



Artical

## Integrated Development and Governance of Children’s Data: Protection and Cross-Boundary Coordination in the Guangdong-Hong Kong-Macao Greater Bay Area

### Abstract

The development of the Guangdong-Hong Kong-Macao Greater Bay Area (GBA) is rapidly advancing as a national strategy, with the construction of a “Digital Bay Area” serving as a key catalyst. Intensive cross-boundary population flows and the rapid growth of the digital industry have precipitated large-scale, cross-jurisdictional transfers of children’s personal data. Despite geographical proximity, the unique reality of “one country, two systems, and three legal jurisdictions” gives rise to systemic disparities in the protection of children’s personal data across the three regions. This context necessitates the establishment of robust coordination mechanisms to balance the imperative of cross-boundary data flow with the need for child protection during the Digital Bay Area’s development. Drawing on a comprehensive analysis of the scenarios and entities involved in the GBA’s cross-jurisdictional processing of children’s data, this paper undertakes a comparative study of the three regions across multiple dimensions, including legislation, administrative supervision, and remedies for rights infringement. Ultimately, the study delineates the disparities in cross-jurisdictional data transfer and children’s data protection, offering actionable perspectives on bridging these gaps and establishing collaborative mechanisms to underpin the GBA’s integrated development.

Li Tingting      Luo Yuwei

Department of Journalism and  
Communication, South China Normal  
University, China

 [li.tingting@m.scnu.edu.cn](mailto:li.tingting@m.scnu.edu.cn)

DOI: 10.64371/7p94jn22

### Keywords

*Integrated Development; Guangdong-Hong Kong-Macao Greater Bay Area;  
Children’s Data Protection; Cross-Boundary Coordination*

## 1. Introduction

Since the formal initiation of strategic planning for the Guangdong-Hong Kong-Macao Greater Bay Area (GBA) in the 2017 Government Work Report, the GBA’s integrated development has achieved substantial progress, both in institutional framework and practical implementation, as a pivotal national strategy. In 2019, the Communist Party of China Central Committee and the State Council issued the Outline Development Plan for the Guangdong-Hong Kong-Macao Greater Bay Area (hereinafter, the Outline Plan). This document serves as the key guiding blueprint for the GBA’s development, signaling the full-scale implementation of the strategy. The Outline Plan explicitly mandates the acceleration of the “Digital Bay Area” construction. It emphasizes the digital transformation of industries, particularly smart manufacturing and FinTech, and highlights the leveraging of digital means to facilitate the flow of production factors and industrial synergy among Guangdong, Hong Kong, and Macao. Subsequently, in November 2023, the Guangdong Provincial Government released the Three-Year Action Plan for the Construction of the “Digital Bay Area.” This plan proposes to tightly integrate the “Digital

Bay Area” development with the GBA’s socio-economic advancement, aiming to accelerate the formation of a unified market and a high-quality living circle, thereby positioning the GBA as the world’s most digitally advanced bay area. According to Guangdong’s provincial planning for communications capacity and computing power, the total data storage volume in the province is projected to exceed 260 exabytes (EB) by 2025, with advanced storage capacity constituting over 30%. Furthermore, core data and critical data equipment in key industries are expected to achieve 100% coverage (Guangdong Communications Administration [GDCA], 2024). Leveraging these substantial data storage capabilities and supporting infrastructure, estimates indicate that the scale of the digital economy in the Greater Bay Area will reach 8.5 trillion yuan by 2025, representing over 45% of its GDP (China Research Network, 2025).

The GBA constitutes a pivotal national strategy aimed at fostering deeper economic and market integration between Mainland China, Hong Kong, and Macao. It is designed to advance domestic reform, address challenges within the Belt and Road Initiative, and strategically position the region to compete with other global bay areas and integrate into the international economic system (Li & Kwok, 2019). Nevertheless, the confluence of intensified cross-regional mobility and rapid digital transformation has driven an increase in the cross-jurisdictional movement of children—a highly sensitive demographic—both when accompanied by parents and when traveling independently. This trend necessitates the large-scale collection and processing of their data. Attaining an appropriate level of data protection while ensuring its lawful and efficient cross-jurisdictional flow requires a clear understanding of the institutional similarities and divergences across the three legal jurisdictions. Consequently, key research questions emerge: How do the three regions, operating under distinct legal systems, establish standards for children’s data protection? What are the similarities and differences in the regulatory approaches and remedial mechanisms for children’s data protection within the “one country, two systems” framework? Furthermore, how can these institutional divergences be reconciled to promote a coordinated cross-boundary protection regime for children’s data, thereby supporting GBA integration? In essence, the cross-boundary flow of children’s data within the GBA must be handled with careful consideration of regulatory boundaries and jurisdictional constraints. Given the overarching goal of GBA integration and the rapid development of the Digital Bay Area, establishing a regional coordination mechanism is imperative. This mechanism must acknowledge both the common principles and the distinct legal and regulatory characteristics of Guangdong, Hong Kong, and Macao, and must be designed to facilitate the smooth flow of data while ensuring robust and consistent safeguards for children’s personal information.

## **2. Institutional Divergence and Coordination Dilemmas in Cross-Boundary Children’s Data Flows within Regional Integration Frameworks**

The establishment and development of the Digital GBA necessitate that entities collecting and processing data for numerous governmental and commercial scenarios address critical legal compliance and standard alignment issues related to data collection and processing as the region pursues integrated development. Under the framework of “One Country, Two Systems,” the stark institutional differences across the Mainland (Guangdong Province), Hong Kong, and Macao—encompassing legislative, judicial, and administrative practices—have resulted in widely divergent approaches to children’s data protection. A primary challenge that the three jurisdictions must urgently address is whether, and how, to impose unified compliance requirements on diverse data collectors during cross-border data transfers. This must be coupled with the establishment of targeted protection, supervision, and relief mechanisms specific to children’s data, given the complex legal environment.

### **2.1 Divergent Legislative Approaches to Children’s Data Protection Across the Three Jurisdictions**

Due to differing legal origins across the Mainland (Guangdong), Hong Kong, and Macao, significant variations exist in the legislative philosophy, recognition standards, and processing principles governing children’s data protection.

The primary distinction in children’s data protection stems from the Mainland’s legislative framework, which utilizes a “dual-track” approach (Zhai, 2021) through the Personal Information Protection Law (PIPL) and the Data Security Law

(DSL). Track 1 (PIPL): Focuses on protecting the rights of natural persons through informed consent regarding personal information. Track 2 (DSL): Focuses on security protection grounded in data risk prevention. This stands in contrast to Hong Kong and Macao, where data protection legislation follows a single-track model centered on private autonomy and the protection of natural persons' rights. The Mainland's dual-track legislation segregates data-related legal interests into two dimensions: individual and societal. Individual dimension centers on protecting private rights and individual will autonomy (i.e., consent). Societal dimension primarily targets national data sovereignty, social risk prevention, and industry regulation. However, as the information environment becomes increasingly complex, this legislative distinction, particularly in the dimension of private autonomy, is facing numerous challenges in practice. Consequently, the crucial next step for enhanced protection is strengthening data security assurance by technology entities under the supervision of state public power (Ye, 2025).

While all three jurisdictions generally affirm the private rights protection status of children's data, they exhibit significant differences in specific recognition standards and processing principles.

### 2.1.1 Defining and Categorizing Children's Data

The standards for defining children's data and its special characteristics vary across the three regions:

Jurisdiction	Status of Children's Personal Identifiable Information	Key Regulatory Approach
Mainland	Explicitly defined as "Sensitive Information"	<b>Rigid Age Restriction:</b> 14 years old and under. Processing requires specific purpose, sufficient necessity, and strict protective measures (PIPL Article 28).
Hong Kong (PDPO)	Not explicitly defined as Sensitive Data.	<b>No Age Restriction:</b> The <i>Personal Data (Privacy) Ordinance</i> (PDPO) does not explicitly categorize sensitive data or set special conditions for processing children's PII.
Macao (PDPA)	Not explicitly defined as Sensitive Data.	<b>No Explicit Inclusion:</b> The <i>Personal Data Protection Act</i> (PDPA) defines sensitive data (e.g., race, political views, health data) but <b>does not include children's data</b> in this list.

### 2.1.2 Divergent Processing Principles and Requirements

These definitional differences lead to considerable inconsistencies in the principles and requirements for processing children's data. Mainland China recognizes children as a special group requiring protection. Regulations explicitly mandate that the processing of children's PII must adhere to: Guardian's Explicit Consent (Explicit Consent); and Prohibition against Inducing Consent. To comply, data processors often must establish separate consent mechanisms, ensure the guardian's informed authorization, clearly define the revocability of consent, and adhere to the Principle of Minimal Necessity in collection and processing. Processors frequently adopt independent, distinct standards to handle children's PII in response to these strict regulatory demands. While in Hong Kong and Macao, neither jurisdiction has similar, explicit regulatory mandates, nor have they established separate consent or additional processing requirements for children's data. The PDPO (Hong Kong) and the PDPA (Macao) lack dedicated clauses for children's privacy protection and do not use age 14 as a specific threshold for differential treatment of personal data.

### 2.1.3 Reliance on Parental/Guardian Oversight

Despite the lack of dedicated statutory clauses, both Hong Kong and Macao have established forms of parental/guardian oversight for children's data protection. In Hong Kong, the Office of the Privacy Commissioner for Personal Data (PCPD) requires parents or teachers to fulfill their supervisory responsibility based on the child's "age and maturity", through its guidelines of Children's Online Privacy (Office of the Privacy Commissioner for Personal Data, Hong

Kong [PCPD], 2015). While in Macao, the PDPA emphasizes the need for special protection in processing minors’ data, relying in practice on Article 113 of the Macao Civil Code which stipulates that the lack of capacity of a minor is compensated by parental authority or guardianship.

## 2.2 Guardian’s Informed Consent and Cross-Boundary Recognition Challenges

In summary, all three jurisdictions adhere to the fundamental principle of “Informed Consent” for processing children’s data. However, when children’s data undergoes large-scale cross-boundary flow, the three regions face disparities and coordination difficulties concerning the definition of the scope of information disclosure, the form of consent, and the guarantee of the Right to Withdraw Consent.

### 2.2.1 The Principle of Informed Consent

At the foundational level of data legislation, all three jurisdictions accept “Informed Consent” as the prerequisite for data processing:

Jurisdiction	Key Legal Mandate	Consent Requirements	Right to Withdraw
<b>Mainland (PIPL)</b>	Articles 13–15 require processors to inform individuals of the scope, purpose, processing, and storage methods. Article 30 delegates PII processing rights for minors under <b>age 14</b> to the guardian.	<b>Explicit Consent</b> is required. Processing requires the development of <b>special rules</b> and a <b>separate written consent mechanism</b> for children under 14.	<b>Explicitly allows</b> the withdrawal of consent.
<b>Hong Kong (PDPO)</b>	Requires collectors to explicitly inform individuals prior to collection regarding purpose, usage, necessity of provision, and potential recipients, ensuring voluntary data provision is the basis of informed consent .	Follows a similar principle of <b>Explicit Consent</b> .	<b>No specific provisions</b> for the Right to Withdraw Consent, but individuals may request the cessation of processing or object to unlawful processing.
<b>Macao (PDPA)</b>	Article 6 stipulates that personal data processing may only occur with the <b>explicit consent</b> of the data subject.	<b>Explicit Consent</b> is required.	<b>No specific provisions</b> for the Right to Withdraw Consent, but individuals may object to illegal processing.

### 2.2.2 Challenges in Implementation and Cross-Boundary Flow

While guardian’s informed consent is widely accepted in personal data protection, practical challenges in identity verification and authorization persist across all three jurisdictions.

As with the confirmation of children’s identity and consent validity. In mainland, the government requires strict real-name verification for children using network services. Although the law mandates parental supervision and explicit consent, in practice, authorization often becomes a mere formality. Children may easily bypass verification by logging in as a parent, or they may grant a blanket authorization to the processor without sufficient information simply to access the service(Xiao & Guan, 2025). While in Hong Kong and Macao lack strict real-name systems or high-threshold authorization mechanisms. They often adopt international practices (Google, n.d.) where the internet company uses the user-provided date of birth to determine age, setting a gateway for service provision or triggering the requirement for parental authorization.

There are also regulatory blind spots in Cross-Boundary data flow. The flow of children’s data between the Mainland and Hong Kong/Macao currently lacks a unified, recognized informed consent mechanism. Especially when mainland child data transfer to HK/Macao processor, when a Mainland child’s information is collected and processed by an HK/Macao entity, there are still systemic blind spots concerning: How to set up data processing under guardian consent that meets

Mainland compliance standards. How to provide an effective Right to Withdraw Consent mechanism (as this right is absent in HK/Macao law). How the entire processing sequence will be recognized and sanctioned by Mainland regulators after the data crosses the border. While in HK/Macao Child Data to Mainland Processor, noted as when an HK/Macao child's data is collected and processed by a Mainland entity, it remains unclear: How to fully comply with the Mainland's guardian's informed consent principle. How to ensure sufficient information disclosure to the guardian. How to establish a clear supervisory framework for the data's entire flow. These issues highlight the need for further clarification and harmonization across the three jurisdictions.

### **3 Coordinated Relief Challenges for Harm Caused by Cross-Boundary Children's Data Flow**

In addition to the compliance difficulties arising from the disparities in legal definitions and processing principles discussed above, the significant differences in the judicial and administrative systems across the Mainland (Guangdong), Hong Kong, and Macao have resulted in major divergences in children's data security supervision. Consequently, if children's data is violated, the regions may face significant obstacles to coordinated relief.

#### **3.1 Divergent Regulatory Frameworks for Children's Data Protection**

Despite the geographic proximity of the Mainland (Guangdong), Hong Kong, and Macao, the unique institutional environment—characterized by “three customs territories, three currencies,” and “two legal systems across three jurisdictions”—has, due to historical reasons, led to the development of distinct approaches to children's data supervision. Mainland China relies on its Civil Law system to establish a fundamental protection framework characterized by “family guardianship as the foundation, social guardianship as the supplement, and state guardianship as the ultimate guarantor” (Xia, 2018). While in Hong Kong, grounded in the Common Law tradition, it links international standards primarily through judicial precedent. Its focus is on balancing children's privacy rights with the free flow of cross-boundary data (Tao, 2021). Macao integrates the Portuguese Civil Law system with European Union rules. It sets a statutory age of consent while emphasizing the Principle of Minimal Intervention within a multicultural context (Wang, 2011).

This regulatory divergence is prominently reflected in the different structures and scopes of authority established for the regulatory bodies overseeing children's data protection across the three jurisdictions. Mainland China formed multi-sectoral and layered supervision system. The Mainland assigns regulatory responsibility for children's Personal Information (PI) processing to a multi-level, horizontally and vertically coordinated management system: Coordination Leading by the Cyberspace Administration of China (CAC) at the national level is responsible for overall coordination and supervision of personal information protection work (PIPL Article 60). And sectoral oversighting by relevant departments under the State Council are responsible for PI protection and supervision within their respective functional scopes. This framework allows local CAC and market supervision departments to enter platforms for special rectification campaigns targeting minors' data (Cyberspace Administration of China et al., 2025). Specific ministries handle their areas, such as the Ministry of Education conducting “Information Technology Security Inspections” (Ministry of Education of the People's Republic of China et al., 2025) and the Ministry of Industry and Information Technology (MIIT) organizing “APP Miscollection Rectification Actions” (Ministry of Industry and Information Technology of the People's Republic of China [MIIT], 2019).

In contrast, the regulatory responsibility in Hong Kong and Macao is more centralized and established independent authorities. In Hong Kong, The Office of the Privacy Commissioner for Personal Data (PCPD) serves as the unified agency responsible for targeted enforcement against illegal data processing. While in Macao, the Gabinete para a Protecção de Dados Pessoais (GPDP), often referred to as the Personal Data Protection Bureau (DSPDP) or Office for Personal Data Protection, handles centralized enforcement. Due to escalating potential risks associated with personal data in recent years, the enforcement powers of both the PCPD and GPDP have been elevated, allowing them to collaborate directly with public security and judicial authorities, including conducting criminal investigations (Tao, 2021). Notably, the Hong Kong PCPD, recognized as one of Asia's earliest independent privacy regulatory bodies, maintains a high degree of independence. The appointed Privacy Commissioner is not subject to the jurisdiction or direction of any other Hong Kong institution or person

(Li, 2010), and the PCPD supervises all organizations managing personal data in Hong Kong, including government departments.

### 3.2 Divergent Relief Mechanisms and Coordination Challenges for Children's Data Violations

Beyond the differences in regulatory bodies and their scopes of power, the crucial question of how to achieve cross-boundary relief following a violation of children's data still requires systematic coordination and improvement. Although all three jurisdictions have established a comprehensive tripartite protection mechanism at the legislative level—encompassing civil remedies, administrative enforcement, and criminal accountability—the underlying principles and implementation pathways for relief differ significantly across the regions. Overall, the core relief principles for children's data protection in the three jurisdictions are characterized as follows: in mainland China, relief is guided by the fundamental principles of guardian representation and the priority of public interest (Gao, 2022). Hong Kong's remedial pathway is characterized by judicial relief under administrative action (Office of the Privacy Commissioner for Personal Data, Hong Kong [PCPD], 2021), whereas Macao's approach features limited administrative intervention under judicial dominance (Feng & Liu, 2023).

Currently, relying on government supervision is the common means of addressing children's data protection and cross-boundary data issues in major countries, including China and European nations (Wang, 2025). However, due to the differences in regulatory bodies and their scopes of authority (as discussed in Section I), the inter-departmental coordination of administrative supervision and enforcement during cross-boundary data flow among the Mainland, Hong Kong, and Macao remains to be clearly defined.

In Mainland China, they follow fragmented multi-sectoral model. As previously stated, the Mainland has not established a single, independent regulatory agency. It relies primarily on the Cyberspace Administration of China (CAC) for overall coordination, collaborating with multiple other departments for supervisory enforcement. Administrative enforcement is the most significant mechanism for combating violations of children's Personal Information (PI) in the Mainland, constructing a multi-departmental, industry-specific supervision model led by the CAC. But there remains systemic flaw: Because agencies like the Ministry of Education, the National Health Commission, and the Public Security Bureau conduct enforcement separately by sector, this model suffers from systemic defects, including functional overlap, ambiguity of responsibilities, and collaborative inefficiency (Tao, 2021).

While in Hong Kong and Macao, they follow much centralized and independent agency model. Both Hong Kong and Macao conduct supervision and enforcement through specially established data protection agencies: in Hong Kong the Office of the Privacy Commissioner for Personal Data (PCPD) oversees the security of children's data according to the PDPO. The PCPD employs various means to raise awareness among teachers, students, and parents regarding children's data protection, including educational materials, a "Children Privacy" dedicated website, lectures, and school promotion schemes. It enforces rules by handling complaints and penalizing those who illegally process or disclose data. The 2023–2024 annual report cited the handling of several hundred data leakage incidents, including cases involving the misuse or leakage of children's data. The PCPD subsequently initiated inspections of education departments and public institutions, mandating rectification and remedial actions (Office of the Privacy Commissioner for Personal Data, Hong Kong [PCPD], 2024). Similarly, Macao has also prioritized data protection, upgrading its former Office for Personal Data to the Gabinete para a Protecção de Dados Pessoais (GPDP) in 2024. The GPDP is responsible for enforcing the Personal Data Protection Act within its mandate and collaborating with other departments on cross-sectoral enforcement in relevant protection areas (Personal Data Protection Bureau of the Macao Special Administrative Region [DPDP], 2025).

All three jurisdictions offer the potential for judicial relief when children's data has been illegally violated. In Hong Kong and Macao, children who suffer unlawful harm can autonomously choose among the tripartite protection mechanisms: civil remedy, administrative enforcement, and criminal accountability. In Hong Kong, relief is characterized by judicial remedy led by administrative action. Notably, this encompasses the class action mechanism (Privacy Commissioner's Office [PCPD], 2021) inherent to the Common Law system. A classic example involves the 2018 data breach at Cathay Pacific, resulting in the large-scale leakage of data for approximately 9.4 million passengers globally, including some children.

Beyond the local administrative penalties, where the Hong Kong Privacy Commissioner found Cathay liable for “failing to identify a well-known and exploitable security flaw, failing to identify the exploitation of the flaw, and failing to take all reasonably practicable steps for proper deployment when setting up the servers” (Office of the Privacy Commissioner for Personal Data, Hong Kong [PCPD], 2019), the airline also faced international consequences. These included a £500,000 fine from the UK Information Commissioner’s Office in 2020 and a settlement of 1.55 million in a Canadian class-action lawsuit in 2021 (Office of the Privacy Commissioner for Personal Data, Hong Kong [PCPD], 2022). As an international hub, Hong Kong’s data protection is secured by various relief pathways under the global Common Law system, which includes local administrative supervision and penalties, as well as the risk of investigation or class actions for improper handling of data belonging to citizens of other countries. In Macao, the relief pathway is characterized by limited administrative intervention guided by judicial action. Litigation primarily relies on individual party initiation rather than the collective action model, making the cost of private redress generally higher in Macao (Feng & Liu, 2023). To date, Macao has seen no civil or criminal cases filed specifically due to data breaches. When a data breach occurs, individuals mainly rely on filing complaints with the GPD (DSDP). Upon receiving a complaint, the GPD promptly handles the matter, imposing fines or issuing warnings (Personal Data Protection Bureau of the Macao Special Administrative Region [DPDP], 2024). In recent years, the Mainland has sought to establish effective protection for children’s Personal Information through public interest litigation (PIL). Since its implementation in 2021, procuratorates have filed multiple PIL cases related to children’s PI protection, publicizing them as typical cases. A case publicized by the procuratorate in 2021 involved a music teaching app that illegally collected, stored, and used personal information. The procuratorate filed a civil public interest lawsuit. Through mediation, the company voluntarily agreed to comprehensive rectification of the app, deletion of all illegally collected and stored user personal information, issuance of a public apology, and a commitment to cease future infringement. The procuratorial organ introduced a third-party representative to assess the app’s subsequent rectification, allowing it to be re-listed only after compliance testing (Supreme People’s Procuratorate - Jian Da Net [SPP-Jian Da], 2021).

The Mainland (Guangdong), Hong Kong, and Macao have established systematic relief pathways for children’s data protection. However, the independent nature of the three jurisdictions’ administrative and judicial systems necessitates institutional adjustments for the coordinated recognition and enforcement of administrative penalties and judicial decisions. While the Hong Kong Mainland Judgments in Civil and Commercial Matters (Reciprocal Enforcement) Ordinance has been enacted and took effect in January 2023 (Department of Justice, The Government of the Hong Kong Special Administrative Region [DOJ], 2024), a mechanism for the reciprocal recognition of administrative and criminal judgments has not yet been established. Consequently, in cases of cross-boundary data violation, several critical questions remain unanswered and require further clarification: Which specific authority should the victim file a complaint with? Specifically, how can judicial decisions resulting from the Mainland’s unique form of administrative public interest litigation be incorporated into a mechanism for judicial mutual recognition?

#### **4. Coordination and Adjustment of Cross-Boundary Children’s Data Protection in the GBA**

To address the multi-dimensional differences in legislation, enforcement, and judicial practices among the Mainland (Guangdong), Hong Kong, and Macao regarding cross-boundary data flow, and to concurrently advance GBA integration, facilitate the construction of the “Digital Greater Bay Area,” and enhance data security cross-boundary coordination, the PRC has undertaken a series of institutional adjustments and integration arrangements in recent years. A critical step in this process was the joint issuance of two documents by the Cyberspace Administration of China (CAC), in collaboration with the Hong Kong SAR’s Innovation, Technology and Industry Bureau, and Macao SAR’s Economic and Technological Development Bureau and the Personal Data Protection Bureau (GPD): The Standard Contract for Cross-Boundary Flow of Personal Information within the Guangdong-Hong Kong-Macao Greater Bay Area (Mainland and Hong Kong) (officially effective December 2023). The Standard Contract for Cross-Boundary Flow of Personal Information within the Guangdong-Macao Greater Bay Area (Mainland and Macao) (officially effective September 2024). The objective is to “jointly formulate and promote the implementation of the Standard Contract for personal information cross-boundary flow in the GBA, and to strengthen the record-filing management of the Standard Contract for cross-boundary personal

information flow” (Office of Cyberspace Affairs of Guangdong Province [GDOCA], 2024).

#### 4.1 Divergent Regulatory Frameworks for Cross-Boundary Data Flow

The Mainland, Hong Kong, and Macao have each established distinct regulatory frameworks governing cross-boundary data flow, which encompass the issue of children’s data movement.

Mainland China focus mainly on security assessment. In 2022, the Mainland’s CAC issued the Measures for Security Assessment of Outbound Data Transfers. This primarily guides and standardizes the flow of commercial and platform data. Within governmental information scenarios, the cross-border transfer of children’s data is often handled by default through government platforms, lacking an independent review process or a specific mechanism for the outbound management of children’s data.

Hong Kong follow liberal flow Policy but left some enforcement gaps. Hong Kong’s Personal Data (Privacy) Ordinance (PDPO) and Macao’s Personal Data Protection Act (PDPA) were modeled on the European Union’s 1995 Data Protection Directive and the 1980 OECD Guidelines on the Protection of Privacy. The PDPO, launched in 1996, marked the beginning of Hong Kong’s data cross-border protection efforts. However, Section 33 of the Ordinance, which pertains to cross-border data transfer, remains unenforced to this day. Consequently, Hong Kong has historically maintained a liberal data cross-border flow policy. Minor amendments were introduced in 2013 (requiring disclosure of cross-border policy) and 2021 (adding “doxing” clauses), but the cross-border mechanism itself was not altered, leaving Hong Kong’s policy as essentially free data flow. It was not until May 2022 that the Hong Kong PCPD issued a non-mandatory cross-border transfer guideline, the Guidance on Cross-border Data Transfer: Recommended Model Contractual Clauses. Given that this compliance advice lacks mandatory force, the Privacy Commissioner’s authority in handling disputes related to cross-border personal information transfer is often deemed insufficient (Cao & Sang, 2024).

Macao obtained conditional transfer model and adopted some Mainland Rules. Macao’s approach to cross-border data transfer is clearly defined in Article 19 of the PDPA: data transfer is only permitted if it complies with the law and the legal system of the receiving jurisdiction ensures an adequate level of protection. This “adequate level of protection” must be assessed based on the totality of the transfer circumstances, considering factors such as the nature of the data, processing purpose and duration, origin and final destination, existing general or specific legal rules, and adherence to professional rules and security measures. Significantly, following the Mainland’s issuance of the Measures for Security Assessment of Outbound Data Transfers, Macao directly migrated this framework into its local regulations, providing a six-month preparation period before its official implementation in March 2023 (Office for Personal Data Protection of the Macao Special Administrative Region [OPDP], 2022).

#### 4.2 Establishing a Coordinated Cross-Boundary Protection Solution via Standard Contracts

Given the differing cross-boundary regulatory philosophies across the three jurisdictions, advancing the adjustment of data flow across these distinct institutional frameworks has become a pivotal issue for GBA integration. It is also a major agenda item for the PRC as it pioneers efforts to facilitate data cross-border movement and improve the digital economy structure. In recent years, the three governments have launched a series of institutional initiatives and breakthroughs:

2019 (Outline Development Plan): Clarified the goal to establish policies promoting the cross-boundary flow and regional integration of innovation factors, including talent, capital, information, and technology, and to jointly construct a GBA big data center.

2021 (Shenzhen Special Economic Zone Data Regulation): Mandated the construction of a data factor market system to facilitate the orderly, efficient flow and utilization of data resources.

September 2021 (Overall Plan for the Construction of the Guangdong-Macao In-Depth Cooperation Zone in Hengqin): Initiated a pilot program for secure cross-boundary data transmission, aiming to realize the interconnection of scientific research data.

2023 (Three-Year Action Plan for the Construction of the “Digital Bay Area”): Explicitly called for data flow to drive the marketization of factors, and explored the implementation of a “White List” system for cross-boundary data circulation.

November 2023 (Implementation Opinions of the People’s Government of Guangdong Province on Accelerating the Construction of a Leading Innovation Hub for General Artificial Intelligence Industry): Proposed exploring the creation of a “GBA Data Special Zone” and establishing a system of internal data circulation rules for the Bay Area.

Under the foundation laid by these policies, the two Standard Contracts were officially released, creating an institutional coordination framework based on regulatory policy texts. This framework employs a contractual record-filing mechanism to establish a secure and orderly cross-boundary data system for the three jurisdictions.

Following the release of the two Standard Contracts, the drafting departments also issued the Implementation Guidelines for the Standard Contract for Cross-Boundary Flow of Personal Information within the GBA, providing detailed regulatory guidance. Public data shows that as of August 2024, the CAC of Guangdong Provincial Committee guided local enterprises to complete 73 Standard Contract record-filings for personal information outbound transfers, and 21 Standard Contract record-filings for the GBA (Mainland and Hong Kong) Cross-Boundary Flow (Wang & Li, 2024). In November 2024, the application of this Standard Contract record-filing mechanism in Hong Kong was expanded from its initial scope (medical, technology, finance) to cover all industries (News Bulletin of the Government of the Hong Kong Special Administrative Region [HKSARG News Bulletin], 2024). The adoption of the Standard Contracts aims to simplify compliance procedures, reduce the compliance burden on enterprises, and promote the secure, smooth, and efficient cross-boundary flow of data, thus establishing a controllable framework for the cross-boundary circulation of personal information. Therefore, while core challenges—such as the legal non-uniformity and regulatory divergences specific to children’s data cross-boundary protection—have not been resolved through unified legislation or enforcement via a formal ordinance, this approach successfully establishes a relatively clear contractual solution for cross-boundary data protection.

### **4.3 Standard Contracts: Adherence to Local Rules and Local Assignment of Responsibility**

The implementation of the Standard Contracts is not a panacea for the institutional differences in cross-boundary data protection among the three jurisdictions. Rather, it establishes a fundamental coordination framework where cross-boundary children’s data protection adheres to the local rules of data flow, thus clarifying the boundaries of responsibility based on territorial arrangements.

#### **4.3.1 Territorial Responsibility Mechanism for Data Processors**

The Standard Contract employs a territorial responsibility orientation mechanism for data processors. The contract provides guidance that local rules must be followed. For example, Article 2(3) clarifies the “Consent Rule” within the basic information processing framework, specifying that consent must be obtained according to the local regulations of the data processor. While Article 8 covers dispute resolution, stipulates that the formation, validity, performance, interpretation, and any disputes arising from the contract shall be governed by the relevant laws and regulations of the personal information processor’s locality. The contract relies on the local regulations of the information processor as the basis for handling, thereby adapting separately to the Mainland’s Personal Information Protection Law, Hong Kong’s Personal Data (Privacy) Ordinance, and Macao’s Personal Data Protection Act.

#### **4.3.2 Managing Regulatory Discrepancies through Collaboration**

Regarding the management of regulatory standard differences, the Standard Contract and the Implementation Guidelines establish a mechanism for accepting complaints and processing them by all regulatory agencies based on local supervision. Articles 9 and 10 of the Implementation Guidelines create a multi-agency cooperation framework, allowing complaints to be filed with any local regulatory authority to trigger joint processing. Article 5 of the Implementation Guidelines helps bridge regulatory gaps by mandating uniform standards for impact assessments. To address the challenges of cross-boundary relief, Article 4 of the contract designates the individual data subject as a third-party beneficiary, establishing a priority of interest principle. This supports children and their guardians in directly demanding deletion or correction from the recipient and allows for flexible selection of relief avenues by initiating arbitration through the Mainland, Hong Kong, or Macao courts.

### 4.3.3 Strict Control over Data Flow Risk

The Standard Contract imposes strict limitations on the scope of data processing, requiring data processors to adhere to the Principle of Minimal Necessity while maximizing the protection of the third-party beneficiary. Articles 3(7) and 3(8) create a closed-loop management system, prohibiting the transfer of data outside the GBA and further restricting secondary transfers. As with restricted dissemination, works in conjunction with Article 4 of the Implementation Guidelines, establishing requirements for restricted dissemination based on a foundation of full informed consent.

The Standard Contract and Implementation Guidelines address the institutional differences among the three jurisdictions by adopting mechanisms like record-filing management and joint notification to achieve regulatory linkage and clarify responsibilities, aiming to construct a relatively comprehensive cross-boundary data protection system. However, children, as a special group, have not been adequately considered. From the perspective of commercial data cross-boundary flow, how the Mainland's dominant role in data processing influences data flow in Hong Kong and Macao and how this forms coordination experience applicable to global data cross-boundary practices still requires further practical exploration and refinement.

## 5.Outlook for Coordinated Cross-Boundary Children's Data Protection in the Greater Bay Area

The economic integration of the Mainland (Guangdong), Hong Kong, and Macao, coupled with the rapid development of the digital industry, has seen considerable progress in GBA children's data protection coordination and institutional development within the context of the "Digital Bay Area" initiative. However, the reality of "One Country, Two Systems, Three Jurisdictions" persists, creating numerous institutional coordination difficulties between children's data protection and the accelerated cross-boundary flow of data that require further refinement. Overall, future development should prioritize strengthening coordination mechanisms in children's data protection across the following dimensions.

Firstly, enhancing data security under the Standard Contract Framework. Future efforts should focus on incorporating specific children's data flow and protection clauses within the Standard Contract framework. This requires legislative coordination across the three jurisdictions to define and clarify: The scope and definition of children's data. The mechanism for guardian processing. The responsible protection entities. The goal is to use definitive clauses to bridge the current practical differences in the recognition of children's data and the designated protection entities. Specifically, it must be clarified and refined whether additional consent and authorization mechanisms are required during cross-boundary transfers.

Secondly, establishing a cross-jurisdictional regulatory coordination mechanism. It is essential to establish a normalized regulatory coordination mechanism to handle complaints related to children's data violations across the three jurisdictions. The establishment of a unified regulatory body is fundamental to resolving cross-boundary children's data transfer disputes and safeguarding the rights of this special group in the GBA. Since a single regulatory department does not yet exist, a prospective approach involves establishing a unified, coordinating body to end the "acting-alone" state of cross-boundary children's data supervision. This would prevent institutional friction, mitigate regulatory gaps, and avoid impeding the flow of children's data (Yu & Zhang, 2023). A basic framework for this unified body could draw upon the existing regulatory models in Hong Kong and Macao, defining statutory functions, constructing the organizational structure, and building an operational model. It should establish a unified cross-boundary complaint handling mechanism to receive reports from parents or children regarding data misuse, leakage, and related risks, and coordinate the enforcement resources of the three jurisdictions for investigation and disposal.

Third, exploring reciprocal recognition of children's data protection litigation. It is necessary to explore mechanisms for the reciprocal recognition of various forms of litigation concerning children's data protection across the three jurisdictions. A basic consensus in data protection is that data violations often go unnoticed by the data subject—especially the more internal, non-consensual collection and utilization through information networks—until the results of the infringement manifest (Zhuhai People's Procuratorate Public Interest Litigation Research Group, 2023). Therefore, the international trend involves exploring and implementing class action or public interest litigation in data protection. While the three jurisdictions currently have different litigation avenues to protect children's data rights, given that the general

mechanism for judicial mutual recognition is still incomplete, a specific opening can be created in the specialized field of children's data protection to push for the mutual recognition of criminal and administrative litigation. By prioritizing the assurance of children's data, this could drive the overall development of data flow across the GBA.

## Funding Information

This work was supported by the Guangdong Provincial Philosophy and Social Sciences *14th Five-Year Plan* Discipline Co-construction Project (Project No.GD22XXW04) on *Coordination and Mutual Learning in Children's Personal Information Protection in the Guangdong-Hong Kong-Macao Greater Bay Area*, and supported by the Ministry of Education Humanities and Social Sciences Research Youth Fund Project (Project No.22YJC860017) on *Dilemmas and Solutions of the Consent Mechanism for Children's Personal Information Protection*.

## References

- Cao, X., & Sang, X. (2024). On the coordinated protection of personal information between Hong Kong and Mainland China. *Hong Kong and Macao Studies*, (01), 38–49, 94–95.
- China Research Network. (2025, March 7). 2025 research report on industrial collaboration and cross-boundary data flow policies in the Guangdong-Hong Kong-Macao Greater Bay Area. <https://m.chinairn.com/news/20250307/162903909.shtml>
- Cyberspace Administration of China. (2025, March 28). Announcement on launching the 2025 series of special actions for personal information protection by the Cyberspace Administration of China, the Ministry of Industry and Information Technology, the Ministry of Public Security, and the State Administration for Market Regulation. [https://www.cac.gov.cn/2025-03/28/c\\_1744867353112759.htm](https://www.cac.gov.cn/2025-03/28/c_1744867353112759.htm)
- Department of Justice of the Hong Kong Special Administrative Region Government. (2024, February 2). Arrangement between Hong Kong and the Mainland on reciprocal recognition and enforcement of judgments in civil and commercial matters. [https://www.doj.gov.hk/tc/mainland\\_and\\_macao/RRECCJ.html](https://www.doj.gov.hk/tc/mainland_and_macao/RRECCJ.html)
- Feng, Z., & Liu, X. (2023, August 28). Governing cross-boundary data flow in the Guangdong-Hong Kong-Macao Greater Bay Area with the rule of law. *Southern Daily*. [https://www.cnbayarea.org.cn/news/voices/content/post\\_1125574.html](https://www.cnbayarea.org.cn/news/voices/content/post_1125574.html)
- Gao, Z. (2022). Public interest considerations in personal information protection: From the perspective of responding to public health emergencies. *Oriental Law*, (03), 17–32.
- Google. (n.d.). Age requirements for Google Accounts. Google Accounts Help. Retrieved August 9, 2025, from <https://support.google.com/accounts/answer/1350409?hl=zh-Hans>
- Guangdong Communications Administration. (2024, March 22). Guangdong Province high-quality development action for computing infrastructure and “Yue Suan” action plan (2024-2025). <https://www.cagd.gov.cn/v/2024/03/4773.html?utm>.
- Li, L. C., & Kwok, M. T. (2019). Unpacking the plan for the Guangdong–Hong Kong–Macao greater bay area: A mechanism for reform. *China and the World*, 2(02), 1950010.
- Li, Y. (2010, July 13). Hong Kong Privacy Commissioner Wu Bin: Emphasizing investigation and education to cultivate a society that respects privacy. *Southern Metropolis Daily*, AA27. <https://news.sina.com.cn/c/2010-07-13/065217795411s.shtml>
- Ministry of Education of the People's Republic of China. (2025, April 11). Opinions of the Ministry of Education and eight other departments on accelerating the digitalization of education (Jiao Ban [2025] No. 3). <https://w>

[www.gov.cn/zhengce/zhengceku/202504/content\\_7019045.htm](http://www.gov.cn/zhengce/zhengceku/202504/content_7019045.htm)

Ministry of Industry and Information Technology of the People's Republic of China. (2019, October 31). Notice of the Ministry of Industry and Information Technology on launching the special campaign for rectifying APP infringement of user rights and interests (Gong Xin Bu Xin Guan Han [2019] No. 337). [https://www.gov.cn/zhengce/zhengceku/2019-11/13/content\\_5451505.htm](https://www.gov.cn/zhengce/zhengceku/2019-11/13/content_5451505.htm)

Office for Personal Data Protection. (2022, November 24). Office for Personal Data Protection urges local sectors in Macao to pay attention to mainland China's data exit regulations. <https://www.gov.mo/zh-hant/news/945992/>

Office of the Cyberspace Affairs Commission of Guangdong Province. (2024, September 18). Notice regarding the implementation of the Implementation guidelines for the standard contract on cross-boundary personal information flow in the Guangdong-Hong Kong-Macao Greater Bay Area (Mainland, Macao). <https://www.cagd.gov.cn/v/2024/09/5773.html>

Office of the Privacy Commissioner for Personal Data, Hong Kong. (2015, December). Children's online privacy: Advice for parents and teachers [Brochure]. [https://www.pcpd.org.hk/tc\\_chi/resources\\_centre/publications/files/leaflet\\_childrenonlineprivacy\\_c.pdf](https://www.pcpd.org.hk/tc_chi/resources_centre/publications/files/leaflet_childrenonlineprivacy_c.pdf)

Office of the Privacy Commissioner for Personal Data, Hong Kong. (2019, June 6). Data leakage incident investigation report: Cathay Pacific Airways Limited and Hong Kong Dragon Airlines Limited's unauthorized access or viewing of passenger personal data [Investigation report]. [https://www.pcpd.org.hk/tc\\_chi/enforcement/commissioners\\_findings/investigation\\_reports/files/PCPD\\_Investigation\\_Report\\_R19\\_15281\\_Chi.pdf](https://www.pcpd.org.hk/tc_chi/enforcement/commissioners_findings/investigation_reports/files/PCPD_Investigation_Report_R19_15281_Chi.pdf)

Office of the Privacy Commissioner for Personal Data, Hong Kong. (2022, October). Protection of personal data in the digital age. [https://www.pcpd.org.hk/tc\\_chi/news\\_events/newspaper/newspaper\\_202210.html](https://www.pcpd.org.hk/tc_chi/news_events/newspaper/newspaper_202210.html)

Office of the Privacy Commissioner for Personal Data, Hong Kong. (2024, October 31). Privacy Commissioner's Office publishes investigation findings on the data breach incident of South China Athletic Association and launches "Data Security" package for schools, NGOs and SMEs [News release]. <https://www.pcpd.org.hk/misc/dpoc/newsletter173.html>

Office for Personal Data Protection, Macao. (2024, November 5). Case study: Domestic helper posting images of a minor on social media without consent. [https://www.dspdp.gov.mo/zh\\_tw/abstract\\_detail/article/m33tc6em.html](https://www.dspdp.gov.mo/zh_tw/abstract_detail/article/m33tc6em.html)

Office for Personal Data Protection of the Macao Special Administrative Region. (2025, July 10). Introduction to the Public Assets Supervision and Administration Office. <https://www.gov.mo/zh-hant/apm-entity-page/gov-department-institutions-of-the-msar/apm-1/apm-8705/>

Privacy Commissioner's Office. (2021, October 8). The Personal Data (Privacy) Ordinance. [https://www.pcpd.org.hk/english/data\\_privacy\\_law/ordinance\\_at\\_a\\_Glance/ordinance.html](https://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html)

Prosecutorial Q&A Network of the Supreme People's Procuratorate. (2021, July 15). Typical cases of procuratorial organs' public interest litigation on personal information protection: Severing the profit chain between personal information infringement and telecommunication network fraud. <http://www.anding.jcy.gov.cn/info/1028/1397.htm>

Tao, N. (2021). The dilemma and response of cross-boundary personal information governance in the Guangdong-Hong Kong-Macao greater bay area. *Journal of Guangzhou Police College*, 31(01), 28-32.

The Government of the Hong Kong Special Administrative Region. (2024, November 1). The Greater Bay Area (Mainland, Hong Kong) cross-boundary personal information flow standard contract facilitation measure extended to all industries. <https://www.info.gov.hk/gia/general/202411/01/P2024110100286.htm>

Wang, C. C. (2025). Law and practice of personal data protection in the digital world: A comparison between

n China, the EU, and the US. *Tulane Journal of International and Comparative Law*, 33(1), 2169–4516.

Wang, Q. (2011). On the right to privacy in the Macau civil code and its implications for relevant legislation in Mainland China. “One Country, Two Systems” Studies, (7), 112–119.

Wang, Z., & Li, Q. (2024). How to protect data security under the wave of artificial intelligence? Listen to experts' opinions. *Southern Metropolis Daily*. <https://www.21jingji.com/article/20240911/herald/568a9b7c0f34b4622ba0561fded818bd.html>

Xia, Y. (2018). On the legislative style of minors' guardianship in the civil code. *Jurist*, (04), 1–15, 191.

Xiao, P., & Guan, Q. (2025). The practical dilemma and improvement path of the guardian's informed consent principle. *Yangtze Forum*, (01), 86–98.

Ye, X. (2025). Personal information protection in the context of generative artificial intelligence: Paradigm shift and rule improvement. *Jurist*, (04), 61–73, 192.

Yu, Z., & Zhang, L. (2023). Analysis of China's cross-boundary data flow rules: Based on the pioneering practices in the Guangdong-Hong Kong-Macao greater bay area. *China Opening Journal*, (02), 86–93.

Zhai, Z. (2021). The systematic positioning of the Data Security Law. *Journal of Soochow University (Philosophy & Social Science Edition)*, 42(1), 73–83.

Zhuhai People's Procuratorate Public Interest Litigation Research Group. (2023). The Zhuhai practice of procuratorial public interest litigation on personal information protection. In S. Wu, S. Chen, H. Tian, et al. (Eds.), *Annual report on rule of law in Zhuhai No. 5 (2023)* (pp. 168–176). Social Sciences Academic Press.