BRUSSELS PRIVACY HUB
WORKING PAPER
VOL. 10 N° 3 FEBRUARY 2024

BRUSSELS PRIVACY HUB
Vrije Universiteit Brussel

Personal Data Protection and Data Transfer Regulation in China

By Yueming Zhang

Contents

Summary

China's digital economy has thrived over the past decade, making China a full global player with significant trade partnerships. China has set forth a horizontal data governance framework consisting of three main pillars: the Cybersecurity Law (CSL), the Data Security Law (DSL), and the Personal Information Protection Law (PIPL) enacted in 2021. The PIPL acts as a foundational layer and applies to both private and public entities, although it is supplemented by other laws and regulations. Most notably, public entities are governed by the PIPL, while being subject to additional requirements stemming from law enforcement and surveillance laws. Overall, the data governance framework aims to strike a balance between two competing interests: the "safe flow" and "free flow" of data.

The PIPL applies to electronic information related to identifiable individuals, which is broadly defined, and extends its subject-matter extraterritorially. The PIPL comprises key data protection principles such as lawfulness, fairness, necessity, sincerity, and purpose limitation. While drawing inspiration from the European Union's regulatory framework, it also bears distinct Chinese characteristics, notably a bespoke hierarchy of transfer tools and stringent restrictions set on "critical information infrastructure operators (CIIOs)" and "important data".

Chinese data protection framework has embedded several Chinese characteristics, such as the lack of constitutional protection of personal data, the extensive surveillance powers wielded by public authorities, the proliferation of administrative departments with seemingly overlapping jurisdictions, and their insufficient independence.

Despite PIPL being in force for two years, the absence of detailed guidelines on regulated cross-border data transfer tools has created legal uncertainty. Industry stakeholders have called for more clarity amidst evolving guidelines.

Rooted in the concept of digital sovereignty, a broad notion with fluid boundaries, China's approach to data governance seeks not only to safeguard citizen rights but also to strengthen cybersecurity and national security interests. On the global stage, China has been actively championing its vision, contributing to international discussions on data governance and indirectly challenging other jurisdictions to reassess their positions. Nonetheless, translating China's domestic regulatory objectives into international standards remains a complicated task.

1 Context

China is the second most populous country worldwide.[1] As of June 2023, the number of internet users in China had reached 1.079 billion, showing an increase of 11.09 million people compared with December 2022, with an internet penetration rate of 76.4%.[2] This makes China the largest digital population in the world.[3]

As one of the world's three most prominent trading partners, alongside the European Union and the USA, China plays a significant role in international trade, investment, and economic cooperation.[4] The People's Republic of China (PRC) has bilateral investment agreements with over 100 countries and economic unions, including Austria, the Belgium-Luxembourg Economic Union, Canada, France, Germany, Italy, Japan, South Korea, Spain, Thailand, and the United Kingdom. China's Free Trade Agreement (FTA) partners include ASEAN, Singapore, Pakistan, New Zealand, Chile, Peru, Costa Rica, Iceland, Switzerland, Maldives, Mauritius, Georgia, South Korea, Australia, Cambodia, Hong Kong, and Macao.[5]

In recent years, China has become one of the countries that stand out in terms of its capacity to engage in and benefit from the data-driven economy.[6] With the rapid development of internet and communication technologies, China's technological influence is being felt globally.[7] This trend has resulted in the global reach of Chinese technologies, and the fostering of data exchanges between China and numerous countries, including the BRICS countries (Brazil, Russia, India, South Africa and Singapore).[8] Products and services offered by Chinese companies such as Huawei, Alibaba and TikTok have increased their market shares in many countries.[9]

With the rise of the digital economy and digital trade, China's data protection regime has been significantly transformed in recent years. The introduction of a comprehensive piece of data protection legislation, the Personal Information Protection Law (PIPL), modelled after the EU's GDPR,[10] represents a noteworthy advancement. However, the Chinese data protection framework is still in the making and continues to raise

[1] Data based on the July 2023-July 2024 estimates from the United Nations Population Division. https://www.worldometers.info/world-population/population-by-country/
[2] https://news.cctv.com/2023/08/28/ARTIjd0yIrXKjLS5XCsef0x1230828.shtml
[3] https://www.statista.com/statistics/262966/number-of-internet-users-in-selected-countries/
[4] European Commission, 'EU Trade Relations with China' (*European Commission*, 9 August 2023) <https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/china_en> accessed 21 April 2024.
[5] China - Trade Agreements' <https://www.trade.gov/country-commercial-guides/china-trade-agreements> accessed 21 April 2024.
[6] UNCTAD, 'Cross-Border Data Flows and Development: For Whom the Data Flow' (2021) <https://unctad.org/system/files/official-document/der2021_en.pdf> accessed 21 April 2024.
[7] Munich Security Conference, 'Munich Security Report 2020' (2020) <https://securityconference.org/en/publications/munich-security-report-2020/> accessed 10 August 2020.
[8] Ministry of Science and Technology of the People's Republic of China, 'China Participates in the First Meeting of the Steering Committee of BRICS Technology Transfer Center Network' <https://en.most.gov.cn/pressroom/202206/t20220622_181227.htm> accessed 21 April 2024.
[9] 'Kristin Shi-Kupfer: "China Sees Digitalization as a Chance to Increase Its Global Footprint"' (*Merics*, 8 April 2019) <https://merics.org/en/podcast/kristin-shi-kupfer-china-sees-digitalization-chance-increase-its-global-footprint> accessed 21 April 2024.
[10] Xinbao Zhang (张新宝), *Personal Information Protection Law of the People's Republic of China - A Commentary (中华人民共和国个人信息保护法释义)* (People's Publishing House (人民出版社) 2021).

serious challenges, particularly when compared with standards adopted by key trade partners, such as the EU.[11]

2 China's Data Protection and Cybersecurity Model

2.1 Constitutional protection

First of all, it is relevant to unpack the connection between the protection of human rights, including the rights to privacy and data protection, and China's constitutional framework.

China's current Constitutional Law was adopted on 4 December 1982 and amended in 1988, 1993, 1999, 2004, and 2018. Article 33 of the Chinese Constitution, introduced by the 2004 amendment, states that "the state respects and protects human rights".[12] The Constitution of China also protects "personal dignity", as specified in Article 38: "*the personal dignity of citizens of the People's Republic of China shall not be violated*". Furthermore, Article 35 of the Constitution refers to freedom of expression and states that the "*citizens of the People's Republic of China enjoy freedom of speech, of the press, of assembly, of association, of procession, and of demonstration*." The Constitution protects the right to freedom of the correspondence [13] and privacy of the correspondence[14] but does not include a general and widely encompassing right to privacy. No express constitutional protection of data protection rights exists, either.

In academic debate, Chinese scholars have proposed a reconstruction of the concept of "human rights" taking into account the development of digitalisation and related changes in society. [15] Scholars have proposed that the constitutional protection of human rights provides a ground to recognise "the right of personal information self-determination"[16] as well as the right to protection of personal information.[17] Yao argues that the right to the protection of personal information can be recognised as a "fundamental human right" in light of Article 33 of the Constitution.[18] Wang considers that "personal dignity", as protected by Article 38 of the Constitution, may provide a ground for protecting personal information.[19] Peng suggests that the right to the protection of personal information should be recognised as a new "basic constitutional right" in order to help form a more detailed personal information protection framework.[20]

---

[11] Yueming Zhang, 'Processing of Personal Data by Public Authorities in China: Assessing Equivalence for Cross-Border Transfers from the EU to China' (2023) 14 European Journal of Law and Technology.

[12] Article 33 of China's Constitution. Peilin Yu (于沛霖), 'Analysis on the Legal Relationship about 'State Respects and Protects Human Rights ("国家尊重和保障人权"之法律关系解读)' (2007) 06 Journal of Law (法学杂志) 28.

[13] Article 40 of China's Constitution.

[14] Article 39 of China's Constitution.

[15] Changshan Ma (马长山), '"Fourth Generation Human Rights" and Their Protection in the Context of a Smart Society (智慧社会背景下的"第四代人权"及其保障)' (2019) 05 China Legal Science (中国法学) 5.

[16] Hong Zhao (赵宏), 'The Protection Status and Legislative Trend of Information Self-determination Right in China (信息自决权在我国的保护现状及其立法趋势前瞻)' (2017) 01 China Law Review (中国法律评论) 147.

[17] Xixin Wang (王锡锌) and Chun Peng (彭錞), 'The Constitutional Basis of the Personal Information Protection Legal System (个人信息保护法律体系的宪法基础)' (2021) 15 Tsinghua Law Review (清华法学) 6.

[18] Yuerong Yao(姚岳绒), 'The Proof of Information Self-Determination as a Fundamental Right in China （论信息自决权作为一项基本权利在我国的证成）' (2012) 04 Political Science and Law (政治与法律) 73.

[19] Kai Wang (王锴), 'The General Personality Rights in the Constitution and Their Impact on Civil Law (论宪法上的一般人格权及其对民法的影响)' (2017) 03 China Legal Science (中国法学) 115.

[20] Chun Peng (彭錞), 'Personal Information Protection from the Perspective of the Constitution: Clarification of Nature, Strength Setting and Mechanism Coordination (宪法视角下的个人信息保护：性质厘清、强度设定与机制协调)' (2022) 04 Law and Modernization (法治现代化研究).

However, the judiciary has not acknowledged this debate. Nor has it influenced lawmakers. As a civil law country, China cannot through case law create the constitutional right to privacy and data protection without an explicit ground (as it is possible in common law countries, such as the US).[21] Furthermore and most significantly, as there is no constitutional court in China, the Constitution is generally regarded as "non-justiciable".[22] This implies that Chinese courts are not empowered to invalidate a law or a regulation on the ground that it violates the Constitution.[23]

2.2 Relevant general rules

The general data protection and privacy framework in China encompasses several legislative sources, including the Civil Code, the Criminal Law, and the Consumer Protection Code.

It is worth noting that the right to data protection is protected as a civil right. On 28 May 2020, China adopted the Civil Code, which came into force on 1 January 2021. The Civil Code replaced several legislative acts, namely the General Rules of the Civil Law (2016), the Contract Law (1999), the Property Law (2007), the Tort Liability Law (2009), etc.[24] The Civil Code is the first Chinese law to carry the title of "code" and aims to strengthen the protection of people's rights. The Civil Law of China protects natural persons' right to privacy[25] and personal information.[26] Specifically, Article 1032 of the Civil Code states that "a natural person enjoys the right to privacy. No organization or individual may infringe upon the other's right to privacy by prying into, intruding upon, disclosing, or publicizing others' private matters". Article 1034 of the Civil Code states that "personal information is the information recorded electronically or in other ways that can be used, by itself or in combination with other information, to identify a natural person, including the name, date of birth, identification number, biometric information, residential address, telephone number, email address, health information, whereabouts, and the like, of the person". Under the section on the "right to personality", the Civil Code includes six articles on the right to personal information. The Civil Code includes a definition of "personal information".[27] The Civil Code also specifies the basic data processing principles of lawfulness, justification, and necessity,[28] the circumstances for exemption from civil liability for processing personal information,[29] the right to consult, copy, rectify and delete personal information,[30] data security principles and obligations[31] as well as the confidentiality of personal information.[32]

[21] Yang Feng, 'The Future of China's Personal Data Protection Law: Challenges and Prospects' (2019) 27 Asia Pacific Law Review 62.
[22] Graham Greenleaf, 'China—From Warring States to Convergence?', *Asian Data Privacy Laws: Trade & Human Rights Perspectives* (Oxford University Press 2014).
[23] Paul De Hert and Vagelis Papakonstantinou, 'The Data Protection Regime in China' (European Parliament, Directorate-General for Internal Policies 2015) PE 536.472.
[24] Civil Code of the People's Republic of China (《中华人民共和国民法典》) , adopted by National People's Congress on 28 May 2020, enforced on 1 January 2021. (Hereinafter referred to as "Civil Code" or "Civil Code of China")
[25] Article 1032 of the Civil Code.
[26] Article 1034 of the Civil Code.
[27] Article 1034 of the Civil Code.
[28] Article 1034 of the Civil Code.
[29] Article 1046 of the Civil Code.
[30] Article 1037 of the Civil Code.
[31] Article 1038 of the Civil Code.
[32] Article 1039 of the Civil Code.

In 2013, the National People's Council Standing Committee amended China's Consumer Protection Law to include provisions for the protection of personal information.[33] The Consumer Protection Law provides rules governing the collection and processing of personal information by "online retailers", and sets forth the general data protection principles of legality, rationality, and necessity.[34] The principles included in the Consumer Protection Law are largely identical to the earlier 2012 SC-NPC Decision.[35] These provisions apply to all industries, including companies that provide goods and services within China, in both online and offline contexts, and thus extend the data protection principles to more sectors.[36] The Consumer Protection Law also provides for civil liabilities and administrative enforcement in case of infringement of the obligations to protect personal information.[37] However, data subject rights of access, rectification, and deletion of personal information are missing from this set of rules.[38]

Additionally, according to Article 253(1) of China's Criminal Law, the crime of infringing on citizens' personal information involves that selling or providing a citizen's personal information in violation of state regulations may result in a maximum three-year imprisonment or criminal detention, along with a fine for serious cases, or a fine along with imprisonment ranging from three to seven years for especially serious cases.

2.3 The three main pillars of data protection and cybersecurity in China

With the rise of the digital economy and digital trade, China's data protection regime has undergone significant transformations. Overall, the three main pillars of China's data governance framework are the Personal Information Protection Law (PIPL),[39] the Cybersecurity Law (CSL),[40] and the Data Security Law (DSL).[41] Notably, the general rules mentioned in the previous section have not been abrogated by the PIPL.

Despite the introduction of several provisions in China's Consumer Protection Law, China did not have a comprehensive data protection framework until 2021. This changed on 20 August 2021, when China passed its first comprehensive data protection law, which came into force on 1 November 2021. The PIPL is modelled, at least in part, on foreign data protection regimes, most notably the GDPR.[42] The PIPL was developed with the aim of "protecting interests of personal information, regulating personal information

[33] Law of the People's Republic of China on the Protection of Consumer Rights and Interests (2013 Amendment) (《中华人民共和国消费者保护法》), amended by the National People's Congress Standing Committee on 25 October 2013, enforced on 15 March 2014.
[34] Article 29(1) Consumer Protection Law.
[35] The 2012 National People's Congress Standing Committee Decision concerning Strengthening Network Information Protection ("2012 NPC-SC Decision") marked the inception of China's data protection regulations. See, Greenleaf, 'China—From Warring States to Convergence?' (n 20).
[36] Graham Greenleaf and George Tian, 'Data Protection Widened by China's Consumer Law Changes' (2013) 126 Privacy Laws & Business International Report 27.
[37] Article 50 Consumer Protection Law.
[38] See, Greenleaf and Tian (n 36).
[39] The Personal Information Protection Law of the People's Republic of China (《中华人民共和国个人信息保护法》), adopted by SC-NPC on 20 August 2021, enforced on 1 November 2021.
[40] The Cybersecurity Law of the People's Republic of China (《中华人民共和国网络安全法》), adopted by SC-NPC on7 November 2016, enforced on 1 June 2017.
[41] The Data Security Law of the People's Republic of China (《中华人民共和国数据安全法》), adopted by SC-NPC on 10 June 2021, enforced on 1 September 2021.
[42] Guan Zheng, 'Trilemma and Tripartition: The Regulatory Paradigms of Cross-Border Personal Data Transfer in the EU, the U.S. and China' (2021) 43 Computer Law & Security Review 105610.

processing activities, and promoting the reasonable use of personal information".[43] The PIPL is also the first data protection law in China that applies to public authorities.[44]

In addition to the PIPL, China's data governance framework also comprises security laws: the CSL and the DSL. The CSL, which came into force on 1 June 2017, included some of the most comprehensive data protection principles at that time. Overall, the CSL focuses on national data security and includes requirements related to data localisation, critical infrastructure protection, and cyber incident response.[45] The DSL, which was adopted on 10 June 2021, aims to ensure the security of data with a view to protect national security and public security interests. The DSL covers both personal and non-personal data.[46]

Notably, Chinese laws, like the CSL, the DSL and the PIPL, often only contain general principles and require more detailed implementation and interpretation rules to make them enforceable to be issued by data protection departments such as the CAC.[47] As a result, in recent years, there has been an abundance of implementing regulations and guidelines in China to fill the interpretative gaps left by these three laws.[48]

The EU's influence on the Chinese data governance framework, particularly the PIPL, is manifest.[49] However, regarding cross-border data transfer rules, lawmakers in China have been developing an original regime with several Chinese characteristics.[50] Overall, the Chinese data transfer regime aims to strike a balance between different competing objectives: the growth of the digital economy, the protection of personal data, and the protection of national security and cyber sovereignty interests.

2.4 Core Personal Data Protection Rules

2.4.1 Personal data under the PIPL

The PIPL defines personal information as "all kinds of information recorded by electronic or other means *related to identified or identifiable natural persons*".[51] This appears similar to the definition given in Article 4(1) of the GDPR.

In addition, information that has been anonymised is excluded from the material scope of the PIPL.[52] Anonymisation in the PIPL refers to the process of processing personal information "to make it impossible to identify specific natural persons" and "impossible to restore".[53] The definition of anonymisation thus uses absolutist language, which will be difficult to interpret on the ground given the practical impossibility of

[43] Article 1 of the PIPL.
[44] Article 33 of the PIPL.
[45] Graham Greenleaf and Scott Livingston, 'China's New Cybersecurity Law – Also a Data Privacy Law?' (Social Science Research Network 2016) SSRN Scholarly Paper ID 2958658 <https://papers.ssrn.com/abstract=2958658> accessed 21 April 2024.
[46] Rogier Creemers, 'China's Emerging Data Protection Framework' (2022) 8 Journal of Cybersecurity tyac011.
[47] European Data Protection Board, 'Legal Study on Government Access to Data in Third Countries' (2021) <https://edpb.europa.eu/our-work-tools/our-documents/legal-study-external-provider/legal-study-government-access-data-third_en> accessed 21 April 2024.
[48] 'Law in China - DLA Piper Global Data Protection Laws of the World' <https://www.dlapiperdataprotection.com/index.html?t=law&c=CN> accessed 21 April 2024.
[49] Daniel Solove, 'China's PIPL vs. the GDPR: A Comparison' (2021) <https://teachprivacy.com/chinas-pipl-vs-gdpr-a-comparison> accessed 21 April 2024.
[50] Graham Greenleaf, 'China Issues a Comprehensive Draft Data Privacy Law' (Social Science Research Network 2020) SSRN Scholarly Paper ID 3795001 <https://papers.ssrn.com/abstract=3795001> accessed 21 April 2024.
[51] Article 4 PIPL.
[52] Article 4 PIPL.
[53] Article 73(4) PIPL.

eliminating all re-identification risks, even with the most sophisticated techniques. Yet, anonymisation is of particular relevance in the context of cross-border data transfers, as it offers, at least in principle, a means to avoid (some) restrictions. The anonymisation standard ultimately adopted by China should therefore be carefully considered to fully grasp the implications of the cross-border data transfer restrictions.

2.4.2 Scope of the PIPL

The PIPL applies to the "processing" of personal information. Article 72 of the PIPL excludes the application of the law under a few circumstances. Purely personal or household activities are exempted from the application of the PIPL. This seems to be in line with the GDPR.[54] Moreover, the PIPL indicates that the specific laws that govern the "personal information processing of statistical or archives administration activities organised and implemented by the governments" will prevail in case of conflict.[55]

Under Article 3 of the PIPL, the law applies to the activities of processing personal information both *within the borders* of the PRC and *outside the borders* of the PRC under three circumstances.[56] These circumstances include:

1) Where the purpose is to provide products or services to natural persons inside the borders,
2) When conducting analysis or assessment of activities of natural persons inside the borders,
3) Other circumstances provided in laws or administrative regulations.

The territorial scope of the PIPL, as determined by Article 3, confirms the legislator's intention to protect personal information of both Chinese residents and foreign people located in China.

With regard to the territorial scope set by Article 3(1), the PIPL applies to the "processing activities" carried out within the territory of China, while an "establishment" in China is not required. As a result, a foreign company with no establishment in China can still be regulated by the PIPL if the processing activities are carried out in China. By contrast, even if a covered entity is established in China, it does not necessarily fall within the scope of Article 3(1) if all its data processing activities are only carried out overseas.[57]

2.4.3 Data processing principles

The PIPL sets forth a number of fundamental personal information protection principles. These principles comprise lawfulness, fairness, necessity, and sincerity,[58] purpose limitation and data minimisation,[59] transparency,[60] data quality,[61] accountability and data security.[62]

2.4.4 Data subjects' rights

Similar to the EU GDPR, the Chinese data protection legal framework grants individuals a series of data protection rights.

---

[54] Article 2 GDPR.
[55] Article 72 (2) PIPL.
[56] Article 3 PIPL.
[57] See Samuel Yang, 'A Look at the Extraterritorial Applicability of China's Newly Issued PIPL: A Comparison to the EU's GDPR' <https://iapp.org/news/a/a-look-at-the-extraterritorial-applicability-of-chinas-newly-issued-pipl-a-comparison-to-the-gdpr/> accessed 21 April 2024.
[58] Article 5 PIPL.
[59] Article 6 PIPL.
[60] Article 7 PIPL.
[61] Article 8 PIPL.
[62] Article 9 PIPL.

The PIPL enhanced the protection of individuals' data protection rights that already existed in the Chinese Civil Code and recognised a series of other rights. It provides that an individual has: the right to know and decide,[63] the right to access,[64] the right to rectification,[65] the right to delete,[66] and the right to request an explanation.[67]

The PIPL does not provide a right to object to processing in general, although the right to decide found in Article 44 of the PIPL could be interpreted as covering this prerogative. Further, the PIPL also aims to protect individuals against automated decision-making and profiling. It recognises an individual's right to refuse decisions made solely through automated decision-making when the automated decision-making produces decisions that may have "a major influence on the rights and interests of the individual". Those conducting automated decision-making for commercial purposes must simultaneously provide the option to not target an individual's characteristics or provide the individual with a convenient method to refuse.

2.4.5 Lawful grounds for data processing

The lawfulness of personal information processing means that the processing should be grounded on a valid legal basis. Both the GDPR and PIPL include an exhaustive list of legal bases to legitimise the processing of personal information, but these two lists are not identical. Under the PIPL, processing of personal information must be based on one of six lawful grounds, with an exception if "other circumstances are provided in laws and administrative regulations".[68] These grounds are:

1) consent,
2) necessary to conclude or fulfil a contract with the individual,
3) necessary to fulfil statutory responsibilities or statutory obligations,
4) necessary to respond to sudden public health incidents or protect natural persons' lives and health, or the security of their property, under emergency conditions,
5) reasonable scope to implement news reporting, public opinion supervision, and other such activities for the public interest, and
6) processing of the personal information disclosed by the individuals or other legally disclosed personal information.[69]

With respect to consent, the PIPL further imposes certain substantive and procedural requirements in Articles 14 and 16. Consent for processing of personal information must be obtained 1) under the precondition of full knowledge, 2) with a voluntary and explicit statement of wishes[70] and 3) on the basis that it is revocable.[71] The PIPL also indicates several circumstances under which specific consent is required, which include the use of facial recognition,[72] transferring personal information beyond the borders,[73] and processing sensitive personal information. Notably, the PIPL drafters have chosen to adopt a broad and open

[63] Article 44 PIPL.
[64] Article 45 PIPL.
[65] Article 46 PIPL.
[66] Article 47 PIPL.
[67] Article 48 PIPL.
[68] Article 13(7) PIPL.
[69] Article 13 PIPL.
[70] Article 14 PIPL.
[71] Article 16 PIPL.
[72] Article 27 PIPL.
[73] Article 39 PIPL.

definition of sensitive personal information.[74] Children in China cannot give consent until they are 14 years old. For children younger than 14, parental consent is needed.[75]

The second lawful basis is contractual necessity. The PIPL allows processing of personal information when "necessary to conclude or fulfil a contract in which the individual is an interested party".[76] In order to achieve this, the scope of the personal information processed must be limited to the scope of the contract. Scholars have been calling for a restrictive interpretation of the "contractual necessity" test.[77]

The third lawful basis is the necessity to fulfil statutory duties and responsibilities or statutory obligations.[78]

The fourth lawful basis, i.e., responding to "sudden public health incidents or protect natural persons' lives and health," finds some of its roots in the COVID-19 pandemic. Under such emergency conditions where it is impossible to notify individuals in a timely manner, it is required to notify them after the conclusion of the emergency circumstances.[79]

The fifth lawful basis allows "within a reasonable scope to implement news reporting, public opinion supervision for the public interest".[80] "Public opinion supervision" generally refers to critical reporting by news organisations or social media users regarding public affairs or public authorities' activities.[81] The reference to the "public interest" should imply that news reporting and public opinion supervision aim to fight against "immoral, illegal and criminal matters or to supervise public power and to uphold social justice".[82]

The sixth lawful basis covers "personal information disclosed by the individuals or other legally disclosed personal information".

Of note, comparing the PIPL's list to the GDPR's list, one important difference is the absence of the legitimate interest ground within the PIPL's list. This may mean that both the consent and the contractual necessity legal bases will have to be interpreted broadly to the detriment of the principle of purpose limitation.

2.4.6 Data protection enforcement

The effectiveness of data protection rules depends on robust enforcement mechanisms. China does not have one independent supervisory authority in charge of the enforcement of data protection rules. Instead,

[74] Article 30 PIPL. Under the PIPL sensitive personal information means personal information that, once leaked or illegally used, may easily cause harm to the dignity of natural persons grave harm to personal or property security, including information on biometric characteristics, religious beliefs, specially-designated status, medical health, financial accounts, individual location tracking, etc., as well as the personal information of minors under the age of 14. See Article 28 PIPL.
[75] Article 15 PIPL.
[76] Article 14 (2) PIPL.
[77] Weixing Shen (申卫星) and Xu Yang (杨旭), 'On the Restrictive Application of the Conclusion of a Contract as the Legal Basis for Personal Information Processing (论订立合同作为个人信息处理合法性基础的限缩适用)' (2022) 04 Nanjing Journal of Social Science (南京社会科学) 76.
[78] Article 14 (3) PIPL.
[79] Article 19 PIPL.
[80] Article 999 of the Civil Code.
[81] Xiao Cheng (程啸), *The Interpretation of Personal Information Protection Law of the People's Republic of China (个人信息保护法理解与适用)* (China Legal Publishing House (中国法制出版社有限公司) 2021).
[82] Cheng (程啸) (n 81).

enforcement prerogatives are shared among several administrative units. The PIPL identifies the relevant departments that are responsible for fulfilling personal information protection duties, which include:[83]

Departments	Comments
State cybersecurity and informatisation department[84]	Responsible for comprehensive planning and coordination of personal information protection enforcement and related supervision and management work
Relevant State Council departments[85]	Responsible for personal information protection, supervision, and management work within their respective scope of duties and responsibilities
County-level and higher People's Governments' relevant departments	Such departments' responsibilities are determined according to relevant State regulations

Table 1 Relevant departments that are responsible for fulfilling the personal information protection duties in China

Overall, these departments are not independent authorities, but departments affiliated to the State Council or other executive administrations. The PIPL includes an overview of the tasks and powers of such departments fulfilling the personal information protection duties, which are: [86]

1) Conducting personal information protection education, and guiding and supervising personal information handlers' conduct of personal information protection work,
2) Accepting and handling personal information protection-related complaints and reports,
3) Investigating and handling unlawful personal information handling activities,
4) Other duties and responsibilities provided in laws or administrative regulations.

The absence of an independent data protection authority has been criticised by Western scholars.[87] The decentralised enforcement model has also been criticised within China. Scholars have found this approach in practice to entail "unclear delineation of responsibilities, individualistic approaches, and deferral of law enforcement actions".[88] It has also been pointed, however, that the creation of a new oversight department may face challenges in terms of human resources, experience and professionalism.[89] During the drafting period of the PIPL, the creation of a separate data protection authority, or a separate body with national

[83] Article 60 PIPL.
[84] Namely, the Cyberspace Administration of China (CAC).
[85] For instance, the Ministry of Industry and Information Technology (MIIT).
[86] Article 61 PIPL.
[87] See De Hert and Papakonstantinou (n 23).
[88] Xinbao Zhang (张新宝), *Personal Information Protection Law of the People's Republic of China - A Commentary (中华人民共和国个人信息保护法释义)* (People's Publishing House (人民出版社) 2021) 463.
[89] Zhang (张新宝) (n 88) 463.

responsibility for enforcement of data protection rules, was proposed.[90] However, this approach was not adopted by the PIPL.

On 16 March 2023, the Chinese Communist Party (CCP) Central Committee and the State Council released the plan to establish a new state-level regulatory body, namely the "National Data Bureau" (NDB).[91] The NDB will be responsible for "coordinating the integration, sharing, development and utilisation of data sources and coordinating the promotion of China's digital economy". [92] The relevant discussions and reports from the government are still emerging. The plan, however, clarified that the NDB will not replace the existing competent departments to become an independent oversight authority for data protection issues in China. Instead, the NDB will take the main task of promoting China's digital economy. The Cyberspace Administration of China (CAC) and the NDB will be the two wings of China's data governance framework, with the CAC concentrating on data security and the NDB concentrating on the data economy.[93]

Article 66 of the PIPL empowers the "relevant oversight departments" to impose administrative sanctions. The types of sanctions include correction orders, warnings, confiscation of illegal incomes, and suspension or termination of services. If the personal information handler refuses to take such corrective actions, the oversight departments have the power to impose high administrative fines. The PIPL follows the GDPR's approach of a tiered system of fines. As a matter of principle, administrative fines can go up to RMB 1,000,000 (about EUR 132,000) and the responsible individuals can be fined up to one tenth of this amount. When the breach is serious, administrative fines can go up to RMB 50 million (about EUR 6,600,000) or 5% of the previous year's annual turnover, whichever is higher.[94] However, the PIPL itself does not clarify the specific factors to take into account to determine the level of fines, nor the specific oversight departments in charge of issuing the fines.

2.5 Data localisation rules

Overall, China does not impose a blanket prohibition on the transfer of data outside its territorial boundaries. However important restrictions are in place, including storage localisation requirements.

In general, Article 37 of the CSL requires critical information infrastructure operators ("CIIOs") to store personal information and important data generated from critical information infrastructures in China. Article 40 of the PIPL also specifies that "Critical information infrastructure operators and personal information handlers handling personal information reaching quantities provided by the State cybersecurity and informatisation department shall store personal information collected and produced within the borders of the People's Republic of China domestically." The PIPL nonetheless provides an exemption from this rule, so that "where they need to provide it abroad, they shall pass a security assessment organised by the State cybersecurity and informatization department".[95] The details of the security assessment are discussed later.

---

[90] Yehan Huang and Mingli Shi, 'Top Scholar Zhou Hanhua Illuminates 15+ Years of History Behind China's Personal Information Protection Law' (*DigiChina*) <https://digichina.stanford.edu/work/top-scholar-zhou-hanhua-illuminates-15-years-of-history-behind-chinas-personal-information-protection-law/> accessed 21 April 2024.

[91] Jia Xu, 'What Does China's Newly Launched National Data Bureau Mean to China and Global Data Governance?' (*Internet Policy Review*, 25 April 2023) <https://policyreview.info/articles/news/chinas-national-data-bureau-and-global-data-governance> accessed 21 April 2024.

[92] 'Establishment of the National Data Bureau in China (组建国家数据局)' (*Xinhuanet*, 7 March 2023) <http://www.xinhuanet.com/politics/2023-03/07/c_1129419141.htm> accessed 21 April 2024.

[93] Xu (n 91).

[94] Article 66 PIPL.

[95] Article 40 PIPL.

Moreover, Article 36 of the PIPL states that personal information "processed by public authorities" shall be stored within the mainland territory of China, with the caveat that when there is an actual need for transferring personal information abroad, a security assessment must be successfully passed.

2.6 Rules applicable to public authorities

An obstacle to China's participation in global discussions on cross-border data regulations is its domestic surveillance and law enforcement rules. One serious concern is that the Chinese national security and criminal law enforcement system is not in line with EU standards.[96]

The PIPL is the first legal instrument restricting public authorities' activities relating to the processing of personal information. It specifically imposes personal information processing requirements on "state organs" and sets forth seven lawful bases for the processing of personal information in this context.[97]

The PIPL specifies that the processing of personal data by public authorities must not exceed the scope necessary to carry out their responsibilities. Moreover, Article 35 of the PIPL specifies that public authorities must inform data subjects of the fact that their personal information is being processed. In addition, Article 36 of the PIPL states that personal information "processed by public authorities" shall be stored within the mainland territory of China, with strict conditions for data exports from China. Overall, the PIPL's data processing requirements also apply to public authorities, while the PIPL also highlights that the principles such as data minimisation and storage localisation shall be strictly respected by public authorities' when they process personal information.

Of note, the PIPL provides various redress mechanisms to individuals when there is a breach by a public authority, including both administrative-oriented compensatory mechanisms and possibilities for judicial remedies. In China, individuals have the right to file a complaint, make a report or an accusation in the event of unlawful processing of personal data, or claim compensation for data privacy breaches before the internal oversight department of each state organ.

Other laws such as the Chinese Criminal Procedure Law as well as national security laws (including the National Security Law,[98] the National Intelligence Law,[99] the Counter-espionage Law,[100] the Counter-terrorism Law[101]) are however also applicable to public authorities.

[96] European Data Protection Board, 'Legal Study on Government Access to Data in Third Countries' (2021) <https://edpb.europa.eu/our-work-tools/our-documents/legal-study-external-provider/legal-study-government-access-data-third_en> accessed 21 April 2024.
[97] Article 33 PIPL.
[98] National Security Law of People's Republic of China (《中华人民共和国国家安全法》), adopted by the SC-NPC on 1 July 2015, enforced on 1 July 2015.
[99] The National Intelligence Law of the People's Republic of China (《中华人民共和国国家情报法》), adopted by the SC-NPC on 27 June 2017, amended by the SC-NPC on 27 April 2018.
[100] The Counter-espionage Law of the People's Republic of China (《中华人民共和国反间谍法》) , adopted by the SC-NPC on 1 November 2014.
[101] The Counter-terrorism Law of the People's Republic of China (《中华人民共和国反恐怖主义法》), adopted by the SC-NPC on 27 December 2015, amended by the SC-NPC on 27 April 2018.

Furthermore, under the Criminal Procedure Law,[102] personal information deemed to be electronic evidence can be collected and used by criminal investigation authorities in China.[103] Under the Counter-terrorism law, organisations and individuals have the obligation to assist and cooperate with relevant counter-terrorism activities,[104] telecommunications business operators and Internet service providers are specifically required to provide assistance for counter-terrorism work.

Overall, given the wide range of personal information that public authorities can collect, the safeguards for personal information processing remain high level and limited.[105]

3 China's cross-border data transfer regime

3.1 Scope

The Chinese cross-border data transfer regime has been established by the PIPL and the CSL. These instruments are supplemented by other measures and standards, which further interpret the data export framework and provide detailed implementation rules.

The CSL provides the general rule on data localisation of "critical information infrastructure operators (CIIOs)". Under the CSL, CIIOs in mainland China must store the collected or generated personal information or important data within mainland China. If it is genuinely necessary to provide such information outside the mainland due to business requirements, they must undergo a security assessment following measures jointly formulated by the State cybersecurity and informatisation departments and relevant State Council departments. Any contrary provisions specified by laws or administrative regulations must be followed.[106]

The transfer of personal data outside the borders of the PRC, for business or other purposes, is regulated by Chapter III of the PIPL. These provisions regulate the transfer of personal information by personal information handlers, who may be natural persons or legal entities, including public authorities.

3.2 Data transfer tools

In general, data transfers to countries outside China must satisfy one of the conditions set out in Article 38 of the PIPL:

- passing a security assessment administered by the CAC;
- undertaking a personal information protection certification run by recognised institutions in accordance with relevant regulations of the CAC;
- executing a standard contract for cross-border transfer provided by the CAC; or
- other bases provided in laws or administrative regulations or by the CAC.

Moreover, all cross-border data transfers initiated from China must be "truly needed": in other words, cross-border data transfers must overcome a "necessity test".[107] Unlike the GDPR, there is no scope for

[102] The Criminal Procedure Law of the People's Republic of China (《中华人民共和国刑事诉讼法》), adopted by the NPC on 1 July 1979, amended by the NPC on 14 March 2012.
[103] Fan Yang and Jiao Feng, 'Rules of Electronic Data in Criminal Cases in China' (2021) 64 International Journal of Law, Crime and Justice 100453.
[104] Article 9 Counter-terrorism Law.
[105] Mei Liu (刘玫) and Yunan Chen (陈雨楠), 'From Conflict to Integration: The Construction of Rules for the Protection of Citizens' Personal Information in Criminal Investigations (从冲突到融入：刑事侦查中公民个人信息保护的规则建构)' (2021) 05 Research on Rule of Law (法治研究) 34.
[106] Article 37 CSL.
[107] Article 38 of the PIPL.

"derogations". Although this is debated, whatever the means chosen to transfer the data, the personal information handler seems to be obliged to obtain the consent of the individual before transferring personal information abroad. In other words, when transferring personal information outside the territory of China, a separate consent appears to be necessity.[108] Making consent a necessary condition in most, if not all data transfer instances, is however likely to dilute this legal basis.

The framework for cross-border data transfers in China is summarised in Table 2:

Transfer of CII information / personal information over set quantities	**Transfer of non-CII personal information under set quantities**
"Necessity" test	
Pass a security assessment	Meet at least one of the following conditions: (1) Pass a security assessment (2) Certification (3) Standard contract
A separate consent	

Table 2. An overview of legal bases for transfer under the PIPL

Importantly, data exporters are *not* always allowed to freely choose among the three data transfer mechanisms, as the PIPL sets strict requirements for CIIOs[109] and when personal information reaches set quantities (cumulatively 100,000 persons' personal information or 10,000 persons' sensitive personal information).[110] For non-CIIO personal information processed in small quantities, personal information handlers can choose among the three cross-border data transfer tools mentioned above.

3.2.1 Security assessment for cross-border data transfers

The first data export mechanism is to pass a "security assessment". On 7 July 2022, the CAC released the Measures for the Security Assessment of Cross-border Data Transfer,[111] which came into effect on 1 September 2022. The Measures provide more details on the implementation of the "security assessment".

Under these measures, the security assessment is necessary in the following circumstances:

- When important data[112] is transferred abroad.

[108] Weiqiu Long (龙卫球), *Interpretation of the Personal Information Protection Law of the People's Republic of China (中华人民共和国个人信息保护法释义)* (China Legal Publishing House (中国法制出版社有限公司) 2021).
[109] The critical information infrastructure operators ('CIIOs') refer to "infrastructure involving the public communication and information services, power, traffic, water, finance, public service, and e-governance as well as other critical information infrastructure that if it is destroyed, loses its ability to function or encounters data leaks, might seriously endanger national security, national welfare and the people's livelihood, or the public interest". See, Article 31 of the CSL.
[110] Measures for the Security Assessment of Cross-border Data Transfer (《数据出境安全评估办法》) 2022 (State Internet Information Office Order No 11 (国家互联网信息办公室令 第 11 号).
[111] Measures for the Security Assessment of Cross-border Data Transfer (《数据出境安全评估办法》) 2022 (State Internet Information Office Order No 11 (国家互联网信息办公室令 第 11 号).
[112] The concept of "important data" refers to "any data which may endanger China's national security, economic operation, social stability, public health or public security, if it is tampered with, destroyed, leaked, or illegally acquired or used", see Article 4 of Measures for the Security Assessment of Cross-border Data Transfer.

- Where critical information infrastructure operators or data handlers handling the personal information of 1,000,000 or more persons provide personal information overseas.
- Where data handlers providing personal information abroad have cumulatively provided 100,000 persons' personal information or 10,000 persons' sensitive personal information abroad since 1st January of the preceding year.
- Other situations where the State Internet Information Department requires reporting on data export security assessments.[113]

The scope of "security assessment" covers both personal information and "important data". "Important data" is defined as "any data which may endanger China's national security, economic operation, social stability, public health or public security, if it is tampered with, destroyed, leaked, or illegally acquired or used".[114]

The security assessment advocates fora risk-based approach.[115] Specifically, the security assessment requires the data exporter to complete a prior self-assessment of its data transfers. The self-assessment must cover 1) the purposes, scope and methods of the data transfers, 2) the quantity, type and sensitivity of the data as well as the risk that may be brought by the transfers to national security, public interest or the rights and interests of other individuals and organisations, 3) the technical measures and compliance capabilities of the data recipients, 4) the channels for individuals to get remedies for their data protection right, and 5) a contract or document with legal force to set data protection obligations for the data recipients.[116] The security assessment must be submitted to the provincial-level Internet Information Department for review by both the provincial and national levels of the CAC departments.[117]

The circumstances under which security assessments are required are broadly defined. As Zhao points out, in the vast majority of cases, the number and scale of commercial data flows between local and foreign entities is so large that it is easy to meet the security assessment triggers. It will leave only a few data-transfer scenarios for the other two mechanisms.[118]

3.2.2 China's Standard Contract

The Chinese Standard Contract, together with the Regulations of Standard Contracts for Cross-border Transfer of Personal Information (the Chinese SCCs Regulations),[119] was unveiled by the Chinese National Information Security Standardisation Technical Committee on 24 February 2023. The Regulations came into force on 1 June 2023 with a six-month grace period running until 1 December 2023. The Chinese Standard Contract can only be used for transferring non-CIIO data, "non-important" data and personal data under set quantities.

---

[113] Article 4 of Measures for the Security Assessment of Cross-border Data Transfer.
[114] Article 19 of the Measures for the Security Assessment of Cross-Border Data Transfer.
[115] Xiaodong Ding (丁晓东), 'The Jurisprudential Reflection and Institutional Reconstruction of Cross-border Data Transfer: With a Comment on Measures of Out bound Data Transfer Security Assessment (数据跨境流动的法理反思与制度重构——兼评《数据出境安全评估办法》)' (2023) 01 Administrative Law Review(行政法学研究) 62.
[116] Article 5 of Measures for the Security Assessment of Cross-border Data Transfer.
[117] Article 4 of Measures for the Security Assessment of Cross-border Data Transfer.
[118] Jingwu Zhao (赵精武), 'On the Systematization of Data Cross-Border Assessment, Contracts and Authentication Rules (论数据出境评估、合同与认证规则的体系化)' (2023) 01 Administrative Law Review(行政法学研究) 1.
[119] National Information Security Standardization Technical Committee (全国信息安全标准化技术委员会), 'The Cyberspace Administration of China Announced the "Standard Contract Measures for the Export of Personal Information" (国家互联网信息办公室公布《个人信息出境标准合同办法》)' <https://www.tc260.org.cn/front/postDetail.html?id=20230224182605> accessed 21 April 2024.

It has been argued that the mechanism for data transfers based on the Standard Contract shows China's choice of a risk-based approach and observance of the principle of proportionality regarding transfer issues.[120] Compared with the EU Standard Contractual Clauses, the Chinese Standard Contract does not differentiate between scenarios based on the role of the parties.[121] However, both the EU SCCs and the Chinese Standard Contract recognise third-party beneficiary rights: data subjects are third-party beneficiaries under the Standard Contract. The Chinese Model Contract includes the data subject's rights under the PIPL to be protected by the data importer in the recipient country. The specific rights do not mirror the EU SCCs, but the idea of providing data subjects with the rights to enforce their data rights from the data recipients is similar to the EU SCCs. In case of data breaches, the Chinese Standard Contract requires the personal information importer to promptly take remedial actions and mitigate the impact on relevant individuals. Further, they must notify the breaches to the data exporter, the competent Chinese authority as well as the relevant individuals.

The Chinese Standard Contract provides a series of obligations for personal information handlers. For instance, the regulators stipulate that before transferring personal information abroad, a personal information handler must conduct a Personal Information Protection Impact Assessment (PIPIA) in advance.[122] The PIPIA requirements under the Chinese Standard Contract share conceptual similarities with the Data Protection Impact Assessment (DPIA) mandate outlined in the GDPR although they are systematically triggered. The primary objective of a PIPIA is to identify and evaluate risks associated with individuals' personal data, mitigating the likelihood of data breaches, and ensuring adherence to data protection regulations.[123]

The Chinese Standard Contract also requires data exporters to notify individuals that they are third-party beneficiaries and to mention the individual's right to access, copy, amend, and delete. Moreover, individuals have the right to request a copy of the Standard Contract.[124]

3.2.3 China's certification mechanism

On 24 June 2022, the Security Certification Guidelines on Cross-border Transfer of Personal Information,[125] which serve as the guidelines for the "certification mechanism" were adopted. On 18 November 2022, the CAC issued the Implementation Rules for Personal Information Protection Certification,[126] which also apply to the certification of cross-border data transfers and provide more detailed rules on the procedures for certification. The certification mechanism can be employed for "cross-border processing of personal

[120] Jing Jin (金晶), 'Standard contractual clauses as a regulatory tool for cross-border transfers of personal information (作为个人信息跨境传输监管工具的标准合同条款)' (2022) 44 法学研究 19.
[121] Reed Smith LLP, 'Cross-Border Data Transfer Mechanism in China and Practical Steps to Take' <https://www.reedsmith.com/en/perspectives/2022/10/cross-border-data-transfer-mechanism-in-china-and-practical-steps-to-take> accessed 21 April 2024.
[122] Article 5 of the Standard Contract Measures for the Export of Personal Information.
[123] 'International: Comparing China's Standard Contract to the EU's SCCs' (*DataGuidance*, 20 June 2023) <https://www.dataguidance.com/opinion/international-comparing-chinas-standard-contract-eus> accessed 21 April 2024.
[124] Article 2 of the Standard Contract Measures for the Export of Personal Information.
[125] National Information Security Standardization Technical Committee, 'Security Certification Guidelines on Cross-Border Transfer of Personal Information (网络安全标准实践指南——个人信息跨境处理活动安全认证规范）' <https://www.tc260.org.cn/front/postDetail.html?id=20220624175016> accessed 21 April 2024.
[126] Cyberspace Administration of China, 'Implementation Rules for Personal Information Protection Certification (个人信息保护认证实施规则)' <http://www.cac.gov.cn/2022-11/18/c_1670399936983876.htm> accessed 21 April 2024. An unofficial translation: https://hankunlaw.com/en/portal/article/index/cid/8/id/12518.html.

information between multinational companies or subsidiaries or affiliated companies of the same economic or business entity".[127]

Despite the name "certification mechanism", China's version of the certification process shares more similarities with Binding Corporate Rules (BCRs) as governed by the GDPR.[128] More specifically, personal information handers are required to 1) conduct a self-assessment, 2) sign a data transfer contract or a legally binding document with the data recipients, 3) appoint a Data Protection Officer in China, 4) keep records of the personal information processing activities, 5) identify and notify personal information breaches, and 6) fulfil the obligations of protecting individual rights.[129]

The professional certification institution in China is the "China Cybersecurity Review and Technology and Certification Centre (CCRC)".[130] The process for certification includes five stages: certification application, technical verification, on-site audit, certification decision, and post-certification supervision.[131]

3.3 Recent evolution: the Provisions on Regulating and Promoting Cross-Border Data Transfers

Relatively quickly after its adoption, the enforcement of the first version of the data transfer regime appeared too strict and complicated. On 28 September 2023, the CAC thus published a draft regulation called the "Provisions on Regulating and Promoting Cross-Border Data Transfers".[132] After minor revisions, it was officially enacted on March 22, 2024.[133] These regulations have eased certain aspects of China's current cross-border data transfer rules, in particular to the benefit of foreign companies and multinationals.[134] This evaluation signals that China may be in the process of rebalancing the compromise initially set between economic growth and national security interests.[135]

According to the Provisions, the transfer of data falling under categories like international trade, academic cooperation, transnational manufacturing, and marketing, which do not contain personal information or

[127] Article 2 of the Security Certification Guidelines on Cross-Border Transfer of Personal Information.
[128] Reed Smith LLP, 'Cross-Border Data Transfer Mechanism in China and Practical Steps to Take' <https://www.reedsmith.com/en/perspectives/2022/10/cross-border-data-transfer-mechanism-in-china-and-practical-steps-to-take> accessed 21 April 2024.
[129] Article 5 of the Security Certification Guidelines on Cross-Border Transfer of Personal Information.
[130] Cyberspace Administration of China (n 127).
[131] Article 4 of Implementation Rules for Personal Information Protection Certification.
[132] Office of the Central Committee for Network Security and Informatisation, 'Notice of the National Internet Information Office on the Public Consultation on Provisions on Regulating and Facilitating Cross-Border Flow of Data (Draft for Opinion (国家互联网信息办公室关于《规范和促进数据跨境流动规定（征求意见稿）》公开征求意见的通知)' (28 September 2023) <http://www.cac.gov.cn/2023-09/28/c_1697558914242877.htm> accessed 13 December 2023.
[133] Office of the Central Committee for Network Security and Informatisation, 'Provisions on Regulating and Facilitating Cross-Border Flow of Data (Draft for Opinion (国家互联网信息办公室《规范和促进数据跨境流动规定》)' (22 March 2024) <https://www.cac.gov.cn/2024-03/22/c_1712776611775634.htm> accessed 21 April 2024.
[134] Arendse Huld, 'China Cross-Border Data Transfer - Regulator Moves to Ease Rules' (*China Briefing News*, 3 October 2023) <https://www.china-briefing.com/news/china-cross-border-data-transfer-draft-regulations-ease-requirements/> accessed 21 April 2024.
[135] Martin Chorzempa and Samm Sacks, 'China's New Rules on Data Flows Could Signal a Shift Away from Security toward Growth | PIIE' (3 October 2023) <https://www.piie.com/blogs/realtime-economics/chinas-new-rules-data-flows-could-signal-shift-away-security-toward-growth> accessed 21 April 2024.

important data, would not need to go through any of the data transfer mechanisms mentioned in section 3.2 of this report. [136]

With regard to "important data," for which there is no definition yet in the law or related guidance, data transfer approval would only be required once competent authorities either explicitly define what categories of data constitute "important data" or if covered entities are directly notified that their data are "important." The intention is thus to reduce the chilling effect of the restrictions set upon important data by enhancing legal certainty.[137]

The Provisions also attempt to clarify other key points of the data transfer regime. For instance, there would be no restrictions on the transfer of personal data outside China for the purpose of entering into or performing a contract to which the data subject is a party, such as cross-border shopping, cross-border bank transfers, airline and hotel bookings, and visa processing. The transfer of employee data, as necessitated by the employment contract and in accordance with relevant laws, such as Chinese employment laws, will also be exempt from the data transfer provisions.[138]

It has been recently reported that Shanghai is set to expedite approvals for foreign firms seeking to transfer local data offshore, presenting another significant relaxation of China's stringent restrictions. The initiative, discussed with representatives of foreign firms in the past few weeks, aims to attract foreign investors amidst China's economic challenges, offering a potential solution to delays and concerns caused by the 2022 regulations requiring security reviews for important offshore data transfers.[139]

4 International commitments

China is a member of the Asia-Pacific Economic Cooperation (APEC). However, APEC's Privacy Framework is not binding on its signatory states, and thus does not have legal status for China.[140] More specifically, the CBPR system is a voluntary, accountability-based framework that serves to facilitate data flows across the APEC region, based on the APEC Privacy Framework. It is a government-backed data privacy certification system. The CBPR was endorsed by APEC Leaders in 2011. APEC members who want to join must demonstrate that they can enforce compliance with the CBPR system's requirements before joining. The Joint Oversight Panel (JOP) administers the APEC CBPR system. China, although acting as an APEC member economy, has never expressed any interest in joining as a member of this system. At present, Singapore and eight other APEC Member Economies are participating in the APEC CBPR system.[141] China is listed among the countries with which the Organisation for Economic Co-operation and Development (OECD) "works closely" within its scope of activities.[142]

---

[136] Article 3 of the Provisions on Regulating and Facilitating Cross-Border Flow of Data.
[137] Article 2 of the Provisions on Regulating and Facilitating Cross-Border Flow of Data.
[138] Article 5 of the Provisions on Regulating and Facilitating Cross-Border Flow of Data.
[139] Reuters, 'Exclusive: Shanghai to Allow Faster Data Transfer from China for Foreign Firms-Sources' <https://www.reuters.com/world/china/shanghai-allow-faster-data-transfer-china-foreign-firms-sources-2024-02-07/> accessed 21 April 2024.
[140] Graham Greenleaf, 'The APEC Privacy Initiative: "OECD Lite" for the Asia-Pacific?' (2004) 71 Privacy Laws & Business 16.
[141] 'APEC CBPR & PRP Questions and Answers'. March 2020. https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2020/03/cipl_cbpr_and_prp_q_a_final__19_march_2020_.pdf accessed 21 April 2024.
[142] OECD, Our Global Reach. <https://www.oecd.org/about/members-and-partners/#:~:text=The%20OECD%20works%20closely%20with,the%20relevance%20of%20policy%20debates.> accessed 21 April 2024.

With this said, in recent years, China has attempted to influence international data transfer rules and has promoted the concept of digital sovereignty. In September 2020, China announced the Global Data Security Initiative,[143] with a view to provide a framework for countries to cooperate on issues related to cross-border data flows. This Initiative is based upon three high-level principles, i.e., multilateralism, secure development, and fairness and justice,[144] together with eight more specific tenets.[145]

The Global Data Security Initiative has been seen as an avenue to build a larger framework for the global digital economy.[146] Since 2020, the Global Data Security Initiative has been mentioned by Xi Jinping in several summits, including the Shanghai Cooperation Organisation (SCO) Summit, the BRICS Summit, and the G20.[147]

At the regional level, China's recent position is reflected in its commitments to the Regional and Comprehensive Economic Partnership (RCEP) agreement.[148] Many of the RCEP provisions, for instance, on data localisation and cross-border data flows, reflect China's vision and preferences in terms of digital commerce, and are framed through the concept of digital sovereignty. The RCEP provisions on cross-border data flows thus provide more autonomy and flexibility to its signatories, when compared, for example, with the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP). Under the RECP framework, signatories consent "not to prevent" cross-border transfers, allowing for varied measures if deemed "necessary" to attain a "legitimate public policy objective".[149] For instance, a footnote to Provision 12.14.3(a), which is the "legitimate public policy objective" exception, states: "[f]or the purposes of this subparagraph, the Parties affirm that the necessity behind the implementation of such legitimate public policy shall be decided by the implementing Party."[150] Notably, there is no stipulation mandating that the measure be the "least burdensome" for achieving the specified objective. Furthermore, the obligations are contingent upon an entirely self-determined and non-disputable national security exception.[151]

Similarly, by actively participating in the E-Commerce Joint Statement Initiative (JSI), China has pledged to propel those negotiations forward.[152] However, it has emphasised that security must be established as a prerequisite for the seamless flow of data across borders, a stance it has consistently taken in various multilateral forums, like the Baise Executive Leadership Academy, the China-ASEAN Information Port Forum, the China-Singapore Internet Forum, and the China-Africa Internet Development Cooperation Forum.[153]

---

[143] Chaeri Park, 'Knowledge Base: China's "Global Data Security Initiative" 全球数据安全倡议' (*DigiChina*) <https://digichina.stanford.edu/work/knowledge-base-chinas-global-data-security-initiative/> accessed 21 April 2024.
[144] Chaeri Park, 'Knowledge Base: China's "Global Data Security Initiative" 全球数据安全倡议' (*DigiChina*) <https://digichina.stanford.edu/work/knowledge-base-chinas-global-data-security-initiative/> accessed 21 April 2024.
[145] Chaeri Park, 'Knowledge Base: China's "Global Data Security Initiative" 全球数据安全倡议' (*DigiChina*) <https://digichina.stanford.edu/work/knowledge-base-chinas-global-data-security-initiative/> accessed 21 April 2024.
[146] Hunter Dorwart, 'China and Global Data Transfers: Implications for Future Rulemaking' <https://papers.ssrn.com/abstract=4526107> accessed21 April 2024.
[147] Park (n 145).
[148] Dorwart (n 146).
[149] Jones, E., Garrido Alves, D. B, Kira, B. and Sand, A. (2021) 'The UK and digital trade: which way forward?', Blavatnik School Working Paper 2021/038
[150] Felicity Deane and others, 'Trade in the Digital Age: Agreements to Mitigate Fragmentation' [2023] Asian Journal of International Law 1.
[151] Anna Sands and others, 'The UK and Digital Trade: Which Way Forward? | Blavatnik School of Government' (2021) <https://www.bsg.ox.ac.uk/research/publications/uk-and-digital-trade-which-way-forward> accessed 21 April 2024.
[152] https://www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm
[153] Dorwart (n 146).

5 Conclusions

As an important global player, China's digital economy has been continuously growing and expanding over the past 10 years. China is one of the most important trade actors in the world, holding significant partnerships with the EU, the US as well as the BRICS countries.

Recognising the importance of safeguarding personal information, China has steadily built its data governance framework on three main pillars: the DSL, the CSL and the PIPL. The PIPL, which was enacted in 2021, serves as China's first comprehensive data protection law. Although highly influenced by the EU GDPR, the PIPL also contains many distinct features. The PIPL applies to "all kinds of information recorded by electronic or other means *related to identified or identifiable natural persons*" including sensitive personal information and biometrics data, while excluding anonymised data. Notably, PIPL also extends its subject-matter extraterritorially.

The cross-border transfer of personal information is regulated by Chapter III of the PIPL. The Chinese model for regulating data transfers is quite unique. Although the EU's influence on the Chinese data transfer regime is manifest, e.g. in the design of the Chinese Standard Contract, many provisions are China specific. These include a bespoke hierarchy of transfer tools and stringent data transfer restrictions targeting "CIIOs" and "important data".

China's regulations on cross-border data transfer aim to strike a balance between ensuring the "safe flow" and the "free flow" of data. That said, the implementation details of the regulated cross-border data transfer tools have not been fully unpacked yet. The first version of the cross-border data transfer regime is currently being reworked, in particular to address the needs of multinational organisations and cross-border e-commerce. Although a comprehensive data protection law, i.e., the PIPL, has been in force for two years, detailed guidelines are still evolving rapidly: the recent draft regulations can be seen as a move to try to preserve China's economic growth. [154] It has thus been argued that the Chinese cross-border data transfer regime is still in its infancy and will continue to evolve.[155] The recent evolution shows many inconsistencies and uncertainties in the interpretation and enforcement of these rules. The industry is calling for clearer definitions of key terms and more specific guidelines to make cross-border transfer rules easier to apply in practice. At the same time, local public entities are tempted to adopt more flexible rules.

Importantly, China's approach to data governance has been driven by the concept of digital sovereignty, which appears to be wide encompassing. China has thus been building a regulatory framework for cross-border data transfers to protect not only the rights of Chinese citizens and entities, but also to strengthen its capabilities to protect its cyber resilience and its national security interests.[156] On the global stage, China has been actively championing its vision in the context of several international initiatives, in particular by waving the digital sovereignty flag.[157] This proactive stance reflects China's commitment to shaping and contributing to international discussions and cooperation in the evolving landscape of global data governance, challenging

[154] Chorzempa and Sacks (n 135).
[155] Zhao (赵精武) (n 118).
[156] Yuan Li, 'Cross-Border Data Transfer Regulation in China' (2021) Rivista Italiana di Informatica e Diritto <https://zenodo.org/records/5266546> accessed 21 April 2024.
[157] A detailed conceptualisation of digital sovereignty and its related tenets such as technology sovereignty, data sovereignty, national cyber resilience, national security, within the Chinese context, will be essential to inform discussions in international fora and build cooperation mechanisms for cross-border data flows.

competing jurisdictions to reassess their positions.[158] Nevertheless, translating China's domestic regulatory objectives into international standards remains a complicated task.[159]

Acknowledgement: This research has been funded by Cerre, Brussels, Belgium

[158] See for example the various proposals emerging in the US to redefine or refocus the US trade policy, e.g., S. Sacks and P. Swire, A framework for assessing US data policy toward China, June 2023 available at https://www.crossborderdataforum.org/a-framework-for-assessing-u-s-data-policy-toward-china/, accessed 21 April 2024.

[159] Dorwart (n 147).