digital government construction in the Shenzhen Special Economic Zone was realized by optimizing information infrastructure, opening over 2,000 data interfaces and breaking the information silos of enterprises, which is an outstanding achievement of the Development Plan's implementation. In addition, it was also stated in the Development Plan that when optimizing information infrastructure, there is a need to strengthen protection of communication networks, major information systems and major data resources, build a sound information security warning mechanism, improve the network security protection level, and realize the objectives of unification of standards, data opening, smart development of cities and security safeguard of information.

Expediting the development of the advanced manufacturing industry

The Development Plan provides that the manufacturing industry should undergo structural advancement and optimization through in-depth integration of the internet, big data and artificial intelligence with the real economy, in order to foster in-depth cooperation between upstream and downstream industries along the industry chain, so as to improve innovative development of the manufacturing industry system in the GBA. According to statistics of the Department of Industry and Information Technology of Guangdong Province, there are 15,000 enterprises which realized digital transformation and 500,000 enterprises which used cloud technology in the province. In the *Implementation Plan for the Digital Transformation of the Manufacturing Industry in Guangdong Province (2021-2025)* and *Several Policies and Measures for Digital Transformation of the Manufacturing Industry in Guangdong Province* released last year, it was mentioned that industrial enterprises will be driven to use new generation of information technology in order to realize digital transformation, and they will be encouraged to migrate to the cloud and use the cloud. Use of artificial intelligence is encouraged to drive industrialization, reduce costs, and improve quality and efficiency.

Nurturing and strengthening strategic emerging industries

As early as 2017, *the Guidance Catalogue of Key Products and Services in Strategic Emerging Industries* issued by the National Development and Reform Commission already laid out the scope of strategic emerging industries, fostering the growth, transformation and upgrading of economy and quality development. There are several places in the Development Plan mentioning that strategic emerging industries will be vigorously developed in the GBA, and the development needs to fully leverage the strengths of scientific research and development (R&D) resources and high-tech industrial base in major cities such as Hong Kong, Macau, Guangzhou and Shenzhen to drive development of the seven major strategic emerging industries and the four major industries in the future. It was also mentioned that the new generation of information technology, biotechnology, IoT, artificial intelligence, big data, 5G mobile network, intelligent robotics, the BeiDou Navigation Satellite System and other emerging industries are to be nurtured with priority; and major projects in strategic emerging industries covering information consumption, new health care technologies, hi-tech service industry and others will be implemented to drive digital development and foster transformation and upgrading of the economy.

Expediting the development of modern service industries

With improving technological capability, edges in digitization development and innovative breakthroughs, professional service industries in the GBA are expediting digital transformation. The Development Plan provides that it is necessary to leverage the economic and finance advantages of Hong Kong, Macau, Guangzhou and Shenzhen to build an international finance hub and vigorously develop a secure financial industry with specific characteristics in the GBA. Application of big data, artificial intelligence, blockchain and other technologies in finance will drive the digital transformation of traditional financial service enterprises. The GBA is expected to have more effective, secure and stable financial services. In addition to the financial service industry, many logistics, catering service and other industries also start to use or leverage the abundant supply of networks and skilled labor, sound logistics infrastructure, government incentives and capital support in the GBA to continue to develop business and expedite transformation and upgrading despite the pandemic.

The strategic initiatives above are closely related with digital development or fall under the category of digital economy or are dependent on digital development. Digital development already becomes a major engine and infrastructure in the GBA.

After the release of the Development Plan, the GBA announced new policies one after another. The governments have made several new regulations and policies, such as regulations released by Department of Industry and Information Technology of Guangdong Province, the *Overall Plan for the Construction of Guangdong-Macao In-Depth Cooperation Zone in Hengqin* issued by *State Council of the PRC,* the *Plan for Comprehensive Deepening Reform and Opening Up of the Qianhai Shenzhen-Hong Kong Modern Service Industry Cooperation Zone* released in Shenzhen, and Hong Kong's Policy Address released in the past years. These policies will further strengthen exchange of opinions and cooperation among GBA cities, including Hong Kong, Macau, Shenzhen and Zhuhai in digital infrastructure, digital transactions, digital finance, high-tech and smart manufacturing.

2 Data governance and data security will be a major area in development

Digital development must involve effective data governance and data security and ensuring effective data governance and data security is the prerequisite of fostering economic integration among the GBA as well as the cross-strait three regions. To be in line with the planning with digital as the development engine, the GBA already gradually laid down requirements in developing data governance and security and implementation initiatives concerned. On 5 July 2021, the People's Government of Guangdong Province issued the *Action Plan for the Reform of the Market-oriented Allocation of Data Elements in Guangdong Province* ("Action Plan") which is the first market-oriented allocation of data elements document in mainland China. It listed 24 tasks in five major areas, including releasing public data resources' value, energizing social data resources, strengthening integration of data resources and their innovative applications, fostering data transactions and flow, and improving data security safeguard to accelerate the cultivation of the data elements market.

In the context of digital development, in addition to the action plans above, the governments in the GBA are introducing or will soon introduce a series of measures to safeguard data security and compliance, and provide strong support for accelerating the flow of data between governments and enterprises, among enterprises, and across borders. Such measures include but not limited to the following:

Unification of data standards, compliance standards and security standards

▸ Data standards

Professional research on data elements standardization is gradually being conducted and pilots of data elements standardization in phases and in different areas in the GBA will take place to support industrial federations, chambers of commerce, enterprises, universities and research institutes in studying the development of standards in data capture, process, application and quality management[1], laying the technical foundation for data flow.

▸ Compliance standards

As Guangdong and the Hong Kong and Macau SARs have different legal systems, the setting up of basic system and standards in the GBA, covering requirements in data flow system, sound data equity, transaction flow, cross-border transfer and security safeguard, clarifying rights and responsibilities of data subjects, data control parties, data use parties, and protecting the interests of data subjects[2] are one of the prerequisites of GBA development.

The GBA is now actively driving relevant work and is studying how to set up a data system and compliance standards with GBA characteristics that comply with the national law and regulations to foster the interchange of data.

1 Article 16 of the Action Plan for the Reform of the Market-oriented Allocation of Data Elements in Guangdong Province
2 Article 18 of the Action Plan for the Reform of the Market-oriented Allocation of Data Elements in Guangdong Province

Security standards

In strengthening data security safeguard, it was stated in the Action Plan and other guides concerned that there will be development in three areas: (1) setting up a data classification and grading and privacy protection system, and a data classification and ranking and protection system led by the governments and participated by various parties with clear definition of responsibilities of the parties; and development of a major data catalog for provincial and municipal departments and industries and areas concerned to provide priority protection of data listed in the catalog. There should also be a sound data privacy protection and security review system, and responsibilities in data security protection, including government departments, enterprises and public institutions and the public need to be fulfilled to improve data protection, including personal privacy, personal information, commercial secrets and confidential commercial information; (2) a need to improve the scheme for data security management, data security risk assessment, reports, information sharing, monitoring and early warning and contingency handling; and support the departments, industrial associations, enterprises, academic and scientific research institutions, and professional institutions concerned in their collaboration in data security risk assessment, prevention and handling; (3) a need to improve the technical data security system; build a coordinated security safeguard system with integration of cloud computing, IoT and digital solutions; leverage data protection measures, blockchain and other new technologies including reliable identity authentication, data signature, interface authentication and data sourcing; and improve security safeguard for computing resources and data resources so as to strengthen data security protection capabilities. These not only show the planning of the People's Government of Guangdong Province in security standards but also show the direction of concerted efforts of various governments in the GBA.

Unified public data resources system

In addition to actively implementing unified standards, the GBA is also actively stepping up the construction of an unified public data resources system, improves basic databases covering population, legal entities, spatial geography and digital passports, and further expanding the databases of credit, finance, health care, transport, ecology, market monitoring, culture and travel, social relief and investment projects, so as to speed up data flow between governments and enterprises. According to statistics of Guangdong Provincial Government Service Data Administration Authority, as at the end of August 2022, The first-level data element market led by the administrative mechanism has published a total of 33,300 data resource catalogs, providing 51.786 billion data call services for 1,144 business systems of 1,567 government departments[3].

During fostering of data sharing and flow, the Action Plan also clearly listed public data management mechanism and public data security safeguard requirements regarding further orderly opening of public data, including listing requirements of various levels of administrative authorities and public institutions in data capture, gathering, sharing, use and management with formulation of Guangdong Provincial Public Data Management Measures[4]; and it is sought to explore the construction of a public data opening list system with the formulation of the Interim Measures for Public Data Open in Guangdong Province to improve the public data opening catalog management scheme and standards, targeted opening of public data and management system for authorized opening[5].

Driving orderly flow of data across the GBA

Current priorities of the GBA are to drive construction of a big data center at the GBA, support construction of Nansha (Guangdong-Hong Kong-Macau) Data Cooperation Pilot Zone and Guangdong-Macao In-Depth Cooperation Zone in Hengqin, explore the construction of "data customs", and initiate the review, assessment and monitor of cross-border data flow. Fostering cross-border flow of data not only involves public data, financial data and daily business data of enterprises, but also includes health care and other scientific research collaboration project data. There should be orderly fostering of cross-border flow of data resources to gradually realize cross-border interconnection of scientific research data, and a series of data application model cases is to be built for industrial development, social governance, services for the public and more.

It can be readily seen that the GBA is stepping up improvement of data resource development and use as well as the policy environment for governance and protection of data, regulation to cope with new governance issues arising from new economy, and issue of a list of policies to deal with data transactions, cross-border data transfer, personal information and privacy protection, and data security strategies to build a good foundation for a sound data flow mechanism.

3 *Guangdong Provincial Government Service Data Administration Authority. Jingjinet / Interview with Yang Pengfei: Guangdong Data Exchange will be "co-constructed by provinces and cities, coordinated by Guangzhou and Foshan" and is expected to be completed before the end of the year, http://www.21jingji.com/article/20220801/herald/193999eb904a942a317130d2b84f1161.html#:~:text=%E9%80%9A%E8%BF%87%E2%80%9C%E5%BC%80%E6%94%BE%E5%B9%BF%E4%B8%9C%E2%80%9D,%E4%B8%AA%E6%95%B0%E6%8D%AE%E6%9C%8D%E5%8A%A1%E6%8E%A5%E5%8F%A3%E3%80%82*

4 Article 2 of the Action Plan for the Reform of the Market-oriented Allocation of Data Elements in Guangdong Province

5 Article 6 of the Action Plan for the Reform of the Market-oriented Allocation of Data Elements in Guangdong Province

3 Favorable conditions for enterprises

With in-depth construction at the GBA, a series of major digitalization initiatives will be launched one by one to create a favorable policy environment to safeguard data security and ensure effective and standard data flow and use. These are certainly major favorable conditions for enterprises in the GBA. Such initiatives include:

Facilitating data flow

The GBA is one of the regions in China which is most open and with strongest economic vigor. According to the *China Urban Agglomeration Integration Report* released by the China Development Research Foundation under the Development Research Center of the State Council, the GDP of the Guangdong-Hong Kong-Macao Greater Bay Area will reach 14.76 trillion yuan in 2022, surpassing the Tokyo Bay Area and becoming the largest bay area by its economy. Economic integration and movement of people among 9+2 cities in the GBA for years is very intensive. With more in-depth development of the GBA, there are already major breakthroughs in bottlenecks in interconnection regarding flow of people, cargos and capital in the area. Construction of data centers and public data resources systems and exploration of cross-border data transfer, including "data customs" will further break through barriers in data flow systems and will further facilitate data flow environment in the area. With implementation of *Cybersecurity Law of the People's Republic of China*, *Data Security Law of the People's Republic of China* and *Personal Information Protection Law of the People's Republic of China*, *Measures for the Security Assessment of Outbound Data Transfer* in mainland China one after another, balancing compliance in cross-border data flow and meeting business needs are major areas to be improved by enterprises in the GBA. In the foreseeable future, exploration of measures to enable cross-border data transfer in the GBA will provide some considerations for the enterprises to solve the issue and facilitate data transfer which will become their competitive advantage.

More data resources may be used

Convenient data flow and readily accessible data resources mean enterprises in the GBA may fully take advantage of accessing a large amount of data and having countless applications which will further bring the potential of data elements into full play and drive innovative-driven development.

In addition, the GBA is driving opening and integration of public data resources in various places and is actively exploring how to open resources concerned to enterprises provided that the data will be kept secure, and compliance of data transfer is ensured. This means in the future, enterprises in the GBA will not only have convenient cross-border transfer of internal data but will also be able to exchange data of enterprises between them which complies with regulations and will be able to fully leverage public data to maximize effectiveness in data decisions and applications.

The following are some data application scenarios in the GBA:

Application scenarios in finance

According to the latest data of the Global Financial Centres Index (*GFCI*), in 2022, Hong Kong, Shenzhen and Guangzhou are among the top 30, ranked third, 10th and 24th respectively. There is a rare concentration of city financial centers in the GBA. In the future, digital resources will further enhance the financial service experience of GBA users and enable the emergence of a more stable financial system. Financial institutions in the GBA may drive remote cross-border identity authentication with e-ID and e-KYC platforms built jointly by the three cities and provide more convenient financial services for the users which will further improve capital liquidity in the GBA. The digital financial system constructed will also meet the risk management demands of financial institutions, such as anti-money laundering. In addition, financial institutions in the GBA may also legally use the large number of cross-industrial data in finance, e-commerce, the internet and financial technology in the GBA; and integrate user data, credit data and behavior data for data modelling and conduct precise mapping of users with big data processing technology to trace and analyze consumption behavior of users as well as their risk and revenue appetite and information on other features so as to recommend products and services based on the preferences of users, do targeted marketing and provide better services to customers. At the same time, they may take the initiative to maintain and manage customer relations based on customer attrition warning model according to the historical transaction model. In addition, financial institutions in the GBA may further leverage big data to analyze customer behavior, creditability and assets and liabilities conditions, conduct comprehensive assessment of their credit risks and set up a sound risk control system

Application scenarios in health care

Under the pandemic, using big data analysis to develop effective public health care development strategies already becomes one of the priorities of governments and public health care institutions. They may trace the infected based on big data to control spread of the virus as much as possible, and leverage health care big data to take the initiative to allocate medical resources, reduce major diseases and the costs of treatment effectively, reduce diseases and promote health in general.

In addition, convenient data flow and rich data resources are also indispensable in the health care industry. The level of medical service digitalization in the GBA is increasing. Guangzhou, Shenzhen, Zhuhai, Foshan, Huizhou, Zhongshan and Jiangmen are the first seven cities which already set up municipal health care information platforms for all people and achieve interconnection, data sharing and business coordination among major health care institutions in the municipals. There is a large flow of population in the GBA. In recent years, Guangdong citizens travel south to Hong Kong and Macau to do body checks, receive dental and aesthetic medical treatments, and have major operations. It is also increasingly common for Hong Kong and Macau citizens to travel north to medical institutions and homes for the elderly in other cities in the GBA to receive health care services. Sharing and flow of data is the foundation of health care information integration in the GBA and will further lead to more effective use of medical resources in the area which is a major factor to enable citizens in the area to enjoy convenient and quality medical service in various cities in the GBA.

Application scenarios in e-commerce logistics

Industrial digital structure in the GBA keeps upgrading and it gradually becomes a major force to drive the digital economic development in the area. Scale of information consumption and e-commerce transaction volume in the GBA ranks first in the nation with cross-border e-commerce transaction volume accounting for almost 70% of the total, and mobile payment accounting for 30% of the total of the nation. In recent years, e-commerce logistics enterprises developed many new cross-border ecommerce services, such as cross-border payment service, overseas warehouse service, cross-border e-commerce language service and cross-border data service. During the whole lifecycle of cross-border e-commerce activities, customs and other government departments, domestic and overseas consumers, cross-border e-commerce enterprises, platform enterprises, domestic service providers and other enterprises interact intensively online and offline, and there is interaction of data among various institutions. With big data, cloud computing and construction of other smart infrastructure, digitalization of information at each part of logistics and online connection is realized which will drive transparency of logistics processes and help e-commerce logistics enterprises in the GBA to effectively improve quality and effectiveness and lower costs and to enable joint development of cross-border e-commerce and logistics in the big data era.

Improvement of digital infrastructure

Sound network and computing infrastructure systems are another inherent advantage of enterprises in the GBA. It was stated in the Development Plan under the 14th Five-Year Plan to expedite digital development and build a digital China. It was also explicitly stated in the 14th Five-Year Plan for National Economic and Social Development and *the Outline Plan of Long-Range Objectives Through the Year 2035 unveiled by* the Guangdong provincial government to construct a digital GBA and a cross-border big data center covering Guangdong, Hong Kong and Macau[6]. It was explicitly stated in the Guiding Opinions regarding Accelerating the Construction of a Coordinated Innovation System for the Nationwide Integrated Big Data Center released by National Development and Reform Commission at the end of 2020 that national hub nodes of big data centers are to be built in Beijing-Tianjin-Hebei, the Yangtze River Delta, the GBA, Chengdu-Chongqing and other major regions. Meanwhile, the GBA has two national supercomputing centers in Guangzhou and Shenzhen with leading computing speed and integrated technological level according to world standards. The overall standard of information infrastructure keeps improving, and capacity of backbone networks and metropolitan area networks keep expanding and the networks are continuously being upgraded. In the data center industry, a hub was formed in Guangzhou, Hong Kong and Shenzhen with tiered radiation in industries in the surrounding areas. Server availability and data storage capacity in these three cities rank first in China. According to data center planning stated in the *Overall Layout Plan for 5G Base Stations and Data Centers in Guangdong Province (2021-2025)*, dual-core nine centers are planned to be built in the province such that there will be two hub data center regions with small latency delays in Guangzhou and Shenzhen, and there will be nine data center cluster regions in Shantou, Shaoguan, Meizhou, Huizhou, Shanwei, Zhanjiang, Zhaoqing, Qingyuan and Yunfu. By 2022, there will be equivalent to around 470,000 standard cabinets in the province and average availability is around 65%. By 2025, the total number of standard cabinets in the province will be around 1 million with average availability at around 75%[7].

In addition, the GBA is different from Beijing-Tianjin-Hebei and the Yangtze River Delta regions, with its unique diversified systems. There are two special economic zones in Shenzhen and Zhuhai; three areas in Nansha in the Guangdong Free-trade Zone, Qianhai and Shekou, and Hengqin; and two Special Administrative Regions, Hong Kong and Macau under "One Country, Two Systems". These create inherent conditions for access of cross-border data. In recent years, the GBA is actively exploring the construction of a global data port, including an international data free trade port in Nansha, and a data center at the Hong Kong-Shenzhen Innovation and Technology Park at Lok Ma Chau Loop in a bid to realize cross-border sharing and flow of data safely and under controlled conditions.

6 Excerpt —— "Promote the aggregation, circulation and sharing of data resources; carry out pilot projects for the safety management of cross-border data flow, and explore the establishment of a mechanism that not only facilitates data flow but also ensures safety"

7 Excerpt —— Overall Layout Plan for 5G Base Stations and Data Centers in Guangdong Province (2021-2025)

4 Data security challenges faced by enterprises

A series of planning and measures in the area will be very favorable to improve digital competitiveness of enterprises in the GBA which comply with legal requirements. However, while enterprises enjoy convenience in the GBA, they at the same time face greater challenges.

Different legal systems in Guangdong, Hong Kong and Macau create higher compliance challenges on enterprises

From a legal perspective, the GBA comprises three different jurisdictions, each of which have different laws and regulations on cybersecurity, privacy protection and cross-border data transfer, as well as different regulations for different industries including health care and financial services. Businesses operating in all three jurisdictions are effectively operating under three different legal systems. Enterprises in the GBA are therefore constantly facing challenges over data security compliance.

In relation to cybersecurity, the *Cybersecurity Law of the People's Republic of China*, the *Data Security Law of the People's Republic of China*, the *Measures for Cybersecurity Review* and related implementation regulations and rules have been enacted in mainland China. The Cybersecurity Law and other laws and regulations have been enacted in Macau. It is reported that Hong Kong is also preparing for legislating for cybersecurity and public consultation is being planned. There are relatively broader definitions on network operators, operators of critical information infrastructure and engaging in digital processing activities under the laws and regulations in mainland China when compared to the two other jurisdictions. Enterprises should analyze their own specific compliance requirements in accordance with the particular circumstances of their own businesses. At the same time, the definitions of "critical information infrastructure operator" under mainland Chinese law and "critical infrastructure operators" under Macanese law are different, and the cybersecurity responsibilities to be respectively borne by such operators are different, of which enterprises should be aware.

In relation to privacy protection, relatively comprehensive and systematic protection requirements have already been established across all three jurisdictions. In mainland China, the Personal Information Protection Law and other supporting laws, regulations and guidelines concerned have been rolled out. In Hong Kong, the *Personal Data (Privacy) Ordinance* has been enacted, and relevant approved *Codes of Practice and Guidelines* have been issued by Privacy Commissioner for Personal Data. In Macau, the *Personal Data Protection* Law has been enacted, and various guidelines have been issued by the Office for Personal Data Protection. While there are similarities in the laws and regulations in the three regions, there are also differences in them, including the following:

Differences in definitions of sensitive personal information and automated decision making:

There are relatively more detailed compliance requirements in mainland China and Macau on processing sensitive personal information and automated decision making. In Hong Kong, while there is no specific provision in the *Personal Data (Privacy) Ordinance on sensitive personal information processing and automated decision making,* there are approved *Codes of Practice/Guidelines* by the Privacy Commissioner for Personal Data defining and regulating the same.

Different regulations for processing personal information out of the jurisdiction:

In mainland China, *Personal Information Protection Law of the People's Republic of China* not only applies to natural persons' personal information processing activities in the PRC but also applies to processing of mainland China natural persons' personal information outside the mainland in specific applicable situations. The *Personal Data (Privacy) Ordinance* in Hong Kong applies to any data user who controls the collection of, holds, processes or uses personal data in or from Hong Kong. In some cases, enforcement can be made against non-Hong Kong service providers. There are no express provisions in the *Personal Data Protection Law* in Macau concerning its application out of Macau, but the Act is applicable to circumstances such as the entire or partial automated processing of personal information, and non-automated processing of personal information held in or to be held in manually operated databases.

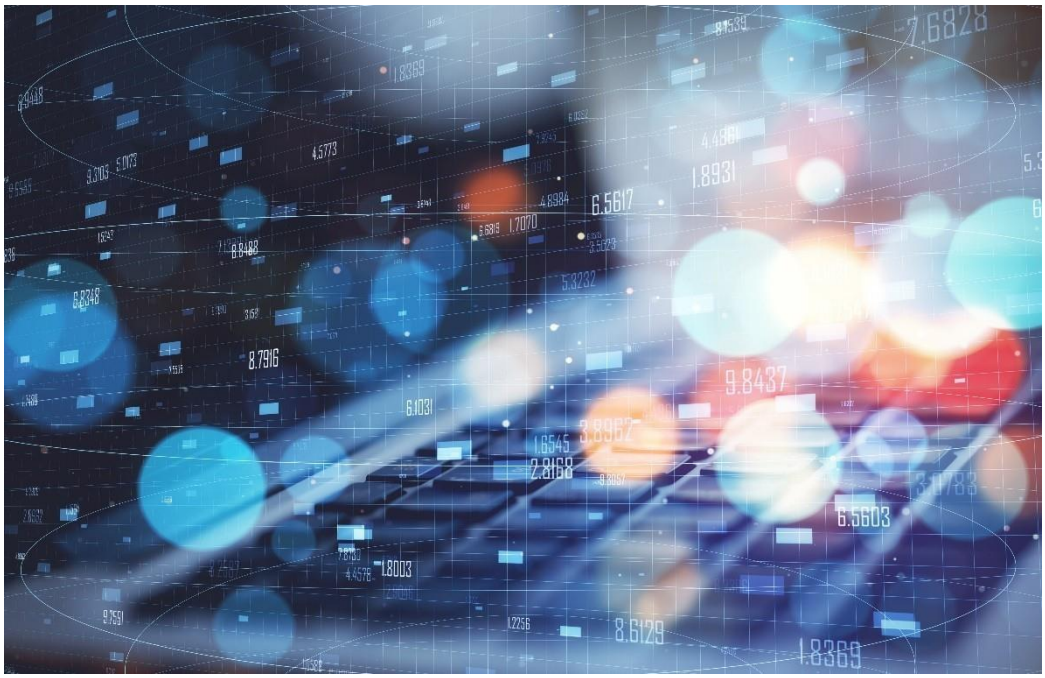
Differences in requirements on collection, use and processing of personal information and access rights of personal information:

The Personal Information Protection Law of the People's Republic of China further stipulates the conditions where separate consent from individuals is necessary. The *Personal Data (Privacy) Ordinance* in Hong Kong, on the other hand, provides different scenarios where different types of consent are required. The *Personal Data Protection Law* in Macau provides that express consent is required in processing personal information, processing sensitive information, disclosing or distributing all or part of personal information and transferring personal information across the border.

There are also differences in laws and regulations in the three jurisdictions on cross-border data transfer, including:

- On data localization, specific requirements are provided in the *Cybersecurity Law of the People's Republic of China*, *Personal Information Protection Law of the People's Republic of China* and other laws and regulations. However, the *Personal Data (Privacy) Ordinance* in Hong Kong and the *Personal Data Protection Law* in Macau do not have express requirements concerning data localization.
- On cross-border transfer of data, the *Cybersecurity Law of the People's Republic of China*, *Personal Information Protection Law of the People's Republic of China*, *Measures for the Security Assessment of Outbound Data Transfer* and other laws and regulations have provisions regarding conditions on cross-border data transfer, including security assessment, personal information protection certification, entering into standard contracts with overseas recipients. There are also provisions in the *Personal Data (Privacy) Ordinance* in Hong Kong concerning cross-border transfer of personal information, but such provisions have not yet been effective. The *Personal Data Protection Law* and *the Cybersecurity Law* in Macau have certain provisions regulating cross-border data transfer, with a list of exceptional cases.

For details of similarities and differences in major laws and regulations on cybersecurity, privacy protection, and cross-border data transfer as well as the challenges in compliance in mainland China, Hong Kong and Macau, please refer to the appendix.



The current capability to comply is insufficient to cope with security challenges

With data security and privacy protection laws in the three places and under the conflicting and complicated legal environment, enterprises need to have sufficient capability in compliance in the security area. Otherwise, enterprises in the three places are unable to cope with the various kinds of data security and compliance issues related to their businesses. Good compliance capability in data security includes:

► Top-down security compliance culture

Only top-down security compliance culture may ensure security compliance is effectively executed internally in enterprises. This requires all people, including management and department leaders of enterprises to understand the importance of compliance in the cybersecurity and privacy areas, but currently it is difficult for many enterprises to build a top-down security compliance culture because of the following reasons:

Awareness of some leaders with management roles in compliance is insufficient and they do not fully understand the importance of cybersecurity and privacy protection in digital transformation, and they still regard this as ordinary compliance and IT internal control issues of enterprises.

Some enterprises still regard security bundled with IT but with digital transformation, security issues are no longer simple IT issues; key departments and boards of enterprises do not trust they are sufficiently secure or understand security enough and there are obstacles in communication on security. Cross-department collaboration is difficult to be achieved and security issues are inevitably ignored by other functions and departments.

Some enterprises lack comprehensive training on security compliance. Trainings of employees are now still mainly confined to those related to jobs and skill trainings and security compliance trainings are not involved. Only a small number of leaders with management roles received training in security compliance and security policy formulation.

Sound organization structure

A sound cybersecurity organization structure is the foundation of security compliance. A cybersecurity organization structure that is embedded throughout an organization may achieve effective breaking of communication obstacles in management, IT and departments and maximize motivation and initiative in cybersecurity and privacy compliance efforts. It is difficult for some enterprises to develop a complete and effective organization structure mainly because of the following reasons:

- Some enterprises only have very limited awareness of security compliance and think all legal and regulation-related issues need to be handled by the legal department. In fact, security compliance also involves management, IT, business departments, internal control and other departments. Legal department alone is unable to cope with all aspects of security compliance and handle all issues well. This will only increase hidden compliance issues.
- Although some enterprises set up cybersecurity organization structure, compliance roles are not well distributed in different departments, leading to ineffective execution of security compliance work.

Sufficient support in human resources

Under a sound organization structure, enterprises should be equipped with sufficient human resources to respond to security issues effectively and promptly. It is difficult for some enterprises to have sufficient human resources to handle mainly because of the following reasons:

- Some enterprises do not understand requirements in security compliance and roles and responsibilities among different departments are not clear. Therefore, they are unable to have better arrangements in this respect.
- Security compliance personnel do not have the required qualifications. There is a serious shortage of employees with cybersecurity professional background and skills

Proper compliance management framework and execution mechanism

Setting up a sound compliance management framework and execution mechanism is the prerequisite of enterprises in driving cybersecurity and privacy compliance. It is on this basis that enterprises may ensure there are proper references to initiate the work concerned and management roles to handle relevant work may be confirmed. It is difficult for some enterprises to build a sound compliance management framework and execution mechanism mainly because of the following reasons:

- Some management and employees of enterprises do not have sufficient awareness of security compliance and organization structure concerned is not sophisticated enough. There may also be a lack of human resources to handle. Based on the actual conditions, it is difficult to build a sound compliance management framework and execution mechanism.
- With different data security and privacy protection laws in the three places, it is difficult to a certain extent to integrate all compliance requirements in the existing security management framework and execution mechanism.

Comprehensive cybersecurity and privacy compliance capability

Only with comprehensive cybersecurity and privacy compliance capability may enterprises ensure full execution of security compliance. It may be difficult for some enterprises to build comprehensive compliance capability mainly because of the following reasons:

- As one of the major elements in security compliance, privacy protection lacks system support internally. From the system perspective, it is difficult to satisfy compliance requirements and guiding implementation of the work concerned cannot be executed.
- Some enterprises already have a compliance system in place but support in areas such as organization structure and human resources is lacking which leads to ineffective execution of processes and mechanism concerned.

For most enterprises in the GBA, various kinds of objective restrictions limit their ability to comply and respond at present to new challenges arising from digital development. How to establish an effective data security compliance system with reasonable deployment of resources will become an issue that needs to be handled by enterprises in the GBA.

Differences in the internet and other conditions in Guangdong, Hong Kong and Macau lead to higher difficulty in security safeguards

There are differences in the internet and other conditions in Guangdong, Hong Kong and Macau. For example,

Difference in internet conditions:

Access to server lines in mainland China is restricted by storage and server traffic of operators and use of server lines requires filing with authorities concerned with standard procedures while network operators in Hong Kong and Macau connect lines with international broadbands. There is no need for filing and no restrictions in lines in these two places. With this kind of difference, the internet environment in Hong Kong and Macau is more complicated and IT resources of enterprises are exposed to complicated internet conditions. Since information assets in mainland China becoming targets of attacks is increasing likely, how to protect information assets under different internet environment is challenging to enterprises.

Difference in technical and security standards:

There is difference in technology and security standards in Guangdong, Hong Kong and Macau, for example, with respect to use of encrypted computing, many mainland Chinese enterprises use mainland China's standards, such as public key algorithm (SM2), cryptographic hash algorithm (SM3) and block cipher algorithm (SM4) while enterprises in Hong Kong and Macau often use commercial computing commonly used globally, such as RSA and DES. Other examples: security standards are set in mainland China while Hong Kong and Macau lack a set of mature network security standards. With this kind of difference in technology and network security standards, how enterprises may manage is one of their challenges.

Difference in users' habits:

Users in Guangdong, Hong Kong and Macau differ in use of the internet. For example, Macau and Hong Kong users mainly use such social media apps as WhatsApp and Facebook but mainland China users mainly use WeChat and Weibo. With differences in the habits of internet users, enterprises face difficulties during unifying security monitoring. Besides, in the post-pandemic era, many employees are forced to work from home. The border of family and office networks is increasingly blurred. How enterprises may manage security and privacy becomes one of the issues that are difficult to be dealt with.

During the process of enabling the cross-border data flow in the GBA, enterprises face differences in the existing network environment, technology and security standards as well as users' habits. These increase their difficulties in security safeguard efforts, and it becomes a new management challenge.

5 How organizations can navigate challenges

Address regulatory differences in Guangdong, Hong Kong and Macau

When developing data governance and security compliance strategy for cross-border data flows, organizations shall take into account the similarities and differences of laws and regulations in mainland, Hong Kong and Macau to enable them to build and execute precise compliance solutions to meet different regulatory requirements simultaneously. Despite differences, there is no contradiction. In the case of highly integrated and overlapping operations, it is recommended a set of solutions in compliance with data security regulations on three sides be built. Besides, organizations need to keep themselves informed of any update and adjust solutions accordingly.

Currently, organizations in the GBA need to give priority to the following issues in terms of data compliance and security.

▸ Privacy protection

As for privacy protection, there are intersections and overlaps among provisions on three sides for collecting, using and processing personal information and data subject rights. As such, organizations need to integrate these requirements to build an unified system to collect, use and process personal information and develop privacy policies and statements applicable to three sides and make modifications based on regulatory differences and scopes of services. For example, in Hong Kong, any direct promotion shall be subject to compliance, while in the Mainland and Macau, organizations shall comply with requirements when conducting cross-border data transmission, automated decision-making and processing sensitive personal information in compliance management.

▸ Cross-border data

Compliant data flow channels in the GBA

As one of the basic elements of digital economy, data requires timeliness and standardization. As such, data flow mechanism shall be built on an easy and standardized process. Going forward, along with measures expected including "data customs" to accelerate the review, evaluation, and supervision of cross-border data flow, developing templates of standard contracts, and obtaining certification for competence in data protection are integral to reducing the costs of transformation of data standards and compliance management to ensure smooth flow of cross-border data.

Standard contract terms. As there is no data exchange mechanism (e.g., whitelist mechanism) among Guangdong, Hong Kong and Macau, it is likely to use business contracts at the organization level to establish standard terms for cross-border data flow, define the responsibilities, rights and obligations of senders and recipients, and develop relevant protection measures. **Standard contract terms** can help ensure data interoperability and security, while cross-border data flow is subject to relevant regulations[8] to enhance mutual trust among organizations on three sides and facilitate data flow.

8 For example, the EU's standard contract clause (SCC) for data transmission within and outside the EU assists stakeholders in complying with the EU's General Data Protection Regulation (GDPR). Meanwhile, ASEAN issued the ASEAN Model Contract Clause on Cross-border Data Flows (MCC) for use by member countries to facilitate the free flow of data under the ASEAN Data Management Framework.

9 In the absence of adequacy determination, the EU provides data transfer mechanisms for organizations to follow with appropriate security measures, including approved Code of Conduct and an approved Certification Mechanism.

Data protection certification. It is likely to engage an independent third party to make an independent assessment of data protection competence of an organization and issue a third-party assurance report to support its competence in data governance and protection pursuant to a unified data governance assessment standards and reporting framework, helping the organization to decide whether data should be sent to recipients[9]. This will facilitate organizations to integrate cross-border data when data security ensured. For example, cross-border group companies can leverage business data in different regional markets and expand their presence when ensuring their competence in data governance and protection.

It is suggested to define roles and responsibilities, rights and obligations of stakeholders based on regulatory, policy and market requirements on three sides, e.g., legal binding, confidentiality agreement, personal data protection measures and terms of suspension of data transmission.

▸ Compliance measures for organizations conducting cross-border data flow activities in the GBA

Compliance of cross-border data flow is particularly important for risk management within an organization, especially for digital technology companies engaged in international trade, cross-border payment, big data, and cloud computing. As complying with requirements for cross-border data flows is not easy and simple, it is suggested that organizations seek measures and paths to ensure compliance based on the following aspects and internal practices.

- **Make clear laws and regulations on cross-border data flow**

This first step is to fully understand legal rules related to cross-border data flow, including local ones and those related to data operations in other jurisdictions. When necessary, organizations should consult with relevant legal professionals to provide guidance on the application of legal rules.

- **Sort out operation-based data**

At the present stage, organizations should sort out all types of data derived from routine operation and specific fields as the basis for preliminary identification. Organizations need to confirm whether written identification standards or identification methods are in place in the industry where they operate. If not, organizations need to judge the possibility of each kind of data to be included as important data in line with the concept defined in existing laws and regulations. As for the data that are more likely to be included as important data, organizations shall fulfill the obligations of data security protection as provided in the Data Security Law. Meanwhile, organizations need to maintain close relationships with competent authorities and keep a close eye on implementation guidelines and details to be issued later to take holistic and targeted measures.

- **Improve internal control system for data security**

The cross-border data flow compliance is not just about cross-border transmission, but includes prior steps including collection and processing, which are relevant to whether data can be transmitted across the border and whether approval procedures are needed. As such, organizations need to establish a complete internal control system for data management, from contract signing to business operation, to give clear guidance to employees and reduce non-compliance risks. According to the data security protection obligations of data processors as provided in Data Security Law, relevant internal control system shall at least include whole-process data security management system, risk monitoring and security incident response system, important data risk assessment and reporting system.

- **Establish cross-border data transmission mechanism within the organization**

Compliance obligations for different subjects vary with legal rules. For example, as provided in Cybersecurity Law, critical information infrastructure operators are subject to stricter data security protection obligations than general network operators. Therefore, organizations need to position themselves based on their operations and applicable legal rules, to define their obligations and what to follow.

Given that operators of critical data and critical information infrastructure in mainland China has not been defined clearly, it is suggested that organizations should identify whether they are likely to fall into the scope of critical information infrastructure by sorting out relevant rules and communicating with competent authorities. Meanwhile, organizations need to identify potential cross-border transmission scenarios in their routine operations, even if some organizations are less likely to be identified as critical information infrastructure operators, it is suggested that organizations make self-assessment prior to transmitting data while maintaining close communication with regulators.

Build security compliance capacity

To build cybersecurity compliance capacity, organizations can take following measures:

Identify data security management functions

Different from traditional information security, data security is not only about IT security, but relevant to legal compliance, internal control, and business security. Therefore, if the traditional security team or legal team takes such responsibilities, data security-related needs are unlikely to be addressed at expertise and skill levels, while at functional level, it is not easy to achieve optimal coordination across departments and business sectors.

To effectively implement security compliance management strategies and systems, organizations need to establish or designate a data security management department, which can be operated as a separate function or managed by an established department.

Data security management department should have the following functions:

- Develop documentation for data management system and define data security compliance management responsibilities at different levels and departments
- Promote data security compliance management and improve compliance management system
- Standardize processes of data collection, storage, usage, processing, transmission, provision and disclosure
- Promote the development of systems and norms, the design and implementation of management measures, and the update of data security technology and applications, to ensure data security compliance

In addition, organizations should designate a person in charge of cybersecurity and privacy protection under given conditions to supervise the implementation of such measures. The designated person should take the following responsibilities:

- Coordinate and hold responsibility for the implementation of cybersecurity and privacy protection measures within the organization
- Organize the preparation of cybersecurity and privacy protection working plan and put it into implementation
- Develop, issue, implement and regularly update cybersecurity and privacy policies and procedures
- Organize the cybersecurity and privacy risk assessments and urge to rectify problems
- Maintain communication with regulators and administrative authorities and report cybersecurity and privacy protection incidents

Develop cross-regional data security system and process

There is no one-size-fits-all solution for data security compliance. With changing businesses and iterating application services, organizations will always be exposed to threats if compliance mechanism doesn't work well. Therefore, organizations need to establish effective systems and processes.

As operations of organizations in the GBA are highly integrated and overlapped in Guangdong, Hong Kong and Macau, it is better to integrate laws on three sides, establish an overall compliance framework and implementation standards and norms at group level, and provide customized configuration at specific control points in line with local requirements.

As for a robust data security systems and processes, priority should be given to the following respects pursuant to existing laws and regulations:

- **Privacy impact analysis**

From the perspective of compliance, privacy impact analysis is required for organizations to perform under given conditions. The Government has issued Information security technology – Guidance for personal information security impact assessment (GB/T 39335-2020) as relevant practice guidance.

Furthermore, privacy impact analysis is an important means to identify privacy and compliance risks within an organization. In terms of data security, most organizations don't have a well-established process to make it difficult to identify risks brought by new businesses and systems but rely on subjective consciousness and cognition of project participants, posing compliance risks. A roust privacy impact analysis includes trigger conditions, individuals and organizations involved, processes and nodes, analysis standards and requirements, validation standards, which can help organizations identify and measure risks without overreliance on subjective consciousness.

- **Privacy by design**

To better embed privacy management and practices into technology, operation, and products, organizations need to incorporate privacy into early-stage design standardization and management processes for new systems and processes. During the whole process from system requirement proposal, implementation to system maintenance, organizations should perform ongoing privacy impact analysis, develop protection requirements, make upfront planning for risk management to avoid inputting a vast number of resources for rectification at a later stage.

- **Data retention**

Having a good understanding of business processes and data usage, organizations should retain data in accordance with laws and regulations and develop a retention plan to ensure that strategic requirements align with provisions of minimum retention period. Moreover, in line with regulations, data retention regimes, consumer requirements, and other business needs, organizations should establish partnerships with business units to understand data lifecycle and data transfer process, build connections among all dimensions of data security, and develop efficient data processing procedures to meet retention and processing requirements while achieving business growth.

- **Data subject rights (DSR)**

The laws and regulations in Guangdong, Hong Kong and Macau provide for DSR in the process of personal information collection and processing. The rights provided include the right to know, the right to access, the right to rectify, the right to be forgotten, the right to restrict processing, the right to object and the right to data portability. Based on legal requirements on three sides, organizations should establish a robust process and mechanism in response to the rights of personal information subjects, to help implement the rights of DSR. When an individual makes such a request, the personal information processor shall explicitly notify the individual of the effective and convenient way to exercise the rights and make a timely response.

- **Authorized consent management**

The requirements for obtaining personal consent during the collection of personal information are specified in mainland's *Cybersecurity Law* and *Personal Information Protection Law*, Hong Kong's *Personal Data (Privacy) Ordinance* and Macau's *Personal Data Protection Law*. So are special scenarios which need to obtain the individual's separate consent. In the context of complex compliance requirements, organizations shall not only obtain authorized consent when collecting personal information, but also restrict the processing of personal information based on the authorized consent subject to compliance. As provided in Article 15 of *Personal Information Protection Law*, individuals have the right to revoke their consents if their personal information is processed based on their consent. Therefore, organizations shall protect users' right to revoke authorized consent at users' touch points, while synchronizing changes in the internal data processing platform.

- **Cross-border data flow**

Cross-border data flow is specified in the mainland's existing laws, regulations, and other regulatory documents, including *Cybersecurity Law*, *Data Security Law, Personal Information Protection Law*, *Measures for the Security Assessment of Outbound Data Transfer*. So are Hong Kong's *Personal Data (Privacy) Ordinance* and Macau's *Personal Data Protection Law* with less strict provisions. These requirements are about strict rules on cross-border data transmitters, users and processors. During the cross-border flow, organizations should develop a detailed cross-border flow plan under the guidance of local laws and regulations and conduct an in-depth evaluation on its legitimacy and justice. Moreover, organizations should conduct gap analysis on their current situations and identify remedies to establish a complete mechanism of cross-border data flow management.

▶ Define compliance related roles and responsibilities

Data security compliance is by no means the responsibility of data security management department. Meanwhile, it needs to engage numerous departments with defined responsibilities.

As the lead of data security compliance, the data security department is responsible for organizing the development of relevant systems and procedures and supervising the execution.	IT department should assist data security department in integrating data security management into routine operations and products through technology, and embedding it into organization-wide systems and business development processes by various means including access control, encryption, desensitization and anti-leakage.	Business units including sales team, product team and procurement team should cooperate with data security department to sort out the data owned by the organization in a systematic way from a business perspective, including identifying the data processor, understanding the data form, storage method and retention time, and conduct data security management within their scope of business in line with data governance requirements.	Compliance or legal department should improve the data security management framework pursuant to laws, regulations and regulatory requirements, and conduct regular compliance check and risk assessment.

By coordinating the resources of all parties, integrating the differences of management demands of each department, and defining roles and responsibilities, can an effective multi-party linkage mechanism and a practical management structure be developed.

Manage post-outbound transmission risks

The management of outbound transmission risks is not just about outbound transmission subject to compliance, but the security management afterwards to fulfil the obligations of data security management. Otherwise, if personal information or other important data are disclosed by a security incident, the organization that transmits data hold it responsible.

Post-outbound transmission risk management includes but not limited to

- **Identity authentication and access control:** strictly control the outbound data access, only open sample data to those with sufficient business requirements, provide granular access, and prevent unauthorized access to data beyond the permission
- **Data usage and retransmission management:** strictly manage the data processing with no processing beyond the initial purposes; control the data retransmission. Any processing conducts different from what is described in assessment and filing for data transmission shall be reassessed and processed to prevent the important data and personal information from being disposed as general data.

Balance business needs and improve privacy protection capability

The GBA is set to bring more convenient cross-border data flow mechanism in the future, while compliance obligations and responsibilities will not be reduced. Organizations need to ensure data security before and after data are transmitted without compromising national development and society. As relevant measures are being developed, it is difficult for organizations to balance compliance requirements, user experience and business needs nowadays. Therefore, organizations are facing pain points amid both intercompany and intracompany data transmission.

In line with current situations and industry practices, it is recommended that organizations use technology-enabled business process control or privacy computing to achieve data invisibility and availability when planning cross-regional data integration and unified application; provide tagging, aggregation, or analysis platforms instead of raw data after computation to enable cross-entity data usage and segregation between data ownership and usage, thus reducing security and compliance risks.

Enhance security management capability

Organizations need to build up security management capacity to prevent and resolve security threats while considering compliance capability. Specifically, organizations can enhance security management in the following aspects:

- **Data security management**

In June 2021, the *Data Security Law* passed by the Standing Committee of the 13th National People's Congress clearly states that the State shall establish a data classification and grading protection system to classify and grade the data, according to the importance of data in economic and social development, as well as the extent of the harm to national security, public interests, or the legitimate rights and interests of individuals and organizations once data are tampered, damaged, leaked, illegally acquired or used. With tightened regulations on data security, organizations shall establish and improve the whole-process data security management system.

As for data asset recognition, organizations may refer to *Information security technology - Important data identification guidelines (draft)* released in 2022, to understand the elements to identify important data, follow the principles of focusing on security influence, highlighting protection priorities, converging with established rules, considering risks as a whole, integrating qualitative and quantitative dimensions and reviewing dynamic recognition to identify important data within the organization, and standardize the formats for important data description.

As for data classification and grading, organizations can refer to implementation guidelines such as *Cybersecurity standard practice guidelines - Network data classification and grading guide*, *Industrial data classification and grading guide (trial)*, to conduct data analysis based on existing internal rules and practical operation at different dimensions including business impacts, compliance risks and social impacts to develop classification and grading standards; define data lifecycle from collection, transmission, storage, processing to destruction at institutional level to build differentiated management requirements and technology-based protection strategy for classified and graded data.

What's more, organizations can refer to some industry standards, such as Data Management Capability Maturity Model (DCMM) and Data Security Capability Maturity Model (DSMM), with data lifecycle as mainstay including 6 phases from collection, transmission, storage, processing, exchange and destruction, and evaluate security capability from perspectives of organization construction, system process, technology and tools and personnel competence, and establish data security management system based on specific situations to sustain standard management of data lifecycle.

- **Cybersecurity management**

As the underlying security capability to support data security, cybersecurity management is of great significance to the overall management and control within an organization. To date, there are no general security standards on building information security system in Guangdong, Hong Kong and Macau i.e., provisions related to information security management system have not yet issued in Hong Kong and Macau, while in mainland China, grade-based cybersecurity protection system is in place as general requirements for sophisticated security management.

Given the operations overlapped, and scenarios that security protection is required after data are transmitted to Hong Kong and Macau, organizations in the GBA , regardless of whether the application system is physically deployed in the mainland, can refer to *Information security technology – Basic requirements for grade-based cybersecurity protection* to develop organization-wide security management system, including security management system, security management organization, security management personnel, security construction system and security operation and maintenance system.

With increased compliance risks, organizations shall establish a compliance training mechanism for all employees, organize security awareness education and security management system publicity training at every key milestone of an employee's career, and regularly organize trainings on compliance awareness and management, to build an effective performance assessment mechanism.

Meanwhile, organizations shall establish processes and mechanisms for reporting non-compliance and security breaches and ensure the mechanisms operate smoothly while processes are optimized and improved on an ongoing basis.

Enhance security protection capability

As the GBA serves as a hub to exchange onshore and offshore data, organizations in the GBA need to have technology-based security protection capabilities in addition to management capacity to ensure business operation and fulfill obligations while enjoying the convenience of data flow provided by the State. To enhance security protection, organizations shall establish a good foundation for network resilience

Like security management, organizations can build up their security capabilities on graded-based security protection system, which is relatively sophisticated and mature in the GBA, regardless of whether security systems are deployed in the mainland. Traditionally, organizations believed that only those registered in the mainland should be improved according to grade-based security protection requirements, while ignoring the fact that the requirements could serve as a guidance for overall security protection as well as the practical value as the most authoritative security standards in GBA. As the most practical security standards, grade-based security protection system can help organizations improve security capability and demonstrate to regulators that their operations can meet China's security obligations no matter where they are within the region.

The grade-based cybersecurity protection system 2.0 reflects the idea of grade-based security protection framework based on one center (security management center) and three defenses (secure computing environment, secure area boundary, secure communication network). By complying with these requirements, organizations can develop internal security protection framework at technology-based dimensions including secure physical environment, secure communication network, secure area boundary, secure computing environment and security management center. Take computing environment as an example, where control points are specified including identity authentication, access control, security audit, hacking prevention, malicious code injection prevention, trusted authentication, data integrity, data confidentiality, data backup and recovery, residual information protection and personal information protection, and detailed control requirements are defined for each grade-based control point, which can serve as a reference for organizations.

Organizations can build a good foundation for network resilience based on grade-based security protection system 2.0 and establish a security-oriented proactive defense and perception mechanism.

Apart from security standards in the mainland, organizations can also refer to relevant international standards according to their specific situations. For example, *NIST SP 800-160 Vol.2* *Developing Cyber Resilient Systems: A Systems Security Engineering Approach* defines network resilience system and how to build it. In a world where security threats have become inevitable, network resilience can help organizations reduce their losses when they suffer hacking attempts.

6 Conclusion

The development of the GBA brings unprecedented opportunities and possibilities for organizations to gain competitive advantages through digitalization. Despite convenient channels and vast resources, organizations may face greater security and compliance challenges.

- Organizations need to address the differences in cybersecurity, privacy protection and cross-border laws and regulations.
- Existing compliance capabilities are struggling to address security challenges and risks
- Differences in network environment increases difficulty in security protection.

It is recommended that organizations enhance security and compliance capabilities when facing security and compliance risks.

- Given differences in laws and regulations in Guangdong, Hong Kong and Macau, establish a set of precise compliance standards inclusive of privacy protection and cross-border flow requirements, and put them into execution, to meet regulatory requirements on three sides
- Comprehensively enhance compliance capabilities, including improving organizational structure, optimizing institutional processes, defining roles and responsibilities, managing outbound risks, and strengthening privacy protection capabilities
- Build up security management capacity to prevent and resolve security threats
- Strengthen security protection capabilities and build a good foundation for network resilience

Organizations should keep in mind that they shall ensure data security and compliance, fulfill the obligations and responsibilities of safeguarding national security and users' rights and interests while accessing green channels. Only with early planning and thoughtful considerations can organizations achieve sustainable growth while enjoying favorable policies.

Appendix – Comparison of laws and regulations in mainland China, Hong Kong and Macau

Areas	Comparative analysis of requirements			Compliance challenges
	Mainland China	Hong Kong	Macau	
Cybersecurity laws	▸ Cyber Security Law, Data Security Law, and relevant implementation regulations, such as the Cybersecurity Review Measures.	▸ Hong Kong at present does not have cybersecurity-specific legislations. Nevertheless, one should comply with the personal data security and disclosure requirements of the Personal Data (Privacy) Ordinance	▸ Cybersecurity Law and others.	The processing of data in the GBA shall be subject to different cybersecurity requirements across three regions and considerations should be given to the following issues: ▸ Given the broader definition of network operators, critical information infrastructure operators and data processing activities provided by laws in the mainland, analysis should be made on the supervisory requirements for the services provided. ▸ The definition of "critical information infrastructure operators" in the mainland and that of "public and private operators of critical infrastructure" in Macau are different, and so are the cybersecurity responsibilities of such operators on both sides. ▸ While Hong Kong at present does not have cybersecurity-specific legislations, the newly amended Personal Data (Privacy) Ordinance provides broader provisions on disclosing personal data without consent, which can be seen as providing potential criminal liabilities for data processors who failed to comply with cybersecurity responsibilities and were reckless as to whether harm would be caused to the data subject concerned by the disclosure.
Scope of application of cybersecurity laws	▸ Network operators, network products and services providers, data processors, critical information infrastructure operators which include public communication and information services, energy, transportation, water, finance, public services, e-government, defense technology and industry, and other important network facilities and information systems which, in the event of damage, disfunction or data leakage, may seriously harm national security, national economy and people's livelihood, and/or public interests.	▸ Data users, third-party data processors engaged and more.	▸ Public and private operators of critical infrastructure; private operators include private entities, whether domiciled in Macau or outside of Macau, engaging in 12 sectors of services including water supply; banking, finance and insurance; audio-visual broadcasting; fixed or mobile public telecommunications network operation and internet access services.	
Cybersecurity responsibility	▸ Network operators shall fulfill a series of security protection obligations according to grade-based cybersecurity protection system. ▸ Network products and services shall meet the mandatory requirements of relevant national standards and obtain relevant security certifications. ▸ Network service providers shall require users to provide real identity information. ▸ Develop emergency plans for cyber security incidents. ▸ Operators of critical information infrastructure shall fulfil further security protection obligations, including potential requirements for national security review when procuring network products and services, security risk-based random checks, and cybersecurity emergency drills. ▸ Establish and improve comprehensive data processes data security management system, take technical measures and other necessary measures to ensure data security. ▸ Conduct national security review of data processing activities that compromise or may compromise national security.	▸ Data users shall take all practicable steps to ensure that any personal data held by data users are protected against unauthorized or accidental access, processing, erasure, loss, or usage. ▸ Data users shall ensure that third party data processors, whether within or outside Hong Kong, engaged to process personal data shall protect the security of personal data through contractual or by other means. ▸ The latest amendments further criminalize the disclosure of personal information without consent, if the disclosure is made with intent to cause any specified harm, or having been reckless as to whether specified harm would be caused (including personal, property or psychological harm) to the data subjects.	▸ Establish a network security management unit capable of implementing internal cybersecurity protection measures. ▸ Designate cyber security responsible persons and their replacements from qualified and experienced individuals with permanent residence in Macau. ▸ Take measures to ensure that cybersecurity responsible persons and their replacements are available to be contacted by to the Alert and Emergency Response Center at any time. ▸ Establish a cybersecurity complaint and reporting mechanism. ▸ Develop cybersecurity management system and related internal operating procedures. ▸ Take internal measures related to cybersecurity protection, review, early warning, and response to cybersecurity incidents in accordance with cybersecurity management system and applicable technical specifications. ▸ Submit annual cybersecurity reports to relevant regulators. ▸ Allow representatives from the Alert and Emergency Response Center to access facilities and information networks, and provide information to such representatives as requested.	

Areas	Comparative analysis of requirements			Compliance challenges
	Mainland China	Hong Kong	Macau	
Privacy protection laws	▸ Cybersecurity Law and Personal Information Protection Law	▸ Personal Data (Privacy) Ordinance and relevant approved codes of practice and guidelines issued by the Office of the Personal Privacy Commissioner of Hong Kong	▸ Personal Data Protection Law and guidelines issued by the Office of Personal Data Protection of Macau	Requirements for privacy and personal information protection are provided in mainland, Hong Kong, and Macau. Requirements across the three regions have similarities but there are also differences. Among them, one should pay particular attention to the following: ▸ Whether the personal information collected in relevant scenarios relates to any sensitive personal information or automated decision-making (legal definitions provided by laws in the three regions are slightly different). ▸ the location of the individuals whose information is processed.
Scope of application of privacy protection laws and extra-territorial applicability	▸ The Personal Information Protection Law applies to the processing of personal information of natural persons both within the mainland of China, and outside of mainland China under specific circumstances. ▸ For the purposes of providing products or services to natural persons within the mainland of China. ▸ To analyze and evaluate the conducts of natural persons within the mainland of China. ▸ Other circumstances stipulated by laws and administrative regulations.	▸ The Personal Data (Privacy) Ordinance applies to any data user who controls the collection, holding, processing or use of personal data in or from Hong Kong. ▸ The latest amendments enable law enforcement agencies to send cessation notices to non-Hong Kong service providers, requiring them to take cessation actions, and such notices could be served by leaving, post, fax and/or email to the last known address outside Hong Kong.	▸ Personal Data Protection Law applies to: ▸ automated processing of personal data either wholly or in part ▸ non-automated processing of personal data held or to be held in a manually operated database ▸ processing of personal data for public security purposes ▸ Recorded surveillance over voices and images of identifiable persons, and obtaining, processing and dissemination of those voices and images by other means ▸ In general, the Personal Data Protection Law has no express provisions for extra-territorial application.	
Requirements for collecting, using, and processing personal data and personal data rights	▸ Both the Cybersecurity Law and the Personal Information Protection Law provide detailed requirements. ▸ The Personal Information Protection Law further provides for circumstances where separate individual consent is required, including processing sensitive personal information, publicly disclosing the personal information processed, providing the personal information processed to other personal information processors, and providing personal information outside of mainland China. However, there are exceptions.	▸ The Personal Data (Privacy) Ordinance provides detailed requirements, including the six data protection principles provided in Schedule 1. ▸ There are different circumstances where different types of consent shall be obtained, including using personal data for new purposes, transferring such data, matching procedures, and direct marketing. One should also note the detailed exemptions as provided in the Ordinance. ▸ There are newly added criminal offence provisions for disclosing personal information without consent including being reckless as to whether the disclosure causes the specified harm to the data subject.	▸ The Personal Data Protection Law provides detailed requirements. ▸ Generally, express consent shall be obtained for processing personal data and sensitive data, disclosing or disseminating personal data wholly or in part, transferring personal data out of Macau. Also, one should note the circumstances provided in the Personal Data Protection Law where consent is not required.	
Provisions related to sensitive personal data and automated decision-making	There are detailed requirements for processing sensitive personal data ▸ For specific purposes ▸ With sufficient necessity ▸ Taking strict protection measures ▸ There are detailed requirements for automated decision-making ▸ Ensuring transparency of the decision-making and the fairness and impartiality of the result. ▸ Must at the same time provide options not specific to individuals' characteristics, or convenient ways for refusal. ▸ Unreasonable differential treatment shall not be given to individuals in terms of trading price or other trading conditions.	▸ There is no specific provision, but the Office of the Privacy Commissioner for Personal Data has approved codes of practice and guidelines in place. Violation of relevant provisions may become evidence of violation of relevant provisions of the Ordinance.	▸ Detailed requirements are provided, including: ▸ The respective prohibited activities and permitted activities of processing of sensitive data ▸ The respective circumstances where an individual shall be bound by automated decision-making, and an individual's right not to be bound by automated decision-making.	

Areas	Comparative analysis of requirements			Compliance challenges
	Mainland China	Hong Kong	Macau	
Data localization	▸ As provided by the Cybersecurity Law and the Personal Information Protection Law, the following information shall be stored within the mainland of China, and relevant security assessment shall be conducted when data are provided across the border. ▸ Personal information and important data collected and generated by critical information infrastructure operators during their operation within the mainland of China ▸ Personal information processed by state agencies ▸ Personal information collected and generated within the mainland of China by personal information processors with personal information processed reaching the threshold specified by the national cyberspace administration department	▸ There is no express requirement for data localization provided in the Personal Data (Privacy) Ordinance. ▸ Attentions shall be drawn to whether there are profession or industry-specific data localization requirements.	▸ There are no express requirements for data localization provided in the Personal Data Protection Law and the Cybersecurity Law.	Businesses engaged in operations in mainland, Hong Kong and Macau shall be subject to laws and regulations in the three regions while conducting cross-border data transfer. One must note: ▸ Whether businesses are subject to data localization requirements provided by laws and regulations. In this regard, attention must be drawn to the requirements in the mainland and any information that is required to be stored in the mainland shall be stored within the mainland ▸ The nature of the cross-border data transfer, and whether businesses have complied with the requirements provided by the relevant laws and regulations of the three regions, as well as requirements of the guidelines of regulatory authorities
Cross-border data transmission	▸ The "Measures for the Security Assessment of Outbound Data Transfer" require data processors to conduct data cross-border security assessment if any of the following conditions are met: ▸ the outbound data comprises personal information and important data collected and generated by operators of critical information infrastructure; ▸ the outbound data contains important data; ▸ a personal information processor that has processed personal information of more than one million people provides that personal information to entities overseas; ▸ the personal information of more than 100,000 people or sensitive personal information of more than 10,000 people are transferred overseas accumulatively; or ▸ the circumstances under which security assessment of outbound data is required as prescribed by the CAC	▸ Section 33 of the Personal Data (Privacy) Ordinance provides for requirements for cross-border transfer of personal data, but these requirements have not yet been in effect. ▸ Cross-border transfer of personal data must comply with the provisions on transfer of personal data with third parties specified in the Personal Data (Privacy) Ordinance as well as the relevant guidelines on cross-border transfer of personal data issued by the Privacy Commissioner.	▸ There are requirements, including: ▸ Ensuring appropriate protection by the local legal system in the jurisdiction where data are to be received. ▸ Complying with other provisions stated in the Personal Data Protection Law. ▸ However, there are exceptions (i.e., cross-border transfer of personal data is permissible in certain circumstances where the receiving party is unable to ensure an appropriate level of protection).	

Contact us

Vincent Chan
Partner
Greater Bay Area Leader
Consulting
Ernst & Young Advisory Services Limited
+852 2629 3751
vincent.chan@hk.ey.com

Winson Woo
Partner
Consulting, China South
Ernst & Young (China) Advisory Limited
+86 20 2881 2731
winson.woo@cn.ey.com

Juliet Zhu
Senior Manager
Consulting
Ernst & Young Advisory Services Limited
+852 3758 5879
juliet.zhu@hk.ey.com

Alvin Guan
Senior Manager
Consulting
Ernst & Young (China) Advisory Limited
+86 20 2838 1113
alvin.guan@cn.ey.com

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

APAC no. 03014465
ED None

ey.com/china

Follow us on WeChat
Scan the QR code and stay up-to-date with the latest EY news.