

Legal Frameworks for Corporate Data Transfers between China and Europe

Eneken Tikk, Fang Fang, Pål Wrangé and Hao Yuan

Sino-European Expert Working Group on the Application of International Law in Cyberspace (EWG-IL), Research Group Report 2025. A joint research initiative between the GCSP and the China Institutes of Contemporary International Relations, EU Cyber Direct, Xiamen University and Suzhou Academy of Xi'an Jiaotong University.



Geneva Centre for Security Policy

Maison de la paix
Chemin Eugène-Rigot 2D
P.O. Box 1295
1211 Geneva 1
Switzerland
Tel: + 41 22 730 96 00
Contact: www.gcsp.ch/contact
www.gcsp.ch

ISBN: 978-2-88947-036-5

© Geneva Centre for Security Policy, December 2025

The views, information, and opinions expressed in this publication are those of the authors and do not necessarily reflect the positions of the five facilitating organizations or the authors' institutions, which are also not responsible for the accuracy of the information provided.



About the partner organisations



The China Institutes of Contemporary International Relations (CICIR) is a long-standing, extensive, and multifunctional research and consultation complex focusing on international strategic and security studies. It covers all geographic areas and major global strategic and comprehensive issues. The CICIR has about 300 staff, including researchers and administrative and logistical personnel, who work for 15 institutes, a number of centres, and several offices. For years it has participated in wide-ranging, comprehensive and high-end international academic exchanges. The CICIR is authorised to confer master's and doctoral degrees, and publishes three academic journals: *Xiandai Guoji Guanxi*, *Contemporary International Relations* and *China Security Studies*.



EU Cyber Direct – EU Cyber Diplomacy Initiative supports the European Union's cyber diplomacy and international digital engagements in order to strengthen a rules-based order in cyberspace and build cyber-resilient societies. To fulfil this aim it conducts research, supports capacity-building in partner countries and promotes multistakeholder cooperation. Through research and events, EU Cyber Direct regularly engages in discussions about the future of international cooperation to fight cybercrime and strengthen criminal justice systems globally.



The Geneva Centre for Security Policy (GCSP) is an international foundation that aims to advance global cooperation, security, and peace. Governed by 55 Member States, this flagship foundation is supported by the Swiss government to provide a unique 360° approach to learn about and solve global challenges. Our mission is to educate leaders, facilitate dialogue, advise through in-house research, inspire new ideas and connect experts to develop sustainable solutions for a more peaceful future.



Xiamen University (XMU), established in 1921, has long been listed among China's leading universities on the national 211 Project, 985 Project, and Double First-Class Initiative, which were launched by the Chinese government to support selected universities in achieving world-class standing. With a graduate school, six academic divisions consisting of 35 schools and colleges, and 17 research institutes, XMU boasts a total enrolment of nearly 47,000 full-time students and has over 3,000 full-time teachers and researchers, 15 of whom are members of either the Chinese Academy of Sciences or the Chinese Academy of Engineering.



Founded in May 2004, Xi'an Jiaotong University Suzhou Academy is a legal-person scientific research unit under Xi'an Jiaotong University and also undertakes management functions. The core mission is to build four key bases in Suzhou for Sino-foreign cooperative education, education and training, scientific research, and the transformation of scientific and technological achievements. Supporting the local social and economic development is one of its important tasks.



Background

This report has been produced in the context of a larger research and dialogue project, in terms of which the China Institutes of Contemporary International Relations, EU Cyber Direct, the Geneva Centre for Security Policy, and Xiamen University and Suzhou Academy of Xi'an Jiaotong University convene a joint Sino-European Expert Working Group on the Application of International Law in Cyberspace (EWG-IL). The working group provides a platform for exchange among European and Chinese legal experts to examine the application of international law in cyberspace and examine related problems from a theoretically legal perspective. The main goal of the work in research groups is to provide more thorough analysis of the selected topics and identify points of divergence and convergence between Europe and China with the aim of creating a more evidence-based and trusted environment for policy discussions in Track 1.5. and Track 1 processes.

Authors

Prof. Fang FANG, Professor, East China University of Political Science and Law

Dr Eneken TIKK, Lecturer on Data and Law, University of Tartu, Estonia

Prof. Pål WRANGE, Professor of Public International Law, Stockholm University, Director, Stockholm Centre for International Law and Justice, Sweden

Mr Hao YUAN, Attorney at Law, Part-time Lecturer at Soochow University

Acknowledgement

This report was sponsored by the Swiss Federal Department of Foreign Affairs, whose generous support is greatly appreciated. The constructive feedback and valuable insights of the reviewers, Prof. Yanqing Hong and Prof. Dr Indra Spiecker, whose expertise has contributed to the quality of this publication, are also gratefully acknowledged.



Contents

Introduction: legal frameworks for corporate data transfers between China and Europe	7
1. China’s framework for data transfers	8
1.1 Overview of China’s legal framework for the governance of cross-border data flows.....	8
1.2 Main pathways for data transfer from China.....	9
1.2.1 Security assessment.....	9
1.2.2 Standard contract filing.....	10
1.2.3 Security certification.....	10
1.2.4 FTZ negative list mechanism.....	11
1.2.5 Exemptions.....	11
2. EU frameworks for data transfers	13
2.1 Main pathways for personal data transfers from the EU.....	13
2.1.1 Adequacy decisions.....	13
2.1.2 Appropriate safeguards guaranteed by controllers.....	14
2.1.3 Derogatory transfers.....	14
2.2 Transfers of non-personal data from the EU.....	15
2.2.1 Open Data Directive.....	15
2.2.2 Data Governance Act.....	15
2.2.3 Data Act.....	16
2.2.4 European data spaces.....	16
3. International law aspects of data transfers	18
3.1 Sovereignty and jurisdiction.....	18
3.2 International rules and protections.....	18
3.3 Trade and data flows.....	19
4. Conclusion	20



Introduction: legal frameworks for corporate data transfers between China and Europe

The European Union (EU) and China have started discussions under the Cross-Border Data Flow Communication Mechanism (hereinafter the Mechanism).¹ This process will focus on practical solutions to address problems European companies face in China regarding the cross-border flows of non-personal data. In this report, we investigate legal frameworks for corporate data transfers currently in place in the EU and China, with a view to building a foundation for a deeper comparative analysis of the implementation of relevant rules and principles in practice.

Both in Europe and China, data transfers are subject to numerous laws, policies, and strategies. In Europe, the EU General Data Protection Regulation (GDPR),² the EU Data Act (DA)³ and the EU Data Governance Act (DGA)⁴ are some of the core elements of the legal framework for cross-border data flows. These foundational legal instruments are complemented by further EU-level specialised regulation⁵ and EU Member States's domestic law. In China, data transfers are governed by fundamental laws such as the Cybersecurity Law of the People's Republic of China (PRC),⁶ the Data Security Law of the PRC,⁷ and the Personal Information Protection Law of the PRC,⁸ as well as normative legal documents at hierarchically low levels all enacted by the central government.

In sum, the law of data transfers for both European and Chinese companies is comprehensive and complex, and still evolving in both China and Europe. Alongside thorough personal data protection regimes, there are exceptions and restrictions that apply in the EU and China to the transfer of further categories of data, e.g. non-personal, industrial and public data. For instance, restrictions on transfers may derive from considerations of public security, public order and other legitimate public policy objectives, as well as corporate policies. To grasp the requirements and guidelines applicable to data transfers between European countries and China, sections 1 and 2 lay out the respective legal landscapes. Because data transfers to other jurisdictions have to be conducted in line with the respective international obligations, further conditions for, restrictions on and imperatives for data transfers derive from international law. Section 3 examines potentially applicable international obligations.

¹ https://policy.trade.ec.europa.eu/news/eu-and-china-launch-cross-border-data-flow-communication-mechanism-2024-08-28_en.

² Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, pp. 1-88.

³ Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), OJ L, 2023/2854, 22.12.2023.

⁴ Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), OJ L 152, 3.6.2022, pp. 1-44.

⁵ These include Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, OJ L 303, 28.11.2018, pp. 59-68; Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, OJ L 172, 26.6.2019; Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847, OJ L, 2025/327, 5.3.2025.

⁶ Text available at <https://www.lawinfochina.com/Display.aspx?Id=22826&Lib=law&LookType=3>.

⁷ Text available at <https://www.lawinfochina.com/display.aspx?id=35666&lib=law>.

⁸ Text available at https://en.spp.gov.cn/2021-12/29/c_948419.htm.



1. China’s framework for data transfers

1.1 Overview of China’s legal framework for the governance of cross-border data flows

Data transfers from China to third countries are permitted provided that national security is safeguarded and the rights and interests related to both personal and non-personal data are protected. This regulatory policy rests on the conviction that data flows are essential for economic and social life.

The current legal basis of cross-border data flow regulation in China is composed of fundamental laws such as the Cybersecurity Law of the PRC, the Data Security Law of the PRC, and the Personal Information Protection Law of the PRC, as well as regulations and normative legal documents, all of which were enacted by the Cyberspace Administration of China (CAC), including Measures for the Security Assessment of Outbound Data Transfer, Measures for the Standard Contract for Outbound Transfer of Personal Information, the Cybersecurity Standards Practice Guide – Cross-Border Personal Information Processing Security Certification Specifications, and Provisions on Promoting and Regulating Cross-border Data Flow. As reflected in Table 1, these systematic rules for outbound data transfers primarily comprise the following basic pathways: security assessment, standard contract filing, security certification, negative lists in free trade zones (FTZs), and exemptions (i.e. exclusions applying to these pathways).

For the majority of data transfers, there is no need to apply to follow one of these data transfer pathways if they constitute a general, non-required process for free data exports. For situations that may require security assessments, standard contract filing (abbreviated to filing),⁹ certification and negative lists, specific enumerations are provided.

Table 1: China’s current framework of cross-border data flow regulation

Higher-level laws	Cybersecurity Law of the PRC (2016) Data Security Law of the PRC (2021) Personal Information Protection Law of the PRC (2021)			
Rules and measures	Measures for the Security Assessment of Outbound Data Transfer (2022)	Cybersecurity Standards Practice Guide – Cross-Border Personal Information Processing Security Certification Specifications (2022)	Measures for the Standard Contract for Outbound Transfer of Personal Information (2023)	Provisions on Promoting and Regulating Cross-border Data Flow (2024)
Data transfer pathways correspondingly regulated	Security assessment	Security certification	Standard contract filing	Exemption/negative list systems in FTZs

⁹ This pathway is conceptually similar to the EU’s standard contractual clauses (SCCs).



1.2 Main pathways for data transfer from China

Among the above four pathways, two – filing and certification – broadly resemble mechanisms found in the EU and have been widely adopted by various jurisdictions. In contrast, a security assessment constitutes an *ex ante* regulatory measure. It evaluates potential risks associated with cross-border data transfers in advance, with a particular focus on whether such transfers may pose threats to national security, and subsequently determines whether the transfer should be authorised. Notably, the negative list mechanism for data exports in FTZs represents a distinctively Chinese regulatory innovation. Put simply, high-risk scenarios fall under the security assessment requirement; lower-risk scenarios may rely on filing or certification; and scenarios for cross-border transfers in which the risks are negligible or *de minimis* are exempt from these transfer pathways and may proceed without hindrance.

1.2.1 Security assessment

1. Clarifying the scope of important data

Issued by the CAC in May 2022 and entering into force in September of the same year, the Measures for the Security Assessment of Outbound Data Transfer (Measures) sets out the particular circumstances in which this pathway applies – which is only when transferring important data to third countries. The scope of important data includes both personal and non-personal data. What constitutes *important data* is defined based on a risk assessment – specifically whether the export of such data could pose any threats to national security or economic development. Data transfers through the security assessment pathway require an application to the local and central CAC, and such transfers can only proceed after receiving authorisation from the central CAC.

2. Transferring personal data overseas

The Measures document sets two benchmark thresholds for personal data transfer overseas: either when the cumulative total in a given year (i.e. since 1 January of the current year) exceeds 1,000,000 individuals' personal information (excluding sensitive personal information) or 10,000 individuals' sensitive personal information.

When the total volume of personal data to be transferred exceeds the above thresholds, such a transfer is considered to be an export of important data, is highly likely to pose potential risks, and therefore requires authorisation from the CAC through the security assessment pathway.

3. Transferring non-personal data overseas

As noted above, the key factor in determining whether personal data qualifies as important data is the scale of the data being transferred. For non-personal data, whether it is deemed important is currently determined in China by industry-specific data catalogues. Each industry develops its own catalogue based on contextual scenarios and its data classification and grading system, which is then formally approved by the CAC.¹⁰ Once approved, any data explicitly listed as

¹⁰ Currently, China has been gradually clarifying the scope of important data through industry categories, technical standards and



“important data” in an industry’s catalogue must follow the security assessment pathway, according to the same logic that such data may pose potential risks if transferred overseas.

However, not all non-personal data is classified as “important”. Non-personal data not explicitly designated as important in an industry catalogue may be transferred abroad through other mechanisms rather than the security assessment pathway, such as on the basis of contractual obligations or under exemption conditions.

1.2.2 Standard contract filing

Filing applies only in scenarios where personal data is transferred to a third country, and explicit specifications are set out regarding both the type of data processor involved and the scale of the data export. The circumstances applying to data exports via the filing pathway are as follows.

1. The organisation transferring the data is not a critical information infrastructure operator.
2. Since 1 January of the current year, the cumulative export of personal information to overseas recipients involves 100,000 or more individuals, but fewer than 1,000,000 individuals (excluding sensitive personal information), or involves fewer than 10,000 individuals’ sensitive personal information.

Filing establishes a “minimum threshold” for the volume of data exports, which makes it the most favoured data transfer pathway for local Chinese enterprises.¹¹ Coupled with its relatively simpler procedural requirements compared with security assessments, this makes it the most commonly used pathway for data flows between Chinese and European companies.

1.2.3 Security certification

Like filing, certification can only be applied to exports of personal information. The scenarios that satisfy the conditions for filing are also applicable to the certification route.¹² However, the lack of sufficient authoritative certification bodies, coupled with the absence of a mutual recognition mechanism between Chinese certification bodies and those of the EU, presents a significant challenge for the widespread application of the certification pathway.

On 21 October 2025, the CAC released a list of the first 13 institutions authorised to conduct personal information protection certification. Among them, two are based in Shanghai, one in Shenzhen and the remaining ten in Beijing. The CAC is expected to approve additional certification institutions in the coming months.

FTZ negative lists.

¹¹ The CAC released the Guidelines for Filing the Standard Contract for Outbound Transfer of Personal Information (2nd edn.) in March 2024, detailing the specific requirements regarding methods, procedures, and materials for applying filing to transfer personal data overseas, and optimising and simplifying the relevant materials that data processors need to submit.

¹² In December 2022, the National Technical Committee 260 on Cybersecurity of Standardization Administration of China (TC260) released the Cybersecurity Standards Practice Guide – Cross-Border Personal Information Processing Security Certification Specifications (Version 2.0), which specifies the situations when personal data can be transferred abroad via the certification pathway.



1.2.4 FTZ negative list mechanism

The FTZ negative list mechanism is a uniquely Chinese pathway for cross-border data transfer that has emerged in recent years and constitutes an important component of China's overall cross-border data transfer framework. Gradually the government has recognised that an overly broad application of the security assessment pathway could excessively restrict data exports, potentially hindering China's digital economy. Consequently, it has begun to explore a more relaxed regulatory approach, representing a deliberate effort to balance security with development. Under this situation, the Provisions on Promoting and Regulating Cross-border Data Flow (Provisions) released by the CAC in 2024 expressly authorises pilot FTZs to capitalise on their institutional innovation advantages to take the lead in exploring a negative list approach for cross-border data transfers.

The negative list mechanism has several features. Firstly, it indirectly expands the applicability of the filing pathway. In principle, data specified in the negative list must undergo a security assessment for enterprises registered in FTZs to transfer data abroad. However, for data not covered by negative lists, enterprises may opt for filing pathway. As a result, the circumstances under which FTZ-registered enterprises can rely on filing have increased substantially compared with the period before the list was introduced. Secondly, negative lists further clarify the scope of what is considered to be important data. The lists cover both personal and non-personal data. In particular, the explicit specification of non-personal data serves as a supplementary mechanism to industry data catalogues in defining important data. Finally, negative lists represent the Chinese government's effort to adopt a more open approach to cross-border data transfers. The upper threshold limits negative lists set for the export of personal data generally exceed those prescribed in the Provisions and industry catalogues.

From May 2024 until the time of writing of this report, a total of eight FTZs in China in the Tianjin, Shanghai, Beijing, Hainan, Zhejiang, Guangxi, Jiangsu, and Chongqing provinces¹³ have released eight negative lists for cross-border data transfers covering more than 20 industries and scenarios.

1.2.5 Exemptions

The CAC explicitly provided exemptions in the Provisions as follows:

1. Transferring personal data, which involves

- a) a contract-based form, in which a private person is a contracting party, such as cross-border shopping, delivery, remittance, payment, account opening, booking of air tickets and hotels, visa application, and academic examination services;
- b) a consent-based form, in which the personal information of any employee must be provided to an overseas recipient when needed for human resource management under the labour rules and regulations developed in accordance with the law and a collective contract signed in accordance with the law;

¹³ The provinces are listed in the order of the dates the lists were released.



- c) emergency considerations, such as to protect the life, health or property safety of a natural person;
- d) when the quantity of transferred personal information to a third country (excluding sensitive personal information) is cumulatively less than 100,000 individuals as of 1 January of the current year, as long as the data processor is not a critical information infrastructure operator; and
- e) data processing activities, in which personal information is collected overseas but processed in China and does not generate any personal information or important data during the processing process.

2. Transferring non-personal data

Non-personal data could be exempted from the above pathways when transferring overseas non-personal data collected and generated in the course of international trade; cross-border transportation; academic cooperation; and multinational production, manufacturing, and marketing.



2. EU frameworks for data transfers

The EU considers flows of data to and from countries outside its borders to be necessary for the expansion of international trade and cooperation. Conditions for transfers from the EU to third countries depend on the categories of data in question and generally require that a high level of protection is afforded to personal data, and that the rights and interests related to non-personal data can demonstrably be safeguarded. For *personal data*, transfers are permitted only either under an (1) adequacy decision of the EU Commission, which equates the target jurisdiction with the EU's legal protections; (2) when appropriate institutional or individual safeguards are in place between the transferring and recipient entity; or (3) as an exception, based on a concrete consent, interest or transaction. For *non-personal data*, other than open data, transfers require the absence of any restrictive circumstances (e.g. copyright) and that they are not in conflict with EU laws and policies. The General Data Protection Regulation (GDPR) provides the main pathways for the transfer of personal data. The Data Governance Act (DGA), Data Act (DA) and Framework for the Free Flow of Non-personal Data provide the framework for transferring non-personal data to third countries.

2.1 Main pathways for personal data transfers from the EU

As far as personal data is concerned, the GDPR establishes three main requirements for such transfers: adequacy decisions, appropriate safeguards to be provided by controllers, or a data subject's consent or legitimate interest for more isolated transfers.

2.1.1 Adequacy decisions

The EU Commission's system of adequacy decisions constitutes the most comprehensive and durable basis for transferring personal data to third countries. For this purpose, the Commission may decide with effect for the entire EU that a third country, a territory or specified sector within a third country, or an international organisations offers an adequate level of data protection, thus providing legal certainty and uniformity throughout the EU as regards the third country or international organisation considered to provide such a level of protection. In such cases, transfers of personal data to this third country or international organisation may take place without the need to obtain any further authorisation, provided other GDPR requirements are complied with.

When assessing the adequacy of the level of protection for the purposes of granting (or revoking) the right to employ adequacy decisions, the Commission shall take into account the rule of law, the independence of supervisory authorities and the international commitments of the target jurisdiction.¹⁴

¹⁴ As of 31 August 2025, the European Commission has recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, United Kingdom under the GDPR and Law Enforcement Directive, United States (commercial organisations participating in the EU-US Data Privacy Framework), Uruguay and the European Parent Organisation as providing adequate protections.



2.1.2 Appropriate safeguards guaranteed by controllers

In the absence of the applicability of an adequacy decision, a controller or processor may transfer personal data to a third country or an international organisation if this controller or processor can provide appropriate safeguards (see below), and on condition that data subjects' rights and the effective legal remedies for data subjects are enforceable. Where such safeguards are applied, controllers are competent to decide the extent and modalities of transfers. The durability of relevant safeguards depends on their legal form and specificity.

The following are considered to be alternative appropriate safeguards for which an additional authorisation is not required, i.e. the controller is entitled to implement the transfer after a general approval of the terms in question:

1. a legally binding and enforceable instrument between public authorities or bodies of the EU and the third country;
2. binding corporate rules in accordance with Article 47 of the GDPR;
3. standard data protection clauses adopted by the European Commission;¹⁵
4. an approved code of conduct pursuant to Article 40 of the GDPR together with the binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; and/or
5. an approved certification mechanism pursuant to Article 42 of the GDPR together with the binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

2.1.3 Derogatory transfers

In limited circumstances, the possibility exists for transfers where the data subject has given his or her explicit consent or the circumstances necessitate a derogation. According to Article 49 of the GDPR, the data subject can explicitly consent to the proposed transfer, after having been informed of the possible risks of the transfer for the data subject due to the absence of an adequacy decision and appropriate safeguards. Similarly, the transfer can be legitimate for the performance of a contract between the data subject and the controller, or the implementation of precontractual measures taken at the data subject's request. Public interest and the data subject's vital interests can also serve as the basis for non-recurring transfers of personal data. This legal basis presumes that the transfer is occasional and necessary in relation to a contract, an essential interest, or a legal claim, regardless of whether within a judicial procedure, or an administrative or any out-of-court procedure, including procedures before regulatory bodies.

¹⁵ See https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.



2.2 Transfers of non-personal data from the EU

The protection of non-personal data is a new legal regime in the EU and its Member States because the 2020 European Data Strategy considers non-personal industrial data and public data in Europe to be a potential source of growth and innovation.

2.2.1 Open Data Directive

The aim of the Open Data Directive (ODD) is to promote the use of open data and stimulate innovation in products and services. Recital 43 of the ODD states that

making public all generally available documents held by the public sector – concerning not only the political process but also the legal and administrative process – is a fundamental instrument for extending the right to knowledge, which is a basic principle of democracy. That objective is applicable to institutions at every level, be it local, national or international.

Access (which can be presumed to include transfers) to non-personal data is unrestricted in case of open data¹⁶ and high-value datasets.¹⁷ (High-value datasets are documents whose re-use is associated with important benefits for society, the environment, and the economy, in particular because of their suitability for the creation of value-added services, applications, and new, high-quality and decent jobs, and the number of potential beneficiaries of the value-added services and applications based on those datasets.) As of 2025, the following categories of data are considered high value in the EU: geospatial, Earth observation and the environment, meteorological, statistics, companies and company ownership, and mobility.

2.2.2 Data Governance Act

The Data Governance Act (DGA) can be considered as the foundational instrument providing conditions for the transfer of non-personal data. It is based on the premise that fostering the international free flow of data needs to go hand in hand with the EU's open strategic autonomy.¹⁸ Accordingly, the DGA sets limits to the circulation and re-use of non-personal data, in particular regarding third countries and/or government access. According to the DGA, undertakings and data subjects should be able to be confident that the re-use of certain categories of protected data held by public sector bodies will take place in a manner that respects individuals' and corporations' rights and interests.

The DGA mandates additional safeguards for situations where data is transferred to third countries. Transfers to third countries of non-personal data that is to be protected from unlawful or unauthorised access in accordance with EU or national law and held by public sector bodies are only allowed where appropriate safeguards for the use of the data are provided. Appropriate safeguards could

¹⁶ Open data as a concept is generally understood to denote data in an open format that can be freely used, re-used and shared by anyone for any purpose.

¹⁷ Open Data Directive, art. 2(10).

¹⁸ Data Governance Act, recital 1.



include equivalent measures ensuring that in the third country the data benefits from a level of protection similar to that applicable by EU law, in particular with regard to the protection of trade secrets and intellectual property rights. Conditions of re-use also stipulate that in cases where a re-user intends to transfer anonymised personal data to a third country, it shall inform the public sector body of its intention to transfer such data and the purpose of such a transfer at the time of requesting the re-use of such data.

2.2.3 Data Act

The Data Act (DA) is aimed at enhancing the EU's data economy and fostering a competitive data market by making industrial data more accessible and usable, encouraging data-driven innovation and increasing data availability. In principle, the European Commission encourages the free and safe flow of industrial data to and from third countries, subject to exceptions and restrictions for the purposes of public security, public order, and other legitimate EU public policy objectives and in line with international obligations, including on fundamental rights.

Recital 101 of the DA summarises the relevant restrictions. In principle, transfers of non-personal data to third countries require a pre-existing international obligation, e.g. as part of mutual legal assistance treaties. In the absence of applicable international obligations, transfers of non-personal data to third countries are allowed on condition that their transfer does not conflict with data protection requirements under EU or Member State law. These may include, for instance:

- the protection of the fundamental rights of the individual, such as the right to security and the right to an effective remedy;
- the fundamental interests of a Member State related to national security or defence;
- the protection of commercially sensitive data, including the protection of trade secrets; and
- the protection of intellectual property rights, including any contractual undertakings regarding confidentiality.

2.2.4 European data spaces

Furthermore, domain-specific common European data spaces and relevant regulation are also to specify conditions of access and transfer for different categories of data, such as in the areas of agriculture, energy, finance, health care, mobility, innovation or research.¹⁹ Common European data spaces are intended to make data findable, accessible, interoperable and re-usable (the “FAIR data principles”), while ensuring a high level of cybersecurity.

As proposed in the European data strategy, such common European data spaces could cover areas such as health, mobility, manufacturing, financial services, energy or agriculture, or a combination of such areas, e.g. energy and climate, as well as thematic areas such as the European Green Deal or European data

¹⁹ These regulations are still emerging. For details, see <https://digital-strategy.ec.europa.eu/en/policies/data-spaces>.



spaces for public administration or skills. Relevant regulations (most of which are still in the planning or draft phases) further detail the prerequisites and conditions for data sharing and data pooling. Drawing on China's FTZ negative list mechanism described in section 1.2.4, the "China-Germany MOU on Cross-Border Data Cooperation" provides a framework under which the automotive industry may emerge as the first sector to achieve a functioning China-EU data space.



3. International law aspects of data transfers

The purpose of this section is to explain the international law framework of Chinese and European regulations related to data transfers. Some of these issues have already been dealt with by previous working groups. In most (if not all) of the cases covered in this report, it is the source state of a data transfer – or a third party with interests in the data – that may want to restrict data transfer. Hence, the receiving state will usually not object to data being transferred into its jurisdiction for licit purposes.

3.1 Sovereignty and jurisdiction

When data moves from state A to state B, other states may also have legal interests, such as state C if the data affects its security or state D if its citizens are affected. Under international law, states are free to regulate as they see necessary, subject to treaty obligations. As explained in a previous working-paper,²⁰ sovereignty is exercised through jurisdiction, commonly based on territoriality, active or passive personality; the protection of national interests; or universality. Overlaps are common.

For data transfers, related conflicts may concern territoriality and active personality. Territoriality can be subjective (where an act originates) or objective (where it ends), with the related “effects” principle potentially reaching further. “Territory” can refer to the location of the data storage, the controller, the owner of the data, etc. In addition, the active personality principle allows states to regulate acts by their citizens abroad, which will then overlap with territorial jurisdiction (and potentially create conflicts). For instance, state A could mandate its corporations to transfer certain data stored in state B to state A, and conversely prohibit that same corporation to transfer data to other states. By contrast the EU’s GDPR applies to entities that process EU residents’ data regardless of the location of the entity, and Chinese privacy laws have a similar approach.

3.2 International rules and protections

Some international frameworks enable data transfers but are not central here. Examples include UN Convention on the Law of the Sea rules on underwater cables, International Telecommunications Union regulations, and standards developed by technical bodies. States may also invoke other rules to protect data from destruction or unauthorised access, e.g. territorial sovereignty, human rights treaties and the Vienna Conventions on diplomatic relations. Regarding cybersecurity, the “norms, rules and principles for the responsible behaviour of States” adopted by the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security of States are relevant.²¹

Other international legal rules exhort states to limit data transfers for reasons of confidentiality and the right to the exclusive use of data. The right to privacy

²⁰ Jurisdiction in Cyberspace, 26 November 2024, <https://www.gcsp.ch/publications/jurisdiction-cyberspace>.

²¹ UN General Assembly (UNGA), A/76/135, 14 July 2021.



is enshrined in the International Covenant on Civil and Political Rights and the European Convention on Human Rights, which are binding on European states as well as arguably under customary law, and it is addressed in the “norms, rules and principles for the responsible behaviour of States”. The GDPR and China’s privacy rules relate to these obligations. States may also restrict transfers for national security reasons, which can be justified, for instance, under the right of self-defence. Further, the need to safeguard proprietary rights may justify limiting data transfers, especially to protect rights holders, e.g. intellectual property rights (Agreement on Trade-Related Aspects of Intellectual Property Rights; World Intellectual Property Organization’s conventions) and domestic protections for trade secrets. By contrast, international cooperation can oblige states to share data, such as for scientific or environmental reporting objectives, or for mutual legal assistance, including the new UN Convention against Cybercrime or the 2001 Budapest Convention.

3.3 Trade and data flows

Binding obligations to allow transfers are most prevalent in international economic law. E-commerce negotiations began in the World Trade Organization in 1998. The main result has been the Moratorium on Customs Duties on Electronic Transmissions, which has been renewed repeatedly, but covers only imports of data. Broader negotiations, such as the plurilateral Joint Statement Initiative on Electronic Commerce launched in 2017, aim to regulate transfers, access, privacy and cybersecurity. A draft text “stabilised” in 2024 covers data transfers and the flow of information, access to data, privacy, cybersecurity, etc. For instance, Article 12 encourages states to make government data available. However, the parties were unable to come to an agreement on controversial issues regarding data transfers.

Most substantive developments occur in regional trade agreements. These now often include “digital trade” chapters covering data flows, investment and privacy. They generally do not favour data localisation and favour data flows, while allowing certain restrictions, e.g. to uphold privacy and protect national security. The EU seeks to prohibit “unjustified” barriers such as localisation requirements, while upholding its privacy framework, notably the GDPR. For its part, China promotes “secure and orderly” flows, with broad exceptions for national security reasons. China participates in the Regional Comprehensive Economic Partnership and has applied to join the Comprehensive and Progressive Agreement for Trans-Pacific Partnership, both of which contain digital trade provisions.



4. Conclusion

It is a complicated task to find common ground between different legal systems, political regimes and conflicting economic interests. However, the EU and China have achieved mutual understanding on issues of international cybersecurity²² and have explicitly expressed political commitment to facilitating cross-border data flows through the Mechanism.

The legal and regulatory frameworks for corporate data transfers between Europe and China are relatively new, complex, and still evolving. However, some differences and similarities can be pointed out after an initial reading. China's cross-border data transfer regime is designed around a risk-based framework, which is reflected in the establishment of data-volume thresholds, the differentiation of data processor types, and the delineation between important and non-important data. Scenarios in which cross-border transfers may generate higher risks are required to undergo security assessments, whereas lower-risk transfers may rely on the filing or certification pathways, and in some cases may even be exempted entirely. European data transfers, while grounded in fundamental rights and freedoms, are also subject to restrictions deriving from, inter alia, public security, public order, and other legitimate public policy objectives. In addition to EU legal instruments, Member States' domestic laws may contain additional restrictions on when and how data transfers are permitted between corporate actors.

Both the EU and China are still developing their respective legal frameworks. Recognising that an overly broad application of security assessment pathways could hinder development, the government of China has authorized FTZs to introduce negative lists to further facilitate cross-border data transfers. The emergence of this mechanism embodies the Chinese government's regulatory logic of risk control in cross-border data governance, while also reflecting its pursuit of greater openness. It represents an effort to reconcile security with development. Further refining the FTZ negative list mechanism will be an important direction in the future evolution of China's cross-border data governance framework. The EU, in turn, is developing data spaces to make data available for access and re-use for the benefit of European businesses and citizens.

Both jurisdictions seek to find a balance between individual rights and freedoms, economic incentives and benefits, and security. What a trustworthy and secure environment for data transfers will mean for European and Chinese companies is an evolving discussion. Also, for both Europe and China, the meaning and impact of international data transfer-related obligations will be an essential consideration.

A deeper comparative inquiry into both legal spaces and best implementation practices could assist companies to navigate the complex and still evolving legal landscape vis-à-vis data transfers. Discussions of applicable international obligations, perhaps bilaterally, could help develop additional mutual understanding of how to best benefit from data transfers, and, potentially, inform international policy processes on this issue.

²² See, for example, the recommendations of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UNGA, A/70/174, 22 July 2015.

Building Peace Together



Geneva Centre for Security Policy

Maison de la paix

Chemin Eugène-Rigot 2D

P.O. Box 1295

1211 Geneva 1

Switzerland

Tel: + 41 22 730 96 00

Contact: www.gcsp.ch/contact

www.gcsp.ch

ISBN: 978-2-88947-036-5