Singapore Law Review
(2024) 41 Sing L Rev

AN ANALYSIS OF THE "ADEQUATE PROTECTION PRINCIPLE" IN THE CROSS-BORDER DATA FLOW SYSTEM IN THE PEOPLE'S REPUBLIC OF CHINA

SHA RUNHE*

The "adequate protection principle" requires recipient countries to provide an adequate level of data protection comparable to that of the originating country in the context of cross-border data transfer. Under its "localisation plus diverse transfer mechanisms" model, the EU uses an "adequacy" whitelist to enable GDPR-compliant data flows. In contrast, under the "localised storage + review" model of the PRC, the "adequate protection principle" is scattered throughout the security assessment and the standard contract for personal information filing as one of the elements to be assessed. While such an approach maximises national security and privacy protection, it risks impeding innovation and development. This article will examine the practices of the GDPR "adequate protection" certification and, in conjunction with PRC data cross-border transfer rules, provide suggestions on how the PRC could apply the "adequate protection" certification as a whitelist system to improve its domestic legislation and enable the country to connect to the international data flow system.

I. INTRODUCTION

The free flow of data is a driving force behind economic globalisation. Information technology and conventional trade have come together to create a fast-growing, high-speed data flow that has boosted information transparency, expanded investment choices, and enabled more efficient capital allocation.[1] Data is no longer just a supporting player in trade; rather, it is steadily becoming

* LLB of East China University of Political Science and Law, Class of 2023; Magister Juris Candidate at University of Oxford, Class of 2025. I wish to express my deepest gratitude to my supervisor, Associate Professor Dai Yi Han, who has provided invaluable suggestions for my research. I also wish to extend my most heartfelt thanks to my friend, Toh Ding Jun for the excellent editing and insightful comments on this work. Furthermore, I am sincerely grateful to the editorial team of the Singapore Law Review for their meticulous revisions and exceptionally thoughtful feedback. Finally, I would also like to place on record my appreciation to the Centre for Asian Legal Studies and the Thammasat University Faculty of Law for the support provided, and the opportunity to participate in the CATPLI Writing Project. All errors remain my own.

[1] Joshua Cooper Ramo, "Globalism Goes Backward", *Fortune* (20 November 2012), online: <https://fortune.com/2012/11/20/globalism-goes-backward/>; Jeffrey Rothfeder, "The Great Unraveling of Globalization", *The Washington Post* (24 April 2015), online: <https://www.washingtonpost.com/business/reconsidering-the-value-of-globalization/2015/04/24/>.

a dominant force steering the growth of international economic exchange.[2] Global businesses will face obstacles if tight restrictions are imposed on data flows or control measures akin to those for traditional commodities.[3] While the free movement of data propels global economic integration, it also introduces a myriad of risks that necessitate a careful balance between the benefits of data sharing and the imperatives of privacy and security. Cross-border data flows are accompanied by risks, including, but not limited to, data leakage, loss of financial information security, cybercrime, and terrorism. While pursuing absolute security and zero risk may seem appealing, such pursuits will likely be futile and counterproductive.[4] Thus, cross-border data flows must address the question of "what data to share, with whom, and under what circumstances."[5] Reconciling the free flow of data with its security is a key issue in designing cross-border data rules.

To this end, three models of cross-border data rules have emerged. The European Union's ("EU") approach places the individual's right to protect personal data at its core. The General Data Protection Regulation ("GDPR") holds businesses to a high standard of security and transparency in handling the personal data of EU citizens. The United States ("US") opposes data localisation and puts strict limits on requirements to store data locally. In contrast, China (or, "the PRC") has adopted a rigorous "data localisation" regime that generally mandates storage of data within the PRC's borders, with only narrow exceptions to this rule.[6]

The PRC's current regulations and practices constrain data-driven trade and business growth. They should be amended to align with international norms. The two main routes for data transfer – security assessment and standard contract filing – involve extensive reviews or filings with the State Internet Information Office (hereinafter referred to as "SIIO") and the Provincial Internet Information Office. These bureaucratic processes impose heavy compliance burdens on companies. According to a survey conducted by South Finance Institute of Compliance Technology, nearly 40% of enterprises find it difficult to classify "important data," and 33% are

---

[2] Chen Yongmei & Zhang Jiao, "New developments in international regulation of cross-border data flows dilemmas and the way forward" (2017) 235 Journal of SUIBE 37 at 52.

[3] Ding Xiaodong, "Jurisprudential Reflection and Institutional Reconstruction of Cross-border Data Flows: A Concurrent Review of the Data Cross-border transfer Security Assessment Measures" (2023) 137 Admin L Res 62 at 67.

[4] *Ibid* at 73.

[5] Peter Swire, "Privacy and Data Sharing in the War on Terrorism" (2006) 51 Vill L Rev 950 at 959.

[6] Matthew P. Goodman & Pearl Risberg, "Governing Data in the Asia-Pacific", *Center For Strategic International Studies* (21 April 2021), online: <https://www.csis.org/analysis/governing-data-asia-pacific>.

"unsure whether they need to file a data security assessment across borders."[7] In addition, many large enterprises are divided into a multitude of departments and sub-departments with their own data centers, making it difficult for an enterprise to identify and assess the content and volume of all its data if there is no unified management.[8] As a result, the stringent data regulations create major obstacles for corporate development. To date, only fifteen cases in the PRC have passed the security assessment and filings,[9] despite the high demand for cross-border transfer from enterprises.

The concept of "data localisation" is often related to digital industrial policy or economic protectionism. Yet, it is also associated with public policy objectives – namely, that of national security.[10] Localizing data within the PRC helps to expand the scope of national security protections against foreign interference in the cyber domain.[11] In 2021, the SIIO launched a cybersecurity review of US-listed internet companies, including "Didi" and "Yunchebang," both of which hold vast user data and operate critical infrastructure.[12] Recently, the extensive data access

---

[7] Wu Liyang et al, "Survey Analysis and Report on the Status of Data Cross-border", *21st Century Business Herald* (2 March 2023), online: <https://m.21jingji.com/article/20230302/herald/df88c48e06b7a00dac5843e88859729c_zaker.html>.

[8] *Ibid.*

[9] "The first two enterprises in Shanghai pass data cross-border transfer security assessment", *Cyberspace Administration of Shanghai* (5 May 2023), online: <https://mp.weixin.qq.com/> ["*Cyberspace Administration*"]; "Jiangsu makes breakthrough progress in data cross-border transfer security assessment", *Cyberspace Administration of Jiangsu* (9 May 2023), online: <https://mp.weixin.qq.com/>; "The first two enterprises in Zhejiang pass data cross-border transfer security assessment", *Cyberspace Administration of Zhejiang* (24 May 2023), online: <https://mp.weixin.qq.com/>; "China's first auto company gains approval for full business scenario data cross-border transfer", *DGXC Data Governance and Cross-border Services Center* (24 May 2023), online: <https://mp.weixin.qq.com/>; "The first enterprise in Shandong passes data cross-border transfer security assessment", *Cyberspace Administration of Shandong* (9 June 2023), online: <https://mp.weixin.qq.com/>; "Zhejiang makes new progress in data cross-border transfer security assessment", *Cyberspace Administration of Zhejiang* (19 June 2023), online: <https://mp.weixin.qq.com/>; "The first three enterprises in Guangdong pass data cross-border transfer security assessment", *Cyberspace Administration of Guangdong* (19 June 2023), online: <https://mp.weixin.qq.com/ >; "Qunar completes data cross-border transfer declaration, marking approval for tourism scenario data cross-border transfer", *China News Service* (25 August 2023), online: <https://www.chinanews.com.cn/cj/2023/08-25/>; "First compliant data cross-border transfer case landed in Suzhou district", *Suzhou FTZ* (8 August 2023), online: <<https://mp.weixin.qq.com/>; "Two data cross-border transfer security assessment cases land in Wuxi", *Wuxi Commerce* (17 August 2023), online: <https://mp.weixin.qq.com/>.

[10] Daniel Crosby, "Analysis of Data Localization Measures Under WTO Services Trade Rules and Commitment" *The E15 Initiative* (March 2016), online: <http://e15initiative.org/wp-content/uploads/2015/09/E15-Policy-Brief-Crosby-Final.pdf>.

[11] Liu Yinuo, "The Interaction of Data Localization Measures and Cyber Security Safeguards" (2023) 14 Chinese JIL 131 at 138.

[12] Central Commission for Discipline Inspection and State Supervision Commission, "Didi, BOSS and

by the PRC's government was the focus of US congressional hearings regarding TikTok.[13] This indicates that expansive state powers to obtain data could make other countries reluctant to allow transfers to Chinese entities. It effectively risks decoupling the PRC from global data flows and hampering international business, revealing how the PRC prioritises national security considerations over economic interests in its data governance.

To prevent the PRC from being isolated from global data systems, the PRC should pursue a balanced approach to balance economic dynamism with reasonable national security safeguards and protection of citizens' data rights.[14] In this regard, implementing the "adequate protection principle" to establish a whitelist system could serve as a viable solution. Such a framework would allow the PRC to screen foreign jurisdictions for baseline data protections, which balances security with openness. In the following sections, this article will examine the EU's "adequate protection principle" and its role within the data protection framework, dissect the PRC's current regulatory landscape, and propose enhancements tailored to the PRC's unique context. In doing so, it aims to elucidate the intricacies of harmonising the PRC's cross-border data transfer protocols with global standards, while duly acknowledging and addressing its national security and privacy concerns.

II. BASIC CONCEPTS OF THE "ADEQUATE PROTECTION PRINCIPLE" AND CERTIFICATION PRACTICES

A. *Definition and Function of "Adequate Protection Principle"*

The "adequate protection principle" is a key component of the EU's data protection framework, which seeks to enable free data flows. First introduced in 1995 via the Data Protection Directive,[15] it was later broadened by the GDPR to expand the applicability of EU data rules. This principle

---

many other internet companies undergo cybersecurity review Data security concerns national security" *Sina Finance* (7 July 2021), online: <https://finance.sina.cn/china/gncj/2021-07-07/>.

[13] Cecilia Kang et al, "TikTok CEO Zhou Shouzi was fiercely criticized during the Congressional hearing" *New York Times* (24 March 2023), online: <https://cn.nytimes.com/technology/20230324/tiktok-hearing-congress-china/>.

[14] Xue Yisa, "The Construction of Multi-Level Data Exit System and the Realization of Freedom of Data Flow – Taking the Change of Substantive Censorship as a Starting Point" (2020) 246 J. Northwest Minzu University 64 at 73.

[15] EC, *Commission Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, [1995] OJEU, L 281/36.

has historical origins – after World War II, Western European countries recognised the right to privacy as a fundamental human right. By the early 1990s, they required mutual data safeguards as a prerequisite for cross-border data flows.[16]

The principle functions as the applicable standard for certification safelists. Under the EU's framework, data controllers or processors can generally transfer data outside of the EU to third-party countries that have been recognised as providing an adequate level of data protection without requiring specific authorisation.[17] This is considered an *ex ante* measure, with the rationale being that there is greater risk of misuse or abuse of data in countries that have not been certified. Consequently, data transfers to countries lacking adequate protection certification are subject to tighter constraints to mitigate this risk. Recipients in non-approved states can still receive EU data by adopting: (1) a legally binding and enforceable instrument between public authorities or bodies; (2) binding corporate rules; (3) standard data protection clauses; or (4) a standard data protection agreement, etc. (hereinafter, referred to collectively as "diverse conditions").[18] So far, fourteen countries have secured EU adequacy decisions and aligned their data rules.[19]

B. *Certification practice of the "adequate protection principle" in the EU*

The principle also takes into account: (1) the existence of an adequate data protection system, including the rule of law, human rights and fundamental freedoms, public security, criminal law, and access to data by government authorities; (2) enforcement system; and (3) international obligations.[20] The Adequacy Referential (the "Referential") provides further clarification that the data protection system must incorporate basic principles of lawful justification, purpose limitation, data retention, security and confidentiality, transparency, the rights to access, rectify, delete and

---

[16] *Ibid.*

[17] EC, *Commission Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, [2016] OJEU, L 119/61 at Article 45.

[18] EC, *Commission Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, [2016] OJEU, L 119/62 at Article 46.

[19] "Adequacy Decisions, How the EU determines if a non-EU country has an adequate level of data protection" *European Commission*, online: <https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en>.

[20] EC, *Commission Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, [2016] OJEU, L 119/61 at Article 45.

object, and restrictions on continued transfer. Procedurally, independent oversight and accountability mechanisms are required, alongside a supportive data protection system.[21]

The laws of non-approved States need not replicate the EU's rules *verbatim*, but should offer implementation, oversight, and enforcement.[22] To obtain EU certification, overall conformity with EU data protections in law and practice must be demonstrated. For example, in the case of South Korea, the "adequate protection" is identified through: (1) legislation such as the Personal Information Protection Act ("PIPA"), the Act on the Use and Protection of Credit Information, the Criminal Procedure Act, and the National Intelligence Act, as well as South Korea's Constitution and its Constitutional Court's rulings, all of which collectively guarantee that the government's power to access data is restricted and are aligned with the data protection requirements of the GDPR;[23] (2) accountability mechanisms, such as the Personal Information Protection Committee ("PIPC") to oversee data processing established by the PIPA; data controllers must also have a privacy officer fully responsible for processing personal information; (3) effectiveness of the oversight regime, such as the EU's assessment of the PIPC enforcement actions revealed a "powerful deterrent effect" of the sanctions, indicating the regime's robustness in protecting data;[24] (4) government access to data, for example, access to data by the South Korean government is primarily limited to two exceptions: criminal law enforcement and national security. These are further constrained by three strict limitations concerning the interpretation of prerequisites, use, and oversight of authority.[25]

While the EU's certification practice provides an ample wealth of experience, applying the EU model raises issues. First, it presumes that constitutional judicial review exists overseas. Consequently, countries lacking equivalent oversight mechanisms for privacy rights may struggle

---

[21] EC, *Article 29 Working Party Adequacy Referential*, [2018] WP 254 rev.01 at Chapter 4.

[22] EC, *Commission Implementing Decision (EU) 2022/254 of 17 December 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the Republic of Korea under the Personal Information Protection Act*, [2022] OJEU, L44/2 at 4.

[23] EC, *Commission Implementing Decision (EU) 2022/254 of 17 December 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the Republic of Korea under the Personal Information Protection Act*, [2022] OJEU, L44/2-3 at 8-13.

[24] EC, *Commission Implementing Decision (EU) 2022/254 of 17 December 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the Republic of Korea under the Personal Information Protection Act*, [2022] OJEU, L44/27-28 at 118-124.

[25] EC, *Commission Implementing Decision (EU) 2022/254 of 17 December 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the Republic of Korea under the Personal Information Protection Act*, [2022] OJEU, L44/32-34 at 139-150.

to meet the EU's strict standards. Second, determining "the rule of law, respect for human rights and fundamental freedoms" is highly discretionary and can easily incorporate political bias, making it challenging to ensure a fair outcome.

In summary, the EU has established extensive and rigorous certification practices under the "adequacy principle" to enable cross-border data flows to vetted destinations. This whitelisting approach provides helpful guidance, but also has limitations when applied externally. As the PRC explores implementing its own adequacy framework, it should consider contextual factors. Rather than directly transplanting the EU model, the PRC needs adaptations to suit its unique legal and political systems.

III. THE "ADEQUATE PROTECTION PRINCIPLE" UNDER THE PRC'S CROSS-BORDER DATA TRANSFER RULES: WEAK EFFECTIVENESS AND DUPLICATION OF ASSESSMENT

A. *Status of "Adequate Protection Principle" in the PRC*

Transitioning from the EU's established framework, the concept of "adequate protection" takes on a different shape within the PRC, influenced by distinct priorities and regulatory practices. Given national security priorities, the PRC's data regulations apply "adequacy" assessments case-by-case rather than taking a whitelisting approach. According to Article 2 of the National Security Law, national security in the PRC refers to a state in which "state power, sovereignty... sustainable economic and social development, and other vital national interests are relatively free from danger and internal and external threats, as well as the ability to guarantee a state of sustained security".[26] Within this expansive concept, data localisation is deemed indispensable for cybersecurity and national security.[27]

The opaque adequacy assessments offer limited utility and transparency. The "adequate protection principle" is set out in the Assessment Measures and Standard Contract for the Cross-border transfer of Personal Information Measures issued by SIIO, which are sub-regulations to National Security Law, Personal Information Protection Law, Data Security Law, and Cyber

---

[26] *National Security Law of the People's Republic of China*, 2015, Article 2.

[27] Wang Yue, "A Pilot Study on the Justification of Local Legislation on Internet Data" (2016) 135 Journal of Xi'an Jiaotong University (Social Sciences) 54 at 56.

Security Law, the latter three being often collectively referred to as the "troika of the PRC data protection system." According to Article 8 of the Assessment Measures, an overseas recipient's data protection level is considered at both the legal and implementation levels. At the legislative level, data security protection policies and regulations, personal information protection regulations, and cyber security environment must meet the PRC's mandatory standards;[28] at the implementation level, the overseas recipient's country must have a supervisory and enforcement body and relevant judicial body, and a data protection level that meets the PRC's mandatory standards.[29]

Besides, the current approval practice of security assessment lacks clear guidance. Since the Assessment Measures came into effect, only fifteen security assessments have been approved.[30] According to the public disclosure, the SIIO did not reveal any substantive analysis and determination of whether the data protection level in the recipient country was adequate. Among them, only the recipient country of "Collaborative Research Project between Beijing Friendship Hospital and the University Medical Center of Amsterdam" was revealed, namely the Netherlands.[31]

There are two possible explanations for this situation: firstly, after a security assessment, the SIIO may have determined that the GDPR, which covers the Netherlands, is adequate and applied that precedent to other GDPR states. Secondly, the SIIO may be conducting merely procedural checks, since the companies and SIIO lack the mandate and capacity to evaluate countries' overall legal systems. If so, reviews would focus narrowly on the data project rather than the overall governance framework.

---

[28] In practice, when conducting assessments, the Personal Information Protection Law the People's Republic of China (2021) is used as the primary reference. The specific criteria are referred to in Chapter II of the Personal Information Protection Law, including Section 1 General Rules, Section 2 Rules for Processing Sensitive Personal Information, Section 3 Special Rules for State Organs in Processing Personal Information, Chapter III Rules for Cross-border Transfer of Personal Information, Chapter IV Rights of Individuals in Personal Information Processing Activities, Chapter V Obligations of Personal Information Processors, and Chapter VI Government Departments Performing Duties of Personal Information Protection.

[29] *Cross-border Data Transfer Security Assessment Measures*, 2022, Article 8; *Standard Contract for the Cross-border Transfer of Personal Information Measures*, 2023, Article 4 ["*Standard Contract*"].

[30] *Cyberspace Administration*, *supra* note 9 and accompanying text.

[31] "The first approved data cross-border transfer security assessment case in PRC landed in Beijing" *Beijing Friendship Hospital* (2 February 2023), online: <http://www.bfh.com.cn/Html/News/Articles/>.

If the first explanation is true, the evaluation process of future assessments will improve. This is because when the SIIO approves a cross-border data transfer project, it would also mean that it has accepted the other country as offering "adequate protection". Over time, this will create a safelist which Chinese businesses can refer to when making their own applications. However, if the second explanation is true, then there is a risk that similar data transfer projects are decided differently, which can only lead to confusion amongst Chinese businesses. Given that, at present moment, the SIIO has stated it has no intention to create a safelist for security assessments, the second explanation is more likely.

In summary, the adequate protection principle has limited effectiveness, as it is not used to establish a certified whitelist system. The content and certification practices should be more transparent to avoid significantly increasing the burden and risk of data cross-border transfer assessments.

B. *Necessity Analysis of the Need for the "Adequate Protection Principle" Application*

1. *Imbalance between security concerns and freedom*

The primary reason the PRC needs to apply the adequate protection principle to establish a whitelist is that the current model is overly stringent, hindering data flows and imposing major compliance burdens. Implementing this principle could diversify the pathways and lessen the focus on security reviews.

Currently, the PRC has minimal data cross-border transfer paths and stringent conditions. According to Article 38 of the Personal Information Protection Law, the leading cross-border transfer routes in the PRC are: (1) passing the security assessment; (2) being certified by a professional institution for personal information protection; (3) concluding a standard contract with the overseas recipient formulated by the SIIO; or (4) through international treaties or agreements concluded or participated by PRC. Among these, the provisions pertaining to certification by professional institutions are not yet in force, and the PRC has yet to conclude or participate in any international treaties with mandatory data cross-border transfer effects. Therefore, there are effectively only two available channels, i.e. passing the security assessment and signing the standard contract.

Firstly, the stringent conditions are seen in the low threshold for triggering security assessment, the long timeframe, and strict approvals. According to the Assessment Measures, companies will be subjected to a declared security assessment if: (1) they provide important data outside of the PRC; or (2) they are operators of critical information infrastructure and data handlers managing personal information of more than 1 million individuals provide personal information abroad; or (3) they are data handlers who, since January 1 of the previous year, have cumulatively provided personal information of 100,000 individuals or sensitive personal information of 10,000 individuals abroad.[32] However, the draft Cross-border Data Transfer Regulations recently issued by the SIIO does not include processing over 1 million individuals' data as a trigger for security reviews. It only requires declaring a security assessment when providing personal information on over 100,000 individuals abroad.[33] If implemented, this could appropriately reduce compliance burdens.

There are still a few problems arising from this. First, the definition of "important data" is a broad one. According to the Assessment Measures, it refers to "data that may endanger national security, economical operation, social stability, public health, and safety once it is tampered with, destroyed, leaked or illegally accessed or illegally used, etc".[34] The blanket clause provided by Information Security Technology Important Data Identification Guide (Draft for Comments) indicates that "other data that may affect national political, territorial, military, economic, cultural, social, scientific and technological, ecological, resource, nuclear facilities, overseas interests, biological, space, polar, deep sea, and other security" – effectively almost any data, are all included in the definition.[35] In addition, the PRC's interpretation of national and social security laws tends to be expansive. In this context, nearly any cross-border transfer could be deemed to "endanger economic operations," or "endanger public security or culture and society", triggering a security review. Second, the time required to conduct a full security assessment is around two months or even longer.[36] The time cost for companies to carry out the estimate is too high, and the assessment timelines are uncertain.

---

[32] *Cross-border Data Transfer Security Assessment Measures*, 2022, Article 4.

[33] *Regulations on Standardising and Promoting Cross-Border Data Flows (Draft for Comments)*, 2023, Article 6

[34] *Cross-border Data Transfer Security Assessment Measures*, 2022, Article 19.

[35] *Guideline for Identification of Important Data for Information Security Technology (Draft for Comments)*, 2022, Article 5.

[36] According to the Cross-border Data Transfer Security Assessment Measures, the State Internet Information Office substantively reviews the security assessment, and the process is (1) the provincial Internet information departments conduct a substantive review for five days; (2) the State Internet Information Office decides whether to accept the security assessment application for seven days; (3) the State Internet Information Office integrates the opinions of the relevant departments of the State Council, provincial Internet information departments and specialized agencies and conducts a substantive review

In addition, Chinese firms seeking overseas data transfers may face "multi-agency regulation" issues arising from inconsistent rules between sectors, industries and regions. For example, the draft Anti-Money Laundering Law requires domestic financial institutions to report to or secure approval from the relevant financial supervision and management agency of the State Council when providing information to foreign authorities that may be related to national security.[37] Meanwhile, the Measures for the Administration of Population Health Information explicitly prohibit the outflow of population health information,[38] which indicates an inconsistency in the legal system. Besides, the National Data Bureau ("NDB") was newly established in 2023 to take over some responsibilities from the SIIO,[39] which was claimed to be "promoting the coordinated development of planning and construction in areas including digital PRC, digital economy, and digital society" but its authority regarding data security remains unclear, risking duplication with SIIO's role.

When companies meet the aforementioned security assessment threshold, they must undergo joint evaluations by the SIIO and industry regulators, involving lengthy procedures and multiple hurdles. The current practice will lead to two adverse outcomes. Firstly, a stringent cross-border data transfer policy may push enterprises to find unofficial workarounds, gradually forming a gray data industry chain that poses data risks and undermines formal regulations. Secondly, punitive enforcement will deter firms from normal business activities, reducing economic vitality. Moreover, multinational companies may opt to divest their data assets and exit the market entirely due to barriers accessing data, which will lead to a significant blow to the domestic economy.

Secondly, while the standard contract serves as a prevalent mechanism for facilitating cross-border data transfers, it is subject to considerable constraints and has inherent limitations in maintaining consistent compliance and ensuring uninterrupted data flow. Consequently, supplementing the standard contract with a robust protection whitelist becomes imperative, offering a more comprehensive and durable solution for data transfer needs.

---

for 45 days; (4) if the declared materials do not meet the requirements of the situation is complicated, the approval time may be extended.

[37] *Anti-Money Laundering Law of the People's Republic of China (Draft Revision for Public Consultation)*, 2021, Article 4.

[38] *Measures for the Management of Population Health Information (Trial)*, 2014, Article 10.

[39] "Establishment of National Data Bureau" *PRC Net News Center* (7 March 2023), online: <http://www.news.cn/2023-03/07/ >.

The primary reason for this is that the scenarios for the filing of standard contract for cross-border transfers of personal information from the PRC are subject to stringent limitations. These include not being part of the critical information infrastructure, managing personal information of less than one million individuals, transferring data of under 100,000 individuals abroad since the previous year's commencement, and handling sensitive information of less than 10,000 individuals.[40] In contrast, the EU's framework allows for the use of standard data protection clauses in transferring data to non-adequate third countries,[41] focusing on the recipient country's capacity to protect personal information. The use of standard contract in the PRC is more specific, emphasising the scale of operations and the volume of transferred data. Large enterprises in the PRC, particularly those handling extensive user data, are thus compelled to pursue security assessments over the simpler option of standard contract adoption.

Moreover, the procedural aspects of implementing the PRC's standard contract demand a meticulous regulatory audit and involve a complex filing process. Chinese data exporters must submit their filings to the appropriate provincial internet information office within ten working days post-enactment of the standard contract. The possible outcomes, as described in the Guide to the Filing of Standard Contracts for Personal Information Cross-border Transfer (First Edition), are binary: "approved" or "not approved."[42] This stipulates that compliance is not automatically ensured through document submission, and there exists a risk of rejection if the materials do not meet regulatory standards. The verification process itself is protracted, with a 15-working-day review period followed by a communication of results, and potential further 10-working-day re-evaluation periods for supplemental material submissions. This procedure is markedly different from the EU's regime, where signing the standard contract clauses ("**SCCs**") typically obviates the need for regulatory registration, focusing instead on adherence to general obligations like conducting a Data Protection Impact Assessment and keeping detailed processing records.

Finally, the specific use cases for the PRC's standard contract lack clarity, complicating their

---

[40] *Standard Contract*, *supra* note 29, Article 5.

[41] EC, *Commission Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, [2016] OJEU, L 119/62 at Article 46.

[42] *Guide to the Filing of Standard Contracts for Personal Information Cross-border Transfer (First Edition)*, 2023, Chapter 3.

practical application. The EU's SCCs clearly outline four distinct data transfer scenarios involving controllers and processors.[43] The PRC's framework, conversely, defines only the roles of "personal information processors" and "overseas recipients."[44] The responsibilities assigned to "overseas recipients" could potentially cover both external personal information processors and controllers. However, the scenarios of processor-to-processor and controller-to-processor transfers, as well as multi-party cross-border exchanges, are yet to be fully explicated and await more detailed regulatory interpretation.

In summary, the current stringent frameworks for cross-border data transfers in the PRC – primarily through security assessments and standard contract – are insufficient in providing a constant, reliable mechanism for data transfer. Security assessments impose heavy compliance burdens and are triggered by broad criteria, while the use of standard contract is narrowly tailored and encumbered by onerous procedural requirements. Consequently, there is a compelling need for the PRC to adopt an "adequate protection whitelist," which would serve as a complementary solution, aligning with the needs of businesses for consistent compliance and uninterrupted data flow, thus fostering a secure yet flexible environment for international data exchanges.

2. *Insufficient integration of international cooperation rules for data flows*

Data flow issues are frequently the biggest challenge in trade negotiations.45 Another reason for the inefficient data transfer is the PRC's lack of integration with global rules. Currently, the US and Europe form a cross-border data ecosystem. The US has entered into agreements including the United States-Mexico-Canada Agreement ("USMCA"), the Comprehensive and Progressive Trans-Pacific Partnership ("CPTPP"), the Safe Harbor Framework, and the Privacy Shield Framework to facilitate data flows. Meanwhile, the EU centers its data regime on protecting individual rights and structuring data flows through legislation like the GDPR. The US utilizes international agreements to advocate for free data flows, while the EU emphasizes safeguarding personal privacy through regulatory measures.

---

[43] EC, *Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council*, [2021] OJEU, L 199/39 at Clause 8 Data protection safeguards.

[44] *Standard Contract*, *supra* note 29, Article 5.

[45] See Li Mosi, "WTO E-Commerce Rules Negotiations: Progress, Divergence and the Way Forward" (2020) 50 Wuhan University Intl L Rev 55 at 76.

Although the PRC has taken the lead in formulating the Regional Comprehensive Economic Partnership ("RCEP") to promote global trade liberalization and regional economic integration, and has applied to join the CPTPP and the Digital Economy Partnership Agreement ("DEPA"), significant gaps remain between its data rules and international standards. Compared to Singapore, which participates in all three pacts with open data policies, the PRC faces growing pressure to adapt to emerging global data norms.[46]

Firstly, the RCEP sets far less stringent standards for cross-border data flows than the CPTPP or DEPA.[47] In terms of the general exceptions, while both allow for an exception on the basis of "legitimate public policy" or "measures necessary to protect public morals or to maintain public order", the CPTPP states that restrictions on transfers of information greater than what is necessary to achieve the objective shall not be imposed.[48] The CPTPP also incorporates the General Agreement on Trade in Services of the World Trade Organization ("GATS") as part of the agreement. The GATS, in turn, states that "the public order exception may be invoked only where a genuine and sufficiently serious threat is posed to one of the fundamental interests of society". This limits the scope of when the state can invoke the public policy exception.[49] However, the RCEP does not incorporate the GATS, providing greater latitude to impose public policy-driven data localisation.

Secondly, the CPTPP and DEPA security exceptions for "essential security interests" and "maintenance or restoration of international peace or security, or the protection of its essential security interests" are broader than under the GATS. The latter expands the scope of the GATS enunciation of "any action which it considers necessary for the protection of its essential security interests."[50] The phrase "essential security interests" is controversial internationally, and countries have avoided discussing it under the Dispute Settlement Understanding mechanism. Some countries have raised strong objections to WTO review. In particular, the US has argued that the

---

[46] He Bo, "Challenges and Responses to China's Participation in International Rules on Cross-Border Data Flows" (2022) 134 Admin L Research 89 at 90.

[47] *Ibid* at 92.

[48] *Comprehensive and Progressive Agreement for Trans-Pacific Partnership*, 8 March 2018, Article 14.11, Article 29.1 (Entered into force 30 December 2018, incorporated the Trans-Pacific Partnership Agreement); *Regional Comprehensive Economic Partnership*, 15 November 2020, Chapter 12, Article 15 (entered into force 1 January 2022) ["RCEP"].

[49] *General Agreement on Trade in Services of the World Trade Organization*, 15 April 1994, Article XIV (entered into force January 1, 1995).

[50] *Ibid.*

WTO has no right to second-guess the ability of WTO members to respond to security threats and that national security cannot be reviewed in the context of WTO dispute settlement.[51]

Even so, the WTO Panel's interpretation provides some insights. In the case of Russia - Measures concerning Traffic in Transit (DS512), the Panel found that the term "essential security interests" should be limited to core national security interests, including the protection of territory and population from threats. In general, it is up to the member states to determine how it should be defined. However, it is understood that member states should interpret these norms in good faith,[52] a principle that does not eliminate the dispute over authority between the members but opens up a Pandora's box of security exceptions.[53] The RCEP security exception is even more expansive than CPTPP or DEPA, allowing states to impose data localisation unilaterally with no recourse to dispute settlement.[54] While this method might be more acceptable to the member states, the free adoption of security measures will inevitably reduce the freedom in the cross-border data flow.

Thirdly, the PRC's current data regulations contradict the international exceptions clause requirements. The essence of general and security exceptions is that localisation should be the exception, not the norm. However, the PRC's legal framework defaults to mandatory domestic data storage.

In summary, the PRC-led RCEP is conservative in terms of permitting data flow. Thus, for the PRC to be able to integrate the CPTPP and DEPA into its cross-border data policies, she will need to find a breakthrough in balancing its internal security concerns and its need to conduct free trade.

IV. PROPOSALS FOR SYSTEMIC REFORM OF THE "ADEQUATE PROTECTION PRINCIPLE"

---

[51] Office of the United States Trade Representative, "Statement from USTR Spokesperson Adam Hodge" *Office of the United States Trade Representative* (9 December 2022), online: <https://ustr.gov/about-us/policy-offices/press-office/press-releases/2022/december/statement-ustr-spokesperson-adam-hodge>.

[52] Russia - Measures Concerning Traffic In Transit – Report of the Panel (5 April 2019) WT/DS 512/R [7.130-7.133].

[53] Liu Mei, "The limited governance of unilateral trade sanctions by WTO security exceptions - an analysis based on the Russian transit restrictions case" (2020) 277 International Economics and Trade Research 98 at 100.

[54] RCEP, *supra* note 47, Chapter 12, Article 15.

A. *Adjusting the Systemic Positioning of the "Adequate Protection Principle"*

To align with international data flow norms and address the PRC's unique regulatory challenges, the "adequate protection principle" requires careful adjustment in the current system. Firstly, the "adequate protection principle" whitelist should be established to enable data controllers or processors to generally transfer data outside of the PRC to third-party countries in the whitelist without requiring specific authorisation. In practical terms, the whitelist system would thoroughly vet the legislative framework of potential partner countries, ensuring adherence to principles like lawfulness, purpose limitation, and data retention, alongside robust security, transparency, and accountability measures. It would also review procedural adequacy ‑the presence of oversight bodies, enforcement mechanisms for redress, and the capacity for social supervision and judicial remedies. Simultaneously, it would evaluate the effectiveness and reach of the recipient country's data protection authorities, their ability to handle caseloads, and the independence of their operations from government interference.

Furthermore, to avoid regulatory fragmentation, it is imperative that the various data-related regulations be harmonised at the national level. The SIIO should be entrusted with the mandate to ensure consistency across different regulatory frameworks. Lastly, for the PRC to foster global data connectivity, it must actively participate in the international discourse on data security rules and standards, promoting safe and free data flows as envisaged by the Data Security Law.

Through these systemic reforms, the "adequate protection principle" can be repositioned to better serve the evolving landscape of global data exchange, while safeguarding national security and public interest.

B. *Establishing a Tiered Regulatory Framework for Data Classification and Transfer*

In order to strike a balance between safeguarding national security and exercising regulatory restraint, it is crucial to establish specific provisions for the handling of "important data". This approach necessitates a nuanced regulatory method. For diverse sectors, such as basic telecommunications, the financial sector encompassing securities and futures, automotive data, medical information and biometric information, the regulatory approach could be more nuanced. The protection level in the recipient country should be assessed and aligned with the rigor of the PRC's legal framework, drawing upon established standards such as the Provisions on Automotive

Data Security Management[55], Guidelines on Data Classification and Grading for Securities and Futures Industry,[56] and National Management Measures for Health Care Big Data Standards, Security and Services.[57] These documents offer a granular perspective on data categorisation that can serve as benchmarks for international transfers.

To guarantee legal transparency and establish accountability, it is advisable to legislate distinct thresholds, documentation requirements, and liability clauses for the transfer of "important data". These regulations need to be adaptable and frequently updated by regulatory bodies to reflect ongoing technological and societal evolution. For data that does not fall into the category of "important data", a more streamlined approach may be appropriate, such as simple notification or obtaining user consent, to ensure the protection of privacy rights without imposing unnecessary burdens on the data flow. The regulatory focus should prioritise data that is intrinsically sensitive and pose greater risks to privacy and security, with the provision for more rigorous oversight. Companies should be encouraged to perform exhaustive risk assessments and implement conscientious data management practices that support lawful business activities.

The creation of a tiered data classification system would serve various objectives: it would define the scope of "important data", specify the duties of data custodians, and promote a more precise and potent regulatory framework. Within this structure, data not classified as "important" would maintain essential privacy safeguards, yet not activate the strict regulatory protocols intended for more sensitive data categories. This structured approach would reconcile the necessity of protecting national security with the ambition to actively engage in the global digital marketplace.

V. CONCLUSION

The central question in this article is how the PRC can achieve the free flow of data across borders whilst taking into account the unique security and public policy considerations that it has. This, in turn, requires us to grapple with the question of whether – and to what extent – the national security and public policy exceptions are justified.

---

[55] *Provisions for the Safe Management of Automotive Data (for Trial Implementation)*, 2021, No. 7.

[56] *PRC Securities Regulatory Commission: Guidelines on Data Classification and Grading for Securities and Futures Industry*, 2018.

[57] *National Management Measures for Health Care Big Data Standards, Security and Services (for Trial Implementation)*, 2018.

It has been argued in this article that the "adequate protection" principle is essential for the PRC to break through the current data barriers it faces from other countries, to gain mutual recognition with those countries, and to join and/or lead the international data exchange. At the same time, the "adequate protection principle" can be used to protect the PRC's own national security and public policy interests. The rich practice from the EU has demonstrated the effectiveness of this model. The PRC should learn from the use of the GDPR, establish a safelist system and a mutual recognition mechanism, and shift to a "localisation plus diverse transfer mechanisms" model, even a "non-localisation" model.

To sum up, the PRC should fully explore and improve the connotation of "adequate protection" and reposition the principle in its legal system to balance national security and the economic value of data flow.