Lee Kuan Yew School of Public Policy

Asia Competitiveness Institute

ACI Research Paper #01-2023

# Navigating Cross-Border Data Transfer Policies: The Case of China

Taojun XIE

Jingting LIU

Ulrike SENGSTSCHMID

Yixuan GE

April 2023

Please cite this article as:

XIE, Taojun, Jingting LIU, Ulrike SENGSTSCHMID and Yixuan GE, "Navigating Cross-Border Data Transfer Policies: The Case of China", Research Paper #01-2023, *Asia Competitiveness Institute Research Paper Series (April 2023)*

## Abstract

This paper examines the new Chinese regulatory framework on personal data protection, with a specific focus on cross-border data transfers. It aims to keep businesses and policymakers informed of the latest updates to China's cross-border data transfer regulatory framework, and serve as a reference to gauge the impact of China's regulations.

China has enforced three new laws and associated guidelines in the past few years, including the Cyber Security Law (CSL), the Data Security Law (DSL) and the Personal Information Protection Law (PIPL). While these laws have laid the cornerstone of data protection for Chinese users, they also display a cautious approach regarding cross-border data transfers to secure national security and other public interests.

After an examination of this legal framework and the various mechanisms firms can use to transfer data overseas, we compare the new regulations with the European Union's General Data Protection Regulation (GDPR) to find that although key definitions and the legal basis for data processing is quite similar, the cross-border data transfer requirements are more stringent in the Chinese case. This can be traced back to a difference in motivation: While the GDPR prioritizes individual rights to data protection, the Chinese laws are based on safeguarding key national interests, especially national security, with individual data rights and ease of business only being secondary concerns.

In our discussion of the implications for firms and the Chinese economy that builds on the previous comparison with the GDPR, we find that firms, and especially non-Chinese firms, will face increased operating costs. Subsequently, these foreign firms are likely to lose market share vis-à-vis domestic competitors. As larger domestic firms are likely to gain market share from smaller counterparts, these policies are likely to foster national IT champions.

On a global scale, China seems to exemplify the emerging trend of multiple data protection models hampering cross-border data flows. Until these differences can be bridged, for example through international agreements, an extended period of uncertainty in this domain is likely.

# Table of Contents

# I. Introduction

Technological change continues to sweep across our societies and businesses at an astonishing pace. What began in the early 2010s as the fourth industrial revolution in the manufacturing sector – connectivity, advanced analytics, and human-machine interaction – has today reached all of us. Data, a by-product of our daily consumption of digital services and connected products, has become a valuable economic input, even regarded by some as the 'new oil' driving economic growth. Today, the global digital economy is worth over 11.5 trillion USD, making up more than 15% of global GDP and growing at a rate that is 2.5 times faster than total global GDP (Henry-Nickie, Frimpong, and Sun 2019).

Firms' use of data to offer more innovative and customized products does not stop at national borders – rather it is enabled and driven by cross-border data flows. International technologies like cloud computing have become central to harnessing the potential of big data, allowing both businesses and customers to reap its benefits. Given the centrality of data to economic growth in today's digitalized and globalized world, governments across the world are trying to find data governance models that balance the need for international interconnectivity with national security concerns and individual privacy demands.

Unlike traditional cross-border trade, data can be re-traded multiple times, a copy of the data can be shared without the original dataset diminishing in value, and the physical storage location of the concerned data is both hard to determine and of little consequence for its use. Given this context that defies traditional understandings of trade, new governance frameworks are called for.

The European Union was one of the first to enforce a new framework for data protection in 2018 – the General Data Protection Regulation (GDPR). Many countries have since then followed suit. However, while key definitions and approaches are often borrowed from the EU's GDPR in other countries' national legislations, the EU's focus on individual data privacy rights is not always shared, with three regulation paradigms emerging: Next to the EU's 'conditional model' that emphasizes individual privacy rights while keeping data flows as free as possible for businesses, the 'open model', employed in countries like the US, Australia, and Singapore, gives primacy to economic and business needs and thus imposes only minimal data-related restrictions. The third model, known as the 'control model' and employed by countries like China, Russia, and Vietnam, stresses national security and other public interests and often enacts significant barriers to data processing and cross-border data flows to protect these interests.

The wide spectrum of policies presents new challenges for businesses operating globally. They are required to adapt to sometimes contradictory regulatory demands from different governments. Studies have found that compliance with data regulations increases the operating costs of firms due to their additional investments in technology, infrastructure, and personnel. Market concentration may also increase as smaller firms usually have thinner profit margins. Extensive data regulations may negatively affect innovation in data-based products and services as data sharing is restricted. When internationally operating businesses simultaneously face various such regulations, these effects are potentially multiplied, and compliance must be balanced with remaining profitable.

Given the wide-ranging impact of data regulations on businesses and the size of the Chinese digital economy, which has doubled since 2016 to reach a value of 6.61 trillion USD or 39.8% of the country's GDP (Chu 2023), this paper will focus on the recent developments in China – a country that is sparing no effort to capitalize on data for its continued development. However, to ensure that data collected and processed by private parties does not undermine its citizens or its national interests, China has enforced three new laws and associated guidelines in the past few years, including the Cyber Security

Law (CSL), the Data Security Law (DSL) and the Personal Information Protection Law (PIPL). While these laws have laid the cornerstone of data protection for Chinese users, they also display a cautious approach regarding cross-border data transfers to secure national security and other public interests.

This paper will examine this new regulatory framework with a specific focus on cross-border data transfers to understand the implications both for individual firms as well as for the global economy at large. After giving an overview of the key new laws and regulations in Section II, Section III will compare the new Chinese framework with the European GDPR to better understand its novelties. Finally, in section IV, the implications for firms and the Chinese economy will be discussed building on the previous comparison to the EU GDPR.

This paper aims to keep businesses and policymakers informed of the latest updates to China's cross-border data transfer regulatory framework, and serve as a reference to gauge the impact of China's regulations.

## II. Overview of China's Data Protection Legal Framework

As China has become aware of both the immense potential and risks stemming from unregulated data collection, data processing, and data flows in the last decade, it has implemented a range of new laws, policies, and guidelines to regulate and manage these issues. This new framework (Figure 1) is centred around three key laws implemented between 2017 and 2021: the Cybersecurity Law (CSL), the Data Security Law (DSL), and the Personal Information Protection Law (PIPL). However, exact guidelines on how compliance on the ground will look like continue to be published, and firms are just beginning to gain practical experience. Thus, the details of the regulatory framework keep evolving.

On 1 June 2017, China implemented the Cybersecurity Law, which addresses the requirement for localisation of data storage for critical information infrastructure operators (CIIOs). Four years later, China's State Council issued supplementary regulations to the CSL – Regulations on the Security and Protection of Critical Information Infrastructure – to shed new light on how the government plans to regulate strict data security requirements among critical information infrastructure operators.

On 1 September 2021, the Data Security Law came into force. This law imposes an even stricter regime governing cross-border data transfer and stipulates rules for managing nationally important data to accommodate the fast-growing digital economy. Besides critical information infrastructure operators, export measures on "important data" collected and generated by any other data processor will also be determined by China's cyberspace administration and other relevant government bodies. Fines and even the revocation of business licenses may be imposed for violating the rules on providing important data abroad. To facilitate the identification of important data held by data processors and to support the security regulation of important data, China published the Information Security Technology Guideline for Identification of Important Data in January 2022, followed a year later by Measures for Data Security Management in the Field of Industry and Information Technology, which classifies industrial, telecommunication, and radio data into general, important, and core data based on the degree of damage in the case of data breach, and outlines the rules regulating data export based on their classifications.

On 1 November 2021, China implemented the Personal Information Protection Law, expected to profoundly impact domestic and foreign companies doing business in China. Extending data localisation requirements to firms processing data above certain volume thresholds, the PIPL is the most sweeping among the three laws regulating cross-border data transfer. The PIPL stipulates conditions for cross-border data transfer and processing and the need for localized storage when the data exceeds the threshold. Furthermore, in 2022, a series of guidelines and measures came into force to assist different stakeholders in the legal transfer and processing of data across borders, including Measures for Data Export Security Assessment, Guidelines for Data Export Security Assessment and Declaration, Cybersecurity Standards Practical Guide – Security Certification Specifications for Cross-Border Processing of Personal Information V2.0 and Standard Contract Provisions on the Export of Personal Information. Published on 22 February 2023, the finalised version of the "Standard Contract Provisions on the Export of Personal Information", together with the Standard Contract (SC) itself, outlines the obligations of both the data processor in China and the overseas receiver, users' rights, contract termination, liability for breach of contract, and dispute resolution. Furthermore, it also provides the contract template that needs to be signed by both the sender and receiver before cross-border data transfer can take place for the eligible firms.

Just recently, during the Two Sessions concluded on 13 March 2023, it was announced that China would establish a new data governance agency — the National Data Administration (NDA). The NDA will take charge of the duties related to promoting data collection, sharing, and trading within the country. These responsibilities previous fell under the Cyberspace Administration of China (CAC), which was the top regulator of the technology industry and data usage, and the National Development and Reform Commission (NDRC), the key national economic planning organization.

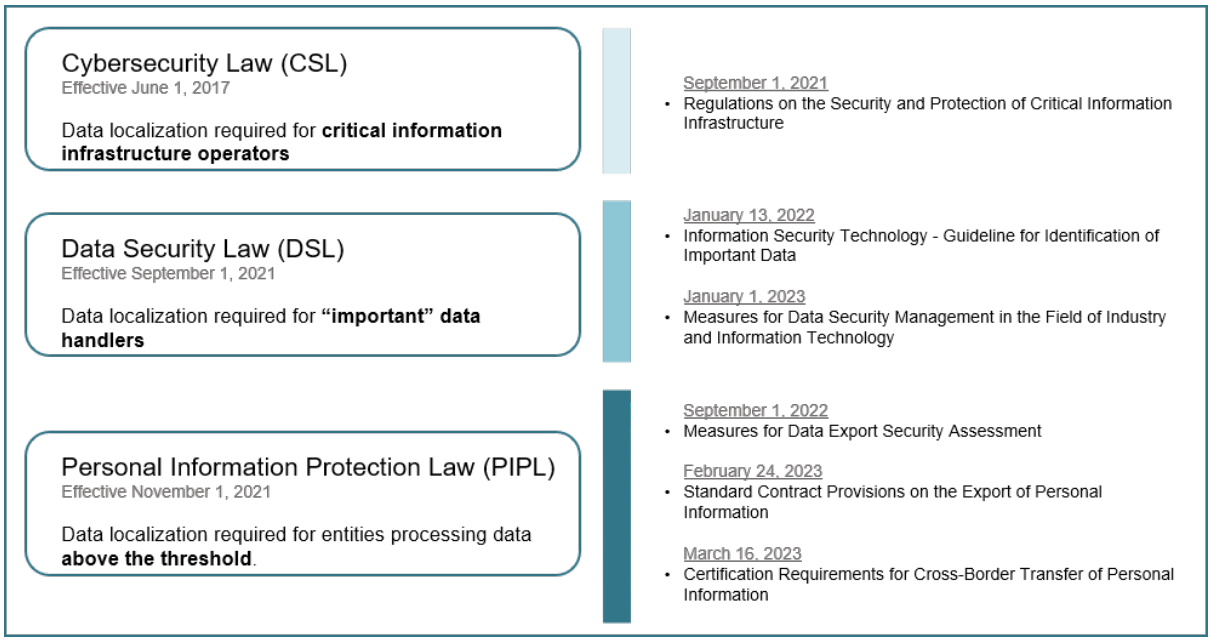


*Figure 1: Overview of cross-border data transfer and processing laws and regulations in China*

## II.a. Mechanisms for transferring data out of China

As China's digital economy is booming, the regulatory system consisting of corresponding laws and regulations is being refined. In this section, we will explain in detail the complying requirements for different stakeholders involved in the full procedure of data exporting.

### Before cross-border data transfer and processing

According to the PIPL, cross-border data transfer and processing will be permitted if one of the four conditions listed in Figure 2 below are met by data handlers.


*Figure 2: Conditions for cross-border data transfer and processing proposed in PIPL*

First, a company can pass a security assessment by Cyberspace Administration of China (CAC) to export data. This is mandatory for:

1) firms processing "important" data
2) operators of critical information infrastructure
3) data processors who handle personal information of more than 1 million persons
4) entities who have provided personal information of 100,000 persons / sensitive personal information of 10,000 persons in aggregate since 1 January of the previous year; or
5) other situations requiring declaration of data export security assessment by the state internet information department.

Before implementing the security assessment, a firm needs to conduct a data export risk self-assessment, covering the following five parts:

1) the purpose, scope and manner of data export
2) the scale, scope, sensitivity and risk of exported data
3) the channels for safeguarding the rights and interests of personal information in the event of data damage and leakage during and after export
4) the legality, legitimacy and necessity of data processing by the overseas recipient
5) whether the recipient of the data export-related contract has fully agreed to the data security protection responsibilities and obligations.

Second, entities involved in cross-border processing of personal information may also seek a personal information protection certification to conduct personal data export. The framework of the certification process includes the technical inspection, on-site review, and post-certification supervision. Regarding the certifying agency, China Cybersecurity Review Technology and Certification Center (CCRC) has been appointed to handle this. Detailed requirements can be found on the official website of CCRC.[1]

Third, companies that do not trigger the requirements for conducting a mandatory security assessment by CAC can sign a standard contract with the overseas recipient and conduct a Personal Information Protection Impact Assessment (PIPIA). Detailed PIPIA requirements and contract templates are included in Standard Contract Provisions on the Export of Personal Information. Once the standard contract is in effect, the personal information processor must submit the standard contract and PIPIA report to the State Cyberspace Administration within ten working days from the standard contract's effective data for record purposes.

Last, a company that satisfies other requirements prescribed by laws, regulations, or the CAC can also transfer data out of China. However, this method needs to be supplemented by subsequent legislation and regulations.

[1] See https://www.isccc.gov.cn/zxyw/sjaq/grxxbhrz/ssgz/index.shtml for the implementation rule and https://www.isccc.gov.cn/zxyw/sjaq/grxxbhrz/sqsxz/index.shtml for the certification application form released by the China Cybersecurity Review Technology and Certification Center (CCRC).

*Box 1: Procedure of obtaining security assessment*

The assessment process can be lengthy and take months to complete. After implementing the security assessment, companies need to submit declaration materials to provincial Cybersecurity Administration for completeness check. These materials include a declaration file, the data export risk self-assessment report, and the legal documents developed by the data processor and the overseas recipient. If they pass the check, the materials will be forwarded to the CAC; otherwise, companies will receive the materials and a one-time notification for additional materials.

Next, CAC shall determine whether to accept, and notify the data processor in writing within seven working days. Then, CAC will organize relevant departments of the State Council, provincial Cybersecurity Administration, and specialized agencies to conduct security assessments. If it is found that the declaration does not meet the requirements, the data processor may be asked for supplementing material or corrections. The CAC can terminate the assessment for data processors that do not comply with these requests without legitimate reasons. If the data handler submits false materials, they will fail the assessment and can be investigated. The assessment shall be completed by CAC within forty-five working days. In the case of complicated circumstances or the need for additional or corrected materials, the data handler can be informed and the assessment will be appropriately extended.

Last, the assessment results will be sent in writing to the data processor. Data processors who disagree with the assessment results can apply for re-evaluation to CAC within fifteen working days. The re-evaluation results will be final. The assessment result is valid for two years.

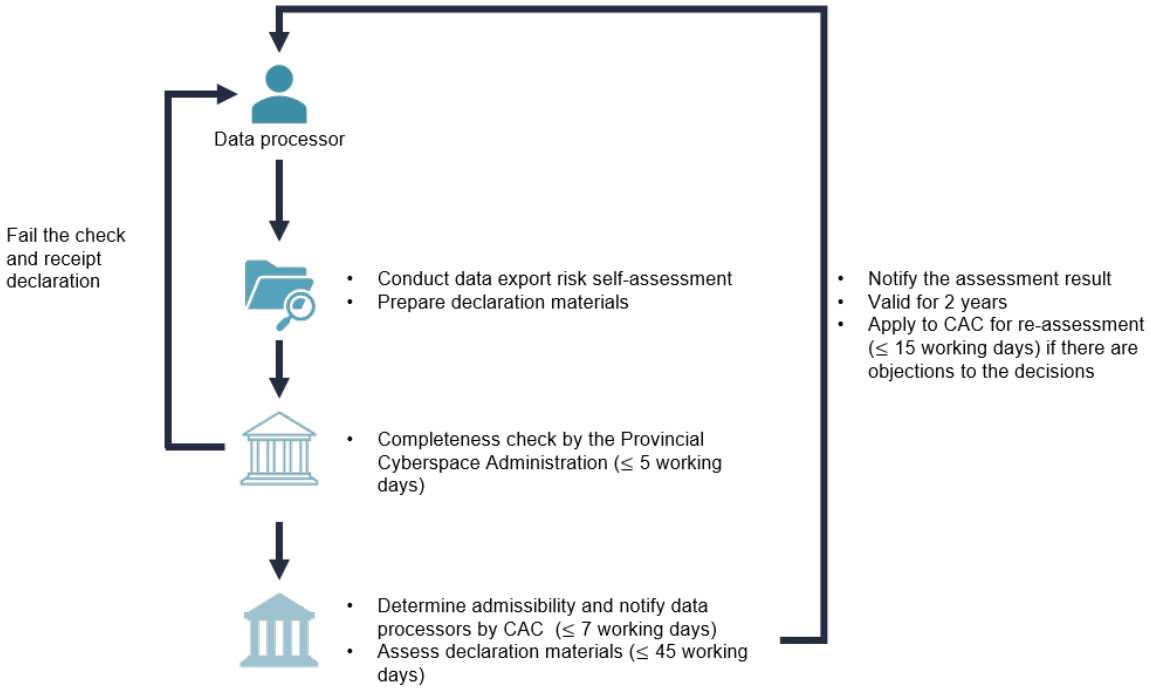


*Figure 3: Detailed procedure for security assessment by Cyberspace Administration of China*

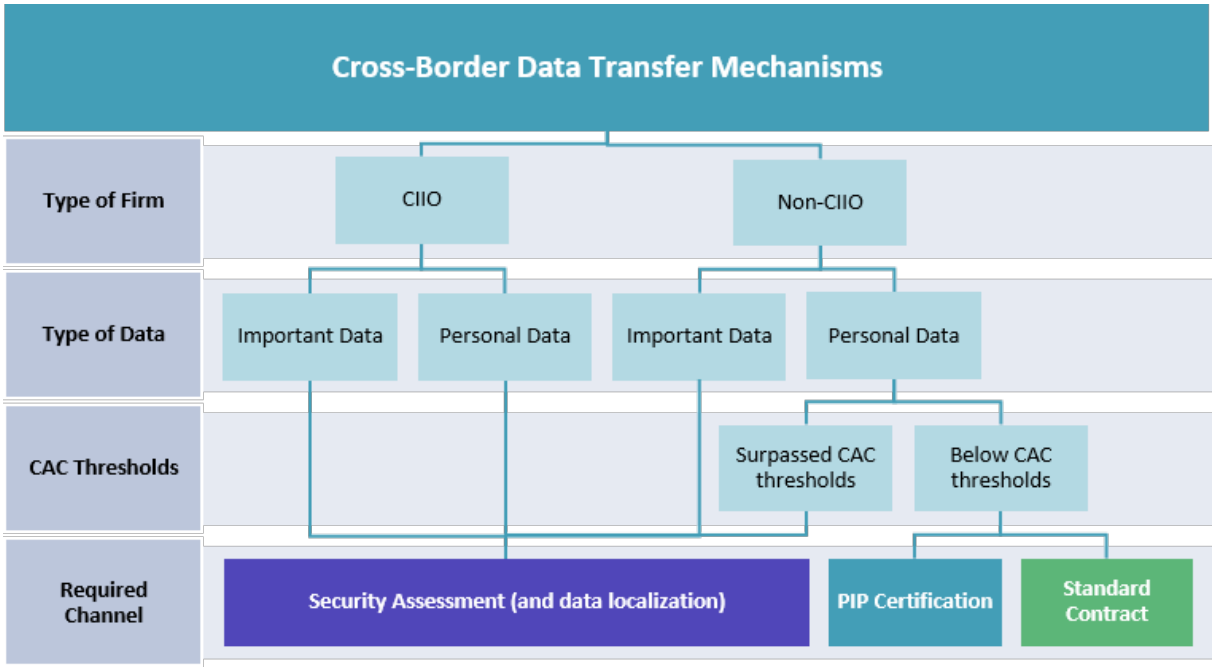


*Figure 4: Suitable cross-border transfer mechanisms based on firm and data type*

### During cross-border data transfer and processing

Besides specifying conditions under which cross-border data transfer and processing is allowed, the PIPL stipulates the obligations for stakeholders involved during and after data processing activities as well.

During the data export, data protection is a crucial duty for all entities involved. Companies must designate a person in charge of personal information protection. The data protector should clarify the main objectives, basic requirements, work tasks, and protection measures of personal information protection. Additionally, they must ensure sufficient human, financial, and material resources are available for the organization's personal information protection. Furthermore, the data protector should guide and support relevant personnel to carry out the personal information protection of the organization. Finally, they compile reports and continuously aim to improve the organization's data protection standards.

In addition to the above requirement, companies need to set up a personal information protection agency. This agency is required to prevent unauthorized access to personal information and leaks, tampering, and data loss. Moreover, it oversees developing and implementing an activity plan for cross-border processing by all involved entities, conducting the PIPIA, supervising the processing of cross-border personal information, and receiving and processing requests and complaints from personal information subjects.

### After cross-border data transfer and processing

Out of the two-year validity period of the security assessment result, if the company still needs to engage in data export operations, it will need to re-declare the assessment sixty working days before the expiration of the validity period.

It is noted that data processors should re-declare the assessment if one of the following circumstances occurs during the validity period: (1) The purpose, manner, scope, and type of data are changed, which will affect data security; (2) Changes in the actual controller or overseas recipient or the legal documents signed by both entities; Or (3) the occurrence of force majeure factors that would affect data security.

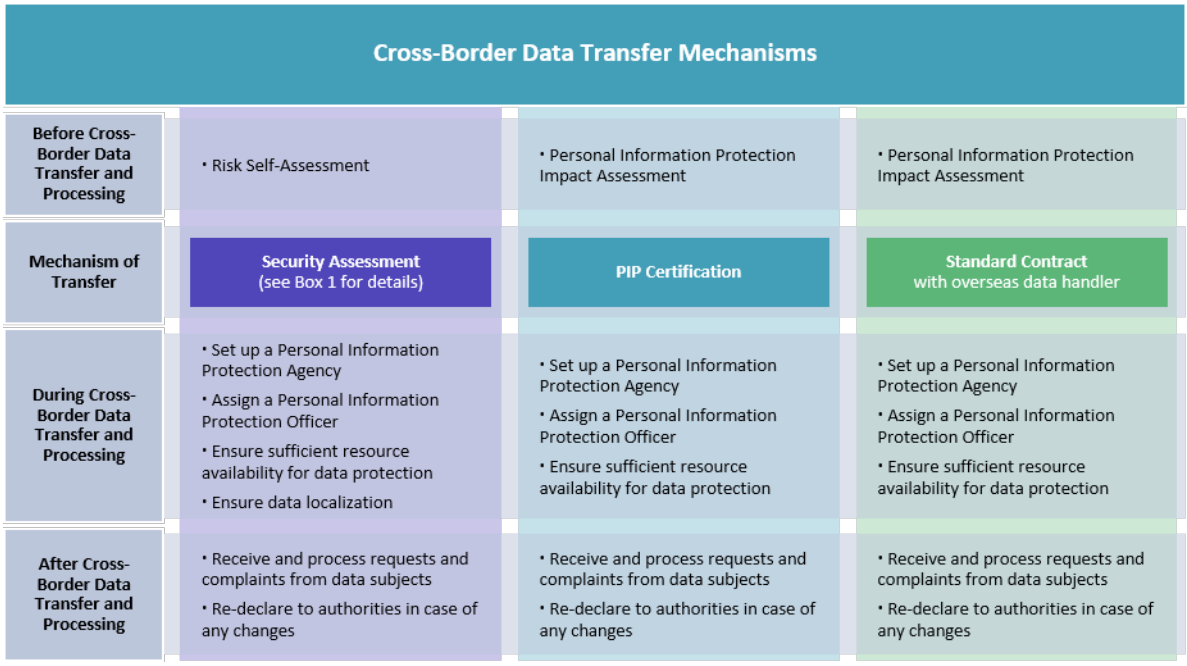


*Figure 5: Detailed procedures for different cross-border data transfer mechanisms*

## Users' rights

Besides the data processors and government authorities, the users who provide personal information are also essential to the data export process. The laws and regulations stipulate that the users can obtain a copy of the relevant legal materials concerning his or her rights and interests. They are allowed to refuse decisions exclusively made by means of automated decision-making until their information has been processed. They also have the right to be informed and to decide whether to consent to, restrict, or refuse processing. In addition, they can request the overseas recipient to access, copy, amend, supplement and delete their personal data when the data is transferred overseas. When users' rights are violated, they can complain to the Chinese regulatory authorities or take judicial action in court.

*Box 2: Key definitions*

### Important data

Before exporting data, companies need to determine whether their data falls under the "important" data category to choose the appropriate data export method. The following provides a list of 14 conditions when data will be classified as important data:

- Data reflecting the national strategic reserve and emergency mobilization capacity.
- Data supporting the operation of critical infrastructure or industrial production in key areas.
- Data reflecting the network security protection of critical information infrastructure, which can be used to implement cyber-attacks on critical information infrastructure.
- Data related to export-controlled items.
- Information that may be used by other countries or organisations to launch military strikes against China.
- Data reflecting the physical security protection of key targets and important sites or the location of undisclosed geographical targets that may be used by terrorists or criminals to carry out damage.
- Data that could be exploited to execute disruptions to the supply chain of critical equipment, system components to launch cyber-attacks such as advanced persistent threats.
- Data reflecting the health and physiological conditions of groups, ethnic characteristics, genetic information, and so on.
- Data on national natural resources and the environment.
- Data relating to scientific and technological strength and affecting international competitiveness.
- Data relating to the production and transaction of sensitive items as well as the equipping and use of important equipment, which may be subject to sanctions imposed on me by foreign governments.
- Information generated while providing services to government agencies, military enterprises, and other sensitive and important institutions unsuitable for public disclosure.
- Non-public government data, work secrets, intelligence data and law enforcement and judicial data.
- Other data that may affect national political, territorial, military, economic, cultural, social, scientific, technological, ecological, resource, nuclear facilities, overseas interests, biological, space, polar, deep sea, and other security.

### Critical information infrastructure operators

Critical information infrastructure operators (CIIOs) are subject to data localisation requirements as stipulated in the CSL. CIIOs include companies engaged in crucial industries, which may seriously harm national security, the economy and people's livelihoods, or public interests in the event of incapacitation, damage, or data leaks. For example, public communication and information services, energy, transport, water, finance, public services, e-government services, and national defence.

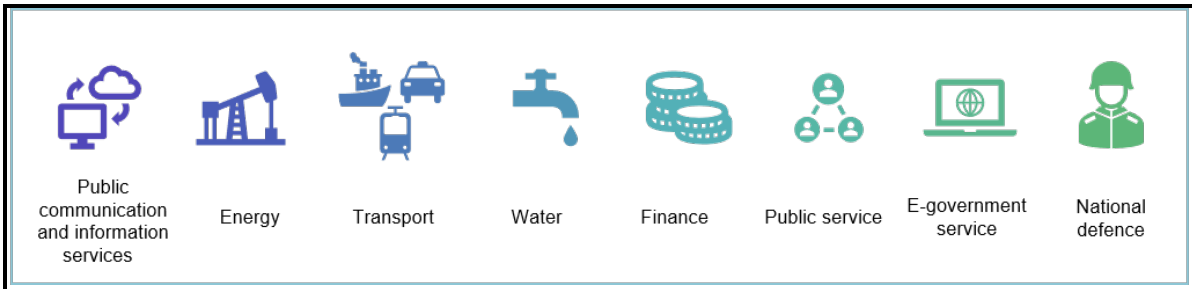


*Figure 6: Examples of critical information infrastructure operators according to Regulations on the Security and Protection of Critical Information Infrastructure*

## Sensitive personal information

Cross-border transfer of sensitive personal information are bound by stricter regulations. According to the PIPL, sensitive personal information refers to the personal information that can easily lead to the infringement of the personal dignity of natural persons or the harm of personal or property safety once leaked or illegally used. This includes biometric information (including fingerprints, facial recognition information, DNA, etc.), religious beliefs and specific identities, medical history, financial accounts, location and whereabouts, and any personal information of minors under the age of 14.

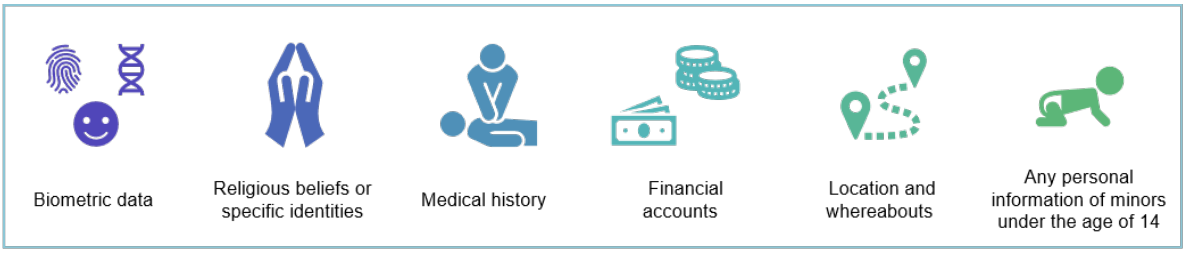


*Figure 7: Examples of sensitive personal information according to the PIPL*

# III. Comparing the PIPL and GDPR

To shed light on the potential implications of China's PIPL both domestically and internationally, a comparison with the European Union's General Data Protection Regulation (GDPR) – one of the first, and most studied, comprehensive data protection regimes – is useful. The GDPR came into force in 2018 and had immediate global impacts due to its extraterritorial nature – meaning that it regulated firms' personal data processing activities no matter where in the world these firms are based, as long as they are handling data of European Union citizens. Thus, multinational firms across the world had to change their practices to comply with the GDPR – and they often did so for their whole operations, not just those in Europe. As a result, from the firm and government levels, the GDPR came to be seen as the "gold standard" in data protection, and many privacy regulations since have been modelled on it, including China's PIPL.

## III.a. Similarities

In many aspects, China's PIPL closely resembles the EU's GDPR, including in its definitions of personal information and data processing as well as its consent requirements. These similarities are advantageous to multinational firms as they often already, at least partially, comply with Chinese regulations if they follow EU standards. Therefore, their compliance costs are lowered, and interoperability is increased.

Both definitions of 'personal information' in the PIPL and 'personal data' in the GDPR refer to information relating to an "identified or identifiable natural person" (Art. 4, PIPL; Art.4, GDPR). Unlike the GDPR, the PIPL excludes "information processed anonymously" from the scope of the regulation. In both regulations, 'data processing' refers to "any operation or set of operations which is performed on personal data or on sets of personal data" (Art. 4, GDPR), including but not limited to the "collection, storage, use, processing, transmission, provision, publication, and erasure of personal information" (Art. 4, PIPL). Importantly, the GDPR distinguishes between 'data controllers', who determine the purpose and means of data processing, and 'data processors', who actually process the data on behalf of the controller. The PIPL treats both equally and refers to both as 'data processors'.

In addition to these similar basic definitions, the legal basis for data processing in both jurisdictions is consent from the data subject. This means that, in general, the individual must be informed how their data will be processed and for what purposes, and their consent must be obtained to process their data. There are several exceptions in the GDPR and PIPL when personal data can be processed without the individual's consent. These include data processing for the "performance of a contract to which the data subject is party" (Art. 6, GDPR), for the protection of vital interests, including the protection of life and health, and for tasks that are in the public interest such as news reporting. The PIPL makes another exception for "other circumstances provided by laws and administrative regulations" (Art. 13), leaving the authorities leeway to adjust consent requirements in the future. This is impossible in the GDPR – here, the GDPR itself must be changed as no exceptions are made for other laws.

An additional key difference between the GDPR and PIPL is that the GDPR makes an exception from consent for data processing under so-called 'legitimate interest'. If firms pursue legitimate and expected interests in processing data, they do not need the individual's explicit consent, even when data is transferred abroad or to third parties. For example, when ordering online, the webshop can process the customer's postal and email address to send the product and send updates on the shipping, even without explicit consent, as the customer is expecting the order to be delivered to the address they provide. However, saving that data for prolonged periods or using the address to send promotional materials would be outside the scope of legitimate interest. Under the PIPL, even such data processing that can be expected and is in the interests of the data subject needs explicit consent.

*Table 1: Key similarities between the PIPL and GDPR (differences underlined)*

| | Personal Information Protection Law (PIPL) of China | General Data Protection Regulation (GDPR) of the European Union |
|---|---|---|
| **Definitions** | "**Personal information** refers to various kinds of information related to identified or identifiable natural persons recorded by electronic or other means, excluding the information processed anonymously." (Article 4) | "**'personal data'** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" (Article 4) |
| | "**Processing of personal information** includes the collection, storage, use, processing, transmission, provision, publication, and erasure of personal information." (Article 4) | "**'processing'** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction" (Article 4) |
| **Legal Basis for Data Processing** | (a) Consent of the data subject;<br>(b) Necessary for the conclusion or performance of a contract to which the data subject is party;<br>(c) Necessary for compliance with a legal obligation;<br>(d) Necessary for coping with public health emergencies or for the protection of the life, health, and property safety of a natural person;<br>(e) For news reporting and supervision by public opinions carried out for the public interest;<br>(f) Where the processing is within a reasonable scope in accordance with the provisions of this Law;<br>(g) Other circumstances provided by laws and administrative regulations. | (a) Consent of the data subject;<br>(b) Necessary for the conclusion or performance of a contract to which the data subject is party;<br>(c) Necessary for compliance with a legal obligation;<br>(d) Necessary to protect the vital interests of the data subject or of another natural person;<br>(e) Necessary for a task carried out in the public interest;<br>(f) Necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject. This does not apply to public authorities. |

## III.b. Differences

However, despite these surface-level similarities, major differences exist between the EU's and China's data privacy frameworks, which can be traced back to the fundamental values and interests underlying these regulations. While EU legislators view data protection as a fundamental right that must be protected yet also balanced with maintaining cross-border data flows that are as free as possible, Chinese authorities highly stress the role of cybersecurity in overall national security and, as such, take a much more restrictive stance towards international data transfers.

### Differences in Motivation

The European Union is one of the few jurisdictions that has enshrined not just privacy but personal data protection in its Charter of Fundamental Rights (Art. 8). This makes individual data protection the main goal of the GDPR. However, the secondary aim remains to be as business friendly as possible. This is shown by aims to reduce the administrative compliance burden as much as possible for firms, for example, through using the so-called 'adequacy decision' to automatically approve many cross-

border data transfers or by setting up the 'one-stop-shop' mechanism, meaning that firms present in multiple EU countries can handle all GDPR-related matters through the data protection authority in one country which shifts the burden of communication and cooperation onto European legal authorities rather than firms.

In contrast, there is little doubt that China's data flow policies stem from national security concerns, as reflected in much more stringent data export requirements as well as data localization measures. Already in 2014, President Xi emphasized that "there is no national security without cybersecurity" (Xinhua 2014). Since then, the recognition of data's value and cyberattacks have only increased. Thus, China's new data protection framework aims at carefully balancing China's economic growth on the one hand, with its national security interests on the other.

Besides motivation, the biggest difference between the GDPR and the PIPL lies in their respective data transfer mechanisms. Cross-border data transfers – or the export of data from within the EU or China to a data handler outside the regulation's territory – are key components of today's globalized data economy, with multinational firms transferring their customer's data between different offices to provide various services, or firms sending collected data to a third party abroad for processing or storing. However, as governments have little control and enforcement power over how data is handled abroad, many impose controls on cross-border data transfers to ensure the privacy and protection of their citizens' data.

Generally, both the PIPL and the GDPR allow data exports for many types of data if certain conditions are fulfilled and specific channels are used. Nevertheless, as will be seen in the comparison below, although China modelled some of its cross-border data mechanisms on the GDPR, the PIPL usually imposes more and stricter export restrictions.

### III.c. Comparing Cross-Border Data Transfer Mechanisms

The GDPR allows for data transfers outside the European Union under four conditions: if (1) the recipient country has adequate levels of data protection; (2) standard contractual clauses are signed between the exporter and the recipient; (3) multinational corporations enforce binding corporate rules; (4) firms sign an approved code of conduct from their industry association; or (5) explicit consent given by the data subject or other exceptions. The PIPL, on the other hand, specifies three conditions for cross-border data transfer: (1) the firm has passed a security assessment from China's Cyberspace Authority; (2) standard contractual clauses are signed between the exporter and the recipient; or (3) the Chinese branch of multinational corporations undergoes a certification process from the relevant authority. See Table 2 for a summary of the respective mechanisms.

Not only does the PIPL not accept codes of conduct for data exports, but it also does not allow cross-border data transfers based on explicit consent from the data subject, public interest, contracts, or legal claims. Under the GDPR, if data transfers occur under either an adequacy decision or appropriate safeguards, consent from the data subject for data export is not required. If these mechanisms are not in place, transfers can still occur as long as the data subject gives explicit consent after being informed of the possible risks. Under the PIPL, consent plays a different role: Here consent is a necessary but insufficient aspect of data transfers. This means that while consent alone does not make data transfers possible, consent is required even if one of the stipulated mechanisms is used.

In addition, the PIPL also includes stringent criteria for which firms must undergo a security assessment, while under the GDPR firms can choose freely which mechanism to use for data transfers. The PIPL's criteria for requiring a security assessment are: the firm is either a critical infrastructure

operator, it exports important data, or it processes the personal information of more than 1 million persons, or it has exported the personal information of more than 100,000 persons or the sensitive personal information of more than 10,000 persons since January 1 of the previous year.

### PIPL's Security Assessment and GDPR's Adequacy Decision

The European Union allows data exports to any country that has an "adequate level of protection" (Art. 45, GDPR), meaning that it has a comparable level of data protection to that provided under the GDPR. The EU Commission assesses countries as a whole to determine their adequacy and has so far deemed 14 countries[2] beyond the European Economic Area as adequate, meaning that personal data from EU citizens can be transferred and processed there without further hurdles.

The PIPL does not allow for such adequacy decisions. Instead, it requires most large firms[3] to undergo a security assessment with the Cyberspace Authority of China. Unlike the adequacy decision, the security assessment is conducted on a case-by-case basis for firms that would like to transfer data abroad and must be renewed every two years. As such, the security assessments are likely to be a high administrative burden for firms while also increasing uncertainties as authorities have more leeway in their decision-making.

Additionally, as firms processing sensitive data have a much lower threshold for requiring a security review, it must be noted that the definition of 'sensitive data' is not as clear in the PIPL as in the GDPR. The GDPR gives an exhaustive list of what is comprised under its 'special category data', and while such data can only be processed in certain situations, such as when consent is given or it is in the public or vital interests and not under the legitimate interest clause, this data is not subject to any different cross-border data transfer requirements from standard data. The PIPL's definition of 'sensitive data' includes but does not limit itself to "biometrics, religious belief, specific identities, medical health, financial accounts, and whereabouts, and the personal information of minors under the age of 14". This non-exhaustive definition raises uncertainties for firms, as it may be unclear who is included.

Furthermore, firms handling 'important data' must also undergo security assessments. According to the 2021 clarification of the DSL by the Ministry of Industry and Information Technology, important data "includes (but is not limited to) any data that poses a threat to core national interests […], as well as data whose security could affect China's national security in key fields". It is likely to still be some time until a clearer catalogue of what is important data is released. For instance, on 24th February 2023, the Shanghai Municipal Communications Adminsitration Bureau has determined the first set of important and core data categories in alignment with 10 key communications and internent firms[4]. These preliminary catalogues will now be passed on to the Ministry of Information and Information Technology for approval. Again, the current impreciseness of the definition creates some uncertainty while leaving decision leeway to the authorities. In contrast, in Europe, the type of data does not have an impact on which transfer mechanism to use.

[2] The 14 countries with 'adequate' protection currently are Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom, and Uruguay.

[3] Security assessments are required for firms that are either critical infrastructure operators, that export important data, or that process the personal information of more than 1 million persons, or that have exported the personal information of more than 100,000 persons or the sensitive personal information of more than 10,000 persons since January 1 of the previous year.

[4] The 10 consulted firms are: Shanghai Telecom, Shanghai Mobile, Shanghai Unicom, Oriental Cable, Pinduoduo, Ctrip, Bilibili, Dewu, Xiaohongshu and Himalaya.

### *Data Localization*

In addition to more stringent cross-border transfer regulations, the PIPL also calls for data localization in certain cases. The GDPR, on the other hand, has no provisions for data localization. Under the PIPL, any data collected by critical infrastructure operators or firms that pass the thresholds for security assessments must store the data locally. Even if they pass the subsequent security assessment and have permission to process data abroad, a copy of the data concerning Chinese citizens must always be stored on Chinese territory. Consequently, many firms will be required to set up new data centres in China to comply with data localization rules.

## Standard Contractual Clauses

If a firm wants to export Chinese residents' data but is not large enough to require a security assessment, it can sign a 'standard contract' with the data processing firm abroad. Similarly, a firm that would like to export data to a country that is not deemed adequate by the EU can also sign 'standard contractual clauses' (SCC) with the foreign processor. Firms cannot make any substantial adaptations to the template contracts provided by European and Chinese authorities, which, although it decreases the flexibility of these contracts, means that they do not have to be individually reviewed by the authorities. The SCCs of the two jurisdictions are rather similar: Prior to exporting data, firms must conduct a 'personal information impact assessment' (self-assessment), focusing on the legitimacy, necessity, scope, risk, and responsibilities of data export. The standard contracts themselves are very similar between China and Europe, with the main distinction being that China does not distinguish between controller-to-controller and controller-to-processor contracts but instead uses the same contract for both. This may increase the requirements for foreign data controllers as they are subject to the same audit requirements as foreign processors. Europe's modular contract structure provides some flexibility here.

## Certification and Binding Corporate Rules

Another option for multinational firms to transfer data from China or the EU to their subsidiaries or affiliates in third countries is to use the PIPL's certification mechanism or the GDPR's binding corporate rules (BCR), respectively. The GDPR's BCR refer to legally binding company-internal rules that regulate the internal cross-border data transfer of multinational group companies. The group companies can adapt a provided template according to their own needs, offering high degrees of flexibility. The relevant supervisory authority must then approve the BCR. Once the BCR is approved and implemented, it applies to the whole group, meaning that there is no need for individual contracts for each data transfer process. Minor non-substantial changes to the BCR must be communicated to the local data protection authority, but no new approval needs to be sought. Compared to the SCCs, the BCR offer significantly more flexibility for a firm as well as covering all its data processing activities in one contract. However, as approval from the local data processing authority can be required, the process can be quite lengthy.

Similarly, the PIPL's certification mechanism also manages cross-border data transfers within multinational firms. Like the SCCs, however, it only applies to firms exempt from the security assessment. Here, the domestic affiliate must undergo certification from a specialized authority and then assume legal responsibility for its affiliate's data handling abroad. Like the GDPR's BCRs, all affiliates of the multinational group involved in data handling must sign legally binding documents and mutual agreements specifying the details of the data handling, including its amount and scope, purpose and method, and technical measures to ensure the security of the transferred data. These documents and procedures must also be approved by local certification agencies – however, the details of who can carry out certification or exactly how the certification process works have not yet been released by the Chinese government.

It is important to not confuse this certification mechanism under the PIPL with the GDPR's voluntary certification scheme. While the former refers to a channel to legally export data, the latter is a voluntary programme that guides companies through the process of becoming compliant with the GDPR and, upon successful completion, confers a seal to build trust and gain reputation and market valuation. While firms can undergo voluntary certification from specialized authorities under the PIPL, the voluntary certification scheme under the GDPR is only approved by the authorities, but run by private partners. For example, the Europrivacy seal – the first and, so far, only certification approved by the European data processing board, a body bringing together the national data protection authorities – was developed under Europe's Horizon 2020 research programme and is maintained and regularly updated by the European Centre for Certification and Privacy. The certification process itself is then carried out by one of six qualified certification bodies[5] and involves comprehensive online resources, guidance from qualified staff, a community website and various other online tools.

### GDPR's Code of Conduct

The GDPR offers firms an additional mechanism for gaining permission to transfer data abroad: The Code of Conduct (CoC). This mechanism is absent under the PIPL. A CoC on data processing can be set up by an industry association. Once it has been approved by the local data protection authority, firms within that association can sign on to it and implement it to transfer data abroad as stipulated in the CoC. This has the advantage that significant flexibility and adaptability exist at the industry level, making the CoC somewhat more personalized for firms than SCCs, while at the same time only requiring one approval process, instead of each firm individually writing their BCRs – this can therefore be especially useful for medium-sized firms.

*Table 2: Comparing Cross-Border Data Transfer Mechanisms under the PIPL and GDPR*

| | **Personal Information Protection Law (PIPL) of China** | **General Data Protection Regulation (GDPR) of the European Union** |
|---|---|---|
| **Channels for Cross-Border Data Transfers** | **Security Assessment by the Cyberspace Authority of China (CAC):** Firms wanting to export data must apply to the CAC and the CAC will examine and approve firms on a case-by-case basis. | **Adequacy Decision by the European Commission (EC):** The EC evaluates relevant legislation in third countries. If they offer similar levels of data protection as the EU, data can be transferred there freely. |
| | **Standard Contract:** After undergoing a Personal Information Protection Impact Self-Assessment, firms must sign a standard contract with the overseas data handler and file it with the local provincial-level cybersecurity office. As the standard contract is the same as the template provided by authorities – with only the details of the data processing operation being adapted – it does not require an audit from a supervisory authority. | **Standard Contractual Clauses:** After undergoing a Transfer Impact Self-Assessment, firms must sign a standard contract with the overseas data handler and file it with the local data protection authority. The GDPR's standard contract is provided in modular form, creating some flexibility depending on the relationship between the parties. Once signed, the contract does not require supervisory review. |
| | **Certification by Specialized Agency:** The Chinese affiliate of a multinational corporation can apply for certification when evidencing a set of internal rules and procedures. This allows data transfers among all affiliates, but the Chinese affiliate remains legally responsible for data protection globally. | **Binding Corporate Rules:** A multinational corporation creates a set of internal rules that must guarantee at least as much data protection as the standard contractual clauses. These rules are approved by the local data protection authority and signed by all affiliates of the group, allowing data transfers between all affiliates no matter geographic location. |
| | | **Code of Conduct:** Industry associations can write a CoC and have it approved by the local authority. Association members that sign it can use it to transfer data abroad. |

[5] As of February 2023, the qualified certification bodies are: SGS, bsi., DNV, eurofins, TAM CERT, and certop. Additionally, numerous consulting and law firms have been qualified to support the process, although they cannot confer the final seal. These include among others: Mazars, EY, pwc, Deloitte, KPMG, Accenture, Osborne and Clarke.

| | | |
|---|---|---|
| **Choice of Channel for Cross-Border Data Transfers** | Security Assessment is mandatory for:<br>- Overseas transfers of "important" data.<br>- Critical Information Infrastructure Operators processing data overseas.<br>- Firms that process the personal information of more than 1 million people.<br>- Firms that have transferred the personal information of over 100,000 people or the "sensitive" personal information of over 10,000 people overseas since January 1 of the previous year.<br>- Other situations as required by the CAC.<br>Firms that do not require a security assessment can choose the channel through which to gain permission for data transfers. | Firms can freely choose the channel through which to gain permission for data transfers. |
| **Consent Requirements** | Even if the appropriate safeguards (above) are in place, separate consent is required from the data subject.<br><br>Exceptions to the above safeguards are only made if:<br>(a) Other laws, administrative regulations, or the state cyberspace administration are complied with.<br>(b) Provisions in international treaties and agreements that China has concluded or participated in are complied with. | If the third country is deemed adequate or appropriate safeguards (above) are in place, no separate consent is required from the data subject.<br><br>If the third country is not deemed adequate and appropriate safeguards are not in place, data can still be transferred if one of the following conditions is satisfied:<br>(a) Consent of the data subject;<br>(b) Necessary for the conclusion or performance of a contract to which the data subject is party;<br>(c) Necessary for important reasons of public interest<br>(d) Necessary for establishment, exercise, or defence of legal claims<br>(e) Necessary to protect the vital interests of the data subject or of another natural person;<br>(f) Transfer is made from a public register which is open to consultation by the general public or any person who can demonstrate legitimate interest. |
| **Data Localization** | All firms that pass the criteria to undergo a security assessment, must also store a copy of all data locally. | No data localization requirements. |

The fundamentally different motivational forces behind the EU's GDPR – the right to personal data protection – and the PIPL – national security interests – are reflected throughout these regulations and account for many of the differences we see, especially in the area of cross-border data transfer. The GDPR generally offers firms more flexibility and lower bureaucratic hurdles, while state control is limited by inflexible and exhaustive regulations that do not allow for case-by-case decisions. In contrast, the PIPL offers firms less flexibility and higher bureaucratic hurdles, with most multinationals likely to be required to undergo a security assessment, but this also gives authorities higher levels of control, as the PIPL often is not exhaustive and allows other regulations to make amendments as well as giving authorities significant leeway as they make case-by-case decisions for each firm, which aligns with the underlying national security interests.

# IV. Implications

Empirical evidence on the impact of data protection regulations remains sparse across all sectors of society. Even in the case of the EU's GDPR, only short-term effects are explored, as it only entered into force in 2018. However, these initial trends may be useful in gauging what the short to medium-term impacts of China's PIPL may be.

## IV.a. Increasing Operating Costs

First, any data protection regulation like the PIPL or the GDPR will negatively impact affected companies through its direct costs of compliance, as they require investments in technology, infrastructure, and personnel. It is estimated that a average European company spent close to 3 million USD on GDPR compliance (IAPP and EY 2018). These costs rise with firm size, with an average US Fortune 500 firm spending around 16 million USD on GDPR regulatory requirements (Prasad and Perez 2020). Similarly, Facebook hired 1000 additional staff globally – ranging from engineers to lawyers – to ensure compliance (Prasad and Perez 2020).

It can be expected that the PIPL will similarly raise the operating costs of firms. Although the use of similar definitions and consent requirements as the GDPR means companies already adjusted to the EU model will have to spend less to adapt to the PIPL, but the bureaucratic hurdles of security assessments or certification, as well as data localization are likely to require significant investments. In a study of firms in Japan – a country that has been deemed adequate by the EU – less than 5% have reported negative impacts due to the GDPR. However, nearly twice as many firms – over 8% – are being negatively affected by China's new data protection framework (Kang, Tomiura, and Ito 2020).

Theoretically, these costs will be faced by both domestic Chinese and foreign firms. However, as the costs of cross-border data transfer and data localization requirements are increasing significantly, firms that are already processing their data within China will be less affected, insulating many Chinese firms somewhat from the rise in operating costs.

By requiring new data handling processes and thereby raising the costs of multinationals, China's data transfer regulations act akin to elevated import tariffs. Traditional import tariffs are taxes charged by customs authorities as goods are brought into the country and thereby protect domestic products by raising the production costs and therefore the price of foreign goods in the local market. While the mechanism in the case of cross-border data flow restrictions is somewhat different the effects are similar: Firms operating abroad must spend more on bureaucratic hurdles like security assessments or certification procedures to continue their operations that include data processing abroad. As such offering data-based products and services in China becomes more costly for them, and impairs their price competitiveness vis-à-vis domestic firms (see, for example, the case of Yahoo below).

While the costly adjustments associated with these policies erect entry barriers and encourage market exits of international competitors and thereby create favourable conditions for Chinese firms in the short run, domestic firms looking to expand globally may also be affected negatively. Once Chinese firms want to expand overseas or tap into globalized business models that involve data processing overseas, they will face the same cost hurdles that foreign firms face. This unintended longer-term consequence could be an impediment to domestic Chinese firms' global competitiveness.

### Case Study 1: Yahoo

The US technology company Yahoo, had been operating on the Chinese mainland since 1999, offering a range of internet services, including news sites, blogs, a weather app, a music and an e-mail service. Although many of these programmes have been downsized in China starting in the early 2010s and it had shut its Beijing office in 2015, its multilingual news site, weather service, consumer technology blog and email service remained running. Coinciding with the coming into force of the PIPL on the 1st of November 2021, Yahoo shut these remaining services, citing "the increasingly challenging business and legal environment in China". Its email service remained running until the end of February 2022 to allow existing users to transition to alternative providers, but was then also shuttered.

## IV.b. Increasing Market Concentration

Second, a data protection framework is likely to increase market concentration, as larger firms generally face proportionately lower compliance costs. These effects were detected in the aftermath of the GDPR's implementation. Multiple studies investigate and explain these trends: The GDPR causes large firms to have a competitive advantage in the technology sector for multiple reasons. On the one hand, small vendors face disproportionately higher costs of compliance, as the compliance process is the same for companies of all sizes. On the other hand, the reliance on third-party domains and cookies on websites decreased by 12.8% since the GDPR came into force (Peukert et al. 2020). Such third-party cookie providers are often smaller companies, resulting in large providers like Google gaining market share. Additionally, some argue that large firms with multiple product offerings can get user permissions more easily as well as aggregate more user data across products (Prasad and Perez 2020). Consequently, despite the high compliance costs mentioned above, no significant negative impacts on either the profits or sales of the GDPR on large information technology companies have been found (Presidente and Frey 2022). Simultaneously, the profits of small IT firms have decreased by around 12% in the same timeframe, potentially indicating that the large firms could offset the increased compliance costs with gained market share. Another study points in a similar direction, suggesting an increase in market concentration in the technology sector of approximately 17% in the seven months post-GDPR implementation (Johnson and Shriver 2020).

Due to the similar design of the PIPL and the GDPR, which also does not distinguish between small and large firms in the compliance process, it is highly likely that the market concentration in the technology sector in China will also increase. However, in China this only applies to the general data protection, as the cross-border data transfer procedures are differentiated by firm size, unlike under the GDPR. This means, that among Chinese firms relying on data exports, market concentration is much less likely to be affected. Nevertheless, in China, differentiated effects are to be expected between domestic and foreign firms: As the strict cross-border transfer regulations and data localization requirements act like tariffs on service imports, the PIPL is likely to have a much more significant effect than the GDPR on increasing the market share of Chinese firms to the disadvantage of international firms. This combination of large domestic firms gaining market share both from small domestic firms and from international firms is likely to foster the growth of national IT champions within China.

## IV.c. Competitiveness and Innovation

Third, these data protection regulations also affect the competitiveness and innovativeness of impacted firms. For example, the PIPL and the GDPR limit the merging of different databases as well as prevent firms from collecting data when the exact purpose of use is not clear and using existing data for future purposes. Additionally, under the GDPR when Artificial Intelligence (AI) is used to make significant decisions about an individual, consumers must have the option to opt out or request a human review of the decision. These regulations not only require more resources, but also significantly limit innovation in data-based products and services. For example, in 2018, 35% of German firms report that the GDPR hampers their innovation activities (Blind, Niebel, and Rammer 2022). However, next to the negative effects on innovation of limited access to input data, privacy-related innovation such as encryption tools and other compliance management software increased following the introduction of the GDPR (Martin et al. 2019) – however, only 4.7% of German firms reported these effects (Blind, Niebel, and Rammer 2022).

Furthermore, studies have found that the GDPR has negatively impacted venture investments in the technology sector, with a decrease of 22.2% and 15.8% in the months following the GDPR implementation from US and EU investors, respectively (Jia, Jin, and Wagman 2020). Nevertheless, as the GDPR targets companies globally that are handling EU citizens' data and other countries are adopting similar standards, the competitive disadvantage of EU firms may not be disproportionately large.

In the case of competitiveness and innovation, there are some significant differences between the GDPR and the PIPL caused by the fundamentally different treatment of foreign and domestic firms under the PIPL. Foreign firms are likely to face decreases in competitiveness due to the required duplication of data centres, staffing, and key operative processes within China to comply with cross-border data transfer and data localization regulations. These impacts are likely to occur across a wide range of sectors, from tourism to financial services: Hotels, for example, use customer information stored in their membership databases to provide customised services at any of their branches, which require free data flows. Yet the sheer volume of data processed by large hotels will trigger data localization requirements. Another example is medical devices that enable remote monitoring of patients. These will also need to transmit health metrics to healthcare professionals for assessment. Health data, which may be categorised as "sensitive" data, are subject to stricter regulations. Firms conducting clinical trials for R&D purposes in China may also face barriers in transferring the clinical trial data to other countries (See Case Study 2 below). Thirdly. in the financial sector, wealth management organisations abroad conducting due diligence checks will necessitate the cross-border processing of "sensitive" customer personal information, including financial status, family background, and even health conditions, which requires security assessment once the processing volume reaches a threshold.

Additionally, it must be noted that data is distinct from other production factors like land or human capital due to its nonrivalry: one firm processing a dataset does not prevent other firms from analysing it. Therefore, welfare gains will rise as data are shared within and across firms for deriving business insights. By restricting data export, China is limiting foreign firms' access to key productive capital. At the same time, Chinese authorities are encouraging smooth data flows across firms within the country, which will boost the firms' productivity as they can leverage on more data to enhance product offerings. One example of this is the Shenzhen data exchange that is aimed at boosting domestic firms' productivity (see below).

In terms of innovation, however, it is likely that China will also see negative effects domestically. The producers will face much higher costs of expanding abroad, collaborating with foreign partners, or benefiting from cross-national datasets. Additionally, Chinese consumers will lose out on foreign firms not offering data-intensive products and services in China as the case of LinkedIn and a US medical device manufacturer below shows.

### Case Study 2: R&D Activities

Singapore hosts the R&D centres of many big companies. In a potential scenario, if one such R&D centre conducted clinical trials in China for consumer product testing, the clinical trial data might be categorised as sensitive personal information if it involves biometrics. Sensitive personal information is subject to stricter regulations. If the company's office in China has exported sensitive information of more than 10,000 people since January 1 of the previous year to the R&D centre in Singapore, the Chinese affiliate will have to store the data in China and must undergo a security assessment before the clinical trial data can be exported out of China. Since going through security assessment with China's Cyberspace Administration can be time-consuming, the R&D centre in Singapore may therefore dispatch researchers to China to analyse the clinical trial data and only bring the analysed data out of China in the interim.

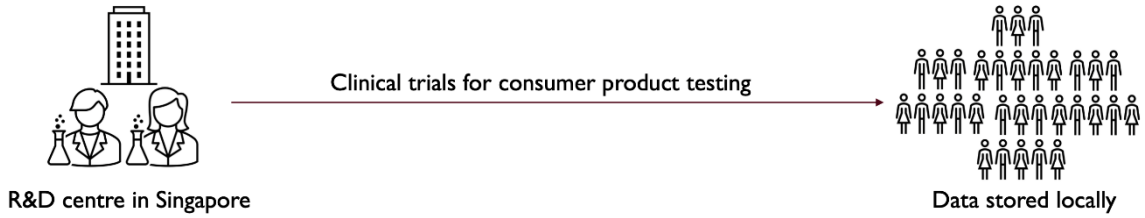


*Figure 8: Illustration of how R&D activities may be affected by cross-border data flow regulations*

### Case Study 3: Shenzhen Data Exchange

To capitalize on the nonrivalry of data domestically, China has begun setting up so-called 'data-exchanges' in all major cities across the country. Such a data exchange works like a commodity exchange for physical production factors, allowing data collectors to sell their data, and other firms and agencies to buy that data and put it to productive use. One of the key cities to experiment with this approach was the city of Shenzhen. On November 15, 2022 the Shenzhen data exchange opened for trading after a one-year trial period. During the trial over 400 trades totalling around USD150 million in value were completed. On the official launch data in 2022, almost 100 data providers and 300 buyers were registered including the Industrial and Commercial Bank of China, China Unicom, and the Shenzhen Power Supply Bureau. Today there are 40 data exchanges already in operation or under planning in China. While most of these are still in experimental stages, a few problems need to be addressed before they can become as successful as the government envisions. These include: clarifying the legal framework around ownership of data, ensuring anonymity of data, convincing more private firms to join the exchange, and integrating the exchanges both inside China and internationally – as the planned Singapore-China data exchange platforms in Tianjin and Chongqing aim to do.

## IV.d. How Firms are Adjusting to the Regulations

While China's cross-border data transfer regulations are new and still unfolding and will pose various compliance challenges to multinationals, the business opportunities present in China's huge consumer market and digital economy landscape may make compliance with the regulations worthwhile for many firms. To remain compliant with the new data protection framework, many firms had to adjust their data handling practices, ranging from duplicating data centres and operative process, to offering a different set of products to Chinese customers, to completely withdrawing from the Chinese market, as the Yahoo case discussed above has shown.

Two large technology giants that adapted to the new data policies – especially the data localization requirements – by changing their data handling practices are Apple and Tesla. Both are now storing the data of their Chinese customers in China. Apple already moved its Chinese customers' data to servers of a state-owned company in 2017 in response to the cybersecurity law. Additionally, Apple has made a company owned by the Guizhou provincial government the owner of its Chinese customers' iCloud data and does not use the encryption technology on data stored in China that it uses elsewhere to allow the government to access this data when necessary. Similarly, Tesla has responded to data localization requirements of important data by opening its own data centre in May 2021. It now stores all data produced by Chinese customers domestically.

Another path to comply with the new regulations without completely withdrawing from China is to simply offer different products that are not connected to the non-Chinese market and thus do not require cross-border data transfers. One example of this is LinkedIn. After launching a localized version in 2014, LinkedIn announced in October 2021 that it would shutter this service by the end of 2021, citing the "significantly more challenging operating environment and greater compliance requirements in China" for the move. This comes just 7 months after LinkedIn had suspended new sign-ups for the platform to "remain in compliance with local law". Rather than withdrawing completely from the Chinese market, however, LinkedIn launched a new platform 'InCareer' in China in December 2021 as a replacement. This new job-posting application has no social feeds or post-sharing features and is completely disconnected from the global LinkedIn platform. Thereby, LinkedIn bypasses the new cross-border data transfer regulations, but also disconnects Chinese users from their global peers.

Another example is a US medical device manufacturer that decided not to offer its latest product in China, as it relies on remote adjustment dependent on continuous cross-border data flow between China and the US, which has become too costly and uncertain with the PIPL. Thus, Chinese customers are deprived of the latest data-based innovations (Douglas and Feldshuh 2022).

# V. Looking Ahead: The Global Policy Environment

Many countries around the world are currently updating or newly creating their legal data protection framework to be better equipped for the opportunities and challenges of a globalized digital economy. Some have followed the path of the European Union, and have implemented regulations very similar to the GDPR both in content and aim. These include among others Chile, Japan, Brazil, South Korea, and South Africa, with South Korea also gaining an adequacy decision from the European Commission after the updated legislation came into force.

However, other countries, like the case of China here has shown, may have followed the GDPR in some aspects, but have opted for frameworks that better suit their own needs and interests. China, as well as countries like Russia and Vietnam, can be classified as 'control models' that have quite stringent rules for cross border data transfers, require data localization, and make significant exceptions to free data processing for issues of national interest. On the other end of the spectrum is the 'open model' with countries such as the US, Canada or Australia that prioritize free data flows by having only minimal protection and focussing on ex-post accountability.

Rather than converging towards one universal model, the currently emerging trend seems towards multiple different models and requirements for firms handling data and transferring it internationally. However, this period of uncertainty may potentially only be short term, as countries and firms across the world come up with new solutions to these issues. Especially in the realm of trade agreements and partnerships, digital economy issues and data protection is becoming increasingly important. One such example is the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) which includes provisions aiming to minimize cross-border data flow restrictions. China's PIPL, for example, makes exceptions for overseas data transfers based on international treaties and agreements, preserving some leeway as China enters discussions on digital economy collaborations with global partners. However, when such agreements will be signed and how compliance will work in practice remains to be seen.

# VI. Conclusion

While the Chinese data protection guidelines may look similar to the European GDPR at first glance, a deeper analysis shows that the two economic powers are following fundamentally different models with subsequently different implications: The EU is focussed on treating data protection and privacy as a citizen's individual right, with ease of business being a second priority. China, on the other hand, although it also has strong data safeguards for individuals, prioritises national security interests, with ease of business following closely behind these two overarching concerns. Data localisation requirements are sweeping and apply to not only firms of key industries, but also any firm that is reasonably large. This has various implications: (1) Firms, especially multinational ones relying on cross-border data transfers face higher costs; (2) Market concentration in the Chinese technology sector is likely to increase, in addition to Chinese firms gaining market share as foreign firms face higher costs and administrative barriers; And (3) while competitiveness will disproportionately be negatively affected for foreign firms, innovation will likely be hampered within the Chinese market as well, as firms face higher barriers to collaboration and international growth and exchange.

However, of course, China will continue to carefully balance economic growth and national security interests to remain competitive in today's globalized digital economy. Exactly which path China will tread will become clearer as authorities begin interpreting and implementing the regulations and assessments. Importantly, developments in China must be seen in their global context, and whether China and other countries that are currently rolling out distinctive standards pertaining to cross-border data flows will find ways to overcome the differences in interests and motivations to support the digital economy with a relatively free framework for international data transfers remains to be seen. Until then, the world will undergo an extended period of uncertainty as global parties look for efficient channels of collaboration and the optimal policy mix.

# References


Blind, Knut, Crispin Miles Niebel, and Christian Rammer. 2022. “The Impact of the EU General Data Protection Regulation on Innovation in Firms.” *ZEW Discussion Papers*, no. 22–047 (October). https://doi.org/10.2139/ssrn.4257740.

Chu, Eric. 2023. “China’s Digital Economy: Full Steam Ahead.” HKTDC Research. February 2, 2023. https://research.hktdc.com/en/article/MTI4OTE5MTYwMg.

Douglas, Antonio, and Hannah Feldshuh. 2022. “How American Companies Are Approaching China’s Data, Privacy, and Cybersecurity Regimes.” US-China Business Council. https://www.uschina.org/sites/default/files/how_american_companies_are_approaching_chinas_data_privacy_and_cybersecurity_regimes.pdf.

Henry-Nickie, Makada, Kwadwo Frimpong, and Hao Sun. 2019. “Trends in the Information Technology Sector.” *Brookings* (blog). March 29, 2019. https://www.brookings.edu/research/trends-in-the-information-technology-sector/.

IAPP, and EY. 2018. “IAPP-EY Annual Privacy Governance Report 2018.” https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/financial-services/ey-iapp-ey-annual-privacy-gov-report-2018.pdf.

Jia, Jian, Ginger Zhe Jin, and Liad Wagman. 2020. “GDPR and the Localness of Venture Investment,” January. https://dx.doi.org/10.2139/ssrn.3436535.

Johnson, Garrett A., and Scott K. Shriver. 2020. “Privacy & Market Concentration: Intended & Unintended Consequences of the GDPR.” *Marketing Science Institute Working Paper Series*, no. Report No. 20-111.

Kang, Byeongwoo, Eiichi Tomiura, and Banri Ito. 2020. “Cross-Border Data Transfers under New Regulations: Findings from a Survey of Japa Nese Firms.” *Vox EU, CEPR Policy Portal* (blog). March 14, 2020. https://cepr.org/voxeu/columns/cross-border-data-transfers-under-new-regulations-findings-survey-japanese-firms.

Martin, Nicholas, Christian Matt, Crispin Niebel, and Knut Blind. 2019. “How Data Protection Regulation Affects Startup Innovation.” *Information Systems Frontiers* 21 (6): 1307–24. https://doi.org/10.1007/s10796-019-09974-2.

Peukert, Christian, Stefan Bechtold, Michail Batikas, and Tobias Kretschmer. 2020. “European Privacy Law and Global Markets for Data.” *Center for Law & Economics Working Paper Series* 1.

Prasad, Aryamala, and Daniel R. Perez. 2020. “The Effects of GDPR on the Digital Economy: Evidence from the Literature.” *Informatization Policy* 27 (3): 3–18. https://doi.org/10.22693/NIAIP.2020.27.3.003.

Presidente, Giorgio, and Carl Benedikt Frey. 2022. “The GDPR Effect: How Data Privacy Regulation Shaped Firm Performance Globally.” CEPR. March 10, 2022. https://cepr.org/voxeu/columns/gdpr-effect-how-data-privacy-regulation-shaped-firm-performance-globally.

Xinhua. 2014. “中央网络安全和信息化领导小组第一次会议召开 习近平发表重要讲话 (‘The First Meeting of the Central Leading Group for Cybersecurity and Informatization Was Held Xi Jinping Delivered an Important Speech’).” Cyberspace Administration of China (中华人民共和国国家互联网信息办公室). February 27, 2014. http://www.cac.gov.cn/2014-02/27/c_133148354.htm.