**How do the European Union's GDPR and China’s PIPL regulate cross-border data flows?**

**Elena Fernández-Novel Escobar**

International Policy Review, IE University, Madrid, Spain

Advocacy & Litigation, Bocconi University, Milan, Italy

E-mail: efernandezno.ieu2022@studemt.ie.edu

Published: 27th of January, 2025

**Abstract**

The growing prominence of digitalisation has made data privacy law a critical point for cross-border data flow regulation. This paper will present a comparative analysis of the European Union’s General Data Protection Regulation (GDPR) and China’s Personal Information Protection Law (PIPL), both foundational regulations aiming to protect data privacy but grounded in different political and legal philosophies. From the GDPR’s perspective, individual rights and transparency are at the core of its democratic framework, while the PIPL prioritises state sovereignty and security under an authoritarian governance model. Thus this research paper will examine these key divergences within data localisation mandates, legal bases, consent requirements and enforcement practices, demonstrating the legal complexities posed by international data transfers. Case law and regulatory developments will be used to underscore how these discrepancies act as a barrier to international trade and privacy protection. The paper will propose a harmonised policy framework  drawing on existing international agreements, looking for a balance between security, privacy and economic collaboration. Such framework will emphasise the necessity of international cooperation in data governance on a global scale.

Keywords: GDPR, PIPL, data privacy, cross-border data flow, policy framework

**1. Introduction**

The arrival and continuous development of the digital era has converted information into one of the most significant values in today’s economy, exerting pressure on data  protection legislation. The reliance on cross-border data flows by its users is being challenged by the lack  of protection within personal information, hence different  countries have adopted rigorous data privacy policies to address the issue. Europe’s GDPR and China’s PIPL both strive for high standards of protection, however, they lie on completely different legal and ideological bases, resulting in operational barriers for economic entities working across their jurisdictions.

China’s PIPL,  based  on the roots of an authoritarian government, emphasises state control and national security. In other words, it provides greater access to governmental authorities and more strict requirements for data localization. China’s approach as stated in Article 42 of the PIPL,

 “*For any overseas organization or individual whose personal information processing activities damage the personal information rights and interests of citizens of the People’s Republic of China, or endanger the national security or public interests of the People’s Republic of China, the State cyberspace administration may include such overseas organization or individual in the list of restricted or prohibited provision of personal information, announce the same, and take measures such as restricting or prohibiting the provision of personal information to such overseas organization or individual.”[[1]](#footnote-0),*

focuses on the state’s role in safeguarding user’s information within its borders, ensuring that data flows are subject to national oversight. By contrast,  the EU's GDPR is grounded on democratic values of individual rights, transparency, and accountability. Prioritising individuals to control their personal data, their regulation looks to limit both private and governmental interference unless based on lawful grounds, which would in turn, protect and defend privacy and autonomy of EU users. These foundational divergences present the central tension of both frameworks; while the PIPL centers on securing state interests within data regulation, the GDPR  upholds personal freedoms and user privacy as a fundamental right that should, above all, be respected.

This paper will undermine how the European Union’s GDPR and China’s PIPL regulate cross-border data flows by exploring their historical as well as political contexts. Thus, analysing their impact on data localisation, consent requirements and legal bases for data processing. Although both frameworks aim to protect data privacy, their contrasting basis in democratic against authoritarian principles create substantial complications of the interchange of data. This paper argues that these disparities not only set a barrier that limits international data governance, but also the need for a balanced regulation which could hold both, individual’s privacy and national interests, hence fostering smoother interchange of information between the EU and China.

**1I. Background and Context**

EU’s GDPR,  intiated on the 25th of May 2018[[2]](#footnote-1), builds on a long-standing tradition of privacy rights within the European Union. Considering the in the post-World War II context, it prioritises protecting individual freedoms against state surveillance. When looking at Article 8 of the European Convention on Human Rights it states that the right to privacy remains essential for individual freedom.[[3]](#footnote-2) After the wrongs suffered, these privacy regulations aimed to establish a legal framework where citizens could employ control over their own personal data and resist unjustified government or companies’ misuse. As Article 1 in the GDPR points; *“This regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data”.[[4]](#footnote-3)*

Examples of Nazi and fascist uses of personal information, were collected through secret police forces includiing the Gestapo[[5]](#footnote-4), presenting an urgent need for robust legal protections to protect citizen’s privacy. Additionally, during the Cold War, communist regimes in Eastern Europe institutionalised mass surveillance as a tool for political control, with the Stasi in East Germany embodying state intrusion into citizens’ privacy.[[6]](#footnote-5) We can see further developments during the late 20th and early 21st Centuries highlighting privacy threats beyond state surveillance. For instance, the 2008 global financial crisis, exposing significant corporate misuse of personal data, and eroding public trust in private entities.[[7]](#footnote-6) Furthermore, the European Union’s growth and rise of the Digital Single Market constructed the need for consistent ans stable privacy standards across member states to ease cross-border trade while protecting individuals' data rights.[[8]](#footnote-7)

As the GDPR was created in a unified manner across member states, it thus extended Europe’s rights-based focus to the digital age, centering on consent, authorization, data minimisation, and transparency.

Placed under democratic values, prioritisation of transparency, accountability and individual autonomy is addressed in the GDPR. EU's commitment to uphold human rights by protecting individual freedom from both corporate and governmental influence, it grants data subjects, rights over their personal information, covering rights to access, rectify, delete, and object to processing on grounds of legitimate interest.[[9]](#footnote-8) Hence, we could state that EU's right-based approach draws as a core philosophy under the GDPR, ensuring data protection as a prerequisite for individual dignity and trust.[[10]](#footnote-9)

China’s Personal Information Protection Law, initiated on November 1st of 2021[[11]](#footnote-10) is a legal code approved by the Standing Committee of the National People’s Congress, applied across the country and standing  on top of China’s  legal hierarchy.[[12]](#footnote-11) It lies under an authoritarian approach where national security and control are prominent over  individual privacy rights. These privacy laws were enacted to complement the nation’s governmental surveillance systems to maintain social  order. It can be argued that it was part of  a strategy for the State or political party to position itself as a notable player in the global digital economy aligning or exceding international expectations.[[13]](#footnote-12) Reported cases about data misuse by Chinese citizens showed the need for government action via the PIPL to show a commitment to address the issues. During July 2022 a data breach with the Shanghai National Police Database, it is claimed that a hacker had collected personal information on one billion Chinese citizens.[[14]](#footnote-13) Although the PIPL covers provisions for individual rights like the right to access, and delete personal data, it also establishes strict data localization requirements where government approval is necessary for cross-border data transfers.[[15]](#footnote-14) In fact, this is underlined in Article 40 of the PIPL mentioning that; *“If it is indeed necessary to provide such information and data to overseas parties, it shall be subject to the security assessment organized by the State cyberspace administration; if laws, administrative regulations, or the provisions of the State cyberspace administration provide that the security assessment is not required, such provisions shall prevail.”* [[16]](#footnote-15)

China’s PIPL is influenced by historical and political developments shaping its approach to data governance. The 1980s economic reforms under Deng Xiaoping[[17]](#footnote-16) meant China’s integration into the global economy, representing a phase of modernisation, globalisation and economic liberalisation. It opened China’s frontiers to  foreign investments, multinational corporations, and international communication networks, driving technological advancements but meaning a greater need for the population’s privacy protection.[[18]](#footnote-17) Unregulated data flows, cyberattacks and misuse of sensitive information was now possible, underscoring the absence of a comprehensive legal framework to address the issue.

The 1989 Tiananmen Square Protests was a crucial moment where China’s approach to data governance was affected. The government’s use of surveillance technologies, including photographic evidence and informant networks, to identify and suppress pro-democracy dissent, reinforced the importance of state-driven information regulation as a tool for maintaining public order and stability under an authoritarian regime.[[19]](#footnote-18) It meant a precedent for prioritising national security and sovereignty, making state surveillance a core value under China’s regulation philosophy. By the 2008 Beijing Olympics, international scrutiny of China’s cybersecurity measures highlighted the dual demand to support domestic data protection while presenting itself as a credible state under the international sphere.[[20]](#footnote-19)

Subsequently, the development of mass surveillance programs, like the Social Credit System[[21]](#footnote-20) and facial recognition, showcased China’s use of data-driven governance while raising significant concerns over privacy violations. Notorious data breaches like  the 2016 Alibaba Taobao breach[[22]](#footnote-21) and the 2020 Weibo leak[[23]](#footnote-22), are examples that meant an urgent need for stricter data protection regulation. Additionally, geopolitical tensions as for instance with the United States, was illustrated by trade conflicts and controversies surrounding Huawei and TikTok. Reinforcing the importance of securing national data sovereignty.[[24]](#footnote-23)

China’s centralised structure, empowers state authorities to access personal data for purposes that agree with the “public interest” or national security uses. It could be argued that this term lacks of a precise definition in China’s legal framework. However, it is broadly used and interpreted to justify restrictions or requirements on data transfers. It introduces legal uncertainties, leaving room for open enforcement, which could conflict with the principles of legitimate neccesity and proportionality under International Law. Nevertheless, when looking at China’s political philosophy, which positions individual freedoms as a secondary aspect behind state sovereignty, remains consistent with these localisation mandates and access rights granted to government agencies. Reflecting a view where personal information, should be controlled by the state to avoid external influences in internal matters, thus prioritising national interests.[[25]](#footnote-24)

**1II. Data Localization Requirements against Free Trade Data Flow**

Europe’s GDPR prioritises free flow of data under specific conditions, demonstrating its commitment to privacy and a smooth digital international economic environment. Free data transfers are permitted within the European Economic Area (EEA).[[26]](#footnote-25) However, when data is transferred to a country outside the EEA, specific provisions apply. These provisions ensure that personal data transferred outside the EEA is protected at a level equivalent to the protection it receives within the EEA, as required by the GDPR.[[27]](#footnote-26)

First, the “basic processing principles” covered under the GDPR shall be respected, as well as accounting the activity under a contract, even if the recipient is acting as a data processor actor.[[28]](#footnote-27) These transfers will take place under the basis of an adequate level of protection where areas like rule of law, respect for human rights, fundamental freedoms, the existence of independent data protection authorities and/or international commitments are assessed. Once a country is addressed as ‘adequate’ data transfers can take place to organisations or corporations outside this non-EEA country. Hence, ‘adequate’ non-EEA countries remain comparable to  those in the EEA. However, there is the possibility for adequacy decisions to cover a limited area instead of the country as a whole, or even limited to a specific sector. Until  today’s date, the adequacy decisions  adopted by the EC are; Andorra,  Argentina,  Canada (for commercial organisations), Faroe Island, Guernsey,  Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, UK, US (for commercial organisations participating in the EU-US Data Privacy Regulation Framework), and Uruguay.

Andorra, Argentina, Uruguay and New Zealand became clear examples in which heir legal frameworks meet the EU’ strict criteria for data protection. They have been deemed adequate through rigorous and constant assessments.[[29]](#footnote-28)

Canada’s adequacy decision applies to commercial organisations under the Personal information Protection and Electronic Documents Act (PIPEDA). This law covers how businesses shall collect, use and disclose personal information in commercial activities, ensuring compliance with GDPR’s principles.[[30]](#footnote-29)

Japan’s adequacy decision involved the adoption of supplementary rules under its Act on the Protection of Personal Information (APPI), addressing differences with the GDPR (like stricter limits on data sharing and enhanced individual rights).  Japan further committed for cooperation with the EDPB.[[31]](#footnote-30)

After Brexit, the UK received an adequacy decision as it retained GDPR principles under its Data Protection Act 2018. It ensures  uninterrupted data flows within the UK and the EEA, being subject to periodic reviews.[[32]](#footnote-31)

The EU-US Data Privacy Framework (DPF) replaced the Privacy Shield Agreement (PSA) as it was invalidated by the Court of Justice of the EU in the Schrems II decision in July 16, 2020. Under the reason of not adequately protecting EU’s citizens personal data from US’ intelligence agencies. The last framework undertakes robust safeguards against government access to personal information as well as enforceable rights for EU citizens via redress mechanisms.[[33]](#footnote-32)

Faroe Islands, Guernsey, Isle of Man and Jersey while are not sovereign states, they have established legal frameworks which assure an equivalent level of user’s data protection.[[34]](#footnote-33)

For countries lacking adequacy status, the GDPR regulation allows data transfers through Standard Contractual Clauses (SCCs). Held under Art 46(2)(c) GDPR[[35]](#footnote-34), these are a set of standard contracts that allow data exporters to proportion appropriate safeguards for the interchange of personal information.  They are legally binding mechanisms for data transfer to countries which lack the adequacy decision. These clauses impose enforceable obligations on both data importers and exporters to ensure compliance with GDPR’s principles. They act as contractual safeguards, securing the rights of data subjects are protected and offering an alternative framework aligning with EU’s standards.[[36]](#footnote-35)

Additionally, Binding Corporate Rules (BCRs) listed under Art 47 GDPR[[37]](#footnote-36) are another option which ensures adequate levels of protection within the share of data within various companies located inside and outside the EEA. These are aimed for multinational groups of companies which normally carry large exchanges of data. These achieve to balance individual privacy rights in times of a globalised economy, as it enables legal pathways to operate internationally at the same time as complying with European data protection standards.

On the other hand,  the PIPL demands strict data localization especially for ‘critical information infrastructure operators’ and data that the government perceives as ‘sensitive’. Article 28 of the PIPL refers to sensitive personal information,  to the data that, if misused, can infringe upon personal dignity ot harm personal or property safety. This includes biometric data, religious beliefs, identities, medical health data, financial accounts, location tracking, among others.[[38]](#footnote-37)

Security assessments are required for international data transfers, as well as explicit government approval. Non-compliance with these measures includes fines  of of up to 5% of annual revenue, RMB 50 million or even suspension of operations.[[39]](#footnote-38) Sensitive data is measured under the Data Security Law (DSL) where information is classified based on its significance to national security, economic stability, and public interest. Furthermore, the third core law for China’s data protection is the Cybersecurity Law (CSL). It obligates network operators and CIIOs to store personal data collected on servers within Chinese borders.[[40]](#footnote-39) Thus,  PIPL’s authorization path for transfers outside China remains large, requiring explicit consent under controlled conditions. Mandating local information storage limits foreign access to Chinese data, generating operational challenges for multinational companies  that must adapt to China’s specific regulatory landscape, specially those businesses that rely their activity on data-driven services.[[41]](#footnote-40)

Therefore, we could say that GDPR’s mechanisms for the exchange of information outside the European Economic Area, at least aim to facilitate international  commerce as it allows corporations to manage, organize and distribute data across jurisdictions with standardised frameworks. This particularly benefits multinational companies which depend on data-sharing networks in order to engage with their delivered product or services. Differently, strict localization and conditions for data transfers held under China’s PIPL are imposing further costs to these corporations which find with the obligation to build and maintain local data infrastructure inside Chinese borders, as well as explicit government approval to export data abroad. For instance in 2017, Apple Inc, was the first multinational company to construct a data center to comply with China’s Data localization law. They invested one billion in partnership with Guizhou Cloud Big Data (GCBD) to construct it in Guizhou province.[[42]](#footnote-41)

The Standing Committee of the National People’s Congress (NPC) of China defends that data localisation achieves national security as it ensures that sensitive personal information is protected from external governments or businesses that could exploit it for economic or political interests.[[43]](#footnote-42) As stated in Art 1, General Provisions (DSL);

“*This Law is enacted for the purpose of regulating data processing, ensuring data security, promoting development and utilization of data, protecting the lawful rights and interests of individuals and organizations, and safeguarding the sovereignty, security, and development interests of the state”.[[44]](#footnote-43)*

 It could be  argued that the free flow of data approach adopted by the EU risks misuse or unauthorised access to personal information, as it exists the possibility that external recipients countries or organisations may cover privacy laws not as strict or robust.[[45]](#footnote-44)

However, we should take into account unintended economic scenarios including trade barriers and decreased innovations data such strict localisation could pose. As mentioned by Jianqiang Li PhD at the theoretical computer science group of Pennsylvania State University in his investigation on China’s PIPL and Impact on International Data Transfers[[46]](#footnote-45) “data localisation can inhibit competitions, reduce productivity, and increase prices for local consumers”. In addition, as previously mentioned the GDPR holds recipient subjects accountable via specific legal provisions and mechanisms like the SCCs and BCRs, requiring strict contractual protections including the external sharing of data outside the EU. It aims to offer a pragmatic regulatory framework that focuses on individual privacy while considering the operational reality of a digital globalised economy.

**IV. Consent, Legal Basis and Data Subject Rights**

As previously noted, EU’s GDPR reaches a flexible regulatory framework through distinct legal basis beyond consent; these include contractual necessity, compliance with legal obligations, and public interest.[[47]](#footnote-46) Article 6(1)(c) GDPR[[48]](#footnote-47) states that businesses or organisations should process personal information when necessary to fulfil a legal obligation, covering those mandated by the EU or member state law. It is often used in cases for financial reporting or court orders. Thus,  it allows organisations to collect the data when consent  is unfeasible while achieving lawful compliance. Furtheron, Article 6 (1)(b)[[49]](#footnote-48) allows personal data processing necessary to fulfil contractual obligations, like a purchase order or offering a service, hence essential for service provider organisations. Additionally, Art 6(1)(f)[[50]](#footnote-49) allows data collection based on legitimate interests, always that such interests do not override fundamental rights and freedoms of the data subject. For this reason, businesses must document a balancing test to demonstrate that their legitimate interest protect and respect subject rights.

Aligning with the fundamental principle of *‘Empowering Data Subjects’[[51]](#footnote-50)*, the GDPR extends rights to data subjects which include access, rectification, eradication and objection, enhancing them with an absolute control over their information.[[52]](#footnote-51)

Contrastingly, the PIPL prioritises explicit consent as the first step for cross-border data transfers. These mean a government-led security evaluation or explicit consent from authoritative subjects, as stated in Article 39 PIPL

*“Where a personal information processor provides personal information for any party outside the territory of the People's Republic of China, the processor shall inform the individuals of the overseas recipient's name and contact information, the purposes and means of processing, the categories of personal information to be processed, as well as the methods and procedures for the individuals to exercise their rights as provided in this Law over the overseas recipient, etc., and shall obtain individual's separate consent”[[53]](#footnote-52);*

highlighting the state’s approach of centralised control. Even though the PIPL includes provisions like contractual necessity or subjects’ rights like access, rectification and elimination, they remain limited to the nation’s security and control, where Chinese sovereignty prevails  over subjects’ autonomy.[[54]](#footnote-53) Cases involving “sensitive personal information”, are described as data that could endanger the safety of persons, property, or mean discriminatory or psychological harm.[[55]](#footnote-54) For it, consent should be clear, valid and voluntarily given, portraying its purpose and data processing methods.

Similarly to EU’s GDPR, China’s PIPL permits data processing if it's needed for the fulfilment of a contract with the subject. Furthermore, personal information can be processed if its purpose complies with a legal obligation, or for purposes of public interest matters. In the case of the threat of public health, life safety or property security, data processing is allowed without consent. Nevertheless, it is tight to a constrained procedure,  being a rare case to occur.

Furthermore, data subject request access to eliminate, edit or correct their information,  but in difference with the GDPR, it must be accepted by the government, complying  with the state’s governmental and social stability.[[56]](#footnote-55)

This heavy reliance on explicit governmental consent and approval limits processing options generates barriers for multinational organisations. They  create operational additional costs and complications, as these companies find the need to adapt to China’s specific regulatory framework, requiring localised storage and protocols.

**V. Regulatory Enforcement and Penalties**

The GDPR assures compliance through a network of independent supervisory authorities (SAs), which are situated in each EU’s member states. As they define, *“The EDPS is an independent supervisory authority responsible for ensuring that EU institutions and bodies comply with data protection law when processing personal data”[[57]](#footnote-56)*. In Spain for instance, it is  the Agencia Nacional de  Protección de Datos (AEPD)[[58]](#footnote-57) or in Italy the Garante per Protezione dei Dati Personali (GPDP)[[59]](#footnote-58), which function independently but attach to the European Data Protection Board (EDPB) to assess their compliance with EU’s GDPR.[[60]](#footnote-59)

Penalties addressed in Art 83[[61]](#footnote-60) for non-compliance of the GDPR are divided into two tiers. Firstly, the less severe ones which result in a fine of maximum 10 million euros or 2%  of the organisation’s annual revenue, whichever option is higher. The second tier, includes fines up to  20 million euros or 4% of the business’ annual revenue, again the one which is greater. These types of penalties violate basic principles for processing, conditions for consent, data subject rights or share information to IOs or recipient countries lacking an adequate level of data protection.[[62]](#footnote-61)

Independent SAs contribute to the decentralised system of the GDPR considering individual legal situations while adhering to a standardised framework. The biggest penalty the GDPR imposed became binding in April 2023 for Meta. They received a fine of 1.2 billion euros settled on the cause of SCCs since 2020. The infringement was characterised by a ‘systematic, repetitive, and continuous’ massive data exchanges across the globe.[[63]](#footnote-62) Their decentralised and coordinated organisation allow supervision to tailor local enforcement while maintaining EU’s standardisation requirements. It sets high expectations for compliance as the assessment procedures remain clear and transparent. Strict fines incentivize companies to respect the GDPR without putting into risk their operational revenues.

China’s PIPL is centralised to the Cyberspace Administration of China (CAC), who has the role of executing and interpreting the PIPL, as well as realising investigations and establishing penalties for non-compliance. Businesses can receive fines up to 50 million RMB  or 5% of annual revenue.[[64]](#footnote-63) This would mean infringements like unauthorised cross-border exchanges of sensitive personal data, or inability to act in accordance with localisation conditions. However, there is the possibility of additional sanctions like the suspension of operating licences,  restriction of operations, or blacklisting businesses to remove them from the Chinese market.[[65]](#footnote-64)

This CAC’s ability poses an additional risk for companies, specially foreign firms that should limit their operations for market access, implementing China-specific compliance protocols which can contradict with international transfer practices. That is to say,  organisations whose activity takes place over both China and the EU would require a customised independent compliance framework, increasing their operational costs.

However, progress had been made in March 2024, when the CAC issued new provisions relieving limitations on cross-border data transfers. It states that cross-border exchanges for non-personal or ‘non-important’ data, and specific categories like cross-border e-commerce and emergency health situations, are exempt from the previously mentioned security measures and contractual obligations under PIPL. These provisions aim to decrease multinational’s burden even though CIIOs and shares within ‘important data’ still remain stringent under China’s state control.[[66]](#footnote-65)

**VI. Conclusion**

This research paper analyses EU’s GDPR and China’s PIPL privacy regulations, influenced by their corresponding historical and political contexts. China being an authoritarian regime focuses on state sovereignty, state security and centralised organisation for the regulation of cross-data transfers. On the other hand, the EU, rooted in the post-World War II situation, prioritises the protection and respect of individual rights, democratic philosophy and transparency. Hence empowering citizens with their fundamental right of privacy. Foundational political philosophies completely shape both frameworks, leaving the debate between a state-controlled model versus a rights-based model.

Both approaches have a distinct significant impact on international trade, mainly for multinationals whose operational activities depend on the massive transfer of personal information. GDPR’s inclusion of legitimate interests or contractual necessity permits these businesses to process data under clear and strict conditions, increasing flexibility and facilitating compliance of such regulation within Member States. Heavy reliance on explicit consent and approval by the central government held under the PIPL, causes on the other hand, barriers for cross-border operations such as need for specific infraestructures under the state of China (increasing individual multinationals’ operational costs).

Regarding the enforcement structures, the GDPR incorporates stringent fines and procedures of transparency increasing incentives for multinationals to adopt privacy protection measures complying within all member states. However, China’s PIPL framework subjects businesses to enforcement standards lining with national interests,  posing a barrier for firms operating within both the PIPL and GDPR.[[67]](#footnote-66)

As digital globalisation continues to  expand, regulatory differences pose a significant barrier for multinationals. Compliance requirements, legal bases and enforcement structures are key areas of compliance on which more divergences are present within both frameworks,  showing the need for mutual privacy protection policies. Mutual adequacy agreements, international outlines, or standarized contractual clauses which respect the essential goals of each government would be key to eradicate such barriers. In fact, the EU-US Data Privacy Framework serves as a prominent example of bilateral agreement designed to facilitate transatlantic data transfers. It establishes binding commitments by US authorities to ensure that access to EU by US government agencies is subject to clear limitations. It also provides for independent oversight mechanisms an robust avenues for redress, ensuring compliance with the GDPR. Similarly, the 2019 Japan-EU mutual adequacy decision enables reciprocal data flows while safeguarding privacy. Japan adopted supplementary rules under its Act on the Protection of Personal Infomration (APPI), addressing the gap between both framework guaranteeing high level of data protection and promoting cooperation between both jurisdictions.[[68]](#footnote-67)

Hence, an expanded-looking data policy  would consider both the rights-based framework of the European Union and state-sovereignty focus of China. For this, a collaborative network would be crucial to ensure that needs and values  from each jurisdiction are covered.

**VII. Bibliography**

“1.2 Billion Euro Fine for Facebook as a Result of EDPB Binding Decision.” 1.2 billion euro fine for Facebook as a result of EDPB binding decision | European Data Protection Board, May 22, 2023. <https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en>.

“Agencia Española de Protección de Datos: AEPD.” Agencia Española de Proteccion de Datos. Accessed January 3, 2025. <https://www.aepd.es/>.

“Analysis of the Highlights of the Personal Information Protection Law: Deloitte China: Risk Advisory.” Deloitte China, September 30, 2021. <https://www2.deloitte.com/cn/en/pages/risk/articles/personal-information-protection-law-analysis.html>.

“Analysis of the Highlights of the Personal Information Protection Law: Deloitte China: Risk Advisory.” Deloitte China, September 30, 2021. <https://www2.deloitte.com/cn/en/pages/risk/articles/personal-information-protection-law-analysis.html>.

“Analysis of the Highlights of the Personal Information Protection Law: Deloitte China: Risk Advisory.” Deloitte China, September 30, 2021. <https://www2.deloitte.com/cn/en/pages/risk/articles/personal-information-protection-law-analysis.html>.

“Apple to Build First China Data Center to Comply with Law.” BloombergNEF, July 12, 2017. <https://about.bnef.com/blog/apple-to-build-first-china-data-center-to-comply-with-local-law/>.

“Art. 1 GDPR – Subject-Matter and Objectives.” General Data Protection Regulation (GDPR), August 30, 2016. <https://gdpr-info.eu/art-1-gdpr/>.

“Art. 46 GDPR – Transfers Subject to Appropriate Safeguards.” General Data Protection Regulation (GDPR), July 8, 2020. <https://gdpr-info.eu/art-46-gdpr/>.

“Art. 47 GDPR – Binding Corporate Rules.” General Data Protection Regulation (GDPR), March 29, 2018. <https://gdpr-info.eu/art-47-gdpr/>.

“Art. 6 GDPR – Lawfulness of Processing.” General Data Protection Regulation (GDPR), January 27, 2023. <https://gdpr-info.eu/art-6-gdpr/>.

“Art. 6 GDPR – Lawfulness of Processing.” General Data Protection Regulation (GDPR), January 27, 2023. <https://gdpr-info.eu/art-6-gdpr/>.

“Art. 83 GDPR - General Conditions for Imposing Administrative Fines.” GDPR.eu, September 14, 2023. <https://gdpr.eu/article-83-conditions-for-imposing-administrative-fines/>.

“Art. 83 GDPR - General Conditions for Imposing Administrative Fines.” GDPR.eu, September 14, 2023. <https://gdpr.eu/article-83-conditions-for-imposing-administrative-fines/>.

Austin et al. , Kelly. “China Passes the Personal Information Protection Law, to Take Effect on November 1.” Gibson Dunn, July 27, 2024. <https://www.gibsondunn.com/china-passes-the-personal-information-protection-law-to-take-effect-on-november-1/?pdf=display>.

Bygrave, Lee A. *Data Privacy Law: A Comparative Perspective* . Vol. 204. Oxford University Press, 2014.

“China’s Emerging Data Privacy System and GDPR.” CSIS. Accessed January 3, 2025. <https://www.csis.org/analysis/chinas-emerging-data-privacy-system-and-gdpr>.

Chumak, Alona. “China’s New Requirements for Cross-Border Data Transfers.” InCountry, January 18, 2024. <https://incountry.com/blog/chinas-new-requirements-for-cross-border-data-transfers/>.

Claessens, Stijn, and Laura E. Kodres. “The Regulatory Responses to the Global Financial Crisis: Some Uncomfortable Questions.” *IMF Working Papers* no. 046 (March 14, 2014). <https://doi.org/https://doi.org/10.5089/9781484335970.001.A001>.

“Commission Finds That EU Personal Data Flows Can Continue with 11 Third Countries and Territories.” European Commission - European Commission. Accessed January 3, 2025. <https://ec.europa.eu/commission/presscorner/detail/it/ip_24_161>.

Creemers, Rogier. “China’s Emerging Data Protection Framework.” *Journal of Cybersecurity* 8, no. 1 (2022). <https://doi.org/https://doi.org/10.1093/cybsec/tyac011>.

Dan Cooper, Laura Somaini. “European Commission Announces Conclusion of First Review of Japan-EU Adequacy Arrangement.” Inside Privacy, May 30, 2023. <https://www.insideprivacy.com/data-privacy/european-commission-announces-conclusion-of-first-review-of-japan-eu-adequacy-arrangement/>

Data Privacy Framework. Accessed January 3, 2025. <https://www.dataprivacyframework.gov/program-articles/FAQs%20%E2%80%93%20EU%E2%80%93U.S.-Data-Privacy-Framework-(EU%E2%80%93U.S.-DPF)>.

“Data Protection Adequacy for Non-EU Countries.” European Commission. Accessed January 3, 2025. <https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en>.

“Data Protection under GDPR.” Your Europe, January 1, 2022. <https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_en.htm>.

“Data Security Law of the People’s Republic of China.” 中国人大网. Accessed January 3, 2025. <http://www.npc.gov.cn/englishnpc/c2759/c23934/202112/t20211209_385109.html>.

Digital Single Market for europe - consilium. Accessed January 3, 2025. <https://www.consilium.europa.eu/en/policies/digital-single-market/>.

The Editors of Encyclopedia Britannica. “Tiananmen Square Incident.” Encyclopædia Britannica, December 9, 2024. <https://www.britannica.com/event/Tiananmen-Square-incident>.

European Commission. “Data Protection: Commission Adopts Adequacy Decisions for the UK.” European Commission - European Commission. Accessed January 3, 2025. <https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3183>.

“European Commission Adopts Adequacy Decision on Japan, Creating the World’s Largest Area of Safe Data Flows.” European Commission - European Commission. Accessed January 3, 2025. <https://europa.eu/rapid/press-release_IP-19-421_en.htm>.

“European Convention on Human Rights - Article 8.” European Union Agency for Fundamental Rights, March 8, 2022. <https://fra.europa.eu/en/law-reference/european-convention-human-rights-article-8-0>.

“GDPR Article 15 Compliance: Empowering Data Subjects across EU.” Security, November 30, 2024. <https://securiti.ai/article-15-gdpr/>.

Global, Autor:Caixin. “China: Weibo Admits to Leak of Personal Data on Millions of Users.” Business & Human Rights Resource Centre. Accessed January 3, 2025. <https://www.business-humanrights.org/es/%C3%BAltimas-noticias/china-weibo-admits-to-leak-of-personal-data-on-millions-of-users/>.

“Home.” Home - Garante Privacy. Accessed January 3, 2025. <https://www.garanteprivacy.it/>.

Hu, Tina Y. Lecture. n.d. “International Data Transfers.” International data transfers | European Data Protection Board. Accessed January 3, 2025. <https://www.edpb.europa.eu/sme-data-protection-guide/international-data-transfers_en>.

Kotska, Genia. “China’s Social Credit Systems and Public Opinion: Explaining High Levels of Approval.” *New Media &amp; Society*, 1565–93. , 21, no. no.7 (February 13, 2019). <https://doi.org/https://doi.org/10.1177/1461444819826402>.

Law, Author Accessible. “Article 39.” PIPL, May 10, 2022. <https://personalinformationprotectionlaw.com/PIPL/article-39/>.

Law, Author Accessible. “Article 40.” PIPL, May 10, 2022. <https://personalinformationprotectionlaw.com/PIPL/article-40/>.

Law, Author Accessible. “Article 42.” PIPL, May 10, 2022. <https://personalinformationprotectionlaw.com/PIPL/article-42/>.

“Learn and Revise with BBC Bitesize.” BBC News. Accessed January 3, 2025. <https://www.bbc.co.uk/bitesize/learn>.

“Legal Text.” General Data Protection Regulation (GDPR), April 22, 2024. <https://gdpr-info.eu/>.

NAVAS, Leonardo CERVERA. “EDPS Homepage.” European Data Protection Supervisor. Accessed January 3, 2025. <https://www.edps.europa.eu/_en>.

Ni, and Vincent. “Hacker Claims to Have Obtained Data on 1 Billion Chinese Citizens.” The Guardian, July 4, 2022. <https://www.theguardian.com/technology/2022/jul/04/hacker-claims-access-data-billion-chinese-citizens?via=indexdotco>.

Office of the Privacy Commissioner of Canada. “PIPEDA Requirements in Brief.” Office of the Privacy Commissioner of Canada, May 1, 2024. <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/>.

“Personal Information Protection Law of the People’s Republic of China.” PIPL, May 10, 2022. <https://personalinformationprotectionlaw.com/>.

“PIPL vs GDPR - Key Differences and Implications for Compliance in China.” China Briefing News, July 21, 2022. <https://www.china-briefing.com/news/pipl-vs-gdpr-key-differences-and-implications-for-compliance-in-china/>.

“PIPL vs GDPR - Key Differences and Implications for Compliance in China.” China Briefing News, July 21, 2022. <https://www.china-briefing.com/news/pipl-vs-gdpr-key-differences-and-implications-for-compliance-in-china/>.

Prasad, Mr. Eswar S. “I Overview.” IMF eLibrary. Accessed January 3, 2025. <https://www.elibrary.imf.org/display/book/9781589062580/ch01.xml>.

“Press Corner: European Commission.” European Commission - European Commission. Accessed January 3, 2025. <https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752>.

Pypker, and Rhys. *PSWG3: Privacy and Data Protection as Fundamental Rights: A Narrative*, n.d.

Reporter, Guardian staff. “Hackers in China Attack 20m Accounts on Alibaba’s Taobao Shopping Site.” The Guardian, February 4, 2016. <https://www.theguardian.com/business/2016/feb/04/hackers-in-china-attack-20m-accounts-on-alibaba-taobao-shopping-site>.

“Rights of the Individual.” European Data Protection Supervisor. Accessed January 3, 2025. <https://www.edps.europa.eu/data-protection/our-work/subjects/rights-individual_en>.

Ryan Hass, Abraham Denmark, Ryan Hass, Geoffrey Gertz, Margaret M. Pearson Joshua P. Meltzer, and Tanvi Madan. “Beyond Huawei and TikTok: Untangling US Concerns over Chinese Tech Companies and Digital Security.” Brookings, March 9, 2022. <https://www.brookings.edu/articles/beyond-huawei-and-tiktok-untangling-us-concerns-over-chinese-tech-companies-and-digital-security/>.

“Sensitive Personal Information Archives.” PIPL, April 13, 2022. <https://personalinformationprotectionlaw.com/PIPL/tag/sensitive-personal-information/>.

Shepferd, Cristian. “China’s Finely Crafted Web of Digital Surveillance for the Beijing Olympics Has Been Years in the Making.” The Washington Post. Accessed January 3, 2025. <https://www.washingtonpost.com/sports/olympics/2022/02/02/china-digital-surveillance-beijing-winter-olympics/>.

“Standard Contractual Clauses (SCC).” European Commission. Accessed January 3, 2025. <https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en>.

TMO Group. “Data Protection Laws in China: Overview (2024).” TMO Group, August 13, 2024. <https://www.tmogroup.asia/insights/china-data-protection-laws/>.

Togni, Andrea. “How East Germany’s Stasi Perfected Mass Surveillance.” Mises Institute, February 3, 2024. <https://mises.org/mises-wire/how-east-germanys-stasi-perfected-mass-surveillance>.

“Understanding China’s PIPL: Key Regulations, Compliance & Impact.” Accessed January 3, 2025. <https://secureprivacy.ai/blog/china-pipl-personal-information-protection-law>.

“Who Are the Members of the Board?” Who are the members of the Board? | European Data Protection Board. Accessed January 3, 2025. <https://www.edpb.europa.eu/about-edpb/faq-frequently-asked-questions/who-are-members-board_en>.

Xiaoping, Deng. “Lessons Learned with the Chinese Economic Reform.” Study. Accessed January 3, 2025. <https://study.com/learn/lesson/deng-xiaoping-chinese-economic-reform.html>.

Yan Luo, Xuezi Dan. “China Eases Restrictions on Cross-Border Data Flows.” Inside Privacy, March 25, 2024. <https://www.insideprivacy.com/uncategorized/china-eases-restrictions-on-cross-border-data-flows/>.

Yuet, Tham Ming. “The Impact of China’s Data Localization Requirements on Cross-Border Data Transfers.” *Journal of Chinese Law* 28, no. no.3 (2022): 345–70.

1. PIPL. “Article 42,” March 2, 2022. [↑](#footnote-ref-0)
2. General Data Protection Regulation (GDPR). “General Data Protection Regulation (GDPR) – Legal Text,” July 13, 2016. https://gdpr-info.eu/. [↑](#footnote-ref-1)
3. European Union Agency for Fundamental Rights. “European Convention on Human Rights - Article 8,” October 25, 2018. https://fra.europa.eu/en/law-reference/european-convention-human-rights-article-8-0.  [↑](#footnote-ref-2)
4. General Data Protection Regulation (GDPR). “Art. 1 GDPR – Subject-Matter and Objectives,” July 12, 2016. https://gdpr-info.eu/art-1-gdpr/. [↑](#footnote-ref-3)
5. Bitesize, BBC. “The Police State - Nazi Control and Dictatorship 1933-1939 - Edexcel - GCSE History Revision - Edexcel.” BBC Bitesize, August 24, 2016. https://www.bbc.co.uk/bitesize/guides/zsvhk7h/revision/2.  [↑](#footnote-ref-4)
6. Togni, Andrea. “How East Germany’s Stasi Perfected Mass Surveillance.” *Mises Institute*, July 21, 2023. https://mises.org/mises-wire/how-east-germanys-stasi-perfected-mass-surveillance. [↑](#footnote-ref-5)
7. Claessens, Stijn, and Laura E. Kodres. “The Regulatory Responses to the Global Financial Crisis: Some Uncomfortable Questions.” *IMF Working Papers* 2014, no. 046 (March 14, 2014). https://doi.org/10.5089/9781484335970.001.A001.  [↑](#footnote-ref-6)
8. Consilium. “Digital Single Market for Europe.” Accessed December 1, 2024. https://www.consilium.europa.eu/en/policies/digital-single-market/.  [↑](#footnote-ref-7)
9. Lee A. Bygrave, *Data Privacy Law: A Comparative Perspective* (Oxford: Oxford University Press, 2014), 204. [↑](#footnote-ref-8)
10. Pypker, Rhys. “PSWG3: Privacy and Data Protection as Fundamental Rights: A Narrative,” n.d. Accessed November 1, 2024.  [↑](#footnote-ref-9)
11. PIPL. “Personal Information Protection Law of the People’s Republic of China,” November 1, 2021. https://personalinformationprotectionlaw.com/.  [↑](#footnote-ref-10)
12. Deloitte China. “Analysis of the Highlights of the Personal Information Protection Law,” August 31, 2021. https://www2.deloitte.com/cn/en/pages/risk/articles/personal-information-protection-law-analysis.html.    [↑](#footnote-ref-11)
13. “China’s Emerging Data Privacy System and GDPR.” Accessed November 1, 2024. https://www.csis.org/analysis/chinas-emerging-data-privacy-system-and-gdpr.  [↑](#footnote-ref-12)
14. Ni, Vincent. “Hacker Claims to Have Obtained Data on 1 Billion Chinese Citizens.” *The Guardian*, July 4, 2022. https://www.theguardian.com/technology/2022/jul/04/hacker-claims-access-data-billion-chinese-citizens.  [↑](#footnote-ref-13)
15. Chumak, Alona. “China’s New Requirements for Cross-Border Data Transfers.” *InCountry* (blog), January 18, 2024. https://incountry.com/blog/chinas-new-requirements-for-cross-border-data-transfers/.  [↑](#footnote-ref-14)
16. PIPL. “Article 40,” March 2, 2022. https://personalinformationprotectionlaw.com/PIPL/article-40/.  [↑](#footnote-ref-15)
17. “Deng Xiaoping.” Accessed December 1, 2024. https://study.com/learn/lesson/deng-xiaoping-chinese-economic-reform.html.  [↑](#footnote-ref-16)
18. Prasad, Eswar S. “I Overview.” IMF eLibrary. Accessed December 1, 2024. https://www.elibrary.imf.org/display/book/9781589062580/ch01.xml.  [↑](#footnote-ref-17)
19. The Editors of Encyclopaedia Britannica. “Tiananmen Square Incident.” *Encyclopedia Britannica*, May 29, 2009. https://www.britannica.com/event/Tiananmen-Square-incident.  [↑](#footnote-ref-18)
20. Shepherd, Christian. “China’s Finely Crafted Web of Digital Surveillance for the Beijing Olympics Has Been Years in the Making.” *The Washington Post*, February 2, 2022. https://www.washingtonpost.com/sports/olympics/2022/02/02/china-digital-surveillance-beijing-winter-olympics/.  [↑](#footnote-ref-19)
21. Kostka, Genia. “China’s Social Credit Systems and Public Opinion: Explaining High Levels of Approval.” *New Media &amp; Society* 21, no. 7 (February 13, 2019): 1565–93. https://doi.org/10.1177/1461444819826402.  [↑](#footnote-ref-20)
22. Reporter, Guardian staff. “Hackers in China Attack 20m Accounts on Alibaba’s Taobao Shopping Site.” *The Guardian*, February 4, 2016. https://www.theguardian.com/business/2016/feb/04/hackers-in-china-attack-20m-accounts-on-alibaba-taobao-shopping-site.  [↑](#footnote-ref-21)
23. Business & Human Rights Resource Centre. “China: Weibo Admits to Leak of Personal Data on Millions of Users.” Accessed December 1, 2024. https://www.business-humanrights.org/es/%C3%BAltimas-noticias/china-weibo-admits-to-leak-of-personal-data-on-millions-of-users/.  [↑](#footnote-ref-22)
24. Abraham Denmark Ryan Hass et al., “Beyond Huawei and TikTok: Untangling US Concerns over Chinese Tech Companies and Digital Security,” Brookings, March 9, 2022 [↑](#footnote-ref-23)
25. Deloitte China. “Analysis of the Highlights of the Personal Information Protection Law,” August 31, 2021. https://www2.deloitte.com/cn/en/pages/risk/articles/personal-information-protection-law-analysis.html.  [↑](#footnote-ref-24)
26. European Data Protection Board. “International Data Transfers.” Accessed November 6, 2024. https://www.edpb.europa.eu/sme-data-protection-guide/international-data-transfers\_en.  [↑](#footnote-ref-25)
27. European Data Protection Board. “International Data Transfers.” Accessed November 6, 2024. https://www.edpb.europa.eu/sme-data-protection-guide/international-data-transfers\_en.  [↑](#footnote-ref-26)
28. European Data Protection Board. “International Data Transfers.” Accessed November 6, 2024. https://www.edpb.europa.eu/sme-data-protection-guide/international-data-transfers\_en.  [↑](#footnote-ref-27)
29. European Commission. “Data Protection Adequacy for Non-EU Countries.” Accessed November 25, 2024. https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions\_en. [↑](#footnote-ref-28)
30. Office of the Privacy Commissioner of Canada. “PIPEDA Requirements in Brief.” Accessed November 25, 2024. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda\_brief/.  [↑](#footnote-ref-29)
31. European Commission. *Report From the Commission to the European Parliament and the Council on the First Review of the Functioning of the Adequacy Decision for Japan.* Brussels, April 3, 2023. [↑](#footnote-ref-30)
32. European Commission - European Commission. “Data Protection: Commission Adopts Adequacy Decisions for the UK.” Accessed November 25, 2024. https://ec.europa.eu/commission/presscorner/detail/en/ip\_21\_3183.  [↑](#footnote-ref-31)
33. “Data Privacy Framework.” Accessed November 25, 2024. https://www.dataprivacyframework.gov/program-articles/FAQs%20%E2%80%93%20EU%E2%80%93U.S.-Data-Privacy-Framework-(EU%E2%80%93U.S.-DPF).  [↑](#footnote-ref-32)
34. European Commission - European Commission. “Commission Finds That EU Personal Data Flows Can Continue with 11 Third Countries and Territories.” Accessed November 25, 2024. https://ec.europa.eu/commission/presscorner/detail/it/ip\_24\_161.  [↑](#footnote-ref-33)
35. General Data Protection Regulation (GDPR). “Art. 46 GDPR – Transfers Subject to Appropriate Safeguards,” July 13, 2016. https://gdpr-info.eu/art-46-gdpr/.  [↑](#footnote-ref-34)
36. European Commission. “Standard Contractual Clauses (SCC).” Accessed November 25, 2024. https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc\_en.  [↑](#footnote-ref-35)
37. General Data Protection Regulation (GDPR). “Art. 47 GDPR – Binding Corporate Rules,” July 13, 2016. https://gdpr-info.eu/art-47-gdpr/.  [↑](#footnote-ref-36)
38. PIPL. “Sensitive Personal Information Archives.” Accessed November 25, 2024. https://personalinformationprotectionlaw.com/PIPL/tag/sensitive-personal-information/.  [↑](#footnote-ref-37)
39. TMO Group. “Data Protection Laws in China: Overview (2024).” TMO Group, August 13, 2024. https://www.tmogroup.asia/insights/china-data-protection-laws/.  [↑](#footnote-ref-38)
40. TMO Group. “Data Protection Laws in China: Overview (2024).” TMO Group, August 13, 2024. https://www.tmogroup.asia/insights/china-data-protection-laws/.  [↑](#footnote-ref-39)
41. Yuet Ming Tham, “The Impact of China’s Data Localization Requirements on Cross-Border Data Transfers,” *Journal of Chinese Law* 28, no. 3 (2022): 345-370. [↑](#footnote-ref-40)
42. BloombergNEF. “Apple to Build First China Data Center to Comply With Law,” July 12, 2017. https://about.bnef.com/blog/apple-to-build-first-china-data-center-to-comply-with-local-law/.  [↑](#footnote-ref-41)
43. “Data Security Law of the People’s Republic of China.” Accessed November 6, 2024. http://www.npc.gov.cn/englishnpc/c2759/c23934/202112/t20211209\_385109.html.  [↑](#footnote-ref-42)
44. “Data Security Law of the People’s Republic of China.” Accessed November 30, 2024. http://www.npc.gov.cn/englishnpc/c2759/c23934/202112/t20211209\_385109.html.  [↑](#footnote-ref-43)
45. “PIPL vs GDPR - Key Differences and Implications for Compliance in China.” China Briefing News, May 18, 2022. https://www.china-briefing.com/news/pipl-vs-gdpr-key-differences-and-implications-for-compliance-in-china/.  [↑](#footnote-ref-44)
46. Hu, Tina Y. “PowerPoint Presentation,” n.d. Accessed November 6, 2024.  [↑](#footnote-ref-45)
47. Your Europe. “Data Protection under GDPR.” Accessed November 5, 2024. https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index\_en.htm.  [↑](#footnote-ref-46)
48. General Data Protection Regulation (GDPR). “Art. 6 GDPR – Lawfulness of Processing,” July 12, 2016. https://gdpr-info.eu/art-6-gdpr/.   [↑](#footnote-ref-47)
49. General Data Protection Regulation (GDPR). “Art. 6 GDPR – Lawfulness of Processing,” July 12, 2016. https://gdpr-info.eu/art-6-gdpr/.    [↑](#footnote-ref-48)
50. General Data Protection Regulation (GDPR). “Art. 6 GDPR – Lawfulness of Processing,” July 12, 2016. https://gdpr-info.eu/art-6-gdpr/.   [↑](#footnote-ref-49)
51. Baig, Anas. “GDPR Article 15 Compliance.” Security, January 1, 2024. https://securiti.ai/article-15-gdpr/.  [↑](#footnote-ref-50)
52. European Data Protection Supervisor. “Rights of the Individual.” Accessed November 5, 2024. https://www.edps.europa.eu/data-protection/our-work/subjects/rights-individual\_en.   [↑](#footnote-ref-51)
53. PIPL. “Article 39,” March 2, 2022. https://personalinformationprotectionlaw.com/PIPL/article-39/.  [↑](#footnote-ref-52)
54. Deloitte China. “Analysis of the Highlights of the Personal Information Protection Law,” August 31, 2021. https://www2.deloitte.com/cn/en/pages/risk/articles/personal-information-protection-law-analysis.html.  [↑](#footnote-ref-53)
55. https://secureprivacy.ai/. “Understanding China’s PIPL.” Accessed November 5, 2024. https://secureprivacy.ai/blog/china-pipl-personal-information-protection-law.  [↑](#footnote-ref-54)
56. Briefing, China. “PIPL vs GDPR - Key Differences and Implications for Compliance in China.” China Briefing News, May 18, 2022. https://www.china-briefing.com/news/pipl-vs-gdpr-key-differences-and-implications-for-compliance-in-china/.  [↑](#footnote-ref-55)
57. European Data Protection Supervisor. “Data Protection.” Accessed November 6, 2024. https://www.edps.europa.eu/data-protection\_en.  [↑](#footnote-ref-56)
58. AEPD. “Agencia Española de Protección de Datos.” Accessed November 6, 2024. https://www.aepd.es/.  [↑](#footnote-ref-57)
59. Garante Privacy. “Home.” Accessed November 6, 2024. https://www.garanteprivacy.it/.  [↑](#footnote-ref-58)
60. European Data Protection Board. “Our Members.” Accessed November 6, 2024. https://www.edpb.europa.eu/about-edpb/about-edpb/members\_en.  [↑](#footnote-ref-59)
61. GDPR.eu. “Art. 83 GDPR - General Conditions for Imposing Administrative Fines,” November 14, 2018. https://gdpr.eu/article-83-conditions-for-imposing-administrative-fines/.  [↑](#footnote-ref-60)
62. GDPR.eu. “Art. 83 GDPR - General Conditions for Imposing Administrative Fines,” November 14, 2018. https://gdpr.eu/article-83-conditions-for-imposing-administrative-fines/.  [↑](#footnote-ref-61)
63. European Data Protection Board. “1.2 Billion Euro Fine for Facebook as a Result of EDPB Binding Decision.” Accessed November 6, 2024. https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision\_en.  [↑](#footnote-ref-62)
64. Kelly Austin et al., “China Passes the Personal Information Protection Law, To Take Effect on November 1.,” Gibson Dunn, September 10, 2021, https://www.gibsondunn.com/china-passes-the-personal-information-protection-law-to-take-effect-on-november-1/?pdf=display. [↑](#footnote-ref-63)
65. Rogier Creemers, “China’s Emerging Data Protection Framework,” *Journal of Cybersecurity* 8, no. 1 (2022), https://doi.org/https://doi.org/10.1093/cybsec/tyac011 [↑](#footnote-ref-64)
66. Luo, Yan. “China Eases Restrictions on Cross-Border Data Flows.” Inside Privacy, March 25, 2024. https://www.insideprivacy.com/uncategorized/china-eases-restrictions-on-cross-border-data-flows/.  [↑](#footnote-ref-65)
67. European Commission - European Commission. “Questions & Answers: EU-US Data Privacy Framework.” Accessed November 25, 2024. https://ec.europa.eu/commission/presscorner/detail/en/qanda\_23\_3752.  [↑](#footnote-ref-66)
68. “European Commission Adopts Adequacy Decision on Japan, Creating the World’s Largest Area of Safe Data Flows,” European Commission - European Commission, accessed January 3, 2025, https://europa.eu/rapid/press-release\_IP-19-421\_en.htm. [↑](#footnote-ref-67)