Scientific Research Publishing

Beijing Law Review, 2025, 16(3), 1721-1741
https://www.scirp.org/journal/blr
ISSN Online: 2159-4635
ISSN Print: 2159-4627

A Comparative Analysis of Customer Data Privacy Protection under the European Union's General Data Protection Regulation and the People's Republic of China's Personal Information Protection Law

Oceanus Ming-Ting Kam

Independent Researcher, Hong Kong, China
Email: c212976@yahoo.com.hk

How to cite this paper: Kam, O. M.-T. (2025). General Data Protection Regulation and the People's Republic of China's Personal Information Protection Law. *Beijing Law Review, 16,* 1721-1741.
https://doi.org/10.4236/blr.2025.163086

Received: July 21, 2025
Accepted: August 31, 2025
Published: September 3, 2025

Abstract

Since its inception and full implementation in 2016 and 2018 respectively, the European Union's (EU) General Data Protection Regulation (GDPR) has been widely regarded as the international community's data protection—privacy protection "gold standard". Many scholars attribute this GDPR status to influential global human rights instruments like the Universal Declaration on Human Rights 1948, European Convention on Human Rights 1950, and International Covenant on Economic, Social and Cultural Rights 1966. There is little doubt about when People's Republic of China's (PRC) data protection policymakers were determining how Chinese data laws should be reformed, as the GDPR provisions strongly influenced the eventual scope and effect of the PRC's Personal Information Protection Law (PIPL). This comparative analysis considers the various GDPR—PIPL similarities and differences, with particular emphasis placed on the broad regulatory powers available to the Cyberspace Administration of China (CAC). The GDPR regulatory framework is tightly structured regarding how its chief oversight agencies are operated. The EU member states' individual "Supervisory Authorities" are the regulators created within each member state, with the European Commission mechanisms providing the entire GDPR regulatory structure, the corresponding CAC powers are only generally defined. The relatively brief PIPL legislative history means that the CAC has not yet published enough rulings, or issued policy guidance that permits interested parties to ensure that their data processing and related activities fully conform to all PIPL requirements. Foreign companies with PRC interests must comply with all PIPL provisions, and absent clearer PIPL regu-

lations regarding precisely how the CAC will deal with data protection—privacy issues, and uncertainty will prevail. The analysis confirms that it is very difficult to predict how the CAC will use its regulatory powers going forward—a reality that is likely the single biggest distinguishing feature when the PIPL and GDPR frameworks are compared. The analysis also considers the extent to which the CAC might be inclined to cooperate with PRC central government agencies regarding personal data being shared with the government for its purposes.

Keywords

General Data Protection Regulation (GDPR), Personal Information Protection Law (PIPL), Cyberspace Administration of China (CAC), Data Privacy, Data Protection, Privacy Law, Cybersecurity, Comparative Law, Cross-Border Data Transfer

1. Introduction

In a world that reveals increasingly deeper and wider geopolitical fractures as the 21st century moves forward, the ways that States' approaches to personal data processing and related privacy protections have followed similar legal paths are seemingly an international law anomaly. The People's Republic of China (PRC) and almost all European Union (EU) member states have engaged in international relationships that are marked by varying degrees of tension (Wang & Shen, 2023). Trade issues are a frequent source of State versus State friction when EU member state and PRC interests come into conflict (Svetlicinii, 2022).

Many commentators have characterised the general tenor of all adversarial PRC-EU dealings in stark PRC authoritarian versus EU Western liberal democracy terms (Oertel, 2020). The EU is seemingly perceived by the PRC leadership as being closely allied to a US administration that has sought to confront the PRC on numerous trade and other geopolitical fronts (Oertel, 2020). Current Chinese and European attitudes expressed regarding the Russian invasion of Ukraine and its ongoing military conflict are a notable example. The EU has consistently supported Ukraine self-defence efforts, where PRC leaders have refused to condemn Russian actions even where these have (prima facie) constituted breaches of international humanitarian law (Bo, 2023).

However, in the following parts, this comparative analysis tends to confirm that the EU's General Data Protection Regulation (GDPR) (European Parliament & Council of the European Union, 2016) and its PRC Personal Information Protection Law (PIPL) (National People's Congress of People's Republic of China, 2021) counterpart have many more conceptual similarities than differences (Zhu, 2022). It is suggested that notwithstanding the geopolitical divides revealed across the international community, there is an emerging global consensus concerning the expected nature and scope of personal data and privacy protections. These atti-

tudes extend directly from human rights universality principles anchored by the 1948 Universal Declaration on Human Rights (United Nations General Assembly, 1948). Globalisation forces, especially the ways that international economic trade networks have continued to evolve and intensify, have also contributed to the notion advocated by numerous scholars that data protection—privacy rights should be relatively similar, if not entirely harmonised across the entire international community (da Silva, 2021).

The GDPR and PIPL common features explained in this project reflect this consensus position. A core argument giving the present analysis its central theme is restated here: the GDPR is now regarded as the international community's data protection "gold standard" (Greenleaf, 2020). Some scholars have employed the term "Brussels Effect" to explain the powerful influence EU data protection legislation has exerted across the globe (da Silva, 2021). It is therefore not surprising that this 2016 EU legal framework (one that was initially proposed 10 years earlier) appeared to exert a direct influence on subsequent PRC policymaker's efforts to craft all PIPL data—privacy provisions (da Silva, 2021).

The literature review is provided in Part 2. The research methodology is discussed in Part 3. The key GDPR and PIPL features are outlined in Part 4. The key Regulation and Law differences are analysed in Part 5 to study how and why the GDPR and PIPL provisions differ regarding the cybersecurity measures that business enterprises must implement in each jurisdiction. Specific Part 5's critical attention is directed towards the designated PIPL national regulator (i.e. Cyberspace Administration of China (CAC)), and the potential powers CAC officials may exercise concerning data protection—ones that are arguably much broader, and less precisely defined than those afforded the EU member states' Supervisory Authorities (also known as their Data Protection Authorities (DPAs)) (Greenleaf & Livingston, 2017). A brief Part 5 commentary (as reinforced by the Part 6 overall project conclusion) offers insights regarding whether the apparent GDPR – PIPL data protection convergence will continue, or whether the CAC will chart a distinct legal path for the foreseeable future. This latter possibility is described throughout the analysis as a possible data protection "third way", a phrase employed by Pernot-Leplay and other PIPL scholars (Pernot-Leplay, 2020) to describe a unique data governance model that diverges from both the rights-centric EU approach and the market-driven US model by prioritising state control and national security interests. The basis for this paper's analysis is derived from the following two research questions that will be explored:

- In what ways do the stated normative principles of the EU's GDPR and the PRC's PIPL align and differ, especially concerning the oversight body's level of power and transparency?
- In what ways does the deliberately vague nature of the CAC's law enforcement powers under PIPL leave room for ambiguity and uncertainty for international businesses, and how does this reflect a potential PRC "third way" in global data governance?

2. Literature Review

There has been significant scholarly interest directed at determining how the 2021 PIPL regulatory regime compares with its supranational GDPR and other more established national data protection—personal privacy frameworks. In addition to the practitioner sources cited above, the following notable journal articles selected for inclusion in this brief review that tend to reinforce a clear GDPR-PIPL comparative analysis proposition: the PRC has advanced a model that departs from what have been regarded as the GDPR's "normative" global standard (Greenleaf, 2020). It is interesting to consider that the Australian scholar Graham Greenleaf correctly anticipated how the final PIPL enactments would align with a published PIPL draft (first available in 2019).

2.1. Greenleaf (2020)

Greenleaf observed that on an initial GDPR-PIPL comparison, the PRC approach to data protection appeared to fall within the "normal global family privacy laws … neither more radical nor more restricted" (Greenleaf, 2020). Greenleaf explains how this PIPL impression is supplemented by its "conventional" definitions of core concepts such as "Personal information", and "consent" that individuals must give to any entities that are gathering, processing, or storing such information (Greenleaf, 2020). It is apparent that in these general respects, the entire PIPL structure reveals clear GDPR influences. However, as Greenleaf establishes later in his comparative study, PIPL standards differ from their GDPR counterparts and earlier PRC laws in key respects, particularly the ways that CAC oversight is likely to be exercised (the ambiguity point introduced above) (Greenleaf, 2020: pp. 3-4).

A final Greenleaf point directly contributes to how one may appreciate the two comparative analysis issues and research questions presented above. Greenleaf suggests that PIPL unexpectedly departed from prior PRC data protection approaches by mandating all State agencies to ensure strict PIPL privacy rules adherence (Greenleaf, China Issues a Comprehensive Draft Data Privacy Law, 2020). His expressed surprise at this PIPL provision (as captured in PIPL Articles 35, 37, and 68) is rooted in the international community's experience with the PRC and other authoritarian central governments: "It is unexpected, perhaps startling, for a data privacy law to have general application to the public sector in a communist country, and it remains to be seen whether it will ever be enforced against the interests of the State" (Greenleaf & Livingston, 2017).

This is a cogent Greenleaf comment, given that the PRC has seemingly placed supreme importance on promoting State interests over individual rights protections whenever the two concepts conflict (Tsai, 2021). It will be interesting to monitor how the CAC exercises its available powers against PRC government organs going forward—a key takeaway from this Review that will also inform the research necessary to complete the proposed project.

2.2. Pernot-Leplay (2020)

This PRC-based scholar offers a relatively optimistic view of the point made by Greenleaf as summarised above (Pernot-Leplay, 2020). Pernot-Leplay sets out a detailed chronological history of how the PIPL emerged from what he describes as the PRC's "latecomer" status in the global data protection—individual privacy rights environment ("China's Belated Building of its Legal Framework") (Pernot-Leplay, 2020: p. 64). Pernot-Leplay suggests that there has been an air of inevitability surrounding the PRC approach to this combined legal regulation—human rights area since at least 2010, given that the PRC's ongoing domestic social economic development and its strong commitments to international trade and economic development would (eventually) compel PRC leaders to observe international privacy and personal data protection standards (Xue, 2010). The fact that PIPL has adopted the above-cited GDPR definitions lends further credence to this Pernot-Leplay opinion.

It is Pernot-Leplay's characterisation of the PIPL as a possible 'third way' that the PRC is charting, one that differs from relatively liberal US approaches and the more rigorous EU endorsement of robust cybersecurity enforcement rules concerning any enterprises that fall within its GDPR data processor definition (Pernot-Leplay, 2020: pp. 65-70). This is an interesting and well-expressed Pernot-Leplay contention, but it remains a speculative one until the CAC established a track record regarding how it will enforce the PIPL requirements against PRC state agencies (the Greenleaf argument outlined above) (Pernot-Leplay, 2020: pp. 65-70).

2.3. Shi & Wang (2023)

This very recent (April 2023) article provides an excellent review of events leading up to the 2021PIPL enactments, ones that Shi and Wang describe as a "groundbreaking blowout of China's data privacy law" (Shi & Wang, 2023). These scholars also offer a significant insight regarding a PRC socio-cultural reality. Until approximately 10 years ago, they suggest that "Chinese society still only paid lip service to privacy protection", notwithstanding that such rights theoretically were enforceable by private citizens. Shi and Wang reference this as a personal information "nothing to hide" argument, where anyone asserting such rights was engaging in protecting something akin to a "dirty little secret" (Shi & Wang, 2023: p. 15).

These scholars readily acknowledge that the PIPL framework is too 'new' to permit any reasonable predictions to be made concerning how its protections will be enforced in practice by CAC regulators. They identify how PIPL Article 24 offers consumers specific protection from commercial enterprises that use "automated decision-making methods" to target an individual's characteristics when promoting goods or services to this individual (Shi & Wang, 2023: p. 28). Once again, how the CAC interprets and applies these rules remains uncertain. If the Shi and Wang analysis is taken to its logical conclusion, one can imagine the CAC

taking similar approaches to those adopted by EU regulators towards private enterprises, but the "State interests" ambiguity ensures this point will remain speculative for at least the immediate future (Shi & Wang, 2023: p. 28).

3. Research Methodology

The above literature review confirms that legal doctrine should be highlighted as the primary research methodology in this project. By its nature, an EU-PRC comparative analysis must be grounded in the relevant legal principles and legislative rules (Creswell & Creswell, 2018). The Shi and Wang attention directed at the traditional PRC societal view of privacy rights being subordinated to State interests also suggests that socio-legal research will attractively supplement the favoured doctrinal approach (Chynoweth, 2013: pp. 670, 672). In this way, the socio-legal materials will encourage a GDPR-PIPL comparative analysis whereby any respective EU and PRC societal influences are given appropriate weight. This approach aligns with the maxim that laws do not exist in a vacuum—they must be understood in terms of specific social or cultural influences that may shape their interpretation.

These two methods will thus rely upon readily available primary (case law and legislation) and secondary source materials. The proposed research methods are also sufficiently flexible to accommodate any breaking developments (legislative, case law, and new academic publications) that might occur as the project is being completed. These research approaches also eliminate the need to conduct potentially expensive independent evidence gathering, such as circulating questionnaires or conducting interviews with noted experts to acquire research material.

4. Key GDPR & PIPL Features

4.1. Overview

There is little question that for over 20 years, data protection and related privacy rights (collectively referenced as 'data protection' throughout this paper) have become important elements in a broader, often multidimensional global debate (Greenleaf, February 10, Global Data Privacy Laws: 16 National Laws and 0 Bills, 2023) The scholarship that has considered these issues usually centres on the different ways that personal data may permissibly be collected, stored, and used by State agencies and private entities (Shi & Wang, 2023). There are two broad intellectual camps identified in this area, ones whose conflicting views regarding what constitutes appropriate data protection are fairly characterised as follows.

The following points are not necessarily specific to the EU or PRC data protection environments. They are presented here to better contextualise the respective GDPR and PIPL features, and what each law is intended to achieve. It is suggested that for many citizens, data protection concepts directly contribute to two opposing attitudes. On one hand, consumer societies enjoy (even demand) greater personal convenience associated with how their personal data can be used in their daily lives (Agarwal et al., 2020). Of numerous examples, online banking and ac-

cess to many government services such as health care are driven by an institutional ability to used stored personal data. If a reasonable consumer was ever asked about what "data protection" means in these contexts, the scholarship confirms a general proposition that likely applies across the EU and PRC societies with equal accuracy. Most consumers are prepared to sacrifice some reductions in their personal data protection if it means they have greater convenience (Agarwal et al., 2020).

Conversely, these same consumers expect that their personal data will be rigorously safeguarded by any enterprise that has acquired it against third party attacks (the well-known database "hacker" phenomenon). The prominence attracted by massive data breaches involving personal financial information (especially credit card data held by financial institutions and large retailers) contributes to this consumer expectation (Makridis, 2021). It is suggested that public expectations regarding how government institutions will deal with personal data protection are different than those attached to consumer transactions. Citizens expect that their data privacy interests will be protected where State agencies ensure that all personal data collected by them "is accurate, complete, and up-to-date, and that it is properly stored and handled in a secure manner" (Mohsin, 2022).

Academic commentators will likely prefer a more technical cybersecurity definition, but the public will equate this cybersecurity phasing used by Kamshad Moshin as one that aligns with their general cybersecurity understandings. The key GDPR and PIPL data protection features are now presented with this Overview providing a useful reference point. It is not necessary to examine every regulatory provision to appreciate why the GDPR and PIPL frameworks reveal them as having more data protection similarities than differences.

4.2. GDPR

The Regulation is based on seven distinct but interconnected principles. These are summarised as: 1) overarching data collection and processing lawfulness, fairness, and transparency; 2) the data collection must only be undertaken for specific purposes (i.e., data cannot simply be collected, stored, or processed for some future, unspecified purpose(s)); 3) "data minimization", where only the data necessary to achieve a lawful objective will be collected; 4) all personal data retained regarding individuals must be accurate; 5) the data may only be stored for so long as it may be necessary to achieve its purposes; 6) all data must be securely held (data 'integrity and confidentiality'); and 7), those who have assumed GDPR data protection responsibilities are accountable for ensuring the first six principles outlined here are followed (European Parliament & Council of the European Union, 2016).

The detailed GDPR 'data controller' definition also assists in appreciating how these seven principles are expected to be upheld under the Regulation (Nettesheim, 2023). These controllers are any "natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law …" (Nettesheim,

2023) In other words, any individual or entity that assumes a data controller's role is bound by the regulation without exception. The possible legal sanctions facing controllers are serious—Maximum fines of €10 million, or 4 percent of annual turnover are permitted (Data Protection Commission, 2020). These serious available GDPR sanctions also underscore how the following preliminary conclusions were reached.

4.3. Principle-Based Preliminary Conclusions

It is suggested that a reasonable person who reads these GDPR principles collectively will reach two preliminary conclusions. The first concerns the ways that each principle is directed at a specific data protection objective, as each cited Article deals with a particular point on the personal data collection, storage, processing, and transmission continuum (Gilman, 2020). The Regulation conveys a sense of regulatory commitment to individual citizen (data subject) rights. The second conclusion builds on the first. There is a clear sense that data protection rights are the rule, and any exceptions that might be sought by private enterprises or State data controllers will likely be strictly limited and restrictively interpreted in the event of any dispute (Gilman, 2020). The reasonable observer would likely characterise the overall GDPR effect as strongly "pro data subject" (Layton, 2017).

Two specific principles highlighted above lend further support to these preliminary GDPR conclusions. The first "lawfulness, fairness, and transparency" principles have potentially far-reaching data protection consequences for its data subjects and data controllers (or processors) alike. "Lawfulness" is a general concept that conceivably might include whether the relevant data was collected with the data subject's consent, a contract exists where the data collection is necessary to fulfil all applicable contract terms, or the collection otherwise satisfies a legitimate interest (institutional, government, or other third parties) (Malgieri, 2020). In a similar fashion, GDPR fairness as defined in its Article 5 provisions is usually understood in procedural terms: fairness means "…the mitigation of data subjects' vulnerabilities through specific safeguards and measures" (Malgieri, 2020: p. 7).

4.4. Data Subject Vulnerability & GDPR

The highlighted word is a key summarised GDPR objective when the Regulation is collectively assessed. There is a logical assumption built into the GDPR framework that data subjects are placed at a natural disadvantage vis-a-vis the relational power wielded by most data controllers. The following example is directly connected to the "consumer convenience - data collection" point introduced above. Consumer X wants to obtain a credit card from Bank Y. Y directs X to complete an application form whereby X must provide all pertinent personal financial information, age, address, occupation, and other data. If X wants a credit card, they must provide Y with this data—Y will not make any individual data subject exceptions no matter what grounds X might rely upon to keep this information from Y (Nettesheim, 2023: pp. 2-3).

It is noted in passing that in addition to the lawfulness elements outlined above, GDPR Article 6(1)(b) sets out the various justifications data controllers may rely upon to process personal data. Article 6(1) is an exhaustive list. It confirms that data controllers act "justifiably if the processing of personal data is necessary for the performance of a contract to which the data subject is party" (Nettesheim, 2023: pp. 2-3). The impressions left in the reasonable observer's mind regarding the 'pro' GDPR reading outlined above are not weakened or otherwise qualified by this observation. The EU leadership plainly wanted clearly defined justification definition parameters to ensure that data subject vulnerabilities cannot be exploited by controllers to their advantage (Malgieri, 2020: pp. 7-9).

4.5. Accountability

This second of the seven enumerated GDPR principles is another important way to appreciate how the Regulation safeguards against controllers exploiting data subject vulnerability. As further considered in Part 5, 'accountability' also assists when comparing the respective Supervisory Authority and CAC roles within each regulatory framework. Under GDPR auspices, it is accepted that different data controllers will adopt data protection measures as best suited to their operations and their data subjects (Ivanova, 2020). A small, independent retailer who processes their customer's credit card transactions will assume GDPR compliance obligations (and all related accountability requirements) that are fundamentally less extensive than what a hospital might assume when dealing with their patients' personal data (Ivanova, 2020: pp. 3-5). The PIPL framework is now considered using these specific GDPR points as comparators.

4.6. PIPL Approaches

The PIPL regime is aligned with the general thrust of all international data protection development as summarised in the project Introduction. It is therefore unnecessary for present comparative analysis purposes to devote significant effort regarding where the two regulatory frameworks are similar. The following summary is a suggested sufficient platform to support a detailed Part 5 analysis of where the PIPL appears to depart from the GDPR "gold standard" directions, especially concerning how each respective regulator is permitted to discharge their oversight role (Yin & Zhang, 2022).

The intended PIPL jurisdiction is similarly defined to that enjoyed by GDPR regulators. PIPL provisions are applicable to any organisations operating within the PRC that collect and process anyone's personal data. The regulation also governs the activities of any legal entities operating beyond the PRC's territorial jurisdiction that collects and processes any PRC citizens' personal data where the entities activities include: 1) providing these potential data subjects with products and services, 2) extracting any information that permits the entity to learn specific information concerning the data subjects' behaviours (such as information that might assist the entity in marketing its products or services to a particular con-

sumer or their demographic), or 3), any other purposes as deemed relevant by the regulatory authority (Penta Security, 2021). This third extra-territorial PIPL regulatory jurisdiction invites specific Part 5 attention concerning how the CAC is likely to exercise it for the foreseeable future (Greenleaf & Livingston, China's Personal Information Standard: The Long to a Privacy Law, 2017: pp. 25, 28).

The PIPL and GDPR jurisdictional scope are similar to the extent that each data protection regime is not limited to where the data collection, control, processing, or transfer might specifically occur. Each Regulation emphasises that where the data subject is located must guide how their data protection is regulated. The reasonable observer introduced above would likely endorse the PIPL approach as sound in this respect. The noted international community data protection trends that have encouraged the "pro" data subject rights attitudes echoed across the current scholarship are relevant here. These trends would lose much of their impetus if foreign-based enterprises could deal with PRC consumers' personal data without being accountable to them for its protection (Wang, 2023).

A small but vital distinction is revealed regarding these GDPR versus PIPL jurisdictional comparisons. The two frameworks differ concerning how foreign based data controllers must comply with the applicable regulations. The PIPL requires all such organisations to appoint a local representative who assumes direct PIPL reporting, and compliance responsibilities as directed by the CAC (as linked to its "Cross-Border Provision of Personal Information" requirements) (Office of Ethics, Risk & Compliance Services, 2025). This PIPL approach is indicative of how the CAC powers (depending upon one's view taken of the entire regulation) are either more flexible, or more susceptible to PRC central government control than the GDPR counterpart, a further point given specific Part 5 comparative attention.

4.7. Personal Information Security Impact Assessment

Consistent with the global trends referenced through Parts 4 and 5 that build on the GDPR "gold standard" characterisation, the PIPL mandates all data controllers to carry out a Personal Information Security Impact Assessment (PISIA), which the GDPR describes as a Privacy Impact Assessment (also PIA) (Office of Ethics, Risk & Compliance Services, 2025: pp. 55, 56). The general PISIA purposes are the same as those declared under the GDPR provisions: the data controller's self-examination concerning a data subject's personal information lifecycle ("including collection, storage, use, processing, transmission, disclosure, deletion, etc.") (Wang, 2023).

The PISIA process has been devised to ensure that all entities that fall within PIPL jurisdiction can effectively assess whether their data gathering, and all related data processing conduct is PIPL compliant. The assessment also encourages these entities to determine whether their data protection measures are effective, particularly when determining whether "the risk… of damage to the legitimate rights and interests of the personal data subjects" exceeds the data collection—

processing benefits (Wang, 2023).

4.8. Triggering Events

It is the three PISIA triggering events that assist in understanding how the general PIPL-GDPR similarities observed in this respect have practical differences when any legal entities are seeking to achieve full PIPL compliance. The first PISIA trigger concerns any entities that are engaged in the processing of a data subject's personal information for any reason that includes: 1) the entity deciding to provide this data to other (third party) personal information processors, 2) disclosing personal information to any third parties for any purposes whatsoever, 3) transferring any personal information to foreign based enterprises of any kind, and an umbrella requirement concerning "other processing activities that have a significant impact on personal rights and interests" (European Parliament & Council of the European Union, 2016). The notional reasonable observer relied upon above who accepts the importance of data protection generally would endorse this first trigger—PISIA requirement as sound and consistent with the prevailing GDPR "gold standard" (Shi & Wang, 2023: pp. 16, 28).

Two other PISIA triggers are philosophically aligned with how the GDPR regime operates in this respect, but their specifics are framed in different terms than the EU law. The PRC Measures of Data Cross-Border Transfer Security Assessment provisions are the second PISIA trigger. This specific assessment type is required when any enterprise as defined by the PIPL engage in certain levels of cross-border personal data transmission. The current level is set by the CAC as one requiring a PISIA is "providing 100,000 pieces of personal information or sensitive information of 10,000 people abroad" (Kennedy, 2022). This level of 100,000 records has garnered attention as, since September 2022, with the entry into force of Measures for Security Assessment of Outbound Data Transfers, when the volume of a specific set of data transfers reaches 100,000 records, it will be subject to a state-mandated, CAC-conducted security assessment, instead of a self-assessment (Cyberspace Administration of China, 2022; Ross, 2022). The CAC mandates companies falling within these data transmission levels to make a self-assessment. Once completed, the CAC is permitted to review the assessment result as part of its process to decide whether a "data cross-border transmission security declaration" (CAC permission) will be issued (Kennedy, 2022). These specific CAC-PIPL requirements are (arguably) more detailed and therefore onerous than those applied by their GDPR Supervisory Authority counterpart.

The Information Security Technology Personal Information Security Specification is the third PISIA trigger (National People's Congress of People's Republic of China, 2021). The CAC is permitted to require a PISIA prior to any commercial enterprise being permitted to engage in any of the following activities: 1) their intended release of any new products or services, 2) when the enterprise decided that it will make major changes to its business model, or 3), when a "personal information security incident occurs" (such as the credit card "hacks" described

above) (Standardization Administration of China, 2020; Kennedy, 2022).

These PISIA triggering events are attractively structured when viewed from the present GDPR-PIPL comparative analysis perspective. One can reasonably assert that in terms of what each Regulation seeks to achieve—a workable balance between robust data subject protection and fair data processing rights—there is little to choose regarding which framework is "best". How the two Regulation regulators operate, and whether the Supervisory Authority and CAC roles reveal similar conceptual and practical similarities are now considered.

5. Data Protection Regulators under GDPR & PIPL

5.1. "Gold Standard"?

This frequently employed GDPR descriptor invites a brief additional critique before turning further comparative attention to the two regulation regulators. One might logically expect an authoritarian State like the PRC to implement data protection laws that give the State greater powers to regulate data protection, including State power to monitor personal data collection, processing, and transfers that might conceivably involve State security interests. The ways that some international commentators have alleged PRC authorities' ability to accessing social media platforms and then obtain data subjects' personal information are items that contribute to this PRC expectation (Lomas, 2022).

The general PIPL language largely contradicts this expectation, leaving aside the Supervisory Authority—Cyberspace Administration of China (CAC) comparisons undertaken below. It is arguably impossible to interpret the PIPL articles' literal language in any other way. PIPL Article 1 states the law accords with the PRC Constitution to "protect personal information rights and interests, regulate the processing of personal information, and promote the reasonable use of personal information" (National People's Congress of People's Republic of China, 2021). Its companion Article 2 provides that any natural person's information "shall be protected by law, and no organisation or individual may infringe upon the personal information rights and interests of any natural person…" (National People's Congress People's Republic of China, 2021) Intentional or otherwise, the PIPL language is a reasonable paraphrasing of its GDPR counterparts. The literal PIPL meaning and its practical interpretation is now considered using the respective Supervisory Authority and CAC roles as primary guidance.

5.2. The Supervisory Authority

The Supervisory Authority has a multi-faceted role within the broader GDPR framework. An independent public authority, the Authority uses a combination of investigative and corrective (sanctioning) powers to supervise how the Regulation is applied at the EU and member states levels (Golden Data, 2023). The Authority is permitted to provide any GDPR stakeholders with expert advice concerning any GDPR-related data protection issues. It is also constructed to administer and resolve complaints made regarding alleged violations of any European

Data Protection Law (including the GDPR), as well as those connected to relevant member state laws) (Golden Data, 2023). The Authority's regulatory ambit is broad. Every EU Member State has its own Authority (European Parliament & Council of the European Union, 2016), and every EU citizen possesses a clear constitutional right to file complaints concerning any alleged violation of their data protection right (pursuant to EU Charter Article 8.3) (European Union, 2009; European Union, 2010).

Under EU law, entrenched constitutional rights necessarily mean that the potential to judicially explore how a Supervisory Authority must operate within defined legislative and constitutional boundaries is significant (European Union, 2009; European Union, 2010). Charter Article 8 is the basis for much of how the GDPR is structured—data protection as akin to a human right. Article 8 defines "Protection of personal data" in terms that include universality (every EU citizen can exercise the right), and the fairness concepts emphasised in Chapter 2 (European Union, 2009: pp. 8.1-8.3).

5.3. An Instructive Legal Opinion

There are various case law and commentary publications that have dealt with different aspects of the GDPR Supervisory Authority role. As outlined in a highly instructive 2019 Dan Svantesson article, the Advocate General's (AG) Opinion regarding the "competence of a supervisory authority in case of a change in circumstances relating to the main or single establishment" is likely as relevant as any other available legal opinion concerning how the respective Supervisory Authority and CAC roles should be contrasted or compared (Svantesson, 2019). It is emphasised that simply because the Opinion has been selected for inclusion in this analysis does not mean that the Opinion reasoning is sound, or that its author has properly defined the Authority's role. A careful reading of this Opinion confirms that Svantesson has accurately described its content in these unflattering terms: "… Its reasoning is unconvincing and its conclusion troubling…" (Svantesson, 2019: pp. 2-3)

In this Opinion, the AG was asked to review certain positions adopted by the European Data Protection Board (EDPB) (Svantesson, 2019: pp. 2-3). For present analysis purposes, the specific dispute facts are less important that the principles cited by the AG and their relevance to how the Supervisory Authority roles should be discharged and understood. The EDPB had issued guidelines governing whether a single Supervisory Authority that was responsible for a particular data controller activities' regulation in State A would continue as the relevant Authority if the controller changed its operations location or otherwise became involved in data controller activities cantered in State B (European Data Protection Board, 2019; European Data Protection Board, 2018).

The EDPB opinion confirmed that in such circumstances, three objectives were likely paramount: 1) both data controller and data subjects were entitled to "a sufficient degree of legal certainty and foreseeability"; 2) good, effective regulatory

administration considerations must be accounted for at all times (avoiding any data controller attempting to engage in "forum shopping" by seeking out a Supervisory Authority that was prepared to adopt a more lenient view of its data controlling activities); and 3), "to limit the risk of concurrent competences between authorities" (the risk of two separate Authorities deciding similar data controller issues in conflicting ways) (European Data Protection Board, 2019: p. 6). It seems logical that the EDPB would seek to increase overall GDPR regulatory efficiency by ensuring that there was overall Authority consistency encouraged among all EU member state regulators wherever possible (Article 29 Working Party, 2017).

5.4. Potential Supervisory Authority—GDPR Article 55 Conflict

Svantesson argues that the AG Opinion fails to properly align with how the GDPR Supervisory Authority Article 55(1) language must be understood. The Article specifically provides that every Supervisory Authority "shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State" (European Parliament & Council of the European Union, 2016) In other words, the learned commentator is advocating for a Supervisory Authority role that gives each State authority greater flexibility when assessing data protection rights—in accordance what the Authority deems appropriate to the individual member state's data protection needs (European Parliament & Council of the European Union, 2016). It is suggested that Svantesson has correctly identified a weakness within the Supervisory Authority structure—a leading Advisory Opinion does not appear to align with what the GDPR provisions require.

However, for present GDPR-PIPL comparative analysis purposes, the cited Opinion 8/2019 leaves no doubt regarding the fact that the EU regulation specifically outlines how Supervisory Authorities are expected to discharge their roles and responsibilities. For example, there is no question left with a reasonable observer when reading the GDPR provisions in their entirety that Supervisory Authorities must observe clearly defined regulatory boundaries. Of numerous examples, if the State A Authority purported to exempt all State financial institutions from complying with GDPR data protection rules on the basis that Regulation compliance costs were unreasonable, such actions would inevitably be overturned on any sensible judicial review. This opinion is based on a clear GDPR Article 55(2) interpretation concerning Supervisory Authorities' competence (European Parliament & Council of the European Union, 2016).

Paraphrased, Svantesson and other EU data protection law scholars (such as a lengthy 2022 Eyup Kun's article dealing with GDPR and impact assessments) may legitimately take issue with specific details or aspects of the prevailing GDPR regime (Kun, 2020). Conversely, it is suggested that there are few credible or persuasive GDPR scholarly sources that could ever challenge the entire Regulation as unsound or lacking in fundamental transparency. The general need to have Supervisory Authorities discharging their combined investigative/corrective/advi-

sory roles explained above is clearly established—one that mirrors the international community data protection trends cited above (Golden Data, 2023). Whether the same optimism can be expressed and supported when the CAC powers are examined is the crucial issue resolved in the final Chapter 2 section.

5.5. CAC

The points presented here are an extension of the introduction reference made to potential CAC role ambiguity, which in this context refers to a lack of legislative precision that grants the regulator significant discretion in its interpretation and enforcement actions, creating unpredictability for regulated entities. When the PIPL enactments were first published, Greenleaf and other data protection comparative scholars expressed significant surprise that the PRC (an undoubted "authoritarian central government") had crafted PIPL to ensure that its application appeared to extend to the PRC public sector (Greenleaf & Livingston, 2017: p. 28). For this reason, Greenleaf remained uncertain that the PRC provisions would ever be enforced in practice against State interests (Greenleaf & Livingston, 2017: p. 28). The possibility that Pernot-Leplay will ultimately be proven correct in his contention that the PIPL represents a "third way" taken between American and EU data protection laws cannot be discounted. The following sources tend to collectively reinforce the notion that the CAC powers are more opaque than transparent, thus revealing the primary difference that distinguished the two otherwise similar legal frameworks.

A 2021 practitioner's note provides a helpful summary of the factors that contribute to uncertainty regarding how CAC powers will be exercised over the medium and longer terms. The PIPL has "ambiguity and wide [CAC] discretion", particularly regarding what steps the CAC might permissibly take to monitor data that is transmitted to offshore third parties by foreign enterprises who either operate in or collect personal data from PRC sources (Penta Security, 2021). These ambiguities mean that making recommendations concerning how such companies should deal with CAC guidance is particularly challenging (Penta Security, 2021). The lack of transparency was highlighted in the July 2022 enforcement action against ride-hailing platform Didi Global. The CAC issued a record fine of approximately US$1.2 billion for violating the PIPL, Data Security Law and Cybersecurity Law. While the CAC identified specific ways in which Didi had over-collected user data, it also concluded that Didi's data practices had posed broader risks to "the nation's crucial information infrastructure and data security", without revealing any details, citing national security concerns (Bu, 2025). The action also showed the CAC's readiness to use such concerns to support heavy-handed enforcement, including levying personal fines against the company's senior executives, while remaining opaque about the actual evidence and rationale behind its most serious conclusions.

It is essential to move beyond any potential geopolitical bias that might be fostered by the events outlined in the project Introduction and thus focus on the

specific PIPL language that supports the CAC "ambiguity-opacity" observations made above (Creemers, 2022). It is facile to suggest that even from an ardent "Western" liberal democratic commentator's perspective, that solely because the PRC is at odds with the EU or any other Western states over geopolitical issues, its PIPL regulator will not act following PRC law. It is essential to avoid this possible research bias and deal directly with the PIPL provisions that might create ambiguities when the CAC regulatory oversight or related guidance is objectively reconstructed (Creemers, 2022).

5.6. Specific PIPL Extracts

Two provisions that govern how the CAC will regulate how data transfers are made from data controllers to other entities are selected here to build out the GDPR-PIPL comparative analysis. PIPL Article 13 deals with "Data transfers to domestic regulators or enforcement agencies" (National People's Congress of People's Republic of China, 2021). These transfers are generally permitted under Article 13, most notably where the relevant processing is deemed necessary to fulfil any identified "legal duties or obligations". The data subject's consent is not required (National People's Congress of People's Republic of China, 2021). It is suggested that this Article 13 power and any interpretation of its scope and effect should be relatively straightforward. For example, where a healthcare institution has personal data concerning Covid-19 rates, and the central government ordered the production of those records (including patients' personal data) (Lum, 2022) to determine how much the government spent to combat the pandemic, the healthcare body is clearly providing this data in accordance with a legal obligation—the government demand for this data.

The corresponding PILP provisions that govern "Data transfers to foreign regulators or enforcement agencies" (Article 41) are not so clear-cut in their apparent scope and effect. Article 41 provides that no PRC based enterprises (or foreign based enterprises that gather PRC citizens' personal data) may provide any personal information stored within the PRC to foreign judicial or law enforcement agencies, unless the CAC or another relevant PRC government agency has given their express permission for this data transfer (National People's Congress of People's Republic of China, 2021). Practitioner Nicholas Lum suggests that Article 41 is "substantively similar" to earlier PRC data protection legislation, where organisations operating within the PRC were prohibited from providing "…certain information to non-Chinese regulators and enforcement agencies…" (Lum, 2022).

To date, the CAC has not provided any additional clarity regarding what the Article 41 phrase "foreign judicial or law enforcement agencies" actually means. In its literal interpretation, one can readily imagine the CAC deciding that PRC-based data controllers cannot send any information concerning PRC citizens to foreign courts or police services. This Article might also invite the restrictive interpretation that national regulators (such as the UK Financial Conduct Authority) must not receive such data. Finally, the CAC has not published any guidance

concerning how a data controller might permissibly seek CAC Article 41 approval (Lum, 2022).

One can immediately conceive of situations where Article 41 permission might advance the greater international community good, as the following hypothetical example confirms. EU scientific research "think tank" (T) is seeking data regarding the incidence of dementia across the selected global population. Pharmaceutical companies (collectively "P") that deal with PRC retailers have data concerning how many PRC citizens are currently taking a particular medication to slow the otherwise devastating dementia effects. The CAC could conceivably prevent P from communicating any information that T might need to advance its study. CAC would not be required to provide any justification for its actions, notwithstanding the overtly humanitarian objective of the T research. The CAC could impose significant financial and other penalties (including asset forfeiture) if its direction given in this area was not obeyed (National People's Congress of People's Republic of China, 2021). The following commentary expands upon the points presented above.

5.7. Commentary—Likely Future Data Protection Directions Taken by the Supervisory Authority & CAC

The Greenleaf observations cited above confirm this scholar's surprise regarding the literal meaning scope and effect of the PIPL regime are revisited here. There is little doubt expressed here that if the CAC powers were excluded from this analysis, the notion that PIPL and GDPR were largely similar data protection and individual privacy regimes would be difficult to convincingly rebut. The fact that PRC is a strongly authoritarian state with a tradition of tight control exercised over all facets of its society does not mean that its data protection laws would remain deliberately outside the international community mainstream. In an era when the ability of States to work within international community expectations concerning data protection is a strong indicator concerning overall trading partner desirability, the PRC has plainly set out to build a data protection framework that satisfies this objective.

It is not troubling, or a looming international law and relations problem that the PRC regulator's powers are not yet clearly defined by either express PIPL regulatory language, or through CAC guidance. Prudent enterprises and institutions that are operating in the territorial PRC (Garg, 2025), or otherwise engaged in PRC individuals' personal data processing must take two important steps. Such entities must thoroughly review every possible PIPL provision that might conceivably apply to or otherwise influence their operations. Secondly, these entities must await further PRC directions as may come from the PRC regulator or its judicial system.

These observations are rooted in simple pragmatism. The PRC leadership has chosen to enact data protection laws that mirror mainstream international community attitudes in many respects. Logic suggests that over time, the CAC will

monitor the global trends that have contributed to the GDPR "gold standard" description. The PRC leadership (through the CAC) will likely assess how best to utilise its data protection laws in ways that preserve PRC desirability as a place for commercial activities, without losing its grip on any data protection issues that might undermine its national security considerations that are likely the primary motivation for the current PIPL Article 41 data restrictions. Part 6 of the conclusions also reflect these commentary sentiments.

6. Conclusion

It is tempting to conclude that the PIPL and GDPR are similar data protection enactments, so long as the PRC central government allows its CAC to operate in the same way as its GDPR Supervisory Authority counterparts. The geopolitical shadow that some commentators accept as coloring how the CAC will ultimately exercise its data protection regulatory powers is an influential factor in this reasoning. The various comparative analysis points developed in this paper tend to confirm a better, more nuanced conclusion. There is no doubt expressed here that the PIPL drafters have taken significant portions of the GDPR regime as their model. The data protection philosophies expressed in PIPL Articles 1 and 2 are consistently reflected throughout the entire Law (Goh & Tang, 2025). The key differentiation that must be made between the GDPR and PIPL frameworks is legitimately made, where the Regulation is clear regarding the roles that its member states' Supervisory Authorities must discharge, and similar language is conspicuously absent from the PIPL provisions.

It is easy to speculate that this PRC approach to defining the CAC's role is an extension of the PRCs traditional concern that centralised government control must be maintained over all facets of any regulatory process. A better conclusion has two parts: 1) the fact that the CAC powers are not currently clearly defined does not mean that such powers will never be defined in the same clear way that the GDPR regime is organised; and as importantly, 2) if the PRC was motivated to enact the PIPL to bring its data protection laws into better accord with the GDPR international "gold standard", a string possibility logically exists that at a future time, CAC guidance on issues such as Article 41 cross border data transfers will mirror how the Supervisory Authorities deal with these issues—only time will tell if current ambiguities and opacities are clarified. For EU, US, and other foreign firms operating in China, this regulatory landscape presents a concrete implication: the necessity of appointing a local representative or establishing a dedicated entity within the PRC to manage PIPL compliance and act as a direct liaison with the CAC, as mandated for overseas processors. The enhancement is not merely a procedural step but a strategic imperative to navigate the opaque and evolving enforcement environment.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

(EU) 2016/679 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union, 50,* 119.

Agarwal, S., Ghosh, P., Ruan, T., & Zhang, Y. (2020). Privacy versus Convenience: Customer Response to Data Breaches of Their Information. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3729730

Article 29 Working Party (2017). *Guidelines for Identifying a Controller or Processor's Lead Supervisory Authority (WP 244 rev.01)*. Article 29 Working Party.

Bo, H. (2023). Implications of the Ukraine War for China: Can China Survive Secondary Sanctions? *Journal of Chinese Economic and Business Studies, 21,* 311-322. https://doi.org/10.1080/14765284.2022.2136933

Bu, Q. X. (2025). The *Didi* Debacle: A Watershed of Financial Decoupling *vis-À-vis* Resilience Epitome of Global Data Governance. *Capital Markets Law Journal, 20,* kmae023. https://doi.org/10.1093/cmlj/kmae023

Chynoweth, P. (2013). *Legal Research in the Built Environment: A Methodological Framework*. CIB. https://www.irbnet.de/daten/iconda/CIB11548.pdf

Creemers, R. (2022). China's Emerging Data Protection Framework. *Journal of Cybersecurity, 8,* tyac011. https://doi.org/10.1093/cybsec/tyac011

Creswell, J. W., & Creswell, J. D. (2018). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (5th ed.). Sage.

Cyberspace Administration of China (2022). *Measures for Security Assessment of out Bound Data Transfers (in Chinese Only)*. https://www.cac.gov.cn/2022-07/07/c_1658811536396503.htm

da Silva, J. (2021). *The EU and the Brussels Effect on Human Rights Protection in the New Era of Technology*. Master's Thesis, University of Nova.

Data Protection Commission (2020). *Data Protection Commissioner v. Facebook Ireland Limited & Schrems*. Data Protection Commission.

European Data Protection Board (2018). *Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3)—Version for Public Consultation*. European Data Protection Board.

European Data Protection Board (2019). *Opinion 8/2019 on the Competence of a Supervisory Authority in Case of a Change in Circumstances Relating to the Main or Single Establishment*. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_201908_changeofmainorsingleestablishme.pdf

European Parliament & Council of the European Union (2016). *Regulation*.

European Union (2009). *Charter of Fundamental Rights of the European Union*. European Union.

European Union (2010). *Treaty on the Functioning of the European Union*. European Union.

Garg, M. (2025). *India's Data Protection Act: A Shield for Privacy or a Tool for State Surveillance*? Tech Policy Press. https://www.techpolicy.press/indias-data-protection-act-a-shield-for-privacy-or-a-tool-for-state-surveillance

Gilman, M. (2020). Five Privacy Principles (from the GDPR) the United States Should Adopt to Advance Economic Justice. *Arizona State Law Journal, 52,* 368-444. https://ssrn.com/abstract=3667795

Goh, G., & Tang, G. (2025). *China Data Protection and Cybersecurity: Annual Review of 2024 and Outlook for 2025 (I)*. Bird & Bird. https://www.twobirds.com/en/insights/2025/china/china-data-protection-and-cybersecurity-annual-review-of-2024-and-outlook-for-2025-(i)

Golden Data (2023). *What Is a "Supervisory Authority" (SA) under EU Data Protection Law*? The Media. https://medium.com/golden-data/what-is-a-supervisory-authority-under-eu-data-protection-law-5ea69d5b0ea2

Greenleaf, G. (2020). China Issues a Comprehensive Draft Data Privacy Law. *Privacy Laws & Business International Report, 168,* 6-10.

Greenleaf, G. (2023). Global Data Privacy Laws 2023: 162 National Laws and 20 Bills. *Privacy Laws and Business International Report, 181,* 2-4. https://doi.org/10.2139/ssrn.4426146

Greenleaf, G., & Livingston, S. (2017). China's Personal Information Standard: The Long March to a Privacy Law. *Privacy Laws & Business International Report, 150,* 25-36.

Ivanova, Y. (2020). Data Controller, Processor or a Joint Controller: Towards Reaching GDPR Compliance in the Data and Technology Driven World. In M. Tzanou (Ed.), *Personal Data Protection and Legal Developments in the European Union* (pp. 61-84). IGI Global. https://doi.org/10.2139/ssrn.3584207

Kennedy, G. (2022). *China's Security Assessment for Cross-Border Data Transfers, Effective September 2022*. Mayer Brown. https://www.mayerbrown.com/en/perspectives-events/publications/2022/07/china-s-security-assessments-for-cross-border-data-transfers-effective-september-2022

Kun, E. (2020). Questioning the Effectiveness of the Data Protection Impact Assessment Under the GDPR in Time of COVID-19 Crisis. In *Koronavirüs Döneminde Güncel Hukuki Meseleler Sempozyumu Bildiri Tam Metin Kitabı* (pp. 743-765). İbn Haldun Üniversitesi Yayınları. https://ssrn.com/abstract=4002566

Layton, R. (2017). How the GDPR Stacks up to Best Practices for Privacy, Accountability and Trust. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2944358

Lomas, N. (2022). *TikTok Privacy Update in Europe Confirms China Staff Access to Data as GDPR Probe Continues*. TechCrunch. https://techcrunch.com/2022/11/03/tiktok-privacy-policy-update-china/

Lum, N. (2022). *The PRC Personal Information Protection Law: Its Impact on Cross-Border Data Transfer and International Investigations*. Clyde & Co.

Makridis, C. A. (2021). Do Data Breaches Damage Reputation? Evidence from 45 Companies between 2002 and 2018. *Journal of Cybersecurity, 7,* 1-13. https://doi.org/10.1093/cybsec/tyab021

Malgieri, G. (2020). The Concept of Fairness in the GDPR. In *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency* (pp. 154-166). ACM. https://doi.org/10.1145/3351095.3372868

Mohsin, K. (2022). Data Privacy and Cybersecurity. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4299439

National People's Congress of People's Republic of China (2021). *Personal Information Protection Law of the People's Republic of China*. National People's Congress of People's Republic of China. http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm

Nettesheim, M. (2023). Data Protection in Contractual Relationships (Art. 6 (1) (b) GDPR). *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4427134

Oertel, J. (2020). *US-China Confrontation and Repercussions for the EU*. European Coun-

cil on Foreign Relations.
https://ecfr.eu/article/us-china-systemic-rivalry-repercussions-for-the-eu/

Office of Ethics, Risk & Compliance Services (2025). *China Privacy Law*. UC Berkeley.
https://ethics.berkeley.edu/privacy/international-privacy-laws/china-privacy-law

Penta Security (2021). *PIPL, How It Differs from GDPR and What It Means for Businesses*?
https://www.pentasecurity.com/privacy-policy/

Pernot-Leplay, E. (2020). China's Approach on Data Privacy Law: A Third Way between the US and the EU? *Penn State Journal of Law & International Affairs, 8,* 51-65.

Ross, L. (2022). *China's New Outbound Data Transfer Security Assessment Measures and Standard Contract Provisions*. WilmerHale.
https://www.wilmerhale.com/en/insights/client-alerts/20220725-china-new-outbound-data-transfer-security-assessment-measures

Shi, Z., & Wang, Y. (2023). *China's Risk Approach to Data Privacy: Analysing China's New Personal Information Protection Law under a Comparative Perspective*. SSRN.

Standardization Administration of China (2020). *Information Security Technology—Personal Information Security Specification (GB/T 35273-2020)*. Standardization Administration of China.

Svantesson, D. (2019). An Analysis of EDPB's Opinion on the Competence of a Supervisory Authority in Case of a Change in Circumstances Relating to the Main or Single Establishment. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3437565

Svetlicinii, A. (2022). China's Defense against Secondary Sanctions: Lessons from the EU Blocking Statute. *Journal of International Trade Law and Policy, 21,* 217-239.
https://doi.org/10.1108/jitlp-09-2021-0048

Tsai, L. (2021). *Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues Concerning the Application of Law in Handling Food Safety Criminal Cases*. Lexology.
https://www.leetsai.com/interpretation-of-the-supreme-peoples-court-and-the-supreme-peoples-procuratorate-on-several-issues-concerning-the-application-of-law-in-handling-food-safety-criminal-cases-2021

United Nations General Assembly (1948). *Universal Declaration of Human Rights (217A(III))*. United Nations General Assembly.

Wang, C., & Shen, T. (2023). Implications of the Eu's Position on Trade Distortion for Eu-China Trade Relations: From Selective Adaptation to Coordinated Compliance. *Asian Journal of WTO & International Health Law and Policy, 17,* 331-370.

Wang, S. (2023). *China Data Compliance through Personal Data Protection Impact Assessments*. Mondaq.
https://www.mondaq.com/china/privacy-protection/1320876/china-data-compliance-through-personal-data-protection-impact-assessment

Xue, H. (2010). Privacy and Personal Data Protection in China: An Update for the Year End 2009. *Computer Law & Security Review, 26,* 284-289.
https://doi.org/10.1016/j.clsr.2010.01.004

Yin, K., & Zhang, G. (2022). *China's Personal Information Protection Law and the Roadmap to Compliance*. Fangda Partners.
https://www.fangdalaw.com/wp-content/uploads/2021/08/China%E2%80%99s-Personal-Information-Protection-Law-and-the-roadmap-to-compliance.pdf

Zhu, J. (2022). The Personal Information Protection Law: China's Version of the GDPR? *Columbia Journal of Transnational Law: The Bulletin*.
https://www.jtl.columbia.edu/bulletin-blog/the-personal-information-protection-law-chinas-version-of-the-gdpr