Comparative Insights from the EU's GDPR and China's PIPL for Advancing Personal Data Protection Legislation

Article *in* Groningen Journal of International Law · September 2024

DOI: 10.21827/GroJIL.11.1.129-146

CITATION
1

READS
353

1 author:

Gulbakyt Bolatbekkyzy
Wuhan University
6 PUBLICATIONS **4** CITATIONS

SEE PROFILE

Comparative Insights from the EU's GDPR and China's PIPL for Advancing Personal Data Protection Legislation

Gulbakyt Bolatbekkyzy*
DOI: 10.21827/GroJIL.11.1.129-146

Keywords:
PIPL; GDPR; PERSONAL DATA; PROTECTION OF PERSONAL INFORMATION; CROSS-BORDER DATA TRANSFER.

Abstract:
The article outlines the fundamental principles of personal data protection and the legal frameworks that safeguard individuals in the ever-evolving digital world. By examining the regulatory frameworks, strategies, and outcomes of the European Union and China, the study aims to provide insightful lessons and potential best practices that can be adapted to suit specific national contexts. Additionally, it discusses the challenges with interpreting, applying, and enforcing the General Data Protection Regulation (GDPR) of the EU and the Personal Information Protection Law (PIPL) of China. Finally, it highlights the features of the PIPL, which is the country's first comprehensive law controlling the protection of personal information comprehensively. The constant comparative method guided the data analysis, which was based on the publications from the official documents of two respective states, which in turn served as the main source to compile the content of the research. It shows the difficulties and shortfalls of both legislations and offers comparative ideas from China's PIPL and the EU's GDPR for advancing personal data protection laws. Concluding remarks highlight the need for continual discussion and revision of legal frameworks to reconcile the benefits of technological advancement with the defense of fundamental rights in digital space.

* Ph.D Candidate and Doctoral Scholar, Wuhan University School of Law, China, e-mail: gulbakyt@whu.edu.cn.

I. Introduction

From a legal standpoint, data protection in digital governance is unquestionably of the utmost importance due to its complex consequences for individual rights, government accountability and openness, as well as its internationally bound obligations. Large amounts of personal data are currently being collected, managed, and stored by government organizations in the age of digital government. Without thorough and efficient data protection safeguards, citizens' rights and privacy may be in danger. Numerous international legal instruments recognize the preservation of individual privacy as a fundamental human right.[1] One of the most noteworthy legal accomplishments in this domain is the observance of Data Protection Laws. To guarantee the appropriate processing of personal data by authorities, numerous states have passed laws and regulations dealing with data protection.[2] When government agencies collect and handle personal data about individuals, they have legal obligations to follow. In the event of not following, [3] may result in penalties, fines, and other legal repercussions.[4]

Transparent data collection and processing, one of the core principles of contemporary governance, fosters citizen-government confidence and demonstrates the accountability and transparency of the government.[5] Therefore, in law and governance, trust is acknowledged as a fundamental component of successful digital government initiatives.[6]

---

[1] Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR) art 12; International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR) art 17.

[2] See here: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1; Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People's Congress of the People's Republic of China), Zhonghua Renmin Gongheguo Geren Xinxi Baohu Fa 中华人民共和国个人信息保护法 (Personal Information Protection Law of the People's Republic of China), http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml accessed 12 March 2023.

[3] Since the 1990s, the British government has passed a number of legislations relating to information security; however, in 2008, the government established Her Majesty's Government (HMG) Security Policy Framework after a noteworthy event in 2007. The loss of 25 million people's dates of birth, residences, bank account details, and national insurance numbers fell under the purview of the government. Another name for this incident is the HM Revenue and Customs (HMRC) problem. The breakdown of trust between state and citizen that exposed half of the British population to the risk of theft and fraud prompted a very attentive government to invest in better, more effective security legislation. It was found that the staff's ignorance of information security and disdain for the HMRC security regulations were the main causes of the event. (Poynter, K., 2008. Review of Information Security at HM Revenue and Customs: Final Report).

[4] Korean phone company KT compromise 8.7 million people's personal information. (Paganini, P., 2012. South Korea, 'Another Data Breach. How Is Changing the Hacking World?' http://securityaffairs.co/wordpress/7775/hacking/south-korea-data-breach-hacking.html accessed 30 July 2023). The public expressed outrage not only because the stolen data was sold to telemarketing companies but also because the hack occurred five months before it was detected. As a result of these and other data breach incidents, legislators pushed for more stringent laws, such as network separation.

[5] United Nations. (2013). UN E-Government Survey 2014: E-Government for the Future We Want.

[6] Cannataci, J. A., Zhao, B., Torres Vives, G., Monteleone, S., Mifsud Bonnici, G., & Moyakine, E. (2016). Balancing Privacy and Transparency and Redefining Their New Boundaries in the Internet Ecosystem. In Privacy, free expression and transparency: redefining their new boundaries in the digital age (pp. 88-91). (UNESCO Series on Internet Freedom). UNESCO. http://www.rug.nl/research/groningen-centre-for-lawand-governance/onderzoekscentra/step-research-group/project-descriptions/unesco-study-privacy-andtransparency.

Research on international law has always been conducted chronologically and with an eye toward the past. Since there were more international interactions, conferences, and agreements in the nineteenth century than ever before, this approach was especially apparent. The abundance of data from official archives made available in the years between the two world wars and it significantly boosted interest in diplomatic history. After the Second World War, however, a new movement focused on the study of power politics and an understanding of international relations in terms of the ability to control and influence others – arose dramatically.[7]

Behavioralist movement success was evident in the ensuing "wave of advance." This line of thinking combined elements of sociology, anthropology, and psychology with the study of international affairs, paralleling similar developments within the realism school. It signaled a change in emphasis from evaluations of the global political order in terms of optimistic or pessimistic (or "realistic") theories to an analytical study of the system as it exists today through the use of social science tools and field research. Actually, it is more of an attitude toward law and society than it is a philosophy in the traditional sense.[8]

This school of thought originated with the development of concepts regarding the role of government in society. The strict limitations on state activity and the individualistic morality of the nineteenth century have given way to a markedly different mindset during the last three generations. One example of how the focus has moved to emphasize the government's commitment to its citizens is the remarkable expansion of welfare legislation. Though it would have seemed unimaginable in the middle of the twentieth century, laws and regulations covering a wide range of human activity have multiplied in the developed world, and theory has had to adapt to keep up with these reorientations.[9]

Currently, one who is concerned and interested must consider the characteristics of a given society, its significant demands, and its customary values in order to fully comprehend the operation and general function of law. As a result, law is now a dynamic process that needs to be examined in the context of society rather than just a collection of ideas that can be understood on their own. The social sciences have assumed the lead in this reviewing of society, and they have greatly influenced the behavioral approach to law, both in terms of overall perspective and in terms of supplying the instruments required to examine society and determine its direction and modes of operation.[10]

Fundamental human rights are safeguarded by international law, and at the moment, many of these rights are intimately linked to the protection of personal information digitally. Data protection must be recognized as a fundamental element of the wider human rights framework in order to develop legal norms that safeguard individuals in the ever-evolving digital world. To reconcile the benefits of technological advancement with the defense of fundamental rights, legal frameworks must be modified. It surely necessitates continual discussion and revision of legal frameworks.[11]

---

[7] Kenneth W. Thompson, *Political Realism and the Crisis of World Politics*: *An American Approach to Foreign Policy* (Princeton University Press 1960).

[8] Wesle L. Gould and Michael Barkun, *International Law and Social Sciences* (Princeton University Press 1970).

[9] Hans Kelsen, *General theory of law and state* (1st 1945, Routledge 2017).

[10] Amnon Lehavi, 'The Dynamic Law of Property: Theorizing the Role of Legal Standards', (2010) vol. 42 Rutgers Law Journal 81.

[11] Igor Calzada, 'Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL)' (2022) vol. 5(3) Smart Cities 1129.

II. Methods

Background information that helped to understand the legal and political context in which e-government projects concerning the issue of protection of personal data in the digital space were conceived and implemented was given by primary data collection methods (interviews of government officials) and a thorough, systematic review of documents (reports, government publications, and state programs in the field of personal data protection). It was therefore possible for us to comprehend the paper's subject matter – which was examined in relation to the countries where those legal frameworks were actually put into practice – more thoroughly and in depth. The data analysis was conducted using the constant comparative approach and was based on publications from the official websites of two countries. These websites were the primary sources used to create the content of the research that is presented further.

III. Discussion

In this regard, the practical experiences of the European Union and China can serve as valuable benchmarks for countries aspiring to enhance and develop their legislation in the protection of personal data. Examining the regulatory frameworks, strategies, and outcomes of these influential entities provides insightful lessons and potential best practices that can be adapted to suit specific national contexts.

"Everyone has the right to respect for his private and family life, his home, and his correspondence", according to the 1950 European Convention on Human Rights.[12] The right to privacy is covered by this provision. By enacting laws based on this principle, the European Union has attempted to ensure the protection of this fundamental right.

The EU recognized the need for new protections as a result of technological advancements and the development of the Internet. Thus, in 1995, it passed the European Data Protection Directive, which set minimum standards for data security and privacy and functioned as the basis for national legislation in each of the member states. But the Internet was already evolving, becoming into the heavy on data environment that it is today. In 1994, the first banner ad on the internet appeared.[13] In 2000, the majority of financial institutions offered online banking.[14] In 2006, Facebook made its public debut.[15] Due to Google scanning the emails, a user filed a lawsuit against the company in 2011.[16] Within two months, the European Union's data protection body determined that the need for "a comprehensive approach on personal data protection" in the EU had arisen, and the 1995 directive update process was under way.[17]

---

[12] United Nations General Assembly. The Universal Declaration of Human Rights (UDHR). New York: United Nations General Assembly, 1948.

[13] HubSpot, 'A Brief History of Online Advertising' <https://blog.hubspot.com/marketing/history-of-online-advertising> accessed 23 July 2023.

[14] Mary J. Cronin, *Banking and Finance on the Internet* (John Wiley and Sons 1997).

[15] Mythili Devarakonda, 'The Social Network': When was Facebook created? How long did it take to create Facebook?' (25 July 2022) https://www.usatoday.com/story/tech/ accessed 28 July 2023.

[16] Warwick Ashford, 'US woman sues Google over Gmail scanning' (11 August 2011) https://www.computerweekly.com/news/2240105327/US-woman-sues-Google-over-Gmail-scanning accessed 2 August 2023.

[17] European Data Protection Supervisor 'The History of the General Data Protection Regulation' (25 May 2018) https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en accessed 3 August 2023.

The GDPR went into effect on May 25, 2018, following its approval by the European Parliament in 2016. This required compliance from any businesses that handled the data of citizens and residents of the EU.[18]

The GDPR is now regarded as the world's most challenging privacy and security legislation. Despite having been developed and authorized by the European Union (EU), it places restrictions on any organizations that seek out or collect data about people living in the EU. Those who violate the GDPR's privacy and security requirements risk facing harsh fines of up to tens of millions of euros.

With the GDPR, Europe is demonstrating its strict stance on data privacy and security at a time when an increasing number of individuals are entrusting cloud services with their personal data and breaches are happening on a regular basis. The GDPR is an overwhelming challenge for small and medium-sized enterprises (SMEs) in particular because of its expansive nature, broad application, and a shortage of detail.

The most notable feature of the EU GDPR is its extraterritorial reach, which increases its applicability outside of EU boundaries. Article 3(2) of the GDPR states that this includes data processing operations done by non-EU businesses that target or monitor EU citizens' behavior. This extraterritoriality challenges the foundational ideas of jurisdiction in international law.[19] Due to the extraterritorial application of the GDPR, worldwide firms have been forced to conform to its standards, which has resulted in a global adoption of stronger data protection measures and a paradigm shift in global business operations.

The General Data Protection Regulation (GDPR) has significantly affected the international transfer of personal data, affecting data controllers and processors worldwide. A number of countries are recognized as providing an "adequate level of protection", as per Article 45 of the GDPR. This acknowledgement affects data flows and necessitates compliance with EU data protection regulations. Such GDPR laws surely affect international data flows and give rise to worries about sovereignty, since the GDPR's severe data transfer restrictions have prompted some businesses to consider data localization strategies.

While company leaders globally may find it challenging and complex to comply with the EU GDPR standards, governments worldwide have used this as a model for implementing similar requirements in their own local data protection authorities. Global data protection standards have been brought into line with the GDPR-inspired regulations that have been adopted by a number of countries, including Brazil, India, and South Korea. International agreements, such as the EU-Japan adequacy decision, which integrates GDPR principles, and talks in international platform about common data protection standards have been influenced by the GDPR as well.

International law has been profoundly impacted by the EU GDPR, which has also altered the data protection landscape. The issues, impact on data flows, global influence, and extraterritorial reach of data protection in the digital era are all reflections of its expanding dynamics. As more countries align their data protection laws with the regulations' requirements, the GDPR's impact on international law is anticipated to continue

---

[18] EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016

[19] Cases like *Google LLC v. CNIL* (2019) show how the GDPR is enforced extraterritorially. The CNIL fined Google, a U.S.-based firm, for failing to follow EU data privacy laws, demonstrating the GDPR regulation's reach outside of the EU.

and shape the direction of global data governance in the future. It is a challenging endeavor that necessitates ongoing attention and international cooperation to maintain a careful balance between the protection of individual data rights and the need for international data flows.

Even if the GDPR's overall project and comprehensive approach were structured in a reasonably ideal manner, there were still a few shortcomings with it.

It is having to do, first and foremost, with the lengthy and difficult process of establishing specific legal terminology in the rule. For example, as stated in Article 32 of the General Data Protection Regulation (GDPR), the concerned companies must create appropriate organizational and technical measures for data protection while "taking into account the state of the art". In the event of non-compliance, Article 83 of the GDPR stipulates penalties of up to more than 10,000,000 EUR, or 2% of the global annual revenue. The penalty may be significantly higher in the event that a substantial provision is broken; it could be up to 20,000,000 EUR or 4% of annual global revenue, whichever is larger.[20] Because of the GDPR's harsher regulations and substantial penalties, compliance is crucial for impacted businesses.[21] Developing security measures requires a thorough understanding of what "state-of-the-art" means in the context of the GDPR. In addition, terms like "disproportionate effort", "likelihood of (high) risk to rights and freedoms", and "undue delay" are vague and may require more explanation from authorities or the courts, or some time for particular market practices to emerge. Similarly, authorities have a great deal of discretion in determining the appropriate fine for data breaches and non-compliance because the legislation does not define what a "reasonable" degree of data protection is.

European nations are demonstrating a strong desire to improve data subject protection (Costeja case).[22] Fines for noncompliance with GDPR are more than ten times greater than those for violating critical infrastructure security rules.

The GDPR and national laws of European nations,[23] are made more confusing by the use of terms like "state-of-the-art". Legislators can avoid enshrining a technology by its name only for it to become outdated in a few years by using the accepted legal term "state-of-the-art". Even while it is still evident that much of the language adheres to internationally or nationally accepted rules, like ISO standards, there is still a tremendous deal of ambiguity and complexity. For example, work would have to be based on ISO 27001 the "State-of-the-Art" for information security management systems (ISMS) requires an understanding of information technology, security techniques, and ISMS requirements.[24] It is unclear what exactly those legal security criteria entail because of the terminology being

---

[20] EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016

[21] Jukka Ruohonen and Kalle Hjerppe, 'The GDPR enforcement fines at glance', vol. 106 Information Systems 101876.

[22] Eleni Frantziou, 'Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos', (2014) vol. 14(4) Human Rights Law Review 761.

[23] I.e.: Germany and its BSI (Bundesamt fuer Sicherheit in der Informationstechnik, Federal Agency for Security of Information Technology) guidelines. For further reading, Jan Pohle, 'Persönliche Verantwortung und Haftung Risiken von IT-Verantwortlichen e Zivilrechtliche Aspekte', (2005) DFN Arbeitstagung über Kommunikationsnetze in Düsseldorf 103.

[24] Sokol, P., Míšek, J., & Husák, M. (2017). Honeypots and honeynets: issues of privacy. EURASIP Journal on Information Security, 2017, 1-9.

purposefully ambiguity.[25] However, incident-related requirements are referenced in the GDPR but lack a clear definition. Things like breach-focused incident response strategies and methods for extracting digital evidence from them become serious matters when one considers the potential legal and social consequences their absence could have on organizations.

Despite this awareness, the ambiguity of the legal security requirement still concerns a lot of enterprises. Especially in light of GDPR Art. 82 No.3, which stipulates that the controller and processor of data bears the burden of proof and that they "... shall be exempt from liability... if it proves that it is not in any way responsible...". Given the significant costs associated with non-compliance with GDPR, organizations would require more specific criteria of appropriate security measures. Lack of proper planning and standards defining what acceptable security mechanisms are required and how to include them could lead to legal instability for both users and companies.

Three more security requirements are listed in GDPR Article 32,[26] in addition to encryption and pseudonymization. These include:

- the capacity to guarantee the system and services' confidentiality, integrity, availability, and resilience;
- the capacity to quickly restore availability in the event of an incident;
- regular testing and assessment of the efficacy of organizational and technical safeguards.

In addition to the regulation's frequently ambiguous and legally complex language, it is observed that adhering to its fundamental guidelines became increasingly problematic. Take the Transparency and Consent Framework that the Interactive Advertising Bureau Europe (IAB Europe) recently developed. A significant number of content creators, marketers, and publishers use this framework extensively. The framework was developed by experts with cooperation from regulators and data protection agencies to guarantee that it complies with GDPR. However, the Belgian Data Protection Authority's (DPA) legislation states that the framework does not comply with GDPR. In other words, even highly skilled individuals find it challenging to adhere to GDPR regulations.[27]

The ruling proved that the GDPR is still in effect, but it doesn't explain the extent to which some of these violations were or how loudly industry opponents had been raising their concerns. Put another way, the IAB responded to the GDPR's requirement that the ad-tech industry get users' approval before tracking them by creating a set of regulations that were so flawed that data could still be gathered without consent. Moreover, currently nobody seems to know exactly how to stop these operations, that they are well known. In this regard, following Google-Spain case, another remarkable court decision comes as an example. The Dutch Preliminary Court in Amsterdam ruled on September 18, 2014, that Google Search was not required to remove information about a guy who had been found guilty in 2012 of a major criminal offense for attempting to kill someone through contract

---

[25] While the BSI (Bundesamt fuer Sicherheit in der Informationstechnik, Federal Agency for Security of Information Technology) in the case of Germany provides some baseline criteria, they are not focused on responding to breach situations and are first and foremost directed at federal agencies.

[26] GDPR (n. 3), art. 32.

[27] Damien Geradin, Theano Karanikioti and Dimitrios Katsifis, 'GDPR Myopia: How a well-intended regulation ended up favouring large online platforms – the case of ad tech', (2021) vol. 17 European Competition Journal, 47.

killing. He requested an injunction in this civil case to make Google delete all search results for specific websites that came up when someone searched for him on Google. He also asked Google to take down the search results that associated his identity with a private investigator in the Netherlands. The claimant cited his rights under the Costeja ruling of the European Court of Justice and the Dutch Data Protection Act. After providing a brief summary of the ECJ's test in the Costeja case, the Dutch Court interpreted it to mean that people would only be shielded from "being pursued" for an extended period of time by information that is "irrelevant, excessive, or unnecessarily defamatory", rather than against all negative communications on the Internet. The Dutch Court made it clear that removal demands, like the one in this instance, affected Google Inc.'s right to information freedom as guaranteed by Article 10 of the ECHR and Article 7 of the Dutch Constitution, as well as the claimant's basic right to privacy (Article 8 of the ECHR). Furthermore, consideration has to be given to the interests of both Internet users and information suppliers. Applying the criterion, the Court observed that a major crime might have a significant negative impact on one's reputation and leave potentially very long-lasting online traces. In general, information about someone who had committed a serious crime would still be useful. Such information would only be considered "irrelevant", "excessive", or "unnecessarily defamatory" under very special circumstances. A situation where the criminal act was brought up again without any obvious cause and seemingly only for the goal of harming the individual involved – a "slanging match" rather than accurate reporting – could serve as an example of such an uncommon circumstance.[28] In that specific case before the Dutch Court, the claimant had not demonstrated sufficient proof that the relevant search results were irrelevant, excessive, or needlessly defamatory, nor had he provided strong, justifiable arguments regarding his circumstances that would have obliged Google to take down the links. In addition, the plaintiff had served a lengthy jail sentence, and the offense had been featured on a television program. For these reasons, the Court was unable to see how Google's actions had a substantial negative impact on the plaintiff's private life. As a result, the claimant's request for an injunction against Google was denied by the court.[29]

This made it possible for the Authority to finally take the IAB straight to court over what it calls a "splash of violations". First of all, IAB Europe was found in violation of the judgment for having "failed to establish any sort of legal basis for the processing of these consent strings under GDPR" and for failing to keep the data "confidential" once it was gathered. Furthermore, the most recent ruling validates the complaints that a lot of us have long had against those cookie pop-ups: that they are blatantly deceptive, difficult to avoid, and inconsistent with what they claim to be.[30]

Rather than being viewed as a reason to declare GDPR ineffective, the difficulties with its interpretation, application, and enforcement should be seen as an opportunity to make

---

[28] Many legal systems recognize the protection provided by domestic law to publishers of information on convicted individuals, provided that doing so benefits the public interest. See judgment of Thailand's Supreme Court no. 7435/2541.

[29] Joran Spauwen and Jens van den Brink, 'Dutch Google Spain ruling: More Freedom of Speech, Less Right to Be Forgotten for Criminals', *Inform's Blog*, 27 September 2014.

[30] Shoshana Wodinsky, 'The Hidden Failure of the World's Biggest Privacy Law', Gizmodo (4 February 2022), available at <https://gizmodo.com/gdpr-iab-europe-privacy-consent-ad-tech-online-advertis-1848469604> accessed 8 August 2023.

improvements so that GDPR, or the updated version thereof, is a more responsive version that takes into account future technological advancements and societal aspirations.

Regarding the Personal Information Protection Law (PIPL), which went into effect on November 1st, 2021, it is China's first comprehensive law controlling the protection of personal information and data of "natural persons" residing within China. The 74 parts that make up the PIPL are divided into eight chapters. Given that China has the largest online population, it is expected to have a significant international impact and change how parties conduct business both inside and outside of China.

The PIPL does not only apply to activities that process personal data inside the PRC; it also applies to activities that process personal data outside the country,[31] so long as it involves the processing of personal data of any Chinese resident for the following purposes:

- supplying goods or services to the Chinese residents;
- analyzing or evaluating the behavior of the Chinese residents; or
- other situations permitted by law.

Similar to the EU GDPR, the PIPL requires international data processors under its jurisdiction to set up special organizations or representatives to manage personal data protection issues, and these representatives must report to the Chinese government on their operations.

Anonymized data is not included in the PIPL's definition of "personal information", which is defined as any information belonging to an identified or recognizable natural person (whether electronically recorded or not). Furthermore, "sensitive personal information" encompasses, among other things, biometric data, health data, financial account data, location data, and data about minors (those 14 years of age or younger) that could readily result in an infringement of human dignity or harm to a natural person's personal or property safety if leaked or used unlawfully. Additional guidelines have been published by PIPL for the processing of sensitive personal data.[32]

Articles 4,5 and 6 of the PIPL govern data processing criteria, and it states that personal information processing includes, among other things, the gathering, storing, using, processing, transferring, providing, disclosing, and erasing of personal information. Processing of personal data is subject to the requirements of lawfulness, fairness, necessity, and integrity; unfair, coercive, or misleading methods are not permitted.[33] Only stated, legal, and closely related purposes that are directly relevant to the purposes for which the data was obtained may be processed using personal information. It is also necessary to minimize the effect on people's rights and interests. The quantity of personal data gathered must be kept to a minimal and must not exceed the processing objective.[34] Personal information processors are only permitted to process personal information under the conditions outlined in the PIPL, which include (1) when an individual's consent has been obtained; (2) when necessary for the creation or performance of a contract, or for the management of human resources; (3) when necessary for fulfilling statutory duties or obligations; and (4) when necessary for responding to public health emergencies, or for the protection of life, health, and safety of others; (5) for the lawful processing of personal data necessary for news reporting, media regulation, and other public interest activities;

---

[31] PIPL (n. 4), art. 2.
[32] *Ibid*, art 4.
[33] *Ibid*, art 5.
[34] *Ibid*, art 6.

(6) for the lawful processing of personal data that has been made publicly available by individuals or is otherwise legally disclosed; and (7) in any other situation made possible by laws or administrative rules.[35] Additionally, it declares that no group or individual may improperly gather, use, process, communicate, trade, supply, or reveal the personal information of another person, nor may they process personal information in a way that compromises national security or materially harms the interests of the general public.[36] Image collection and personal identification technology in public spaces should only be used when absolutely necessary to protect public safety, together with prominent notices posted. The collection of identifying data and personal photographs may only be used to ensure public safety if the subjects have not provided their separate consent.[37]

In relation to the legal standards for data processing, it is important to note the following guidelines:

1. The PIPL has established particular guidelines for the processing of personal data in certain circumstances. It places matching legal requirements on the data processors and makes distinctions between joint processing, entrusted processing, and providing personal information to other processors.
2. The use of personal information for automated decision-making is particularly restricted under the PIPL. Before using automated decision-making processes to assess a person's financial situation and creditworthiness, it is required to undertake a security impact assessment, and upon a person's request, to explain the situation and offer alternatives. It is necessary to offer data subjects options that are not tailored to their unique features or to give them a straightforward way to refuse in the event of information push and commercial marketing to people through automated decision-making processes.[38]
3. The PIPL has provided four ways to enable the movement of personal data across international borders (cross-border transfer of personal information):[39]

- Pass the security evaluation conducted by the state cyberspace authorities, namely the Cyberspace Administration of China (CAC);
- Obtain certification in relation to personal information protection from professional institutions in accordance with CAC regulations;[40]
- Enter into a standard contract as prescribed by CAC with the overseas receiving parties to stipulate the rights and obligations of both parties;
- Fulfill accordingly to the conditions outlined in other laws or regulations or in the guidelines established by the state cyberspace authorities.

After one year of the PIPL's implementation, on January 16, 2022 the "Practical Guidance of Cybersecurity Standards - Technical Specifications for Certification of Cross-

[35] *Ibid*, art 13.
[36] *Ibid*, art 10.
[37] *Ibid*, art 26.
[38] *Ibid*, art 7.
[39] *Ibid*, art 38.
[40] The Implementation Rules for Personal Information Protection Certification (the Rules) were published jointly on November 18, 2022, by the State Administration for Market Regulation (SAMR) and the Cyberspace Administration of China (CAC). According to Article 38(2) of the PIPL, the Rules provide better guidance on the certification of personal information processors in connection to their cross-border personal information processing operations. In connection to the collection, storage, use, processing, transmission, provision, disclosure, erasure, and cross-border transfers of personal information, among other things, the Rules lays forth the fundamental principles and specifications for certification of personal information processors.

border Processing of Personal Information Version V2.0" (the Guidance) was released in a second edition by the National Information Security Standardization Technical Committee (TC260). The Guidance outlines a number of fundamental principles regarding the cross-border processing of personal information, requiring both personal information processors and the pertinent data receivers outside the jurisdiction to adhere to Mainland laws and regulations.[41] In addition, before engaging in cross-border processing activities, parties must, among other things, enter into legally enforceable agreements, appoint an officer to oversee the protection of personal information, and perform a personal information protection impact assessment. In addition, the Guidance provides protection for a variety of rights and interests of subjects of personal information, including as the right to revoke consent and the right to view and delete their personal data.[42]

Along with that it worth mentioning other major requirements of the Guidance, which are:

- Personal information processors applying for certification should be a legitimate legal entity currently engaged in business with a good reputation and goodwill;[43]
- Personal information processors and data recipients outside the jurisdiction should set up respective personal information protection agencies in order to fulfill their personal information protection obligations;[44]
- Cross-border personal information processing should be done in accordance with the guidance.[45]

As for legal liabilities that the PIPL impose on those who violate the regulations, it is comprehended in the following requirements. Personal information protection authorities may order rectification, give a warning, and seize illegal gains if the processing of personal information violates the PIPL's provisions. Those who refuse to correct their behavior may be fined up to RMB 1,000,000. A punishment of not less than RMB 10,000 but not more than RMB 100,000 may be imposed on the person in charge who is directly responsible as well as other staff members who bear direct accountability. Personal information protection authorities above the provincial level have the authority to order correction in serious situations, seize illicit gains, and levy fines of no more than RMB 50,000,000 or 5% of the prior year's annual turnover. In addition to ordering the suspension of pertinent business activities and business for correction, the personal information protection authorities may also notify the appropriate authorities to revoke pertinent business permits or licenses. In addition to being subject to a fine of not less than RMB 100,000 and not more than RMB 1,000,000, the person in charge and other staff members who bear direct responsibility may be barred from serving as directors, supervisors, senior managers, or personal information protection officers in the relevant corporations for a predetermined amount of time.[46] Penalties under the public security administration may be applied if the violation of the PIPL's provisions constitutes conduct that violates public security management. It will be accountable for criminal liabilities if it amounts to

---

[41] Guidance, part 5 (Basic Requirements).
[42] *Ibid*., part 6 (Protection of the Rights and Interests of Personal Information Subjects).
[43] *Ibid*., part 2 (Certification Bodies).
[44] *Ibid*., part 5.2.2 (Personal Information Protection Organization).
[45] *Ibid*., part 6.2 (Obligations for Personal Information Processors and Data Recipients located outside the jurisdiction).
[46] PIPL (n. 4), art. 66.

a criminal offence.[47] Infractions of the PIPL's requirements may be recorded in the relevant credit record and made public.[48]

China's implementation of the PIPL is a significant step in aligning its data protection framework with international standards. Its vast scope, emphasis on permission, rights of data subjects, and burdensome cross-border data transfer regulations are all reflections of global digital privacy trends. In order to maintain compliance, protect individual rights, and avoid legal issues, companies that handle personal data in China or deal with Chinese nationals need to be aware of their responsibilities under the PIPL. The PIPL affects cross-border data flows and global data governance since data protection is still a global priority.

It is preferable to incorporate the comparative analysis method into the current study in order to comprehend the greater reach of these two legislations. Even though PIPL was only recently put into effect, compared to its previously examined peers, it has received a lot more attention and specific details lately.[49] While there are some similarities between China's PIPL and Europe's GDPR, there are some differences as well. Since the PIPL obtains some principles from the GDPR, it is advantageous if the organization is already GDPR compliant. A similar compliance process can be applied for the PIPL. Nonetheless, there are still a few significant distinctions between the PIPL and the GDPR. These variations, along with China's distinct corporate, legal, and IT environments, can provide significant difficulties for international businesses operating with China or within China. [50]

The "establishment" of the business, which is typically defined as the location of the company's headquarters, is the primary focus of the GDPR for any enterprise that processes personal information (PI). If the business is incorporated in the EU, the GDPR will govern all PI processing activities the business undertakes, whether they take place inside or outside of the EU. On the other hand, the PIPL is more concerned with the location of the PI processing activity. The PIPL depends on whether the PI processing activity takes place on Chinese ground, whether it is done by a Chinese corporation or a foreign company operating out of China.[51]

This means that if a Chinese-established business processes the personal information of citizens of other nations, such as those in ASEAN nations, the PIPL does not apply to the business's processing activities because they do not occur in China and do not include the processing of Chinese citizens' personal information. Considering how strict the PIPL is, this gives businesses which operate in other nations and depend on the extensive processing of PI some freedom, particularly if local PI protection regulations are more lax than the PIPL. Companies outside of the territorial jurisdiction area – that is, outside of the EU and China, respectively – still have to abide by the PI rules because both the GDPR and the PIPL are extraterritorial.

The definition of PI is similar in the GDPR and the PIPL, however the PIPL expressly leaves out "anonymized" PI. The scope of "sensitive" PI (as defined in the PIPL) and "special category data" (as defined in the GDPR) is one of the key distinctions between the two

---

[47] *Ibid*., art. 71.
[48] *Ibid*., art. 67.
[49] Péter Molnár, 'Comparison of the new Chinese Personal Data Protection Law (PIPL) with GDPR and CCPA', Published in KRE-Dit 2021/2. <http://www.kre-dit.hu/tanulmanyok/peter-molnar-comparison-of-the-new-chinese-personal-data-protection-law-pipl-with-gdpr-and-ccpa/>.
[50] Ziwen Tan and Channing Zhang. 'China's PIPL and DSL: Is China following the EU's approach to data protection?', (2021) vol. 5(1) Journal of Data Protection & Privacy 7.
[51] Rogier Creemers, 'China's emerging data protection framework', (2022) vol. 8(1) Journal of Cybersecurity 11.

laws. Compared to special category data under the GDPR, the PIPL's definition of sensitive personal information is far more expansive. In the meanwhile, businesses and people can easily determine whether or not the PI they are processing falls within this category according to the GDPR's clear listing of all special category data. While lacking a comprehensive list, the PIPL's definition is nonetheless more detailed than the GDPR's.

According to Article 28 of the PIPL, "information that is likely to result in damage to any natural person's personal dignity or damage to his or her personal or property once disclosed or illegally used" is classified as sensitive information.[52] This is followed by a non-exhaustive list that include biometric information, details on religious views, "specific identity", health information, bank accounts, and whereabouts and location, in addition to any personally identifiable information (PII) pertaining to kids under the age of 14. Many international businesses were taken away to learn that financial account information is considered sensitive personal information (PI) because it suggests that handling sensitive PI is a part of nearly every commercial activity that involves a payment transaction. In this regard, Hangzhou Huatai vs Tencent case (杭州华泰房产中介 vs 腾讯) is noteworthy. In this case, Tencent was sued by Hangzhou Huatai, a real estate company, for unlawfully gathering personal data through its QQ platform. Tencent was found to have violated the PIPL by the court for improperly obtaining user consent prior to the collection and processing of personal data. This case emphasized the necessity for businesses to adhere to stringent data collection and processing requirements and underscored the significance of gaining explicit user consent under the PIPL.[53] Another significant case is related to the personal credit information, when an individual sued the bank for sharing his personal credit information with third parties without his consent. The bank was found guilty by the court of failing to obtain the required consent for data sharing, which was a violation of the PIPL. This judgment upheld the PIPL's mandate that data controllers, especially in delicate industries like banking and finance, have explicit and informed consent prior to disclosing personal information.[54]

While some EU member states have lower age limits, down to 13, the GDPR treats personal information of minors under the age of 16 as special category data. In contrast, the PIPL sets the age at 14, meaning that high school students' personal information will not be considered sensitive PI by default.

Deceased individuals are the subject of yet another, more significant distinction in the GDPR and PIPL's defined scope. Unlike the GDPR, the PIPL does not extend to the personal information of the deceased. On the other hand, a close relative of the dead may request access to or duplicate pertinent PI under the PIPL. Additionally, they have the limited ability to amend, remove, or replicate any pertinent PI in order to further their legal objectives.

Two key responsibilities in PI processing are defined in Article 4 of the GDPR: the data controller, who determines how and why to process personal data, and the data processor,

---

[52] PIPL (n. 4), art. 28.

[53] 中国长安网 '房屋中介非法贩卖个人信息，判刑！'in Chinese only（*trans: Housing agent illegally sells personal information, sentenced!*）available at: https://new.qq.com/rain/a/20230526A06P4F00

[54] 上海市浦东新区司法局 '上海首例！未经同意被查征信？投诉无果的消费者把人民银行告了！法院这样判'in Chinese only *(trans: The first case in Shanghai! Was your credit checked without your consent? Consumers who complained to no avail sued the People's Bank of China! The court ruled this way!)* available at: https://www.thepaper.cn/newsDetail_forward_14690683

who handles the data on the controller's behalf. This definition is simple to follow and comprehend. When two persons or entities make decisions jointly, there may be more than one controller (referred to as "joint controllers") or the same person or entity acting in both the controller and processor roles.[55]

On the contrary hand, the PIPL specifies the roles in a different way, defining a "PI handler" (or "handler") role. In certain situations, the handler's obligations overlap with those of the controller and processor (as those terms are defined in the GDPR). In some circumstances, the handler may designate a third-party entity to handle the PI on their behalf. In this instance, the handler would fulfill the controller position under the GDPR, while the third party they have entrusted would fulfill the processor role. But this also means that the Civil Code, which outlines the third-party body's liabilities, as well as other obligations specified in other laws, such as the Cybersecurity Law (CSL) or the Data Security Law (DSL), as specified in Article 59 of the PIPL regulates the shared responsibilities between the handler and the entrusted third party in addition to the PIPL.

Two regulations also provide distinct duties for the person in charge of protecting personal information and the data protection officer. The General Data Protection Regulation (GDPR) delineates the responsibilities, status, and designation requirements of a data protection officer (DPO). In light of the GDPR, the DPO will provide guidance and oversee the organization's efforts to protect personal data internally and in its interactions with the data protection agency (DPA). A third-party service provider may fill the role of DPO; however, the DPO is not responsible for the work product or performance of this role.

While this is going on, the PIPL outlines two roles that are somewhat different from those of the DPO. One of them is named "the person in charge of PI protection" when the amount of PI processed by a company reaches a quantity threshold defined by the Cyberspace Administration of China (CAC).[56]

Personnel either within the organization or outside the company may hold the position of PI protection coordinator. Nevertheless, unlike the DPO position, it cannot be filled by a service provider because Article 52 of the PIPL mandates that the employer notify the supervisory authorities of the personnel's identity.[57] Notably, network operators are asked to designate a "person in charge of cybersecurity" by the CSL. To satisfy the criteria of the PIPL and the CSL, a corporation may designate the same individual to serve in both the cybersecurity and PI protection capacities.

An additional function is that of the company's representative, who is in charge of offering goods or services to private individuals in China in the event that the business does not maintain an office there. The supervisory authorities must be notified of the identity and contact details of this representative, who should be a real person. But the primary duty of this representative is to keep the lines of communication open between the business and the authorities in charge. The law does not define any further duties or obligations.

---

[55] GDPR, art, 4.

[56] This threshold is set in the national standards number GB/T35273-2020 as the PI of over 1 million people, the sensitive PI of over 10,000 people, or where "the company's main business is processing PI and employs more than 200 staff members".

[57] PIPL, art 52.

Large internet platforms are also subject to unique duties under Article 58 of the PIPL, commonly referred to as "gatekeepers".[58] The gatekeeper is a separate PI protection organization that is mandated to keep an eye on the business's PI protection efforts. It employs outside specialists. There are no comparable regulations for the GDPR. After talking about the applicability, the defined roles, and the scope of PI in the PIPL and GDPR, it will now take a look at the circumstances in which a business is allowed to process PI in accordance with the two laws. Common fundamental principles for PI processing, including lawfulness, fairness, and transparency, are established by both the GDPR and the PIPL. From a legal standpoint, there are still not many distinctions between the legal foundations that allow businesses to process PI in the GDPR and the PIPL.

Under both the GDPR and the PIPL, one common legal ground for processing PI is consent from individuals or data subjects. However, because of the PI's sensitivity and the circumstances surrounding the processing, the PIPL specifies additional consent requirements. For instance, when processing sensitive personal information (PI) or in situations where the PI needs to be shared with third parties or transferred outside of China, the PIPL mandates that the PI handler secure the individual's separate consent. This indicates that in addition to multiple customized consent forms for various situations, the organization requires one general consent form. It expected that many international businesses that employ IT systems housed at foreign headquarters will have this as a standard requirement.[59]

Companies are permitted by the GDPR to process personal information for third-party or the controller's legitimate interests. Nevertheless, the PIPL makes no mention of a comparable legal authorization. However, without obtaining the individual's consent, the PIPL expressly permits the processing of PI for media reporting.[60]

Notifying the individual or data subject is essential even in situations where the company is allowed to process PI without getting agreement from them, such as when fulfilling legal requirements. Under the PIPL, the PI handler is always required to notify, with the exception of situations in which laws and regulations limit disclosure of the individual for reasons of secrecy.

Many foreign companies who do business in China or with China are still unsure about whether they need to get employees' permission before processing their personal information (PI) in order to hire new employees or complete contract fulfillment. Consequently, rather than citing Item 2 of Article 13, which specifies "implementation of human resource management in accordance with the collective HR contract" as a legal basis for PI processing, it is advisable to take permission into consideration.[61] This is due to the fact that the "collective HR contract" is rarely utilized and needs particular prerequisites, such worker's congress or labor union approval.

When a business plans to use new technology to process personal information (PI) and there is a significant risk to the data subjects, the GDPR requires the business to do a data protection impact assessment (DPIA). Several examples of these situations are: 1) large-scale, automated processing of particular data, including profiling; 2) comprehensive and

---

[58] *Ibid*., art. 58.
[59] Jordan Shapiro, *Why Digital Privacy Is So Complicated* (Progressive Policy Institute May 2022).
[60] Andoni Gorostiza and Jordan McMillan, 'An Analysis of Privacy-Impacting Regulatory Efforts and Their Effects on Service Providers and Individuals', (2022) CAP 5150, 2022, Orlando, FL.
[61] PIPL (n. 4), art. 13 (2).

systematic evaluation; or 3) large-scale, systematic surveillance of a publicly available location.

Though it is known as a Personal Information Protection Impact evaluation (PIPIA), the PIPL has identical evaluation requirements. Under the GDPR, conducting a PIPIA and a DPIA have comparable criteria. For both procedures, businesses must determine the reason why they are processing personal information (PI), whether there are any possible dangers to individuals, and whether they have implemented the necessary controls to secure the PI. Businesses must keep handling records and the PIPIA report for a minimum of three years, respectively.

For international companies conducting business in China, cross-border data transfer (CBDT) is a significant risk. Data localization is another word that is strongly related to CBDT. A business must construct separate IT infrastructure or facilities in China to isolate the data from its foreign offices, including the headquarters, in order to accomplish tight and comprehensive data localization. Users reminded that viewing remotely from an overseas office, even data saved in China, is still covered by CBDT since, technically speaking, viewing is also a form of data processing. In the PIPL, CBDT is permitted under certain circumstances, and the majority of international businesses are not required to construct independent IT infrastructure in China in order to localize data. However, compared to the GDPR, the PIPL is still quite ambiguous in certain aspects when it comes to CBDT-related requirements.[62]

The GDPR places considerably less restrictions on the free flow and transfer of data; in contrast, China's CBDT has more stringent regulations. This is brought about not only by the provisions of the PIPL but also by other laws and rules like the DSL and the CSL. For instance, until a national security assessment is approved, PI or "important" data gathered by Critical Information Infrastructure Operators (CIIO) must be stored within China, as per the requirements of the CSL and the DSL.[63] The quantity of PI that can be transported before a security evaluation is necessary is further specified by other regulations, such as the Cybersecurity Review Measures and the Measures for the Security evaluation of Outbound Data (Exposure Draft).

The "security assessment" of the PIPL is comparable to the "adequacy decision" under the GDPR. The primary distinction is that the PIPL applies rules on a case-by-case basis, whereas the GDPR applies standards by nation. The SCC in the GDPR and the "contract" in the PIPL are comparable.[64]

As mandated by the GDPR, every EU member state must set up a supervisory body for the protection of personally identifiable information. In order to preserve uniformity, it also governs the qualifications of the lead supervisory authority in situations where there are several supervisory authorities. This means that while operating a business in an EU nation, enterprises typically only have to deal with one supervisory body. In China, the situation is more complicated since there are several entities that have the authority to

---

[62] *Ibid*., art. 39.

[63] *Ibid*., art. 59

[64] It's interesting to note that the cross-border data transfers chapter makes no mention of an adequacy framework. The decision was made after careful consideration, no doubt, and it stems from the work of prominent Chinese academics who portrayed the US and EU's respective regulatory models for data transfers as "exclusionary blocks" of cross-border data flows based on geography ("adequate" jurisdictions for the US, and APEC economies taking part in the CBPR system for the EU). A set of measures targeted at protecting China's strategic interests serve as a counterweight to these provisions that can serve as a foundation for collaboration with other countries.

implement the standards for protecting PI, and several laws and regulations intersect and designate various monitoring bodies. Therefore, there are three primary oversight organizations for PI protection and information security:

1. The Chinese Cyberspace Administration (CAC)[65]: Positioned above the entire regulatory hierarchy, the CAC typically serves as a liaison between other departments. Nonetheless, the CAC is handling an increasing amount of law enforcement-related tasks directly. In addition, the CAC is in charge of planning the significant national security evaluations and creating departmental regulations that supplement the PIPL and other legislation. The CAC has been in charge of the majority of PI-related law enforcement proceedings.

2. The management of industries, particularly the telecommunications sector, is supervised by the Ministry of Industry and Information Technology (MIIT).[66] The MIIT is responsible for granting permissions needed to operate telecommunications firms, including ICP licenses and ICP filings. The MIIT is also in charge of handling non-monetary sanctions, like blocking access to websites or IT systems, removing mobile apps from the app store, and so forth.

3. The Public Security Ministry (MPS)[67]: Enforcing and overseeing the Multiple Layer Protection Scheme (MLPS) is the MPS's primary duty in the areas of cybersecurity and PI protection. Companies must adhere to specified procedures under the MLPS in order to assess and rank the "importance" of their network (from level 1 to level 5) and then put in place the necessary security measures. Cybersecurity breaches are likewise handled by the MPS, and businesses are expected to notify the MPS immediately when one occurs.

IV. Conclusion

The research discusses the challenges and complexities of establishing specific legal terminology in the context of data protection legislation. It highlights the ambiguity and vagueness of terms such as "state-of-the-art" and the challenges of defining what constitutes "reasonable" data protection measures. Along with that it emphasizes the need for legal frameworks that safeguard individuals in the ever-evolving digital world and reconcile the benefits of technological advancement with the defense of fundamental rights. It provides comparative insights from the EU's GDPR and China's PIPL for advancing personal data protection legislation and highlights the challenges and shortcomings of the GDPR as well as PIPL. The study also outlines the fundamental principles of data protection and the legal frameworks that govern cross-border processing of personal information. Despite the fact that there is no existing international cyberspace law, one is undoubtedly essential. It might consist of a distinct set of regulations or incorporate elements of the ones that are already in place. Although security and privacy are widely understood to be synonymous, they are actually more separate ideas. Security is the process

---

[65] Zhonghua Renmin Gongheguo Hulianwang Xinxi Bangongshi 中华人民共和国国家互联网信息办公室 (The Cyberspace Administration of China), Zhonghua Renmin Gongheguo Wangluo Anquan Fa 中华人民共和国网络安全法 (The Cybersecurity Law of the PRC), 07/11/2016. http://www.cac.gov.cn/2016-11/07/c_1119867116.htm accessed 6 April 2023.

[66] Zhongguo Gongye he Xinxi Hua Bu 中国工业和信息化部 (Ministry of Industry and Information Technology of China) https://www.miit.gov.cn accessed 10 April 2023.

[67] Zhongguo Gongan Bu 中国公安部 (Public Security Ministry of China) https://mps.gjzwfw.gov.cn accessed 10 April 2023.

of putting in place the necessary controls to safeguard the resources and data associated with any user or organization. On the other hand, the idea of privacy refers to a user's rights over their PII – Personally Identifiable Information. As a result, these characteristics are covered differently by various laws and standards, and this should be taken into account. The present study examines a number of laws, rules, and guidelines. Each of these has a distinct target audience and applies differently in various contexts. Individuals who are involved in an organization's governance activities must determine the pertinent and applicable compliance requirements for their particular organization. Every person has a personal responsibility to understand the IT laws in their country and the consequences of breaching them. It suggests that continual discussion and revision of legal frameworks are necessary to ensure that they remain relevant and effective in protecting individuals' rights in the digital age.

*****