The GDPR and the PIPL: a comparative analysis

Ana Sistac Plaza, Júlia Olifiers, Lasse Rheinboldt, Liv Vieira

Machine Learning
20/12/2024
Word count: 3358

Introduction

The rapid development of the internet fundamentally changed how people go about their everyday life. A significant portion of interactions now takes place online, where businesses often rely on the processing of personal data, making it one of the most valuable assets of the information age. However, the vast amount of collected data also attracts malicious actors, posing significant security and privacy risks. Consequently, establishing good data protection regulations has become essential. Two prominent examples of such regulations are the EU's General Data Protection Regulation (GDPR) and China's Personal Information Protection Law (PIPL). This paper aims to contrast the two by means of individual analysis and a comparative case study, highlighting their core motivations, regulatory approaches, and enforcement practices.

Europe's GDPR

The General Data Protection Regulation (GDPR) is the European Union's data protection law, which replaced the previous Data Protection Directive in 2018. Before examining the specific regulations imposed by law, it is important to clarify what is meant by personal data. Since personal data is a vague term, the GDPR applies the definition to a broad range of data, as defined in Article 4(1) "Personal data are any information which are related to an identified or identifiable natural person." For example, this includes anything from names, IPs, licence plates, work hours, and location, or summed up, it is interpreted as broadly as possible. The GDPR only applies when a process involves personal data.

Data processing under the GDPR is prohibited by default. However, it is possible to obtain authorization for processing, through direct consent by the data subject, and/or through lawmakers, when collection is necessitated by contract, legal obligations or legitimate interests that do not interfere with the individual's freedom and privacy. The GDPR states that it is necessary to obtain consent before collecting any type of personal data. Every person also has the following rights: the right to be informed, forgotten, object, rectify, erase, restrict processing, and the right to access their data. The right to access guarantees that the data subject can gain insight into the data a collector has on them, as well as the purpose of that data and the processing behind it. This also enables the data subject to either request rectification or erasure of the data, which the controller must comply with unless certain legal requirements are met, such as the justified necessity of the data by law enforcement. Every person is also entitled to not be subjected to an entirely automated decision-making process, as long as that process produces “legal effects concerning him or her or similarly significantly affects him or her” (GDPR, Art. 22).

Once collected, keeping records of the processing activity is also mandatory, even when processing is commissioned outside of the EU, which will be discussed in detail later. During processing, the GDPR states: “The higher the risks involved in the data processing and the more likely these are to manifest, the stronger the taken security measures have to be and the more measures must be taken.” (GDPR, Encryption, (refers to: Art. 32)) This means that while the GDPR does not enforce a specific type of encryption, it requires some sort of it, to reduce fines in case a data breach occurs. Data breaches must be reported immediately, s.t. the affected individuals can be notified as soon as possible.

Establishments must be designed or restructured with the GDPR in mind, including interactions with “third countries” (countries outside of the EU). This is especially important when processing is commissioned by the controller. Under the GDPR, countries are classified as either secure, meaning they have data protection laws comparable to the EU’s, or unsecure. Secure countries are: “Andorra, Argentina, Canada (only commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay, Japan, the United Kingdom and South Korea.” Note the absence of both the US and China. The EU-US Data Privacy Framework existing since 2023, allows US companies to obtain a certificate from EU authorities labeling them as adequate for data transfer. Although the transfer to unsecure countries is not prohibited, the controller must ensure through contract clauses that the data is sufficiently protected.

With all these regulations, it is also important to analyse the actual enforcement of these. On the company level, if a company engages in large-scale data processing, a Data Protection Officer (DPO) has to be appointed either internally or externally. While the DPO is responsible for compliance with the GDPR, the company itself remains accountable for any infringements. Companies must also perform a Privacy Impact Assessment before processing, in which the impact of the collected data is assessed and documented. Compliance is enforced through fines that should be effective and proportionate, which gives national authorities some adjustability for individual cases. The main problem with enforcing the GDPR is the detection of infringements, where the GDPR relies on proactive inspection by authorities, unsatisfied employees or customers, investigative journalism, or the company making a self-denunciation.

To summarize, the GDPR is meant to enforce stronger data protection by both collectors and processors, in and outside of the EU. It grants the data subject vital rights, as well as determining who is accountable in case of infringement. While it is strict in some instances, it can also be quite flexible in others, since complex factors are at play, and it is set up in a way that allows national authorities to use it as a guideline when determining an adequate course of action for individual cases.

The Chinese PIPL

The Personal Information Protection Law (PIPL) of the People's Republic of China, enacted in November 2021 represents a pivotal step in China's efforts to establish comprehensive data protection and regulate the collection and use of personal information. The PIPL's significance lies in its integration with China's broader legal system, which includes the Cybersecurity Law (CSL) and the Data Security Law (DSL). These three laws together form the foundation of China's approach to data governance, with the intersection of privacy protection, national security, and economic strategy.

The Role of PIPL is to protect personal information and strengthen national security legislation. It grants individuals rights over their data and imposes obligations on organizations to ensure lawful, transparent and secure data processing. The PIPL's provisions address issues raised by global surveillance disclosures, particularly the misuse of personal data, by mandating stricter consent mechanisms and limiting the scope of cross-border data transfers. The global surveillance disclosures of the 2010s, particularly the revelations of Edward Snowden, a formal NSA contractor, served as a wake-up call for governments worldwide about the risks of unchecked data collection and foreign surveillance. These disclosures exposed the extensive data collection practices of the U.S. National Security Agency (NSA) and its close partnership with federal agencies like the FBI and CIA. The leaks revealed programs, such as PRISM, which accessed internet communications via major tech companies, and XKeyscore, a powerful data analysis tool, alongside financial arrangements with telecommunications partners, including Britain, France and Germany. Secret treaties facilitated the sharing of intercepted data about each other's citizens. These revelations sparked widespread concerns over privacy and data security, leading to global advocacy for stronger legal protections, transparency, and a reexamination of data sovereignty. Subsequent countries, including China, strengthened their data protection laws to address these vulnerabilities. The PIPL's provisions on cross-border data transfers and transparency reflect lessons learned from these disclosures, aiming to reduce the risks of unauthorized access by foreign entities.

As previously mentioned, the PIPL is based on the CSL and DSL. The CSL was enacted in 2017, which laid the groundwork for data governance by emphasizing the security of critical information infrastructure and personal data. The PIPL extends from this law by providing an additional framework for personal information protection. It also extends beyond the CSL by granting individuals rights such as access, correction, and deletion of their data, while also addressing the systematic vulnerabilities exposed by global surveillance programs. The CSL's emphasis on securing critical infrastructure complements this by protecting the digital backbones that store and transmit personal and national data. The DSL focuses on safeguarding all types of data, not just personal data, emphasizing the strategic importance of data to national security and economic stability. The PIPL complements the DSL by regulating personal data within this broader context. While the DSL governs, for instance, data categorization and localization, the PIPL ensures that personal data is handled ethically and securely, even when it intersects with other types of critical or core data. The junction of the PIPL and DSL reinforces data sovereignty, addressing concerns about foreign access to sensitive Chinese data. The DSL explicitly addresses the broader implications of data security in national and global contexts, reflecting China's awareness of how data can be weaponized for surveillance or economic leverage.

China's approach to data sovereignty and Global Governance is distinctive. China's data governance strategy, as reflected in the PIPL, DSL and CSL, is distinguished by its focus on national security and state control. These Chinese laws prioritize less individual privacy as a fundamental right, but more data sovereignty, economic independence, and state oversight. Thus, the PIPL plays a dual role. While protecting individual rights, the PIPL operates within a framework that aligns with the DSL and CSL to advance national interests. Restrictions on cross-border transfers under PIPL are motivated not only by privacy concerns but also by broader strategic considerations, including economic competitiveness and geopolitical tensions. China's comprehensive governance model challenges Western approaches, particularly the open flow of data. In the aftermath of the global surveillance disclosures, this model highlights an alternative path that prioritizes sovereignty and security over unrestricted global connectivity.

In conclusion, the Personal Information Protection Law represents a critical component of China's evolving data governance framework, addressing privacy and security concerns within the broader context established by the CSL and the DSL. Influenced by the 2010s surveillance disclosures, these laws reflect China's pursuit of a secure, sovereign and strategically advantageous data ecosystem. By embedding personal data protection within a broader security framework, PIPL offers a distinct approach that aligns individual privacy with national priorities, positioning China as a key player in shaping global data governance norms.

The GDPR vs. The PILP

The GDPR and the PIPL represent two comprehensive frameworks designed to regulate the collection, processing, and transfer of personal data. Despite sharing some common goals, such as granting individuals control over their data and ensuring lawful data processing, they reflect fundamentally different priorities shaped by legal and cultural contexts.

At the heart of these differences lies the question of how each framework approaches data sovereignty, cross-border transfers, and international compatibility. The GDPR’s emphasis is on fostering trust in the global digital economy by ensuring that personal data transferred outside the EU remains protected to a level equivalent to EU standards. To this end, it evaluates other countries’ data protection laws based on their ability to provide adequate safeguards, classifying them as secure. This distinction raises an important question: why does the GDPR not classify China as a secure country?

Despite China’s implementation of the PIPL and its increasing focus on personal data protection, several key differences prevent it from meeting the GDPR’s adequacy requirements. First and foremost, as explained before, state control plays a significant role in data governance in China. Laws such as the PIPL, CSL, and DSL grant the government extensive powers to access and process personal data for purposes such as national security and public interest. While these priorities are central to China’s strategy, they conflict with the GDPR’s strict limits on data access, which aim to safeguard individual privacy and autonomy.

Second, the enforcement mechanisms in China differ fundamentally from those in the EU. The GDPR relies on independent supervisory authorities in each member state to oversee compliance, investigate violations, and ensure individuals’ rights are respected. In China, however, enforcement is closely tied to government agencies, which integrate personal data protection with broader national goals. This oversight dependency creates potential conflicts of interest and limits the transparency required by the GDPR.

Another key difference is in cross-border data transfers and localization requirements. The GDPR permits the free flow of data to countries deemed secure, encouraging international collaboration and economic activity, provided personal data remains protected. China’s approach imposes strict localization rules, requiring critical data to be stored within its borders. This divergence underscores China’s focus on data sovereignty, where personal data is seen not only as an individual’s right but also as a strategic national resource. By emphasizing control over international integration, China diverges from the GDPR's required openness.

These differences highlight the broader contrast in objectives between the GDPR and PIPL. The GDPR’s goal is to create a global benchmark for data protection, fostering trust in the digital economy while ensuring personal data remains secure, regardless of where it is transferred. The PIPL, on the other hand, aligns privacy with China’s national priorities, balancing individual rights with the need to maintain sovereignty and control over critical data infrastructure.

As a result, the GDPR’s decision to exclude China from its list of secure countries is not merely a technical judgment but a reflection of these deeper philosophical differences. While both frameworks seek to address the challenges of modern data governance, they do so from fundamentally different perspectives. Ultimately, this divergence shapes how these frameworks interact with the global data economy. The GDPR positions the EU as a leader in human-rights-centric data protection, promoting compatibility and collaboration with countries that share similar values. Meanwhile, the PIPL exemplifies a sovereignty-driven model, prioritizing the security and independence of national data ecosystems.

The contrasting approaches of the GDPR and PIPL not only highlight the distinct priorities of the European Union and China but also reflect the broader tension between openness and sovereignty in global data governance. These differences are not only theoretical, they influence how nations, businesses, and individuals engage with data in a globalized economy. As challenges in data security and privacy grow, the GDPR and PIPL will shape the future of global data governance as competing models. Their differences show how laws can reflect the unique goals and priorities of their regions, shaping the direction of digital policies worldwide.

Aspect	GDPR	PIPL
Primary Focus	Individual Rigths and Privacy	State Sovereignty and National Security
Cross-boarder Transfers	Permitted with Safeguards	Heavily restricted, with mandatory assessments
Sensitive Data	Defined narrowly, user focused	Defined broadly, state focused
Consent	User-centric, broad withdrawal rights	Risk-focused, stricter for sensitive data
Enforcement	Fines and procedural compliance	Fines, operational restrictions, personal liability
Broader Goals	Trust and global cooperation	Sovereignty, security, and economic independence

Table 1 Key comparisons between the GDPR and the PIPL

The GDPR and PIPL in practice

Clearview AI, a U.S.-based facial recognition company, has faced significant enforcement actions across Europe for violating the GDPR. Between 2021 and 2024, Clearview AI faced substantial fines across Europe for GDPR violations related to unauthorized data collection and processing. France, Italy, and Greece each fined the company €20 million for scraping images and processing biometric data without a legal basis, failing to uphold transparency, and disregarding individuals' rights. The Netherlands issued a €30.5 million penalty, also citing the failure to appoint an EU representative. In all cases, Clearview AI was ordered to delete unlawfully collected data and cease processing activities involving residents of the respective countries. Across these cases, several recurring violations were identified: unlawful data collection without consent or a legal basis, processing sensitive biometric data without meeting GDPR requirements, failure to inform individuals about the collection and use of their data, and non-compliance with data subject rights, such as access, deletion, and objection. Clearview AI also failed to appoint an EU representative, as required for companies outside the EU that process data of EU residents.

In July 2022, the Cyberspace Administration of China (CAC) imposed a record fine of $1.2 billion (RMB 8.026 billion) on Didi Global Inc., China's largest ride-hailing company, for significant violations of the PIPL, the DSL, and the CSL. The fine, representing nearly 4.6% of Didi’s total revenue for the previous year, approached the maximum penalty of 5% allowed under the PIPL. Additionally, the company’s CEO and President were personally fined RMB 1 million each, highlighting individual accountability for corporate misconduct under China’s data protection laws.

Didi's violations included the illegal collection of personal data, such as screenshots from users’ phone albums, clipboard data, and app lists. The company also collected sensitive biometric data, including facial recognition images, and detailed personal information about users, such as their ages, occupations, family relationships, and addresses, without obtaining proper consent. Furthermore, Didi excessively tracked users’ geolocation, even when the app was running in the background, and failed to specify the purposes for processing certain types of personal information, such as device data. The CAC's investigation also uncovered significant failures in Didi’s data management practices, which posed risks to national security and the privacy of millions of users. As part of the penalty, Didi’s apps were removed from app stores during the investigation, and the company was prohibited from accepting new users, leading to substantial revenue and market share losses.

Clearview AI’s violations underscored Europe’s commitment to individual rights, emphasizing user empowerment and transparency . Enforcement actions against Clearview AI were coordinated by individual data protection authorities across EU member states, with fines ranging from €7.5 million to €30.5 million. These penalties focused primarily on breaches of transparency, the legal basis for data processing, and adherence to GDPR’s requirements for handling special categories of data, such as biometrics. The extraterritorial application of the GDPR was also evident, as Clearview AI, a U.S.-based company, faced fines for processing data of EU residents, demonstrating the regulation’s global reach.

In contrast, China’s PIPL reflects a dual focus on privacy and state sovereignty over data, blending individual rights with national security concerns. The Didi Global case, resulting in a record fine of $1.2 billion (RMB 8.026 billion), illustrates this approach. Didi was penalized not only for privacy violations, such as the unauthorized collection of geolocation and biometric data but also for failing to address national security risks posed by its inadequate data management practices. Enforcement by the Cyberspace Administration of China (CAC) was centralized, with personal accountability extending to Didi’s executives, who were fined RMB 1 million each. The penalties also included operational restrictions, such as removing Didi’s apps from app stores and banning new user registrations, underscoring the PIPL’s emphasis on systemic and strategic risks rather than solely on individual rights.

The GDPR and PIPL also differ in their handling of transparency and user empowerment. Under the GDPR, transparency obligations require organizations to clearly inform individuals about the collection and use of their data. Clearview AI’s failure to meet these obligations was a critical factor in its penalties. The PIPL also emphasizes transparency but within a broader framework of organizational accountability. In Didi’s case, inadequate disclosure of data collection purposes was penalized, but the focus extended to addressing systemic risks and aligning with China’s strategic priorities.

Conclusion

The exploration of the differences between the PIPL and the GDPR highlights how regional contexts and priorities shape the development of data protection laws. The GDPR, widely regarded as a global benchmark for privacy, centers on safeguarding individual rights, ensuring transparency, and empowering users to control their personal data. It reflects the European Union’s strong emphasis on privacy as a fundamental human right and its commitment to fostering a culture of trust. In contrast, the PIPL balances individual privacy with state and public interests, reflecting China’s broader strategic focus on data as a critical national resource. While the PIPL incorporates elements of individual privacy protection, it also underscores the importance of national security, economic development, and social governance in shaping its provisions. This dual emphasis aligns with China’s vision of leveraging data to advance its domestic and geopolitical goals.

Together, these regulatory frameworks illustrate the evolving nature of global data protection, highlighting the diversity of legal approaches in addressing privacy concerns and managing data-related violations. They also reveal how cultural, political, and economic factors influence the priorities embedded in privacy laws, offering valuable insights for navigating the complexities of cross-border data management in an increasingly interconnected world.

References

Adequacy Decision. (2018). European Data Protection Supervisor. https://www.edps.europa.eu/data-protection/our-work/subjects/transfers-data/adequacy-decision_en

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

Facial recognition: Italian SA fines Clearview AI EUR 20 million | European Data Protection Board. (n.d.). Www.edpb.europa.eu. https://www.edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en

General Data Protection Regulation (GDPR) – Official Legal Text. (2024). General Data Protection Regulation (GDPR). http://gdpr-info.eu/

Hellenic DPA fines Clearview AI 20 million euros | European Data Protection Board. (2022). Europa.eu. https://www.edpb.europa.eu/news/national-news/2022/hellenic-dpa-fines-clearview-ai-20-million-euros_en

Lomas, N. (2023, May 10). *Clearview fined again in France for failing to comply with privacy orders | TechCrunch*. TechCrunch. https://techcrunch.com/2023/05/10/clearview-ai-another-cnil-gspr-fine/?

Lomas, N. (2024, September 3). *Clearview AI hit with its largest GDPR fine yet as Dutch regulator considers holding execs personally liable | TechCrunch*. TechCrunch. https://techcrunch.com/2024/09/03/clearview-ai-hit-with-its-largest-gdpr-fine-yet-as-dutch-regulator-considers-holding-execs-personally-liable/?

Simmons & Simmons. (2024). Simmons-Simmons.com. https://www.simmons-simmons.com/en/publications/cl5v6pa5m1psb0a87n8dzap97/china-fines-didi-usd-1-18-billion-for-data-violations?

The French SA fines Clearview AI EUR 20 million | European Data Protection Board. (2022). Europa.eu. https://www.edpb.europa.eu/news/national-news/2022/french-sa-fines-clearview-ai-eur-20-million_en?