

Cross-border Personal Data Transfers in the Greater Bay Area

Zhihong Dai

Guangdong Institute for International Strategies, Guangdong University of Foreign Studies, Guangzhou 510000, Guangdong, China

Corresponding author: Zhihong Dai (e-mail: a470781905@outlook.com)

ABSTRACT This article investigates how regulatory fragmentation across Mainland China, Hong Kong, and Macao shapes cross-border transfers of personal data in the Guangdong–Hong Kong–Macao Greater Bay Area (GBA) and its impact on data-intensive sectors such as finance, digital services. As next-generation wireless communication networks and electromagnetic information transmission technologies increasingly support cross-border digital infrastructure, establishing secure and legally compliant data flows has become an essential prerequisite for regional digital integration. Adopting a doctrinal and comparative approach, this study analyses the Personal Information Protection Law (PIPL), Hong Kong’s Personal Data (Privacy) Ordinance (PDPO), Macao’s Personal Data Protection Act (PDPA), and the GBA Standard Contract. It identifies three major fault lines involving export pathways and procedures, definitions and lawful bases for processing, and enforcement architecture across the three jurisdictions. These divergences generate duplicative compliance obligations, increase operational costs, and impede data mobility for finance, research, services. The article further evaluates the GBA Standard Contract as a pragmatic sub-regional mechanism that simplifies compliance while preserving local autonomy and proposes a roadmap based on minimum-standard harmonisation, mutual recognition, coordinated complaint handling, third-party certification, technical safeguards including encryption and anonymisation, and sectoral pilot sandboxes. The proposed legal framework facilitates secure and efficient cross-border data flows while supporting interoperable digital infrastructures under the “one country, two systems” framework.

INDEX TERMS cross-border personal data transfer, Greater Bay Area, digital infrastructure, electromagnetic information transmission, legal harmonisation

I. INTRODUCTION

A. BACKGROUND AND SIGNIFICANCE

The Guangdong–Hong Kong–Macao Greater Bay Area (GBA) stands as a flagship initiative in China’s regional integration agenda. It brings together nine principal cities in the Pearl River Delta and the two special administrative regions of Hong Kong and Macao, covering roughly 56,000 square kilometres and home to over 87 million residents. The region generates an economy of more than RMB 14.5 trillion (around US \$1.95 trillion) and is a key engine for China’s innovation-driven development. Deepening integration within the GBA aims to harness the complementary advantages of its constituent cities, encourage coordinated economic growth, and bolster China’s participation in global economic governance. Data are the lifeblood of the GBA’s “digital bay” agenda. Cross-border data flows enable businesses and governments to deliver integrated services, facilitate seamless financial and trade transactions, and foster new digital industries. This is especially critical for the GBA’s traditional but highly digitised sectors. Official pronouncements recognise that the free flow of data within the GBA is essential to innovation and high-quality

economic development. As people and firms increasingly operate across regional boundaries, the ability to exchange personal data securely and efficiently has become a practical necessity [1,2]. However, while the economic rationale for data mobility is clear, the legal and regulatory environment is fragmented.

B. REGULATORY DIVERGENCE AND RESEARCH MOTIVATION

Mainland China, Hong Kong, and Macao each operate under separate legal regimes for the protection of personal data. Recent reforms on the mainland—most notably the 2021 Personal Information Protection Law (PIPL)—have introduced stringent conditions for transferring personal information abroad, including obligatory security reviews, certification by qualified bodies, or reliance on state-approved standard contractual clauses. In contrast, Hong Kong’s Personal Data (Privacy) Ordinance (PDPO) presently places no binding constraints on cross-border transfers; Section 33, which would restrict data export to jurisdictions lacking “comparable protection,” has not taken effect, meaning that transfers outside Hong Kong remain generally unregulated provided

the basic data protection principles of notice and consent are observed.

Macao applies a European-inspired model: under the 2005 Personal Data Protection Act, data may be exported only if the receiving jurisdiction guarantees an adequate level of protection or when specific legal conditions are met. These differing regulatory models produce a fragmented landscape, increasing the complexity of cross-border compliance and hindering smooth data movement within the GBA. Scholars have noted that this lack of regulatory harmonisation is a principal obstacle to realising the economic potential of the GBA. Tao Ning's 2021 study on cross-border governance of personal information observed that differences in legal principles, institutional structures, and operational mechanisms prevented effective legal convergence and mutual trust; Tao urged the mainland to accelerate legislation, establish dedicated regulators, and adopt model laws or sector-specific co-regulation to break the governance impasse. More recently, Au and Witzleb argued that expecting complete legal unification is unrealistic in the short term; instead, they proposed a coordinated framework for cross-border data export as a practicable interim solution [3]. For high-volume data users like manufacturers, these divergences translate into significant operational burdens and compliance costs when managing customer data for personalised marketing or transferring employee data across GBA offices. Taken together, these studies highlight the necessity of comparative legal inquiry to identify key divergence, assess their practical implications, and evaluate mechanisms for narrowing regulatory gaps. In June 2023, the Cyberspace Administration of China and Hong Kong's Innovation, Technology and Industry Bureau executed a co-operation memorandum aimed at facilitating cross-boundary data flows. This cooperation produced the GBA Standard Contract, a simplified contractual regime for personal data transfers between the mainland and Hong Kong that removes certain volume thresholds and impact assessment requirements found in the PIPL and limits onward transfers outside the GBA. Similar measures have been announced for transfers between the mainland and Macao. These initiatives mark an important step toward regulatory coordination, yet their effectiveness depends on how well they reconcile the underlying differences in the three jurisdictions' data protection laws.

II. LEGISLATIVE AND PRACTICAL FRAMEWORK OF CROSS-BORDER PERSONAL DATA TRANSFERS IN MAINLAND CHINA, HONG KONG, AND MACAO

A. MAINLAND CHINA: A COMPREHENSIVE FRAMEWORK FOR CROSS-BORDER PERSONAL DATA TRANSFERS

1) Legal Framework

In the last decade Mainland China has progressively established a comprehensive architecture for regulating personal data and its outbound transfers. The centrepiece is the Personal Information Protection Law (PIPL), enacted in 2021,

the first legislation to regulate personal data processing comprehensively. The PIPL requires personal information processors to obtain separate consent and, when exporting personal data, to proceed via security review, certification, or the Standard Contract [4]. In addition, exporters must state the overseas recipient's identity and location and conduct personal information protection impact assessments (PIAs). Taken together, these rules create a three-track compliance structure for cross-border transfers, with the Cyberspace Administration of China (CAC) as the lead supervisory authority. Prior to the PIPL, regulation relied largely on the Cybersecurity Law and sectoral localisation requirements for "important data" and for critical information infrastructure operators. With the PIPL in force, the regulatory framework has broadened markedly. Policymakers have developed a "3+N" governance architecture that takes the Cybersecurity Law, Data Security Law, and PIPL as its core statutes, complemented by the Measures for Security Assessment of Cross-Border Data Transfers, the Personal Information Protection Certification Implementation Rules, the Measures on the Standard Contract for the Outbound Transfer of Personal Information, and the Provisions on Promoting and Regulating Cross-border Data Flows [5]. Collectively, these instruments delineate three lawful export routes—security assessment, certification, and the Standard Contract. Under CAC oversight, the security assessment path is triggered by exports that involve important data or high-volume personal information; the certification path enables organisations to evidence compliance via accredited third-party audits; and the Standard Contract provides a ready-to-use template suitable for small- and mid-scale transfers. The PIPL and its implementing rules impose risk and PIA obligations and require record-filing with the CAC so regulators can oversee the full lifecycle of outbound transfers.

2) Practical Developments

The coming into force of the PIPL has rendered the regulation of cross-border data more structured and coherent. Since the Measures for Security Assessment of Cross-Border Data Transfers took effect in 2022, numerous China-based companies—especially multinational groups—have filed their outbound data schemes for review by the CAC. After the Measures on the Standard Contract for the Outbound Transfer of Personal Information became effective in 2023, many firms adopted the Standard Contract and completed the requisite filings with regulators, which in turn improved domestic firms' awareness and capability in managing cross-border compliance. Meanwhile, the authorities have initiated regional pilot programmes and differentiated management approaches to balance security requirements with operational efficiency; within free trade zones and the GBA, regulators have eased selected requirements for particular sectors. Overall, China has shifted from a largely uncoordinated landscape to a highly detailed and comprehensive regime for cross-border personal data transfers, featuring strong safeguards for data security and privacy while setting

specific procedural requirements for outbound flows.

B. HONG KONG: FLEXIBLE RULES WITH VOLUNTARY CROSS-BORDER SAFEGUARDS

1) Legal Framework

Hong Kong's current legal framework for cross-border transfers is comparatively permissive. The Personal Data (Privacy) Ordinance (PDPO), which entered into force in 1996, is a comprehensive privacy law that articulates six data protection principles requiring data users to protect personal data security, limit its use to stated purposes, and ensure fair handling. However, Section 33 of the PDPO—designed to restrict cross-border transfers to jurisdictions with comparable protection—has not commenced and remains unenforced. Owing to industry concerns that implementation might hamper business operations, the Hong Kong government has not issued the requisite code of practice. As a result, Hong Kong lacks a dedicated, destination-based cross-border transfer restriction comparable to the mainland's export regime or Macao's adequacy model. Nevertheless, Data Protection Principle 3 (use limitation) and Principle 4 (data security) impose binding constraints on how personal data may be handled and disclosed, including when data is sent overseas: data may not be used or transferred for new purposes without the data subject's prescribed consent, and data users must take practicable steps to ensure security throughout the data lifecycle. Data users may therefore transfer personal information abroad without prior authorisation, but they remain accountable for complying with these principles before and during any export [6]. Data users may transfer personal information abroad so long as they comply with the PDPO's purpose-limitation and notice obligations [7]. Despite the absence of a mandatory export regime, the Office of the Privacy Commissioner for Personal Data (PCPD) advances best practices via soft-law instruments. In 2014 and again in 2022, the PCPD released guidance on cross-border data transfer, including recommended model contractual clauses that organisations may use to safeguard data flows. These clauses address key matters such as restricting use of transferred data to defined purposes, ensuring only necessary data are exported, protecting data-subject rights, implementing appropriate security measures, curbing onward transfers, and mandating data destruction once the contractual purpose is fulfilled. Although optional, many Hong Kong organisations employ the model clauses to evidence compliance. In addition, the PDPO's data protection principles obligate data users to maintain security measures and prevent unauthorised access or misuse, including when processing occurs outside the jurisdiction. This means Hong Kong's regime tends to facilitate data flows, while industry practice relies on contractual arrangements and internal governance to bridge regulatory gaps.

2) Practical Developments

Hong Kong's open regime allows companies and institutions to transfer personal data abroad for storage or processing

without prior approval. This flexibility facilitates commerce and data-driven services but has raised concerns about the potential risk of data leakage. In practice the PCPD has responded by issuing reports, conducting workshops, and encouraging organisations to adopt encryption and contractual safeguards. As global data protection becomes more stringent and Mainland China strengthens its laws, Hong Kong has moved to engage with mainland regulators to develop region-specific coordination mechanisms. Within the GBA framework, the Hong Kong government has recognised the need to balance data mobility with security and has actively liaised with the CAC to explore solutions. Although Hong Kong's law does not yet impose Section - 33 - style, destination - based export prohibitions, cross - border transfers remain indirectly regulated through the PDPO's purpose-limitation and security obligations, and recent guidance points to a clear trend toward enhancing governance and fostering regional cooperation.

C. MACAO: A EUROPEAN-STYLE MODEL OF STRICT CROSS-BORDER CONTROL

1) Legal Framework

The Macao Special Administrative Region (SAR) established a stringent personal data protection regime earlier than the mainland. The Personal Data Protection Act (Law 8/2005) is largely modelled on the European Union's 1995 Data Protection Directive and establishes distinct rules for personal data and for non-personal data. Under the PDPA, personal data may be transferred abroad only if the destination guarantees an adequate level of protection for personal data or if specific exceptions apply. Absent such assurance, the data controller must secure the data subject's explicit consent or rely on one of the narrow statutory derogations, and generally must notify or seek authorisation from the Personal Data Protection Bureau (PDPB). This system aligns with the EU model of "adequate protection plus derogations", reflecting Macao's strong emphasis on privacy. Macao's data protection framework is supplemented by the Cybersecurity Law (effective 2019) and a notification regime requiring data controllers to inform the PDPB of any processing activities within eight days of commencement. The PDPB supervises compliance, including granting or refusing approvals for cross-border transfers. Unlike Hong Kong's permissive system, Macao sets a high threshold for cross-border personal data flows and imposes few restrictions on non-personal data. Because of Macao's small market size, cross-border personal data transfers primarily involve the mainland and Portuguese-speaking countries. In practice, many Macao organisations must evaluate whether Mainland China's level of protection meets the "adequate" threshold and may need to obtain data subjects' consent or additional approvals before sending data across the border [8]. This rigorous regime ensures robust privacy protection but also raises compliance costs and slows data exchange.

2) Practical Developments

Macao has consistently enforced its cross-border control regime, requiring exporters to obtain licences and file notifications. The PDPB frequently reviews cross-border projects and publishes annual enforcement reports. Many businesses adopt a cautious approach, avoiding the transfer of Macao residents' personal data abroad when legal certainty is lacking and using anonymisation or aggregation to reduce risk. Recognising that strict controls could impede digital integration within the GBA, the Macao government has recently engaged in dialogue with the CAC to address regulatory incompatibilities. While Macao continues to enforce its privacy law rigorously, both regulators and industry stakeholders are considering ways to balance privacy with data flow efficiency.

D. CROSS-BORDER DATA FLOW PRACTICE AND THE GBA STANDARD CONTRACT MECHANISM

1) Growing Demand and Legal Barriers

Cross-border personal data flows have become critical for the functioning of the GBA. Frequent cross-border movement of people and businesses means that financial, trading, medical, transportation, and other services depend on sharing personal data—for instance, through cross-border wealth management, unified vehicle licensing and toll arrangements, and joint medical programmes. Yet divergent regulations have created substantial barriers. Following the entry into force of the PIPL, many Mainland enterprises discovered that transmitting users' personal information to Hong Kong or Macao for storage or customer service triggered onerous compliance requirements, including security assessments and contractual obligations. Meanwhile, Macao entities faced restrictions when sending data to the mainland and had to ensure that the recipient met "adequate" protection standards or obtain explicit consent. Legal uncertainty and differences in standards caused delays and pushed firms to consider less efficient alternatives. Data controllers often had to comply with both the stringent mainland rules and the less prescriptive Hong Kong or Macao regimes, increasing cost and complexity.

2) Creation of the GBA Standard Contract Mechanism

To address these obstacles, the GBA governments have launched regional facilitation measures. In June 2023, the Cyberspace Administration of China and Hong Kong's Innovation, Technology and Industry Bureau concluded a cooperation memorandum aimed at facilitating cross-boundary data flows. Similar arrangements were reached with the Macao authorities later that year. These memoranda aim to simplify data transfers within the GBA under existing legal frameworks [9]. The first concrete initiative was the GBA (Mainland–Hong Kong) Standard Contract introduced in December 2023. In September 2024, a comparable Mainland–Macao version followed. The GBA Standard Contract offers a parallel route for cross-border

personal data transfers, coexisting with the national Standard Contract mechanism. Key features include:

1. Limited territorial scope. The contract applies solely to exchanges between the nine mainland cities in the GBA and either Hong Kong or Macao. Data sent under the contract is not permitted to be passed on to parties outside the GBA. For multinational groups or regional supply chains that require subsequent transfers to other jurisdictions, this restriction may necessitate parallel compliance pathways and thus limit the mechanism's attractiveness for global operations.

2. Broad data coverage. With the exception of "important data", all personal information can be transmitted using the GBA contract. The mechanism eliminates the data-volume threshold applicable under the national standard contract, allowing even large datasets to flow under this simplified regime.

3. Simplified but not eliminated compliance obligations. Unlike the national standard contract, the GBA contract does not require submission of a full personal information protection impact assessment report to the CAC. Personal information processors must still perform a substantive internal impact assessment and maintain records, and they must file three documents—the signed contract, a commitment letter, and proof of the legal representative—with the Guangdong CAC and the relevant Hong Kong or Macao regulator within ten working days. Accordingly, the mechanism reduces filing-related procedures and lifts the data-volume threshold but leaves intact the core analytical burdens associated with PIAs.

4. Choice of law and dispute resolution. Parties can choose Mainland or Hong Kong law for governing the contract, and disputes may be resolved through litigation or arbitration in either jurisdiction. Each party remains subject to its local regulator, and complaints can be lodged with the CAC, Hong Kong's Digital Policy Office, or Macao's PDPB as appropriate.

The GBA contract is voluntary, meaning organisations may elect to use it or continue using the national standard contract or other export paths. It is designed to complement rather than replace existing rules, providing a streamlined pathway for transfers where the parties are located within the GBA.

3) Pilot Operations and Expansion

The GBA Standard Contract was first trialled in the banking, credit and healthcare fields—sectors with particularly acute demands for cross-border data exchange. On 1 November 2024, the Hong Kong government broadened the scheme to cover all industries. The Mainland–Macao iteration of the contract entered into force on 10 September 2024. Under this mechanism, personal information processors in the nine Guangdong cities may execute the Standard Contract with Hong Kong or Macao counterparts and lodge filings with the relevant regulators, thereby enabling lawful cross-border transfers. Regulators indicate that implementation

has proceeded smoothly; firms have welcomed the lighter compliance load; and there is broad anticipation of further refinements and added facilitation measures to meet industry needs.

E. CONCLUSION

The legislative and practical settings for cross-border personal data flows in Mainland China, Hong Kong, and Macao differ substantially. Mainland China operates a comprehensive and highly stringent regime; Hong Kong retains a permissive framework grounded in voluntary safeguards; and Macao follows a European-style approach that hinges on adequacy or, failing that, explicit consent. These regimes have developed in parallel with limited coordination, producing misaligned standards and heightened compliance costs for firms operating across the GBA. To meet rising demand for data-driven integration, GBA governments introduced the GBA Standard Contract as a pragmatic measure to narrow these differences. Although at an early stage, the mechanism seeks to lighten compliance obligations while leaving the underlying laws intact. The success of this and future harmonisation efforts holds particular significance for the Greater Bay Area's vibrant sector, where efficient and legally compliant cross-border data flows are crucial for maintaining its competitive edge in the global supply chain, optimising smart manufacturing, and facilitating consumer engagement across the region. The next chapter examines the legal challenges arising from these differences and explores the deeper sources of regulatory fragmentation.

III. LEGAL PROBLEMS AND UNDERLYING CAUSES IN THE CROSS-BORDER FLOW OF PERSONAL INFORMATION IN THE GREATER BAY AREA

A. SPECIFIC PROBLEMS ARISING FROM NON-UNIFORM LEGISLATION

1) Conflicting Standards for Cross-Border Transfers

The three GBA jurisdictions exercise significantly different levels of control over the outbound transfer of personal information. Mainland China sets a stringent bar: exporters must obtain separate consent and meet at least one of three routes—a security assessment overseen by the Cyberspace Administration of China (CAC), certification by an accredited body, or the CAC-issued Standard Contract. The law also requires impact assessments, identification of the foreign recipient and its location, and filing with the CAC; the mainland treats transfers to Hong Kong and Macao as overseas exports, with no special carve-outs. Macao bars transfers to destinations without adequate legal protection, unless adequacy is ensured or the data subject's explicit consent is obtained. Hong Kong has no dedicated, destination-based export restriction because Section 33 has not commenced, and it likewise does not require prior approval or notification, but data users must still comply with Data Protection Principles 3 and 4 when exporting data. Consequently, firms may assume that dispatching data from Hong Kong to the mainland or Macao is unconstrained,

yet face strict conditions in the destination jurisdiction. A transfer lawful in one jurisdiction may breach rules in another, obliging businesses to meet two sets of requirements, thereby raising coordination costs and compliance burdens.

2) Divergent Definitions and Scope

The three jurisdictions likewise diverge in how they define personal information and in the substantive legal notions that underpin their regimes. Although each definition targets data concerning an identified or identifiable individual, the breadth of “personal data” and the taxonomy of “sensitive information” vary across the three systems. Mainland law defines “sensitive personal information” to encompass biometrics, medical and health records, financial account details, and location data, and places such information under enhanced protective measures. Hong Kong's Personal Data (Privacy) Ordinance (PDPO) has no equivalent category. The Macao PDPA sets out a narrowly framed definition of “sensitive data” (political beliefs, religious faith, union membership, health or sex life) and employs this classification chiefly to determine whether special authorisation is necessary. Consequently, material treated as ordinary in Hong Kong may be regarded as sensitive in Mainland China, thereby triggering further safeguards. These divergences have concrete implications for cross-border economic activities. In cross-border wealth management and payment services, for example, financial account details and transaction histories are subject to enhanced consent, minimisation and localisation requirements on the mainland, even though Hong Kong treats them as ordinary personal data subject to general purpose-limitation and security duties. Likewise, health-related data used in joint medical programmes or employee-benefits schemes may need to satisfy Macao's narrow sensitive-data rules or Mainland China's broader sensitive-information protections. These mismatches increase compliance costs for regional banks, insurers and healthcare providers and complicate the design of standardised, GBA-wide data-processing protocols. The lawful bases for processing personal information further exemplify these divergences. Macao adopts the European model: beyond consent, processing may rely on the performance of contractual obligations, compliance with legal duties, the protection of vital interests, tasks carried out in the public interest, or the controller's legitimate interests, so long as those interests do not prevail over the data subject's rights. Mainland China's PIPL likewise recognises several lawful grounds, yet in enforcement practice particular emphasis is placed on obtaining informed consent. By contrast, Hong Kong's PDPO is anchored in purpose limitation: data cannot be used for new purposes—including cross-border transfer—absent the data subject's prescribed consent. The PDPO lacks a general “legitimate interests” lawful-basis clause. Moreover, the PIPL possesses extraterritorial reach: it applies to overseas entities that handle data concerning mainland residents for providing products or services or for analysing their activities. Neither Hong Kong nor Macao

extends comparable reach. As a result, a company operating across the GBA must navigate and apply three discrete frameworks of lawful processing grounds, a task rendered even more complex by the divergent geographic scope of each statute.

3) Lack of Coordinated Enforcement and Remedies

Fragmentation in regulatory powers and judicial remedies exacerbates the difficulties described above. Within the “one country, two systems” constitutional arrangement, the three jurisdictions maintain independent legal and administrative systems, and no clear channels exist for coordinated oversight. If a mainland resident’s personal data is misused in Hong Kong, the CAC may treat the export as an unlawful outbound transfer, but it lacks jurisdiction to enforce sanctions against a Hong Kong entity. The Privacy Commissioner may accept a complaint, yet the complainant is not a Hong Kong resident and the PDPO has no extraterritorial effect, raising questions about the Commissioner’s authority and the calculation of damages. Similarly, once Macao personal data enters the mainland or Hong Kong, the PDPB cannot pursue overseas offenders, and the laws of the receiving jurisdiction may not adequately protect Macao residents. There is currently no dedicated cross-border judicial cooperation mechanism for data-privacy breaches, making it difficult to collect evidence, secure reciprocal recognition of decisions or enforce penalties. This lack of regulatory and judicial coordination lowers the cost of non-compliance, undermines the deterrent effect of existing laws and increases legal risks for businesses that must navigate multiple jurisdictions.

B. UNDERLYING CAUSES OF THE FRAGMENTATION

1) Differences in Legal Philosophy and Legislative Timing

The roots of the regulatory divergence lie partly in the jurisdictions’ distinct legal traditions and historical trajectories. Hong Kong and Macao inherited privacy frameworks derived from Western legal concepts, placing strong emphasis on the protection of individual privacy rights. Hong Kong introduced the PDPO as early as 1996, and Macao adopted the PDPA in 2005, drawing heavily on the European Union’s 1995 Data Protection Directive as a template. Mainland China, by contrast, enacted its first full-fledged data-protection statute only in 2021, at a time when digitalisation and data security had become strategic priorities. The PIPL reflects a dual commitment to protecting personal information and safeguarding national security, typified by the classification of “important data” and “core data” and by rigorous export controls [10]. These differing philosophies produce divergent emphases: Mainland laws are grounded in national sovereignty and public interest—requiring security assessments to ensure data exports do not endanger national security or the public good—whereas Hong Kong and Macao laws are more individual-rights-oriented, focusing on preventing private actors from misusing personal data. This broader ‘data sovereignty’ turn

and the spread of localisation measures across Asia are well documented in the comparative literature [11, 12]. The timing of legislative reforms compounds these differences. Macao’s PDPA, inspired by the 1995 EU Data Protection Directive, was deliberately calibrated to satisfy the EU’s adequacy standard and therefore adopts a stringent adequate-protection-plus-authorisation model for cross-border transfers. This choice reflects a regulatory strategy of aligning with high European benchmarks rather than an outdated legislative accident, even though the statute predates more recent instruments such as the GDPR and does not yet incorporate some now-common features, such as a general data-breach notification duty. Hong Kong’s PDPO has undergone only incremental amendments since the 1990s and does not embed more recent constructs such as comprehensive data-export rules or an extraterritorial scope. Mainland law, conversely, integrates numerous features of the EU’s General Data Protection Regulation (GDPR) and layers on stricter obligations, including broad-based requirements for explicit consent. As a result, “old” and “new” laws coexist within the GBA, and the lack of synchronisation magnifies regulatory incompatibility.

2) Regulatory Architecture and Enforcement Disparities

The administrative structures and enforcement styles in the three jurisdictions are also uneven. Mainland China has established a powerful, centrally directed regulatory regime: the CAC orchestrates data export controls, requiring prior approval and imposing severe penalties—including fines of up to five percent of annual turnover—for violations. Hong Kong’s Privacy Commissioner and Macao’s PDPB, by contrast, are independent bodies with limited enforcement powers. They often favour post-event supervision and guidance over punitive measures; serious sanctions have been relatively rare. This contrast complicates compliance strategies for businesses operating across jurisdictions: they must exercise heightened caution when dealing with mainland data while potentially relaxing controls for Hong Kong or Macao, resulting in an inconsistent compliance posture. In addition, prior to the recent memoranda and standard-contract initiatives, the three regulators lacked formal channels for sharing information or cooperating on investigations. Such gaps allowed cross-border infractions to slip through the cracks and fostered mistrust about the adequacy of each other’s enforcement—mainland authorities may view Hong Kong and Macao enforcement as lax, whereas Hong Kong and Macao may question the fairness or transparency of mainland procedures.

3) Structural Obstacles under the “One Country, Two Systems” Arrangement

A more fundamental source of fragmentation lies in the constitutional structure of the “one country, two systems” arrangement. Hong Kong and Macao enjoy considerable autonomy and operate separate legal systems under their Basic Laws; Mainland Chinese law does not automatically

apply in the two special administrative regions, nor do the PDPO or PDPA have effect on the mainland. There has been no national-level framework coordinating data governance within the GBA. Early regional cooperation focused primarily on trade and economic facilitation, leaving data—an emergent factor of production—outside the scope of integration. Consequently, each jurisdiction has developed rules based on its own needs and international commitments without considering regional harmonisation. Only recently have the legal vacuum and its negative consequences become apparent. The signing of memoranda on cross-border data flows and pilot trials of the GBA Standard Contract represent the first steps toward coordinated governance. Nonetheless, addressing the underlying structural obstacles requires overcoming the constitutional divide between national and local laws and designing mechanisms that respect legal autonomy while promoting convergence.

C. CONCLUSION

The Greater Bay Area's attempt to foster a unified digital economy faces significant legal hurdles. Divergent export requirements, conceptual differences and a lack of coordinated enforcement create complexity and uncertainty for cross-border data transfers. These problems reflect deeper divergences in legal philosophy, legislative timing, regulatory resources and the overarching constitutional framework. Acknowledging these causes is crucial to formulating effective solutions, which the following chapters will explore.

IV. LEGAL STRATEGIES FOR IMPROVING CROSS-BORDER PERSONAL DATA FLOWS IN THE GREATER BAY AREA

A. BUILDING INSTITUTIONAL COOPERATION FOR CROSS-BORDER ENFORCEMENT

Beyond harmonising substantive rules, effective institutional coordination in enforcement is essential. The spirit of the cross-boundary data flow memoranda should be realised through a permanent tripartite regulatory working group for the GBA. This body would meet regularly to exchange information on legal developments and enforcement cases and to draft joint guidelines on cross-border data issues. For instance, it could establish procedures for notification and investigation of cross-border data breaches: when one side discovers a breach or unlawful processing involving another jurisdiction's data, it should promptly notify its counterpart for coordinated action. A dedicated cross-border complaint mechanism should also be created. The Implementation Guidelines already stipulate that if an organisation or individual identifies a breach of the Standard Contract, a complaint may be filed with the CAC, the Guangdong Provincial CAC, the Innovation, Technology and Industry Bureau, the Office of the Government Chief Information Officer or the Privacy Commissioner for Personal Data. This provides an initial channel for cross-boundary regulatory intervention; however, the subsequent procedure needs to be clarified and standardised to ensure that complaints are

not lost in jurisdictional gaps and that financial and other data-intensive industries can rely on predictable enforcement pathways.

Judicial cooperation should be explored in tandem with regulatory collaboration. Although Mainland China, Hong Kong and Macao maintain arrangements for civil and commercial judicial assistance, there is no specialised mechanism for enforcing administrative penalties or judgments relating to data privacy. Given the constitutional and jurisdictional complexities of the “one country, two systems” framework, a comprehensive supplementary judicial assistance memorandum covering administrative penalties is likely to be politically and legally challenging and, at best, a medium-to long-term goal. In the near term, more modest steps—such as refining existing mutual legal assistance arrangements to facilitate evidence-gathering in cross-border data cases, or piloting mutual recognition of specific types of civil judgments (for example, injunctions to preserve evidence or orders mandating data deletion)—may offer more realistic pathways. Over time, these incremental arrangements could pave the way for a more formalised mechanism for the recognition and enforcement of regulatory orders and judgments in data-privacy matters. Only through the combination of administrative cooperation and appropriately calibrated judicial remedies can the law's deterrent and protective functions be fully realised, ensuring that wrongdoers cannot evade liability by exploiting jurisdictional differences [13,14].

B. HARMONISING THE TREATMENT OF SENSITIVE DATA

One central obstacle to integrated data governance in the GBA is the divergent treatment of sensitive personal data in Mainland China, Hong Kong and Macao. Mainland law defines “sensitive personal information” broadly and attaches heightened duties, whereas Hong Kong has no statutory sensitive-data category and Macao's PDPA recognises only a narrow list. Data that is routine in Hong Kong, such as financial account details or certain health-related records, may therefore trigger stringent safeguards once transferred to the mainland. This misalignment complicates compliance for healthcare, wealth management and undermines mutual trust in regulatory outcomes. The three jurisdictions should first develop a GBA-wide reference taxonomy of core sensitive personal data. Regulators could designate biometric identifiers, health information, financial account and credit data, precise location data and data about minors as a shared “GBA-core” list. Each jurisdiction would retain its own statutory concepts but accept that, for intra-GBA flows, these categories warrant special protection. Hong Kong could give effect to this taxonomy through a code of practice under the PDPO that treats GBA-core data as functionally sensitive and requires stricter internal governance and due diligence when exporting or receiving such information. Macao's PDPB could issue interpretative guidance applying the same list to cross-border transfers, so that these data

types are reviewed to a heightened standard even where the statute does not expressly classify them as sensitive. On this basis, the three jurisdictions should coordinate substantive safeguards for transfers of GBA-core sensitive data. Minimum measures should include explicit and informed consent from data subjects, strict data-minimisation and purpose-limitation, and robust technical and organisational safeguards such as encryption, access controls and audit trails. These measures could be tested and refined in sectoral sandboxes in finance, healthcare, where large volumes of employee, customer and logistics data regularly cross borders. For example, a Hong Kong apparel brand centralising customer preference profiles and factory-audit reports from Guangdong and Macao would be required to obtain explicit consent for the cross-border use of workers' biometric attendance data, limit its use to defined compliance purposes, and ensure encrypted transmission and storage throughout the data lifecycle. The GBA Standard Contract should serve as the main vehicle for embedding this harmonised approach. Future iterations of the contract and its guidelines should require parties to identify whether transferred datasets contain GBA-core sensitive data and, if so, to undertake the agreed catalogue of heightened safeguards. In this way, the Standard Contract would not only simplify procedures, but also promote substantive convergence in the protection of high-risk personal data, providing a workable pathway for secure and efficient cross-border flows in key sectors.

C. EXPANDING PILOT PROJECTS AND DESIGNING LONG-TERM INSTITUTIONS

The introduction of the GBA Standard Contract is a landmark in cross-border data governance, yet it should be regarded as a starting point. Further efforts are warranted in the following areas.

First, the scope of pilot projects should be broadened. Platforms such as the Qianhai Shenzhen–Hong Kong Modern Service Industry Cooperation Zone, together with the Hengqin Guangdong–Macao Deep Cooperation Zone, could be used to experiment with more open data-flow policies. For specific domains such as scientific research and healthcare, a regulatory sandbox approach could be adopted: under this model, projects could conduct real-time cross-border data queries and sharing under strict controls to test technical and legal arrangements while maintaining privacy [15].

Second, third-party certification and technological safeguards should be introduced. Besides the Standard Contract, the PIPL recognises certification by accredited bodies as another route for data export. The GBA could pilot a cross-border data-protection certification scheme, inviting qualified independent institutions to audit data-processing procedures. If Hong Kong or Macao entities were certified under Mainland standards, Mainland authorities could allow them to receive personal data freely, and vice versa. Complementary technologies—such as anonymisation, encryption, and federated learning—should be deployed to reduce risks

and provide a technical basis for legal exemptions.

Third, in the longer term, lawmakers might consider developing a regional data law or incorporating GBA-specific provisions into national legislation. This would resemble the EU's internal free-flow rules, enabling harmonisation across multiple legal systems within one country. In the short term, scholars argue that it is more realistic to use coordinated frameworks to promote regional data flows rather than to impose immediate uniformity. Hence, the immediate priority remains strengthening pilot measures and dialogue mechanisms to build consensus gradually.

D. CULTIVATING A CULTURE OF TRUST AND LEGAL CONSENSUS

Ultimately, legal solutions must rest on a foundation of shared values among governments and society. Achieving both “controllability” and “flowability” of personal information within the GBA requires balancing security and development, private rights and public interests. During legal harmonisation, Mainland authorities should appreciate the weight that Hong Kong and Macao place on personal privacy and respect their legal traditions, avoiding the impression that national security concerns override privacy interests. Hong Kong and Macao, for their part, should recognise Mainland China's international data-security challenges and the imperative of maintaining sovereignty, and accordingly consider adopting stricter export controls to build trust. Regular forums—bringing together legislators, regulators, enterprises and scholars—could help cultivate a common discourse and shared values. Moreover, public education and training should be intensified. Enterprises need clear guidance on using the GBA Standard Contract and conducting impact assessments; individuals should understand how to exercise their rights and protect their data. Once a virtuous circle is formed—where businesses are motivated to comply, the public trusts cross-border services, and regulators coordinate effectively—the legal integration process will proceed more smoothly. This chapter proposes a suite of mutually reinforcing strategies—standard-setting and mutual recognition, regulatory coordination, pilot projects and institution-building, and trust-building—to enable the secure and efficient movement of personal information across the Greater Bay Area while respecting the diverse legal traditions under “one country, two systems”.

AUTHOR CONTRIBUTIONS

The author Zhihong Dai confirms being the sole contributor to this work and is responsible for the conception, research design, legal analysis, and writing of the entire manuscript.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

FUNDING

The National Natural Science Foundation of China (Grant: 0000009); the National Natural Science Foundation of China (Grant: 000000005).

ACKNOWLEDGEMENTS

The author acknowledges the National Natural Science Foundation of China (Grant: 00000009), the National Natural Science Foundation of China (Grant: 000000005).

REFERENCES

- [1] J. Chaisse, "Special Economic Zones in the Greater Bay Area," IEEM Policy Paper (June 2025), Institute of East Asian Economics and Management, 2025, [Online]. Available: <https://ieem.org.mo/wp-content/uploads/2025/12/June-2025-Policy-paper-SEZs-in-GBA1.pdf> (accessed 20 February 2026).
- [2] J. Chaisse, G. Dimitropoulos, and I. Mosquera, "Law and Digital Transformation in the Indo-Pacific: An International Economic Law Perspective," *The Journal of World Investment & Trade*, vol. 26, no. 4, pp. 575-620, 2025, doi: 10.1163/22119000-12340376.
- [3] A. Adam and W. Normann, "Data Flows and Data Protection in the Greater Bay Area: The Need for a Coordinated Legal Framework," *The Chinese Journal of Comparative Law*, vol. 12, cxae013, 2024, doi: 10.1093/cjcl/cxae013.
- [4] I. Calzada, "Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL)," *Smart Cities*, vol. 5, pp. 1129-1150, 2022, doi: 10.3390/smartcities5030057.
- [5] Y. C. Chin and J. Zhao, "Governing Cross-Border Data Flows: International Trade Agreements and Their Limits," *Laws*, vol. 11, p. 63, 2022, doi: 10.3390/laws11040063.
- [6] L. Hao, "Research on the Cross-boundary Data Transfer within the Greater Bay Area," *Science of Law*, vol. 6, pp. 79-94, 2024.
- [7] J. Wu, "The Legal Framework for Cross-border Data Transfer Between Mainland China and the Hong Kong Special Administrative Region," *Journal of International Commercial Law*, vol. 3, pp. 420-589, 2025.
- [8] Y. Zhang, "Personal Data Protection and Data Transfer Regulation in China," *Brussels Privacy Hub Working Paper*, vol. 10, no. 3, pp. 1-36, 2024, [Online]. Available: <https://brusselsprivacyhub.com/wp-content/uploads/2024/04/Personal-Data-Protection-in-China.pdf> (accessed 20 February 2026).
- [9] M. Du, "From market access to regulatory cooperation in the Greater Bay Area (GBA): an international economic law perspective," *Asia Pacific Law Review*, pp. 1-21, 2025, doi: 10.2139/ssrn.5412005.
- [10] S. Liao, "AI-Driven Media Compliance: Technical Innovations and Regulatory Challenges in Hong Kong-Mainland Data Flows," *Journal of Education, Humanities and Social Sciences*, vol. 52, pp. 117-125, 2025, doi: 10.54097/3fz2aq70.
- [11] D. W. Arner, G. G. Castellano, and Selga ĒK, "The Transnational Data Governance Problem," *Berkeley Technology Law Journal*, vol. 37, no. 2, pp. 623-699, 2021.
- [12] G. Greenleaf, "Personal Data Localization and Sovereignty along Asia's New Silk Roads," in *Data Sovereignty: From the Digital Silk Road to the Return of the State*, A. Chander and H. Sun, Eds. Oxford, UK: Oxford University Press, 2023, p. 301.
- [13] M. Taylor, "Transatlantic Jurisdictional Conflicts in Data Protection Law: Fundamental Rights, Privacy and Extraterritoriality," Cambridge University Press, 2023, pp. 193-195, doi: 10.1017/9781108784818.
- [14] A. H. Zhang, "High Wire: How China Regulates Big Tech and Governs Its Economy," Oxford, UK: Oxford University Press, 2024, p. 57, doi: 10.1093/oso/9780197682258.001.0001.
- [15] J. Gao, "Global Governance of Cross-border Data Flows and China's Response," *Journal of Information Economics*, vol. 3, no. 2, p. 47, 2025, doi: 10.58567/jie03020001.