ANALYSIS

Economic Security and Digital Trade: The Future of EU–China Data Flows

2026

Executive summary

This report examines the state of cross-border data flows between the European Union (EU) and China in the context of rising economic security concerns and diverging regulatory approaches. It finds that while bilateral dialogue on data governance has increased, including the establishment of a new communication mechanism for non-personal data, structural differences remain largely unresolved. The EU operates under a conditional and rights-based data transfer regime, whereas China's model is centred on cyber sovereignty and national security. China's legal framework imposes far-reaching restrictions on data transfers and enables broad state access, resulting in regulatory uncertainty, high compliance costs and operational challenges for European firms.

Given these persistent barriers and the broader geopolitical environment, the report concludes that meaningful regulatory convergence is unlikely. Instead, EU policy should focus on managing divergence in a way that limits economic, operational and strategic costs for European firms. This includes exploring practical risk management tools such as encryption for EU companies operating in China. In parallel, the EU should deepen integration with trusted partners by expanding its network of modern digital trade agreements and digital partnerships and work through initiatives such as Data Free Flow with Trust (DFFT). This way, the can EU safeguard its economic security and competitiveness while incentivising open and rules-based digital trade.

Table of contents

This analysis was written by Hannes Berggren and Hillevi Pårup. Valuable comments were provided by Hannes Lenk, Heidi Lund and Isaac Ouro-Nimini Hansen.

1 Introduction

Cross-border data flows have become a central policy issue of international trade. Over the past three decades, data access, sharing and use have become central drivers of economic growth and social well-being (OECD, 2022a). Since the world entered the Age of AI, and for technological developments such as quantum computing, data has only become more important (National Board of Trade, 2025a).

However, data flows are also linked to other policy objectives such as privacy, national security, competition and consumer protection (OECD, 2022b; OECD, 2025a). For that reason, jurisdictions across the world have increasingly legislated how data can be accessed and transferred across borders (Digital Policy Alert, 2025; Greenleaf, 2023). This rapid increase in data legislation, which often differs across jurisdictions, has made cross-border data transfers more difficult and hampered international trade (National Board of Trade, 2025c). Estimates indicate that convergence toward balanced data flow regulations through either open or pre-authorised safeguard regimes could yield sizeable benefits, with increases of 3.6 per cent in global exports and 1.77 per cent in global GDP (OECD & WTO, 2025).

Two jurisdictions that differ significantly in their approach to data regulation are the EU and China. The EU's framework for regulating how companies can access and transfer data across borders rests on legislation such as the General Data Protection Regulation (GDPR) and the Data Act. Such legislation could generally be described as an 'open conditional transfer model'. In China, relevant legislation includes the Cybersecurity Law, the Data Security Law and the Personal Information Protection Law (Creemers, 2022). These laws establish a more controlled/closed model, with a high degree of data localisation (National Board of Trade, 2025b). The difference in regulatory models hampers data flows – and thereby international trade – between the EU and China. The negative effect is exacerbated by China's controlled/closed model, which reduces trade more than an open or conditional model (Ferracane & van der Marel, 2024; OECD & WTO, 2025; OECD, 2025c).

In 2024, the EU and China launched a Cross-Border Data Flow Communication Mechanism in an attempt to address some of the issues hampering bilateral data flows, at least with regard to non-personal data (European Commission, 2024). Meanwhile, concerns have arisen around China's role in the global economy, its increasing geopolitical assertiveness and the strategic vulnerabilities created by excessive reliance on the country. Accordingly, the EU has adopted a strategy to 'de-risk' from China and is increasingly seeking to promote its economic security, for which data security is a key priority (European Commission, 2023; European Council, 2023).

This analysis explores the EU's cross-border data flows with China. The intention is to understand what data flows between the two are possible and what that means for EU policy. We begin by outlining key challenges affecting EU–China trade in relation to the EU's strategies for economic security and de-risking. Following that, the respective party's regulatory regime and international commitments on cross-border data flows are outlined. Finally, we conclude with a few policy recommendations aimed at promoting digital trade while ensuring economic security.

2 The EU's changing trade relationship with China

China is one of the European Union's largest trading partners, with a relationship characterised by strong interdependence alongside long-standing structural imbalances. In 2024, China was the EU's third-largest export destination and its largest source of imports: the EU exported goods to a value of EUR 213.3 billion and imported EUR 519 billion, predominantly manufactured products. This resulted in a substantial and persistent goods trade deficit of EUR 305.8 billion, equivalent to 44.5 million tonnes, which has doubled in value and quadrupled in volume since 2015. By contrast, services trade presents a more balanced picture: China was the EU's fourth-largest services partner in 2024, and the EU recorded a services trade surplus of EUR 21.7 billion (European Commission, 2025p).

Despite the large and deep relationship, there are significant hurdles in EU–China trade. In recent years, the EU has expressed growing concerns regarding the conditions faced by European companies in China. EU companies, like other foreign firms, face discrimination in the Chinese market, and it remains difficult for international businesses to stay competitive due to the lack of a level playing field. Moreover, despite the Chinese government's stated ambition to pursue a high-level opening of its market and build mutually beneficial trade partnerships, China still remains largely closed in many sectors of importance to European companies (European Commission, 2025p).

Many European companies report that the business environment in China has become more politicised in recent years (European Union Chamber of Commerce in China, 2025). Regulatory obstacles have remained largely unchanged, which has further negatively impacted the business outlook. A complex and non-transparent cybersecurity framework, restrictive rules on cross-border data flows subject to broadly applied security approvals, weak enforcement of intellectual property rights, technology transfer requirements, and a broad concept of national security all undermine the business environment (European Commission, 2025p).

Despite persistent challenges for foreign firms, China's large consumer market and growing technological capabilities continue to attract foreign investment. Across sectors such as electric vehicles, batteries, drones and rare earth magnets, China has moved to the global technological frontier, reshaping its position in both goods and services trade. Accordingly, access to leading technical innovation is now a motivation for European firms investing in China, even as geopolitics increasingly shapes corporate decisions (the Economist, 2026; Chan, 2026).

At the same time, the EU's concerns regarding China increasingly relate to systemic differences in economic governance, geopolitical behaviour and the security implications of deepening dependencies. Analysts note that China has become more authoritarian and is promoting its authoritarian model through the Belt and Road Initiative and the Digital Silk Road (Hillman, 2020; Rudd, 2022). The country has also begun acting more assertively and maintains an "unlimited friendship" with Russia after the full-scale invasion of Ukraine (Fix & Crebo-Rediker, 2024; Applebaum,

2023). China has also illustrated that it has both the capacity and willingness to use economic dependencies to pressure the EU. For example, China recently enforced export controls on critical raw materials, which impacted EU supply chains (European Commission, 2025p; Verhelst, 2025). It was also reported that European companies had been forced to hand over potentially sensitive data to the Chinese government to access rare earths (Leonard, 2025).

Security concerns have emerged specifically around digital trade and related investments with China, as flows of advanced technology risk enabling repression, military build-up or strategic coercion. The rise of dual-use technologies such as AI and quantum computing heightens these risks (Hillman, 2020; Atkinson, 2021; Miller, 2022; Gaida et al., 2023; Tardell, 2023; Bown, 2024; Mejean & Rosseaux, 2024; Ferry et al., 2024). The Chinese state retains extensive control over technology through ownership and intervention, while reports point to forced technology transfers and systematic infringements of foreign companies' intellectual property (USTR, 2018; ISDP, 2018; Sapir & Mavroidis, 2021; Ezell, 2021; DiKötter, 2022; Hillman, 2020; Rudd, 2022; Greig, 2023; Enright, 2024).

For cross-border data flows with China, several security-related risks linked to China's domestic legal environment and the potential use of data once transferred have been identified. Under the National Security Law and the 2017 National Intelligence Law, Chinese companies and citizens are obliged to "support, assist, and cooperate" with state security and intelligence bodies, and these obligations apply without judicial oversight or the requirement for court orders (Czarnocki et al., 2021). As a result, the Chinese government retains extensive authority to access sensitive data. This has raised concerns, especially in Europe and the United States, that such data could be leveraged for espionage, influence campaigns, mapping of critical infrastructure, and that connected technologies such as electric vehicles (EVs), drones and Internet-of-Things (IoT) devices could be exploited for cyber or physical disruptions (Harell, 2025).

Chinese practices increasingly come into conflict with the EU's growing extra-territorial regulatory toolbox aimed at policy goals such as human rights (Czerniawski & Svantesson, 2024). Regulatory responses have increasingly centred on targeted investigations and security frameworks. TikTok, for instance, has faced scrutiny and enforcement actions, including an Irish Data Protection Commission fine and warnings concerning the implications of China's surveillance laws (Bologa, 2025). In parallel, the European Commission has indicated that its ongoing security assessments of connected and automated vehicles may lead to the development of an ICT supply-chain toolbox, building on the existing 5G security toolbox to address vulnerabilities associated with Chinese technologies (Haeck et al., 2024).

Because of the specific risks pertaining to China, the EU has also developed a multifaceted policy approach of 'de-risking' towards the country. The EU sees China simultaneously as a partner, a competitor and a systemic rival. In that regard, the EU's overarching strategy is to continue to trade with China but seek to reduce critical dependencies and vulnerabilities, including in its supply chains, and to de-risk and diversify where necessary and appropriate (European Council, 2023).

The EU has also adopted a strategy for economic security, which increasingly shapes its trade policy strategies. The EU's economic security strategy outlines that the Commission and member states will deepen their analysis of critical supply chains, stress test them and establish the level of risk. It identifies the following broad and non-exhaustive categories of risks to economic security: 1) resilience of supply chains; 2) physical and cyber security of critical infrastructure; 3) technology security and technology leakage; and 4) weaponisation of economic dependencies or economic coercion. It is noted that these risks can occur along the entire value chain, from knowledge creation and basic research to commercialisation and manufacturing at scale. Since the launch of its economic security strategy, the European Commission has together with member states carried out risk assessments for four critical technologies (AI, quantum, semiconductors and biotechnology), while six more risk assessments are planned (European Commission, 2023a). Finally, in its doctrine for economic security, the European Commission (2025r) announced that one of its immediate economic security priorities would be protecting sensitive information and data.

3 The EU's and China's data flow regimes

The EU, the US and China constitute what can be described as three distinct data realms – or digital empires – with different approaches to data governance. The EU's and China's approaches to the regulation of cross-border data flows differ markedly. To illustrate these differences, we constructed Table 1 below in National Board of Trade (2025b) by building on previous work by Ferracane and Van der Marel (2025), Aaronson and LeBlond (2018) and Bradford (2023). In this section, we dig deeper into these differences by comparing relevant legislation in the EU and China, respectively.

Table 1. Three models of data transfer governance

Data model	Cross-border transfers	Data realm /digital empire
Open	Self-certification, self-assessment schemes, ex-post accountability, trade agreements and plurilateral/bilateral arrangements as only means to regulate data transfers.	United States
Conditional	Conditions to be fulfilled ex-ante, including adequacy of the recipient country, binding corporate rules (BCR), standard contract clauses (SCCs), data subject consent and codes of conduct, among others.	European Union (EU)
Controlled /closed	Strict conditions including bans to transfer data cross borders, local processing requirements, ad hoc government authorisation for data transfers, infrastructure requirements, ex-ante security assessments.	China

3.1 The EU's regime for cross border data flows

In the EU, the protection of *personal data* is enshrined in the Charter of Fundamental Rights of the European Union (CFR). The CFR guarantees fundamental respect for the private life of citizens and, more specifically, for the protection of personal data. This puts the protection of personal data – and the GDPR – in a very strong position in the EU. The basic rule of the GDPR is that data handlers cannot process personal data without a legal basis. The GDPR provides an exhaustive list of legal bases, such as the data subject's consent to the processing of their data or if such processing pursues a legitimate interest or is necessary for the performance of a contract to which the data subject is party. In addition to this are two important principles for the processing of personal data. First, personal data must be collected only for well-defined purposes and may not be further processed for other purposes (the 'purpose limitation principle'). Second, the collected data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (the 'data minimisation principle'). These requirements collectively limit the ability of EU businesses to transfer personal data across borders. Such transfers are deemed particularly sensitive when the level of data protection in third countries is lower than in the EU (European Commission, 2025a; National Board of Trade, 2025c).

The GDPR, however, has several provisions that allow for cross-border transfers of data. The 1995 European Data Privacy Directive (EDPD), the predecessor to the GDPR, introduced provisions on cross-border data transfers between the EU and non-

EU countries as an anti-circumvention measure, rather than as a measure that was protectionist in nature (Newman, 2020; Allen, 2024). Similarly, the GDPR has a toolkit which enables international transfers under certain conditions, such as adequacy decisions, an example of which is the EU–US Data Privacy Framework (DPF). Businesses may also transfer personal data to third countries if they have provided 'appropriate safeguards' – such as standard contractual clauses – to protect the rights of data subjects. In the absence of an adequacy decision or other appropriate safeguards, the transfer of personal data to a third country may be permitted in specific circumstances defined in the GDPR. Such transfers are subject to other strict conditions, for example, the informed and explicit consent of the data subject, the existence of a public interest, or the need to perform a contract concluded in the interest of the data subject (European Commission, 2025a; European Commission 2025b; National Board of Trade, 2025c).

It should be noted that it is unrealistic to think that China would gain an adequacy decision for data transfers under the GDPR. Moreover, data transfers to the country under any of the other alternatives remain very challenging, given the difficulty of protecting personal data from government access in China. It should also be noted that, while significantly more permissive for cross-border data transfers than China's rules, the EU's rules are also perceived complex by companies. We have previously concluded that the GDPR has had negative effects on EU international trade and productivity by making cross-border data flows more difficult, creating regulatory uncertainty and inducing high compliance costs for companies (National Board of Trade, 2025b).

For *non-personal data*, relevant legislation includes the Data Act from 2023, which establishes harmonised rules across the EU for fair access to and use of non-personal data generated by connected products and related services. The regulation also sets rules to allow data sharing for commercial and non-commercial purposes, fosters switching between data-processing services and enhances interoperability of data interfaces. In addition, it introduces safeguards to prevent government bodies from third countries from accessing non-personal data where this would go against EU or national law. Article 32 of the Regulation sets conditions under which non-personal data stored in the EU may be accessed or requested by foreign governments. It requires providers to prevent unlawful foreign access, allows recognition of such requests only when based on an international agreement, and – where no agreement exists – permits access solely if the third-country legal system meets specific safeguards such as proportionality, specificity, judicial review and protection of Union and member state legal interests, with providers obliged to inform customers and limit disclosure to the minimum data necessary (European Commission, 2025c; European Commission, 2025d).

The Data Governance Act (DGA)[1] and the Open Data Directive, in concert, regulate the reuse of publicly held but protected data, aiming to encourage data sharing. They establish mechanisms to facilitate the reuse of sensitive public-sector data (such as

[1] The European Commission's so-called Digital Package of 2025 proposed to repeal the Data Governance Act and instead incorporate relevant rules under the Data Act.

health data), create measures to enable data to flow across sectors and borders so the right data can be found and used, aim to ensure that data intermediaries act as trustworthy organisers of data sharing or pooling within Common European Data Spaces, and make it easier for citizens and businesses to make their data available for societal benefit (European Commission, 2025e). The DGA establishes GDPR-like safeguards for non-personal data by requiring that any third-country re-user of public-sector data, data intermediation services or data-altruism arrangements ensures an EU-equivalent level of protection and accepts EU jurisdiction. It also empowers the Commission to issue adequacy decisions and model contractual clauses for transfers of protected public-sector data, mirroring the mechanisms used for personal-data transfers under the GDPR (European Commission, 2025f).

Data flows are also increasingly regulated by EU cybersecurity rules. The Network and Information Security (NIS) Directive was the EU's first horizontal cybersecurity law, later expanded through NIS2 to cover more sectors with stricter, harmonised requirements and enforcement. The Cybersecurity Act strengthens the mandate of the European Union Agency for Cybersecurity (ENISA) and creates an EU-wide certification framework for ICT products and services, while the Digital Operational Resilience Act (DORA) adds detailed obligations for ICT risk management, incident reporting, resilience testing and oversight of critical third-country ICT providers in the financial sector. Together, these instruments shape cross-border data flows by imposing security, risk-management and oversight requirements on entities relying on non-EU providers, with NIS2 and DORA obliging organisations to assess and mitigate risks linked to extra-EU services and DORA enabling restrictions on high-risk dependencies. The Cybersecurity Act further affects such flows through certification schemes that help determine the trustworthiness of foreign ICT products and services (European Commission, 2025j; 2025k; 2025l).

The EU's approach to data regulation has additionally been guided by the Data Strategy from 2020, which focuses on putting people first in developing technology and defending and promoting European values and rights in the digital world. This approach will be updated with the 2025 Data Union Strategy, which intends to increase the availability of data for AI development, simplify EU data rules and strengthen the EU's global position on international data flows (European Commission, 2025h; European Commission, 2025i). The European Commission's proposed Digital Package also aims to simplify data rules by making certain changes to the GDPR and the Data Act (European Commission, 2025o). We have previously suggested a simplification of such rules as a way to promote EU digital trade, building on empirical evidence and industry feedback (National Board of Trade, 2025a; National Board of Trade, 2025b).

3.2 China's regime for cross-border data flows

China's regime for cross-border data flows is built on an integrated, security-centred governance model that seeks to balance national security with economic development (Zhu, 2025). Unlike the EU, which builds its rules around individual rights, China applies a unified framework grounded in cyber sovereignty and the belief that the state

has the authority and responsibility to control data generated within its territory (Creemers, 2022; Erie & Streinz, 2021).

The Chinese leadership views data as a strategic resource central to national security, social stability and technological self-reliance. As such, unauthorised access to data or the infrastructure storing it is viewed as a potential threat to sovereignty (Zhu, 2025). This philosophy is embedded across China's main data-related laws: the Cybersecurity Law (2017), the Data Security Law (2021) and the Personal Information Protection Law (2021). These laws are complemented by a series of implementing measures, and together, they form an interconnected set of requirements that regulate the export of data (Creemers, 2022).

Rather than creating separate protections for personal and non-personal data, China categorises data according to its strategic sensitivity. Regulations affecting cross-border transfers therefore vary depending on the nature of the operator, the scale of the dataset and the perceived risks to national security (Creemers, 2022).

The Cybersecurity Law was the first to establish a legal foundation at national level for China's control of data flows (DLA Piper, 2025). Under the Cybersecurity Law, operators of *critical information infrastructure* must store personal information and "important data" generated in China domestically (Cybersecurity Law, 2017, art. 37). Transferring data abroad requires a security assessment and approval from relevant authorities. Data localisation under the CSL extends not only to where data is stored but also to ownership and control. For example, cloud service providers must ensure that their data centres are physically located in China and that control remains with Chinese entities (Tsoi et al., 2025).

The Data Security Law extends the scope of data regulation by introducing a national classification system under which *all* data (except state secrets and military data) must be assessed for its relevance to national security, economic development and public interest (Data Security Law, 2021, art. 21). Terms such as "important data" and "core data" remain vaguely defined. The absence of clear criteria has consequently led foreign companies to adopt a cautious approach, typically localising data by default to avoid regulatory breaches (European Chamber of Commerce in China, 2025).

The Personal Information Protection Law (PIPL) complements these laws by regulating the collection, processing and transfer of personal data. Modelled in part on the EU's GDPR, it defines personal information broadly as data relating to an identified or identifiable individual and applies extraterritorially to foreign entities handling such data within China (Dai & Deng, 2022). As with the GDPR, one purpose of the law is to protect citizens' information from misuse by private actors and foreign organisations. However, it differs from the GDPR as it preserves extensive state access to data for reasons of public security and national interest (He, 2023). Reflecting this approach, the PIPL establishes strict conditions for cross-border data transfers. Data handlers must obtain individuals' explicit and separate consent and comply with at least one of three mechanisms: a security review led by Cyberspace Administration of China (CAC), certification by an approved institution or the conclusion of a standard contractual agreement with the foreign recipient. (Creemers, 2022).

China's framework for cross-border data flows is constantly evolving, in part because its core legal architecture is intentionally broad and vague in order to preserve regulatory flexibility and state control. This approach is typical of how legal frameworks are implemented in China, where broad legislation is introduced first, followed by a number of implementing measures and regulatory guidelines that seek to, for example, clarify definitions and close gaps in earlier legislation (Cui, 2014). Instruments such as the Measures of Security Assessment for Data Export (2022), the Provisions on Promoting and Regulating Cross-Border Data Flows (2024), the Regulations on Network Data Security Management (2025) and the recent amendments to the Cybersecurity Law illustrate how China regularly updates and recalibrates its data governance system as new regulatory priorities emerge.

China's restrictive regime imposes significant costs on both domestic and foreign companies. Forced localisation, limits on data transfers and extensive government oversight increase compliance costs and disrupt cross-border business operations (Arcesati et al., 2023). Such restrictions can complicate supply-chain management, hinder data-driven innovation and make it difficult to operate integrated global value chains. More broadly, regulatory fragmentation and barriers to data flows undermine the economic benefits of digital connectivity. When companies cannot move data freely or must store it locally, they are often forced to run multiple ICT systems that cannot seamlessly communicate. Maintaining parallel systems increases operational costs and prevents firms from streamlining processes or achieving efficiencies across markets. In many cases, firms must also place both data and personnel in each jurisdiction, reducing their ability to consolidate operations globally or reach scale. The result is not only higher costs and lost business opportunities but also reduced consumer choice and weaker incentives for innovation (National Board of Trade, 2015f; National Board of Trade, 2025c). Such constraints also diminish the competitiveness of China's own economy by discouraging foreign investment and hindering the efficient functioning of global value chains (Xiao & Dong, 2022).

Recognising these constraints, China has begun experimenting with more flexible arrangements. Pilot free-trade zones (FTZs) and free-trade ports are being used to test eased data-transfer rules in selected sectors such as telecommunications, cultural industries and certain cross-border digital services (He, 2025). The Regulations to Promote and Standardize Cross-Border Data Flows (2024) allow FTZs to develop "negative lists" that specify which categories and volumes of data remain subject to government controls, while permitting all other data within designated industries to move overseas with fewer procedures. The lists clarify compliance obligations based on data sensitivity, such as whether it qualifies as "important data" and the volume of personal information involved. However, so far, the pilots remain limited. Only a few FTZs have issued negative lists, with some covering a single industry. In September 2024, The Ministry of Commerce (MOFCOM), the CAC and other agencies expanded this approach by calling for exploration of a national negative list for FTZ cross-border data transfers. This initiative aims to unify fragmented policies among FTZs and could, to a certain extent, improve predictability for firms operating across multiple zones (Huld, 2025).

4 Approaches to data flows in international agreements

World Trade Organization (WTO) rules such as the General Agreement on Trade in Services (GATS) do not address digital trade specifically, but have been deemed to apply equally regardless of whether services are delivered digitally or not. Moreover, the OECD (2025c) notes that WTO agreements which may affect the flow of non-personal data across borders include the Trade Facilitation Agreement (TFA), the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) and the Agreement on Technical Barriers to Trade (TBT). However, the basic rules establishing the WTO were negotiated 30 years ago – before digitalisation took off – while multilateral rules specifically targeting digital trade remain scarce. One notable exception is the recently negotiated plurilateral 'JSI on e-commerce' in the WTO, but that agreement is yet to take legal effect and commitments on cross-border data flows were excluded during its negotiation (National Board of Trade, 2024a).

Global harmonisation of data regulation is currently unrealistic, as countries have widely diverging views on how to balance economic development, privacy, free speech, national security and other concerns that shape the regulation of data flows (National Board of Trade, 2025c; Cory, 2023). In the absence of a global agreement on cross-border data flows, plurilateral initiatives offer avenues for facilitating data transfers. For example, the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) is a voluntary, principles-based framework that facilitates cross-border data flows among Asia-Pacific economies by ensuring that businesses comply with key privacy standards, such as transparency, accountability and security (Christakis, 2024).

The Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108), negotiated under the Council of Europe, is a key source of data-protection principles in Europe, including inspiration for the EU's GDPR. While Convention 108 itself does not directly govern EU cross-border data transfers, its modernised version, Convention 108+, aims to facilitate cross-border data flows with both Parties and non-Parties by ensuring that data protection "travels with the data". Under Convention 108+, the Council of Europe has adopted Model Contractual Clauses (MCCs) that parties can use to lawfully transfer personal data to countries that are not Parties to the Convention, helping to align global safeguards and reduce barriers to international data exchange. These MCCs are designed to complement existing mechanisms (e.g. EU Standard Contractual Clauses) and to support interoperability with partners beyond Europe. MCCs under Convention 108+ offer an additional framework that can be used by data exporters and authorities to support cross-border transfers with external trade partners, particularly where no adequacy decision exists. These clauses aim to foster convergence of protection standards and may reduce trade frictions by providing widely accepted, principled safeguards for international data flows (Council of Europe, 2023; Portnoy & Nauwelaerts, 2023; O'Donoghue & Lysik, 2023).

Another initiative is Data Free Flow with Trust (DFFT), which is currently being developed at the OECD. DFFT aims to promote the free flow of data by creating legal certainty and trust through good governance, clear rules and robust data protections. Since its introduction, DFFT has been adopted by the G7, endorsed by the G20 in the 2019 Osaka Declaration and advanced by the OECD's 2022 Ministerial Declaration on government access to data. The G7 has also supported Japan's proposal for an institutional arrangement for partnership (IAP) to operationalise DFFT, addressing issues such as trusted government data access, regulatory cooperation and data localisation (Christakis, 2024; OECD, 2022a; OECD, 2022c).

In addition to political initiative and support, DFFT benefits from existing legal instruments that have been developed within the OECD. The OECD Privacy Guidelines, which were adopted in 1980 and revised in 2013, outline eight principles for protecting personal data: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability. The guidelines have provided a foundation for governments and businesses to build trust in data ecosystems and remain adaptable to technological changes, and there has been some convergence around these principles (OECD, 2013; OECD, 2022c). The OECD Declaration on Transborder Data Flows from 1985 sets out principles aimed at promoting cross-border data flows by ensuring access to data, enhancing transparency, avoiding unjustified barriers and developing common or harmonised approaches (OECD, 1985).

The OECD Recommendation on Enhancing Access to and Sharing of Data from 2021 is a set of guidelines aimed at fostering the efficient and responsible access to and sharing of data across sectors, nations and disciplines. The recommendation identifies key areas where these principles should be applied to public and private sector data, including research data (OECD, 2021). The Declaration on Government Access to Data Held by Private Sector Entities from 2022 establishes that government access to personal data held by private sector entities must be grounded in a binding legal basis, pursue legitimate aims under the rule of law, require appropriate approvals, ensure secure and restricted data handling, maintain transparency, be subject to independent oversight and provide effective redress (OECD, 2022d). In addition, the OECD works on emerging issues such as privacy-enhancing technologies and practices for finance, banking and health data (OECD, 2016; OECD, 2023a; OECD, 2023b; OECD, 2025a).

4.1 The EU’s approach to international data agreements

The EU is a signatory to the GATS and all other foundational WTO agreements. It is also a participant in the negotiated text for the so-called ‘Joint Statement Initiative (JSI) on e-commerce’ (National Board of Trade, 2024a). Of the relevant plurilateral discussions outside of the WTO, the EU is not party to the CBPR, but is to Convention 108+. Moreover, the EU is participating in the DFFT discussions in the OECD, and the EU’s member states are party to the privacy guidelines and other legal instruments that preceded the DFFT.

Bilaterally, the EU has recently negotiated several modern digital trade agreements, which include binding commitments on cross-border data flows, protection of source

code and rules against localisation requirements for the storage and compute of data. Agreements with such modern digital trade chapters are either in place or being negotiated with countries such as the UK, Chile, Japan, Singapore, the Republic of Korea, Australia and New Zealand (European Commission, 2025n; National Board of Trade, 2024b). It should, however, be noted that the EU always seek a broad privacy carve-out to these commitments, meaning the adequacy decisions that permit cross-border data transfer under the GDPR are important for EU data flows (National Board of Trade, 2025b; Ferracane et al., 2025).

In its International Digital Strategy from 2025, the European Commission places an emphasis on continuing to deepen and expand digital trade agreements, as well as other existing cooperative formats such as Digital Partnerships (European Commission, 2025m). The EU has also begun discussions about deepening digital cooperation with the members of the CPTPP and the Association of Southeast Asian Nations (ASEAN). This is in line with recommendations we have previously made (National Board of Trade, 2025d, National Board of Trade, 2025e). However, it should be noted that the EU's approach to data flow commitments in free trade agreements remains slightly different from those originating in Pacific agreements such as the CPTPP and the Digital Economy Partnership Agreement (DEPA). For example, the EU approach includes a broader carve-out on privacy/data protection.

4.2 China's approach to international data agreements

China's approach to data flows in international trade agreements reflects the same sovereignty-centred logic that underpins its domestic data governance. While China participates actively in global and regional trade discussions, it consistently emphasises that cross-border data flows must remain subordinate to national laws and security priorities (Erie & Streinz, 2021).

China's participation in the WTO Joint Statement Initiative (JSI) on e-commerce illustrates this duality. Although China joined the JSI in 2019, partly to signal support for multilateralism at a time of stress for the WTO, it has consistently argued that data flows must be "orderly" and fully aligned with domestic legislation such as the Cybersecurity Law, Data Security Law and Personal Information Protection Law (Gao, 2020). China's contributions to the JSI tend to highlight consumer protection, trade facilitation and digital inclusion, but its proposals on national security exceptions and content regulation diverge sharply from the demands of some Western countries and other proponents of open data flows (Gao, 2020). This has raised questions about whether China could realistically accept rules that prohibit localisation requirements or ensure unrestricted cross-border movement of information.

China is not party to Convention 108+, the DFFT or the CBPR. Its absence from Convention 108+ and the DFFT is perhaps not unexpected, given that China does not share the human rights approach of the Council of Europe and is not a member of the OECD. By contrast, China is a member of APEC, yet it has shown no interest in joining the CBPR framework (Cory, 2019). Instead, China has sought to advance its own data-governance model. In 2024, President Xi used the APEC meeting in Peru to announce the launch of a "Global Cross-Border Data Flow Cooperation Initiative".

According to the State Council, the initiative “advocates the principles of openness, inclusiveness, security, cooperation and non-discrimination” and aims to “promote efficient, smooth and secure cross-border data flows” (Xinhua, 2024).

China’s regional trade commitments show a pattern of engagement combined with careful protection of its regulatory autonomy and state control. This explains why China participates in the Regional Comprehensive Economic Partnership (RCEP) but still faces significant obstacles to joining the CPTPP.

RCEP includes provisions that in theory prohibit restrictions on the free flow of data and data localisation. RCEP, Article 12.14 (2) and Article 12.15 (2) state that a party shall not 1) prevent a covered person to use or locate computing facilities in that Party’s territory as a condition for conducting business in that Party’s territory, and 2) prevent cross-border transfer of information by electronic means. However, in practice, these commitments are impacted by the fact that RCEP also provides exceptions that allow members substantial domestic policy space. First, the agreement allows for members to impose any measures it considers necessary to achieve “legitimate public policy objectives” or to “protect essential security interests”. Second, such measures cannot be challenged by other members, in practice making the commitments non-enforceable (RCEP, Article 12.14 (3); Article 12.15 (3)). Given China’s restrictive regime for cross-border data flows, its theoretical adherence to RCEP´s general principle of free data flows and prohibition of data localisation relies on the ability to invoke these broad exceptions (Zhang, 2024).

China has applied to join both the CPTPP and the Digital Economy Partnership Agreement (DEPA). Membership in these agreements could increase China’s participation in global digital trade norms, but given China’s restrictions on data flows and data localisation, it would be difficult for China to meet the demands embedded in the CPTPP and DEPA (He, 2022). Although some argue that both agreements contain public policy and security exceptions that might, in principle, accommodate China’s regime, many members remain sceptical (Feldshuh, 2022). Concerns relate not only to China’s restrictive data controls, such as security reviews, volume-based transfer thresholds and the ambiguous category of “important data”, but also to fears that China could exert disproportionate influence on the future interpretation of these agreements (He, 2025).

4.3 EU–China negotiations on data flows

High-level dialogue between the EU and China on digital policy has developed gradually, but often in an inconsistent manner and without significant results. The first structured channel, the Dialogue on Information and Communication Technologies (ICT) was launched in 2009, yet it has not convened since 2020. The same year, however, the two sides introduced the High-level Digital Dialogue, intended to identify priorities in digital transformation and exchange views on emerging technologies such as AI (European Commission, 2020). Although this newer platform has met twice, it has remained largely focused on general digital-policy themes rather than addressing concrete challenges in data governance or cross-border data flows (European Commission, 2023b).

In 2024, the EU and China established a Cross-Border Data Flow Communication Mechanism, marking the first structured format for dialogue on data issues between the two sides (European Commission, 2024q). The initiative stems from a 2023 political agreement and responds to concerns raised by EU businesses in China regarding persistent obstacles to transferring non-personal, industrial data (Walter, 2024). While data-related matters have appeared in earlier exchanges, substantive discussion on easing cross-border data flows has largely been absent. In the CAI negotiations, for instance, references were limited to market access for European cloud services and did not extend to data transfers or broader regulatory barriers (European Commission, 2025q).

The newly introduced mechanism remains narrow in scope, focusing exclusively on non-personal data. According to the Cyberspace Administration of China (CAC), the purpose is to facilitate the exchange of policies and practices related to cross-border data flows and to promote the movement of data between the EU and China (Cyberspace Administration of China, 2024). The EU, in turn, emphasises a more operational objective: identifying practical solutions to the challenges European companies encounter when seeking to comply with Chinese data legislation, including uncertainties surrounding data security requirements (European Commission, 2024).

To date, public communication from both the CAC and the European Commission has remained general and cooperative in tone, focusing on regulatory dialogue rather than concrete commitments. As such, while politically notable, the mechanism has not yet delivered measurable and commercially meaningful improvements to the conditions for transferring non-personal data between the EU and China.

5 Conclusion and policy recommendations

EU–China data flows continue to face structural barriers, which appear unlikely to change. Although dialogue between the EU and China is ongoing, and China has shown interest in international trade agreements with ambitious data flow rules, its approach to data governance remains largely unchanged. Measures such as pilot free-trade zones and negative lists for data transfers offer limited flexibility, but they do not significantly change the core legal framework. Moreover, China's increasing geopolitical assertiveness and state control over data and technology raise concerns for the EU. These include risks related to data access, technology leakage and control over critical digital infrastructure. As a result, the EU has reason to de-risk from China, including when it comes to sensitive technologies and related data.

At the same time, European companies cannot fully withdraw from China, which remains a key market and a growing source of technological innovation. The EU should continue to insist on improvements to Chinese data governance and market access policies, while recognising that more policy integration remains unlikely. In parallel, the EU should therefore focus on managing ongoing differences in a way that minimises economic, operational and strategic costs for European businesses. In that regard, greater attention to practical risk management measures such as privacy-enhancing technologies and encryption could help European companies operating in China and deserves more attention in future research.

Given the challenges in data flows with China – which are likely to persist and could be exacerbated over coming years – the EU should in parallel strengthen digital ties with trusted partners. This includes expanding the EU's network of modern digital trade agreements, seeking ambitious outcomes from the structured dialogue with CPTPP members and working through initiatives such as Data Free Flow with Trust (DFFT). That would increase the EU's digital competitiveness, resilience and economic security while strengthening the incentive for more countries to engage in open and rules-based digital trade.

6 References

Aaronson, S. A., & LeBlond, P. (2018). Another digital divide: The rise of data realms and its implications for the WTO. *Journal of International Economic Law, 21*(2), 245–272. https://doi.org/10.1093/jiel/jgy019

Allen, S. (2024). *The geopolitics of privacy policy: Lessons and implications for the EU*. Institute of International and European Affairs. https://www.iiea.com/images/uploads/resources/The_Geopolitics_of_Privacy_Policy_Lessons_and_Implications_for_the_EU.pdf

Applebaum, A. (2023). *Autocracy, Inc.: The dictators who want to run the world*. Doubleday.

Arcesati, R., von Carnap, K., Groenewegen-Lau, J., & Hmaidi, A. (2023). *Fragmenting cyberspace: The future of the internet in China.* Mercator Institute for China Studies. https://merics.org/en/report/fragmenting-cyberspace-future-internet-china

Arroyo, V., Hess, K., Grünbaum, N., & Ribeiro, G. (2023). *What specific measures could the US, the EU and China take in order to foster and facilitate cross-border data flows?* Sciences Po Digital Governance and Sovereignty Chair. https://www.sciencespo.fr/public/chaire-numerique/wp-content/uploads/2023/09/policy-brief-data-flows.pdf

Atkinson, R. D. (2021). China's innovation mercantilism reduces the rate of global innovation. In S. Kennedy & J. Blanchette (Eds.), *Chinese state capitalism: Diagnosis and prognosis* (pp. 43–48). Center for Strategic and International Studies. https://www.csis.org/analysis/chinese-state-capitalism

Bologa, A. (2025, July 10). *Handing selfies to Beijing: The West's leaky data pipeline to China*. Center for European Policy Analysis. https://www.cepa.org/article/handing-selfies-to-beijing-the-wests-leaky-data-pipeline-to-china/

Bown, C. P. (2024). Trade policy, industrial policy, and the economic security of the European Union. In J. Pisani-Ferry, B. Weder di Mauro, & J. Zettelmeyer (Eds.), *Europe's economic security: Paris report 2* (pp. 135–180). CEPR Press & Bruegel. https://cepr.org/system/files/publication-files/200566-paris_report_2_europe_s_economic_security.pdf

Bradford, A. (2023). *Digital empires: The global battle to regulate technology.* Oxford University Press. https://doi.org/10.1093/oso/9780197649268.001.0001

Cory, N. (2019). *Why China should be disqualified from participating in WTO negotiations on digital trade rules.* Information Technology and Innovation Foundation. https://itif.org/publications/2019/05/09/why-china-should-be-disqualified-participating-wto-negotiations-digital/

Cory, N. (2023). *How the G7 can use "data free flow with trust" to build global data governance.* Information Technology and Innovation Foundation. https://itif.org/publications/2023/07/27/how-g7-can-use-data-free-flow-with-trust-to-build-global-data-governance/

Council of Europe. (2023, June 27). *Model contractual clauses for the transfer of personal data (Module 1)*. https://www.coe.int/en/web/data-protection/-/model-contractual-clauses-for-the-transfer-of-personal-data

Creemers, R. (2022). China's emerging data protection framework. *Journal of Cybersecurity, 8*(1), Article tyac011. https://doi.org/10.1093/cybsec/tyac011

Cui, W. (2014, December 25). *The legal maladies of "federalism, Chinese-style"* [Working paper]. SSRN. https://ssrn.com/abstract=2843308

Cyberspace Administration of China. (2024, August 27). *The China–EU cross-border data flow exchange mechanism was officially established and the first meeting was held* [Press release; in Chinese]. https://www.cac.gov.cn/2024-08/27/c_1726446002030713.htm

Czarnocki, J., Giglio, F., Kun, E., Petik, M., & Royer, S. (2021). *Government access to data in third countries*. European Data Protection Board. https://www.edpb.europa.eu/system/files/2022-01/legalstudy_on_government_access_0.pdf

Czerniawski, M., & Svantesson, D. (2024). Challenges to the extraterritorial enforcement of data privacy law: EU case study. *Stiftelsen Juridisk Fakultetslitteratur, 2*, 127–154. https://doi.org/10.53292/bd1fa11c.f5b3afbe

Dai, J., & Deng, Z. (2022, April 12). *China's Personal Information Protection Law (PIPL)*. Bloomberg Law. https://pro.bloomberglaw.com/insights/privacy/china-personal-information-protection-law-pipl-faqs/

Dikötter, F. (2022). *China after Mao: The rise of a superpower*. Bloomsbury Publishing.

Digital Policy Alert. (n.d.). *Activity tracker*. https://digitalpolicyalert.org/activity-tracker

DLA Piper. (2025, January 20). *Data protection laws in China*. https://www.dlapiperdataprotection.com/index.html?c=CN

Enright, T. (2024, September 10). *Rising challenges for foreign firms in China*. Hinrich Foundation. https://www.hinrichfoundation.com/research/article/us-china/rising-challenges-for-foreign-firms-in-china/

Erie, M. S., & Streinz, T. (2021). The Beijing effect: China's Digital Silk Road as transnational data governance. *New York University Journal of International Law & Politics, 54*, 1–92. https://www.nyujilp.org/wp-content/uploads/2022/02/NYUJILP_Vol54.1_Erie_Streinz_1-91.pdf

European Chamber of Commerce in China. (2023). *European Chamber flash survey: The impact of China's data regulations on European business.* https://www.europeanchamber.com.cn/en/flash-survey-on-impact-of-china-rsquo-s-data-regulations

European Chamber of Commerce in China. (2025). *European business in China: Business Confidence Survey 2025*. https://www.europeanchamber.com.cn/en/publications-archive/1278/Business_Confidence_Survey_2025

European Commission. (2020, September 10). *EU-China: Commission and China hold first High-level Digital Dialogue* [Press release]. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1600

European Commission. (2023a, June 20). *An EU approach to enhance economic security* [Press release]. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3358

European Commission. (2023b, September 18). *EU–China: Commission and China hold second high-level digital dialogue* [Press release]. https://digital-strategy.ec.europa.eu/en/news/eu-china-commission-and-china-hold-second-high-level-digital-dialogue

European Commission. (2024, August 28). *EU and China launch Cross-Border Data Flow Communication Mechanism*. https://policy.trade.ec.europa.eu/news/eu-and-china-launch-cross-border-data-flow-communication-mechanism-2024-08-28_en

European Commission. (2025a). *Legal framework of EU data protection*. https://commission.europa.eu/law/law-topic/data-protection/legal-framework-eu-data-protection_en

European Commission. (2025b). *International dimension of data protection*. https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection_en

European Commission. (2025c). *Regulation (EU) 2023/2854.* EUR-Lex. https://eur-lex.europa.eu/eli/reg/2023/2854/oj

European Commission. (2025d). *Data Act explained*. https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained

European Commission. (2025e). *European Data Governance Act.* https://digital-strategy.ec.europa.eu/en/policies/data-governance-act

European Commission. (2025f). *Data Governance Act explained*. https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained

European Commission. (2025h). *A European strategy for data.* https://digital-strategy.ec.europa.eu/en/policies/strategy-data

European Commission. (2025i). *European Data Union Strategy*. https://digital-strategy.ec.europa.eu/en/policies/data-union

European Commission. (2025j). *NIS2 Directive: Securing network and information systems*. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive?utm_source=chatgpt.com

European Commission. (2025k). *Digital Operational Resilience Regulation (DORA): Implementing and delegated acts*. https://finance.ec.europa.eu/regulation-and-supervision/financial-services-legislation/implementing-and-delegated-acts/digital-operational-resilience-regulation_en

European Commission. (2025l). *Digital Operational Resilience Regulation — Finance.* https://finance.ec.europa.eu/regulation-and-supervision/financial-services-legislation/implementing-and-delegated-acts/digital-operational-resilience-regulation_en?utm_source=chatgpt.com

European Commission. (2025m). *Joint Communication on an International Digital Strategy for the EU*. https://digital-strategy.ec.europa.eu/en/library/joint-communication-international-digital-strategy-eu

European Commission. (2025n). *Digital trade in EU trade agreements*. https://trade.ec.europa.eu/access-to-markets/en/content/digital-trade-eu-trade-agreements-0

European Commission. (2025o). *Digital Omnibus Regulation Proposal*. https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal

European Commission. (2025p). *EU trade relations with China*. https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/china_en

European Commission. (2025q). *EU–China: The agreement explained*. https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/china/eu-china-agreement/agreement-explained_en

European Commission. (2025r). *Commission announces strategic approach to strengthen Europe's economic security*. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2889

European Council. (2023, June 30). *European Council conclusions on China* [Press release]. https://www.consilium.europa.eu/en/press/press-releases/2023/06/30/european-council-conclusions-on-china-30-june-2023/

Ezell, S. J. (2021). *False promises II: The continuing gap between China's WTO commitments and its trade practices*. Information Technology and Innovation Foundation. https://itif.org/publications/2021/07/26/false-promises-ii-continuing-gap-between-chinas-wto-commitments-and-its/

Feldshuh, H. (2022, August 5). China and CPTPP: *Does China's emerging data regime live up to CPTPP principles?* U.S.–China Business Council. https://www.uschina.org/articles/china-and-cptpp-does-chinas-emerging-data-regime-live-up-to-cptpp-principles/

Ferracane, M. F., & van der Marel, E. (2024). Regulating personal data: Data models and digital services trade. *Review of International Economics, 33*(1), 243–264. https://doi.org/10.1111/roie.12735

Ferracane, M., Hoekman, B., van der Marel, E., & Santi, F. (2025). *Digital trade, data protection and the EU adequacy club* (CEPR Discussion Paper No. 19882). CEPR Press. https://cepr.org/publications/dp19882

Ferracane, M. F., & van der Marel, E. (2025). Governing personal data and trade in digital services. *Review of International Economics, 33*(1), 243–264. https://doi.org/10.1111/roie.12735

Fix, J., & Crebo-Rediker, L. (2024). *China's double threat to Europe*. Foreign Affairs. https://www.foreignaffairs.com/china/chinas-double-threat-europe

Gao, H. S. (2020, June 19). *Across the Great Wall: E-commerce Joint Statement Initiative negotiation and China* [Working paper]. SSRN. https://doi.org/10.2139/ssrn.3695382

Greenleaf, G. (2023). Global data privacy laws 2023: 162 national laws and 20 bills. *Privacy Laws & Business International Report,* (181), 1–4. https://ssrn.com/abstract=4426146

Greig, A. (2023, February 17). *Multiple Chinese APTs are attacking European targets, EU cyber agency warns*. The Record. https://therecord.media/multiple-chinese-apts-are-attacking-european-targets-eu-cyber-agency-warns

Haeck, P., Dahl, J., Palmer, D., & Roussi, A. (2024, September 27). *After US, Europe probes Chinese car software*. Politico. https://www.politico.eu/article/europe-looks-to-follow-on-tackling-risk-of-chinese-car-software/

Harrell, P. E. (2025, January 30). *Managing the risks of China's access to U.S. data and control of software and connected technology. Carnegie Endowment for International Peace*. https://www.carnegieendowment.org/research/2025/01/managing-the-risks-of-chinas-access-to-us-data-and-control-of-software-and-connected-technology?lang=en

He, A. (2022, June 20). *Trade deals might induce Beijing to bend on data restrictions*. Centre for International Governance Innovation. https://www.cigionline.org/articles/trade-deals-might-induce-beijing-to-bend-on-data-restrictions/

He, A. (2023). *State-centric data governance in China* (CIGI Paper No. 282). Centre for International Governance Innovation. https://www.cigionline.org/publications/state-centric-data-governance-in-china/

He, A. (2025, May 21). *China's changing approach to digital trade*. Centre for International Governance Innovation. https://www.cigionline.org/articles/chinas-changing-approach-to-digital-trade/

Hillman, J. E. (2020). *The Digital Silk Road: China's quest to wire the world and win the future.* Harper Business.

Huld, A. (2025, October 8). *China data export policy in FTZs: A guide to the negative list approach.* China Briefing. https://www.china-briefing.com/news/china-data-export-policy-ftzs/

Institute for Security and Development Policy. (2018). *Made in China 2025*. https://www.isdp.eu/publication/made-china-2025/

Leonard, J. (2025, October 24). *German firms hand over secrets that China could use for leverage.* Bloomberg Law News. https://news.bgov.com/author/jenny-leonard-20602668

Mejean, I., & Rousseaux, P. (2024). Identifying European trade dependencies. In J. Pisani-Ferry, B. Weder di Mauro, & J. Zettelmeyer (Eds.), *Paris report 2: Europe's economic security* (pp. 45–78). CEPR Press. https://cepr.org/publications/books-and-reports/paris-report-2-europes-economic-security

Miller, C. (2022). *Chip war: The fight for the world's most critical technology.* Scribner.

National Board of Trade. (2024a). *Important but modest success as WTO e-commerce negotiations are finalised*. https://www.kommerskollegium.se/en/analyses-and-seminars/trade-policy-insights/important-but-modest-success-as-wto-e-commerce-negotiations-are-finalised/

National Board of Trade. (2024b). *Analysis: Time for an EU-US digital agreement.* https://www.kommerskollegium.se/en/analyses-and-seminars/trade-policy-insights/time-for-an-eu-us-digital-agreement/

National Board of Trade. (2025a). *Policy brief: Trade policy for the age of AI*. https://www.kommerskollegium.se/en/analyses-and-seminars/trade-policy-insights/policy-brief-trade-policy-for-the-age-of-ai/

National Board of Trade. (2025b). *The GDPR and international trade.* https://www.kommerskollegium.se/en/analyses-and-seminars/trade-policy-insights/the-gdpr-and-international-trade/

National Board of Trade. (2025c). *Navigating cross-border data flows and the GDPR.* https://www.kommerskollegium.se/en/analyses-and-seminars/trade-policy-insights/navigating-cross-border-data-flows-and-the-gdpr/

National Board of Trade. (2025d). *A new era in international trade requires a new rules-based trade coalition*. https://www.kommerskollegium.se/en/analyses-and-seminars/trade-policy-insights/a-new-era-in-international-trade-requires-a-new-rules-based-trade-coalition/

National Board of Trade. (2025e). *Priorities for EU digital trade in a new world order*. https://www.kommerskollegium.se/en/analyses-and-seminars/trade-policy-insights/priorities-for-eu-digital-trade-in-a-new-world-order/

Newman, A. (2020). *Digital policy-making in the European Union*. Oxford University Press.

Organisation for Economic Co-operation and Development. (1985). *OECD declaration on transborder data flows* (OECD Digital Economy Papers No. 1). OECD Publishing. https://doi.org/10.1787/230240624407

Organisation for Economic Co-operation and Development. (2013). *OECD legal instrument: OECD-LEGAL-0188.* https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188

Organisation for Economic Co-operation and Development. (2016). *OECD legal instrument: OECD-LEGAL-0433.* https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0433

Organisation for Economic Co-operation and Development. (2021). *OECD legal instrument: OECD-LEGAL-0463.* https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0463

Organisation for Economic Co-operation and Development. (2022a). *Cross-border data flows*. https://www.oecd.org/en/publications/cross-border-data-flows_5031dd97-en.html

Organisation for Economic Co-operation and Development. (2022b). *Going digital to advance data governance for growth and well-being*. https://www.oecd.org/en/publications/going-digital-to-advance-data-governance-for-growth-and-well-being_e3d783b0-en.html

Organisation for Economic Co-operation and Development. (2022c). *Fostering cross-border data flows with trust*. https://www.oecd.org/en/publications/fostering-cross-border-data-flows-with-trust_139b32ad-en.html

Organisation for Economic Co-operation and Development. (2023a). *Data portability in open banking*. https://www.oecd.org/en/publications/data-portability-in-open-banking_6c872949-en.html

Organisation for Economic Co-operation and Development. (2023b). *Open finance policy considerations*. https://www.oecd.org/en/publications/open-finance-policy-considerations_19ef3608-en.html

Organisation for Economic Co-operation and Development. (2025a). *Privacy and data protection*. https://www.oecd.org/en/topics/privacy-and-data-protection.html#related-publications

Organisation for Economic Co-operation and Development. (2025b). *Privacy-enhancing technologies*. https://www.oecd.org/en/topics/privacy-enhancing-technologies.html

Organisation for Economic Co-operation and Development. (2025c). *A preliminary mapping of measures affecting the cross-border flow of non-personal data*. https://www.oecd.org/en/publications/a-preliminary-mapping-of-measures-affecting-the-cross-border-flow-of-non-personal-data_0825c57c-en.html

Organisation for Economic Co-operation and Development & World Trade Organization. (2025). *Economic implications of data regulation: Balancing openness and trust.* https://www.wto.org/english/res_e/booksp_e/data_regulation_e.pdf

Pisani-Ferry, J., Weder di Mauro, B., & Zettelmeyer, J. (2024). *How to de-risk European economic security in a world of interdependence*. Bruegel. https://www.bruegel.org/policy-brief/how-de-risk-european-economic-security-world-interdependence

Rudd, K. (2022). *The avoidable war: The dangers of a catastrophic conflict between the US and Xi Jinping's China*. PublicAffairs.

Sapir, A., & Mavroidis, P. C. (2021, April 29). *China and the WTO: An uneasy relationship*. VoxEU. https://cepr.org/voxeu/columns/china-and-wto-uneasy-relationship

Tardell, M. (2023). *Restructuring for self-reliance: The implications of China's science and technology overhaul*. Nationellt kunskapscentrum om Kina. https://kinacentrum.se/publikationer/restructuring-for-self-reliance-the-implications-of-chinas-science-and-technology-overhaul/

The Economist. (2026, January 15). *Geopolitics is warping multinationals' commercial decisions*. https://www.economist.com/briefing/2026/01/15/geopolitics-is-warping-multinationals-commercial-decisions

The State Council of the People's Republic of China. (2024, November 21). *Chinese economy progressing well in pursuit of 2024 targets.* https://english.www.gov.cn/news/202411/21/content_WS673f3c4cc6d0868f4e8ed4b5.html

Tsoi, V., Yan, Y., Seow, T.-Y., Tang, P., & An, R. (2025, May 19). *Breaking barriers: China's new IDC open-up opportunities for foreign investors.* White & Case LLP. https://www.whitecase.com/insight-alert/breaking-barriers-chinas-new-idc-open-opportunities-for-foreign-investors

United States Trade Representative. (2018). *2018 Special 301 report.* https://ustr.gov/sites/default/files/files/Press/Reports/2018%20Special%20301.pdf

Walter, A. (2024, August 30). *EU and China to tackle challenges in cross-border transfer of non-personal data*. Pinsent Masons. https://www.pinsentmasons.com/out-law/news/eu-china-tackle-challenges-cross-border-transfer-non-personal-data

Wong-Leung, J., Gaida, J., Robin, S., & Cave, D. (2023). *Critical technology tracker.* Australian Strategic Policy Institute. https://www.aspi.org.au/report/critical-technology-tracker

Xiao, Y., & Dong, D. (2022, November). *What do China's data export regulations mean for its trade competitiveness?* World Economic Forum. https://www.weforum.org/stories/2022/11/china-data-export-regulations-threaten-trade-competitiveness/

Yun, H. (2025). China's data sovereignty and security: Implications for global digital borders and governance. *Chinese Political Science Review, 10,* 178–203. https://doi.org/10.1007/s41111-024-00269-9

Zhang, Y. (2024). *Personal data protection in China*. Brussels Privacy Hub. https://brusselsprivacyhub.com/wp-content/uploads/2024/04/Personal-Data-Protection-in-China.pdf

Zhu, X. (2025). Conflict and coordination between data sovereignty and digital trade liberalisation: An analysis of cross-border data flow policies in China and the EU. *Studies in Law and Justice, 4*(5), 56–65. https://doi.org/10.56397/SLJ.2025.10.07

Sammanfattning på svenska
Summary in Swedish

Denna rapport undersöker förutsättningarna för gränsöverskridande dataflöden mellan Europeiska unionen (EU) och Kina. Analysen sker mot bakgrund av ökat fokus på ekonomisk säkerhet och länders olika sätt att reglera data, som påverkar utrikeshandeln.

Rapporten visar att den bilaterala dialogen om datastyrning har intensifierats. Bland annat har parterna inrättat en dialog om icke-personuppgifter. Trots detta kvarstår stora skillnader mellan EU:s och Kinas regelverk. EU tillämpar ett villkorat och rättighetsbaserat system för dataöverföringar, medan Kinas modell bygger på cybersuveränitet och nationell säkerhet. Kinas rättsliga ramverk innebär omfattande begränsningar för dataöverföringar och ger staten långtgående tillgång till data. Detta skapar rättslig osäkerhet, höga kostnader för regelefterlevnad och praktiska svårigheter för europeiska företag som är verksamma i Kina.

Mot denna bakgrund bedömer rapporten att en djupare samordning av lagstiftningen mellan EU och Kina är osannolik. EU:s politik bör därför i stället inriktas på att hantera skillnaderna på ett sätt som minskar de ekonomiska, operativa och strategiska kostnaderna för europeiska företag. Det kan till exempel handla om att använda praktiska riskhanteringsåtgärder, såsom kryptering, för företag med verksamhet i Kina. Samtidigt bör EU stärka samarbetet med betrodda partnerländer. Det kan ske genom att utöka nätverket av moderna digitala handelsavtal och digitala partnerskap samt genom initiativ som Data Free Flow with Trust (DFFT), som syftar till att möjliggöra säkra dataflöden med pålitliga länder. På så sätt kan EU värna sin ekonomiska säkerhet och konkurrenskraft och samtidigt främja en öppen och regelbaserad digital handel.

The National Board of Trade Sweden is the government agency for international trade, the EU internal market and trade policy. Our mission is to facilitate free and open trade with transparent rules as well as free movement in the EU internal market.

Our goal is a well-functioning internal market, an external EU trade policy based on free trade and an open and strong multilateral trading system.

We provide the Swedish Government with analyses, reports and policy recommendations. We also participate in international meetings and negotiations.

The National Board of Trade, via SOLVIT, helps businesses and citizens encountering obstacles to free movement. We also host several networks with business organisations and authorities which aim to facilitate trade.

As an expert agency in trade policy issues, we also provide assistance to developing countries through trade-related development cooperation. One example is Open Trade Gate Sweden, a one-stop information centre assisting exporters from developing countries in their trade with Sweden and the EU.

Our analyses and reports aim to increase the knowledge on the importance of trade for the international economy and for the global sustainable development. Publications issued by the National Board of Trade only reflect the views of the Board.

The National Board of Trade Sweden, February 2026, ISBN: 978-91-89742-81-9

Kommerskollegium
National Board of Trade Sweden

Box 6803, S-113 86 Stockholm, Sweden
Phone +46 8 690 48 00
E-mail registrator@kommerskollegium.se
www.kommerskollegium.se