From Consent to Accountability: Legal Approaches to Data Subject Rights in the Context of Global Privacy Regulations

1. Shirin Azizi: Department of Trade Law, Allameh Tabataba'i University, Tehran, Iran
2. Masoud Parsa*: Department of International Law, Ferdowsi University of Mashhad, Mashhad, Iran
***Correspondence: e-mail: Drparsamasoud1@gmail.com**

Abstract

In the digital era, the protection of personal data has emerged as a critical issue, prompting the development of robust privacy regulations aimed at safeguarding data subject rights. This article explores the evolution of legal frameworks for data protection, emphasizing the shift from traditional consent-based models to accountability-driven approaches in global privacy regulations. The General Data Protection Regulation (GDPR) is examined as the gold standard for privacy laws, with a focus on its provisions related to consent, transparency, and organizational accountability. The article also compares the GDPR with other regional frameworks, such as the California Consumer Privacy Act (CCPA), highlighting the similarities and differences in their approaches to consent and accountability. Additionally, the challenges associated with enforcing data subject rights across borders are discussed, with attention to jurisdictional issues, cultural differences, and the impact of emerging technologies like artificial intelligence, blockchain, and big data. The article concludes by proposing future directions for enhancing accountability in privacy regulations, including innovations in enforcement mechanisms and the potential for global harmonization of privacy laws. Ultimately, the article emphasizes the need for a dynamic, adaptable legal framework that empowers data subjects and holds organizations accountable for their data processing practices, ensuring a more secure and transparent digital ecosystem.

Keywords: Data protection, privacy regulations, GDPR, accountability, data subject rights, global harmonization.

Received: 14 November 2022
Revised: 15 December 2022
Accepted: 28 December 2022
Published: 01 January 2023

Citation: Azizi, S. & Parsa, M. (2023). From Consent to Accountability: Legal Approaches to Data Subject Rights in the Context of Global Privacy Regulations. *Legal Studies in Digital Age*, 2(1), 27-38.

1. Introduction

In the contemporary digital age, the protection of personal data has become one of the most pressing issues for governments, organizations, and individuals alike. As the world becomes increasingly interconnected through digital technologies, vast amounts of personal information are being generated, shared, and processed across borders. This has created significant challenges for privacy regulation, as personal data is no longer confined to a single jurisdiction. With the proliferation of the Internet of Things (IoT), social media platforms, e-commerce, and digital healthcare services, the need to safeguard individuals' privacy and ensure the responsible use of their data has never been more critical. The legal landscape surrounding data protection is evolving rapidly, as policymakers strive to create frameworks that balance the benefits of data-driven innovation with the fundamental rights of individuals. At the heart of this evolution lies the concept of data subject rights, which

encompasses the rights individuals hold regarding their personal data, such as the right to access, rectification, erasure, and objection to processing (Teatini & Matinmikko-Blue, 2020).

Data subject rights have become a cornerstone of modern privacy regulations, particularly with the advent of the General Data Protection Regulation (GDPR) in the European Union, which has influenced privacy laws worldwide. The GDPR has set a high standard for data protection and has instilled a greater sense of accountability among organizations that handle personal data. Central to the regulation is the emphasis on obtaining explicit consent from individuals before processing their data. However, as privacy concerns have grown more complex and data-driven practices have evolved, there has been a shift from a mere focus on consent to a more comprehensive accountability-driven approach. While consent remains a vital aspect of data protection, there is an increasing recognition that organizations must be held accountable for how they collect, store, and use personal information, even when consent is not explicitly required or obtained (Lindén et al., 2020).

In this context, the importance of protecting personal data goes beyond individual rights and extends to broader societal concerns, including cybersecurity, public health, and economic stability. The widespread use of digital technologies has brought about numerous advantages, such as increased access to services, enhanced communication, and improved healthcare. However, it has also led to an exponential increase in the volume of personal data being collected, which, if misused, could have severe consequences for individuals. Privacy breaches, identity theft, and data exploitation have become real threats that necessitate robust legal frameworks to protect individuals' privacy. Furthermore, in the context of globalized data flows, the challenge of ensuring consistent privacy protection across diverse legal systems has become a priority for international regulators. Data protection laws, therefore, must adapt to the rapidly changing technological landscape, ensuring that privacy rights are upheld, while also promoting the responsible use of data to foster innovation and economic growth.

The primary aim of this paper is to explore the evolution of legal frameworks that address data subject rights, with a specific focus on the transition from consent-based approaches to accountability-driven models. This shift is significant, as it reflects the growing recognition that privacy protection cannot rely solely on individual consent but must also involve a systemic commitment to data protection across organizations and jurisdictions. The paper will examine the legal developments that have shaped data subject rights in the context of global privacy regulations, highlighting key trends such as the expansion of individual rights, the rise of accountability mechanisms, and the harmonization of regulatory standards across borders. By analyzing various international privacy frameworks, such as the GDPR, the California Consumer Privacy Act (CCPA), and other regional regulations, this paper aims to provide a comprehensive overview of how data protection laws are evolving to address the challenges of the digital era.

The paper will also explore the implications of these legal developments for businesses, policymakers, and individuals. While much attention has been given to the role of consent in ensuring privacy protection, there is an increasing emphasis on the need for organizations to demonstrate accountability in their data processing activities. This includes adopting transparent data practices, implementing robust security measures, and fostering a culture of privacy awareness among employees. As data breaches and privacy violations continue to make headlines, the responsibility of organizations to protect personal data has become a key concern. At the same time, individuals must also be empowered to assert their rights and hold organizations accountable for any misuse of their personal information.

2. The Evolution of Data Subject Rights

The evolution of data subject rights and privacy protection has been deeply shaped by the growing recognition of the significance of personal data in the digital age. Historically, privacy laws were primarily concerned with protecting individuals' physical space and personal information from government intrusion or physical surveillance. However, as technological advancements facilitated the collection, storage, and transmission of personal data in unprecedented volumes, the focus of privacy laws expanded to include the protection of data itself. In the early stages, privacy protection was often fragmented, existing in the form of national legal frameworks and industry-specific regulations rather than comprehensive, cross-border standards. These laws were generally focused on controlling the use of personal data in specific contexts, such as credit reporting or the use of health data (Jusić, 2022; Krishnamurthy, 2020).

In many countries, the first significant legal frameworks focused on consent as the foundation of data protection. The consent model held that individuals should have the right to control their personal data by explicitly giving or withholding their

permission for its collection and use. The concept of consent has roots in earlier legal protections, such as the right to privacy as it was understood in the mid-20th century. For example, in the United States, the right to privacy was initially framed within constitutional rights, particularly in relation to individual autonomy in areas such as reproductive rights and freedom from unwarranted searches. This concept gradually extended to cover the use of personal data, particularly in industries like healthcare, banking, and telecommunications, which were among the first to collect sensitive personal data on a large scale (Ribeiro-Navarrete et al., 2021).

As technology progressed, so did the need for more sophisticated legal frameworks to address new challenges posed by the use of personal data. The rise of the internet in the 1990s, for example, introduced a new era of data collection and sharing that surpassed anything previously imaginable. This was the era in which the first privacy and data protection laws began to be formalized at a more global level. In the European Union, the 1995 Data Protection Directive (95/46/EC) marked a significant turning point. It established a legal framework for the protection of personal data, articulating key principles such as data minimization, purpose limitation, and transparency, all of which are core tenets of modern data protection laws. However, even under this directive, consent was the primary mechanism for ensuring data protection. It required organizations to obtain the explicit consent of individuals before processing their data, but the enforcement of these provisions was often lax, and there were no clear or uniform standards for accountability in the event of violations (Adib, 2023; Santos & Pandit, 2023).

The growing complexities of digital technologies and the rise of big data analytics led to the realization that consent alone was insufficient for ensuring comprehensive privacy protection. This marked the beginning of a shift towards more robust, rights-based privacy frameworks. Over time, a broader range of data subject rights began to emerge, shifting away from merely obtaining consent to a model where organizations were held accountable for ensuring that individuals' data was not only protected but also handled in a transparent and responsible manner. The most prominent example of this shift is the General Data Protection Regulation (GDPR), which came into force in May 2018. The GDPR represents a paradigm shift in data protection law, incorporating a wide range of rights for individuals, from the right to be informed about the use of their data to the right to be forgotten. While consent remains a fundamental principle under the GDPR, it is no longer the sole basis for processing personal data. Instead, the regulation adopts a broader, accountability-driven approach. Under the GDPR, organizations must demonstrate that they are taking appropriate measures to protect personal data, regardless of whether consent is obtained. For example, the regulation mandates that organizations implement data protection by design and by default, ensuring that privacy considerations are integrated into all stages of data processing, from collection to storage and eventual destruction (Amali, 2022; Bentotahewa et al., 2022; Human et al., 2022; Vlahou et al., 2021).

One of the key provisions introduced by the GDPR is the concept of "data subject rights." These rights empower individuals to have more control over their personal data, irrespective of where it is processed or stored. The right to access allows individuals to request information about how their data is being used, while the right to rectification enables them to correct inaccuracies. The right to erasure, or the "right to be forgotten," allows individuals to request that their data be deleted in certain circumstances. Additionally, the GDPR establishes the right to object to data processing and the right to data portability, providing individuals with the means to transfer their data from one service provider to another. These rights place the individual at the center of the data processing ecosystem, ensuring that their privacy is safeguarded not just through consent, but through an active, ongoing relationship with organizations that process their data (Gray et al., 2021; Hou, 2021; Yilmaz & Seval, 2022).

This shift toward a more comprehensive and proactive approach to data protection was also influenced by increasing concerns about data security breaches, cyberattacks, and the exploitation of personal data by large tech companies. The implementation of the GDPR was partially a response to high-profile scandals such as the Cambridge Analytica scandal, where the unauthorized use of personal data exposed serious vulnerabilities in existing privacy frameworks. These events highlighted the need for stronger regulatory oversight and accountability, prompting a global conversation about privacy and data protection. As a result, the GDPR has become a model for other countries seeking to strengthen their own privacy laws. Many countries in Asia, Latin America, and the Middle East have since adopted similar frameworks, often drawing directly from the GDPR's principles. For instance, countries like Brazil and India have introduced national data protection laws that mirror the GDPR's emphasis on data subject rights and organizational accountability (Amali, 2022; Vlahou et al., 2021; Wagner, 2022).

While the GDPR has set a high bar for privacy protection, it has also underscored the complexities of regulating personal data in a globalized digital economy. One of the key challenges of implementing data protection regulations is ensuring that they are enforceable across borders. As organizations increasingly operate in multiple jurisdictions, the question of how to ensure compliance with data protection laws has become a major concern. The GDPR addresses this by introducing mechanisms such as the one-stop-shop system, which allows companies to deal with a single lead supervisory authority in case of cross-border data processing activities. However, such cross-border enforcement remains an ongoing challenge, particularly in regions where data protection laws are less developed or where enforcement mechanisms are weak (Binardy, 2021; Hou, 2021).

The evolution of data subject rights also brings to the forefront the concept of accountability, which has become an integral part of modern privacy laws. Accountability is the idea that organizations are not only responsible for protecting personal data but also for demonstrating their commitment to privacy and data protection principles. This shift is particularly evident in the GDPR, which mandates that organizations take specific actions to ensure compliance, such as conducting data protection impact assessments, appointing data protection officers, and maintaining records of processing activities. Furthermore, organizations are required to notify supervisory authorities and affected individuals in the event of a data breach, ensuring transparency and prompt action. This emphasis on accountability goes beyond the traditional model of consent, placing greater responsibility on organizations to demonstrate that they are taking active steps to protect personal data and uphold data subject rights (Human et al., 2022; Islam, 2022).

At its core, the evolution of data subject rights reflects the growing recognition of privacy as a fundamental human right, one that is essential for personal autonomy, dignity, and security in the digital age. With the increasing reliance on personal data for commercial, governmental, and technological purposes, the need for robust privacy protection laws is clearer than ever. As privacy frameworks continue to evolve, the shift from a consent-based model to one centered around accountability and comprehensive rights-based protection represents a crucial step toward ensuring that individuals' data is treated with the respect and care it deserves. Key concepts such as data subject rights, consent, accountability, data protection, and privacy form the foundation of modern privacy regulations. Data subject rights refer to the set of rights granted to individuals to control and protect their personal data. Consent, while still a cornerstone of privacy protection, is increasingly seen as one aspect of a broader, more comprehensive framework. Accountability, as embedded in regulations like the GDPR, requires organizations to demonstrate compliance with privacy laws through concrete actions and transparent practices. Data protection refers to the policies, measures, and practices implemented to safeguard personal data from misuse, loss, or unauthorized access. Privacy, in this context, is the overarching principle that encompasses all these elements, ensuring that individuals retain control over their personal information and that their privacy is respected in an increasingly digital world.

3. Global Privacy Regulations: A Comparative Analysis

The General Data Protection Regulation (GDPR), enacted in 2018, is widely regarded as the gold standard in global privacy regulations, setting a benchmark for other countries to follow when it comes to the protection of personal data. The regulation, which applies to all entities handling the personal data of European Union (EU) citizens, has reshaped the landscape of data privacy by establishing a comprehensive framework that emphasizes individual rights and organizational accountability. One of the central tenets of the GDPR is its focus on enhancing data subject rights, providing individuals with greater control over their personal information, and ensuring that organizations handling such data are transparent and responsible. Under the GDPR, data subjects are granted a range of rights, including the right to access, the right to rectification, the right to erasure (commonly known as the "right to be forgotten"), and the right to data portability. These rights are fundamental in empowering individuals to exercise control over their personal data in a world where information flows freely and often uncontrollably (Adib, 2023; Yue & Skiera, 2022).

The GDPR's approach to consent is one of its defining features. Consent, under the GDPR, must be informed, specific, unambiguous, and given freely. It must be provided through a clear affirmative action, such as ticking a box or signing a statement, to ensure that individuals understand what they are consenting to. The regulation also stipulates that consent can be withdrawn at any time, and organizations must make it as easy to withdraw consent as it is to give it. This ensures that individuals retain ultimate control over their personal data throughout the data processing cycle. Moreover, the GDPR places

a strong emphasis on accountability, requiring organizations to demonstrate compliance with its provisions. This is particularly evident in the obligations placed on organizations to implement data protection by design and by default, meaning that privacy measures must be integrated into the core operations and systems of a business from the outset, rather than as an afterthought. Organizations must also appoint data protection officers in certain cases and carry out Data Protection Impact Assessments (DPIAs) to assess the potential risks to individuals' rights and freedoms before initiating any processing activity that may impact personal data (Wagner, 2022; Yilmaz & Seval, 2022).

In contrast to the GDPR, the California Consumer Privacy Act (CCPA), which came into effect in 2020, represents a significant privacy regulation in the United States, although its scope and approach differ in several key ways. While both the GDPR and the CCPA focus on enhancing individuals' privacy rights, the CCPA operates in a more consumer-centric manner, emphasizing transparency and giving individuals the right to opt-out of data collection rather than explicitly requiring affirmative consent for all processing activities. The CCPA provides consumers with the right to know what personal data is being collected, the purpose for its collection, and the ability to request that this data be deleted. Additionally, the act gives consumers the right to opt-out of the sale of their personal information to third parties. This opt-out right is somewhat similar to the GDPR's right to object, but it is more narrowly focused on the specific issue of data sales rather than the broader scope of data processing activities under the GDPR (Rosenberger et al., 2021; Vlahou et al., 2021).

One of the major differences between the CCPA and the GDPR lies in their approach to consent. While the GDPR mandates that consent must be obtained for most forms of data processing, the CCPA does not require businesses to seek consent for data collection unless they are selling data to third parties. Instead, the CCPA requires businesses to provide consumers with a clear and conspicuous "Do Not Sell My Personal Information" link on their websites, giving consumers the ability to opt-out of data sales. This approach reflects a more consumer-driven, opt-out framework compared to the GDPR's more robust, opt-in consent model. Furthermore, the CCPA imposes stricter penalties on businesses that fail to comply with its provisions, particularly in cases where a consumer's personal data is compromised or misused. Despite the similarities, the CCPA's narrower focus on consumer protection and its more limited scope of coverage (applying only to for-profit businesses in California) set it apart from the GDPR, which has a broader international reach and more comprehensive provisions (Bentotahewa et al., 2022; Binardy, 2021).

Beyond the GDPR and CCPA, there are several other significant privacy regulations worldwide that aim to safeguard data subject rights. Brazil's General Data Protection Law (LGPD), for example, was enacted in 2020 and bears many similarities to the GDPR, with a focus on enhancing individual rights and increasing organizational accountability. Like the GDPR, the LGPD grants individuals various rights over their personal data, such as the right to access, correction, and deletion. It also emphasizes the need for explicit consent, which must be informed, free, and specific. However, the LGPD differs in certain respects, particularly in its approach to consent and enforcement. While the LGPD aligns with the GDPR on key principles such as data minimization and purpose limitation, it takes a slightly different approach to the collection of personal data. For example, the LGPD provides certain exceptions to the need for consent, such as when data processing is necessary for compliance with legal obligations or the performance of a contract. This makes the LGPD more flexible than the GDPR in some respects, although the overall approach remains similar, with a strong emphasis on both data subject rights and organizational accountability (Jusić, 2022; Ribeiro-Navarrete et al., 2021).

Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) provides another important example of a privacy regulation that emphasizes data subject rights, although it operates within a different legal and cultural context. PIPEDA applies to private sector organizations in Canada and is designed to protect the personal information of individuals while balancing the need for organizations to use personal data in a responsible and secure manner. PIPEDA grants individuals the right to access their personal data, request corrections, and challenge organizations if they believe their data has been mishandled. However, compared to the GDPR, PIPEDA places less emphasis on consent as a central concept. While organizations are required to obtain consent for most forms of data collection and use, PIPEDA allows for a broader range of acceptable uses of personal information without explicit consent, particularly when it comes to business operations or legal obligations. Moreover, the enforcement mechanisms under PIPEDA are less stringent than those under the GDPR, with the Office of the Privacy Commissioner of Canada handling complaints and investigations on a more advisory basis rather than imposing direct fines or penalties (Wagner, 2022).

China's Personal Information Protection Law (PIPL), which was introduced in 2021, marks another significant step in global privacy regulation, particularly in light of China's emerging status as a global digital powerhouse. The PIPL closely mirrors the GDPR in its structure and scope, with a strong focus on protecting personal data, safeguarding individual rights, and holding organizations accountable for data processing activities. Like the GDPR, the PIPL provides individuals with the right to access, correct, and delete their personal data, and requires businesses to obtain informed consent before processing sensitive information. However, the PIPL also reflects China's distinct political and legal context, with certain provisions that allow the government greater oversight and control over data flows. For instance, the PIPL mandates that organizations conducting cross-border data transfers must ensure that the data is stored in compliance with Chinese regulations, and it allows for the imposition of fines or sanctions on foreign companies that do not adhere to these rules. This highlights the tension between privacy protection and national security concerns, a theme that is becoming increasingly important in global privacy debates (Yue & Skiera, 2022).

These regional frameworks, while differing in their specifics, share common goals of protecting data subject rights, ensuring transparency in data processing, and enhancing organizational accountability. The global trend is clearly toward more comprehensive and robust privacy regulations that give individuals greater control over their personal data while holding organizations to higher standards of responsibility and transparency. As the world continues to become more digitized and interconnected, these regulatory frameworks will likely evolve further, with international collaboration and harmonization becoming essential to ensure the protection of privacy in an increasingly globalized digital economy.

4. From Consent to Accountability: A Paradigm Shift

The traditional consent model, which has long been the cornerstone of privacy regulations, has faced increasing criticism as the scale and complexity of data processing in the digital age have expanded. While consent has been seen as a means of ensuring that individuals maintain control over their personal data, the model is increasingly viewed as inadequate in addressing the full range of privacy challenges posed by modern technologies. One of the primary limitations of the consent model is the issue of informed consent. For consent to be valid under traditional frameworks, individuals must have a clear understanding of what they are agreeing to. However, the rapid pace of technological advancements and the complexity of many data processing activities make it difficult for individuals to fully grasp the implications of consenting to data collection. The use of personal data often involves opaque, multilayered processes, making it nearly impossible for the average user to understand how their data will be used, stored, or shared. This complexity is further compounded by the tendency of many organizations to present privacy policies and consent forms in dense, legalistic language that is inaccessible to the majority of users (Amali, 2022).

Another significant challenge with the consent model is power imbalances between individuals and organizations. In many cases, individuals are not in a position to negotiate the terms of consent, especially when interacting with large, powerful corporations or when using services where consent is a condition for participation. The "take-it-or-leave-it" nature of many consent agreements means that individuals may have little choice but to accept terms that they do not fully understand or agree with, simply to gain access to a service or platform. This raises serious concerns about the voluntary nature of consent and undermines the notion of free will in decision-making. Moreover, this dynamic often results in what has been referred to as consent fatigue, where individuals, overwhelmed by the sheer number of consent requests they encounter daily, are likely to click through consent forms without reading or understanding them, simply to move on with their activities. As a result, the principle of consent can become little more than a box to tick, rather than a meaningful expression of autonomy over personal data (Barati et al., 2020).

In response to the limitations of consent, newer privacy regulations have increasingly focused on the concept of accountability as a key element in safeguarding personal data. The shift from consent to accountability reflects a growing recognition that organizations must bear responsibility not only for obtaining consent but also for how they collect, store, process, and share personal data. The GDPR, for example, places a strong emphasis on organizational accountability by requiring data controllers and processors to demonstrate compliance with the regulation, regardless of whether explicit consent is obtained for all data processing activities. This shift towards accountability is intended to create a framework where

organizations are incentivized to take proactive steps in protecting data, rather than merely relying on consent as a safeguard (Bentotahewa et al., 2022).

One of the primary mechanisms through which accountability is ensured under the GDPR is the appointment of data protection officers (DPOs). These officers are tasked with overseeing an organization's data protection activities and ensuring that data processing complies with the regulation. DPOs play a critical role in monitoring data protection strategies, advising organizations on compliance, and serving as a point of contact for both individuals and regulators. By making data protection a formal, dedicated role within organizations, the GDPR establishes a clear line of responsibility for data privacy. This is complemented by requirements for organizations to conduct Data Protection Impact Assessments (DPIAs), which are designed to identify and mitigate potential risks to individuals' privacy before data processing begins. DPIAs provide a structured approach for assessing the implications of data processing activities and ensuring that privacy risks are considered at every stage of project development. These assessments are particularly important when new technologies or data processing activities that pose a high risk to individuals' rights are being introduced (Beauvais & Knoppers, 2021).

In addition to these measures, the GDPR also mandates transparency requirements, ensuring that organizations are clear and upfront with individuals about how their personal data will be used. This transparency is achieved through the requirement to provide detailed privacy notices and to notify individuals in the event of a data breach. Transparency helps mitigate the power imbalance that often exists in the consent model, as individuals are better informed about the data processing activities they are subject to. However, while transparency is a vital component of the accountability framework, it also requires organizations to be proactive in communicating with users, which can be challenging in an environment where privacy policies are often neglected or ignored.

The growing emphasis on accountability has been seen as a necessary response to the shortcomings of the consent-based model, particularly in light of real-world cases where organizations have been found to violate privacy rights. Several high-profile data breaches and misuse of personal data have highlighted the inadequacies of relying solely on consent as a safeguard. For instance, one case involved a social media platform that had gathered vast amounts of personal data under the pretext of providing a free service, only for this data to be used for targeted political advertising without explicit consent. While users had technically agreed to share their data by consenting to the platform's privacy policy, the lack of clear, meaningful information about how their data would be used, coupled with the organization's failure to ensure appropriate safeguards, led to a massive public outcry and regulatory scrutiny. This case demonstrated the importance of accountability measures, as the organization was eventually required to pay fines and implement more robust data protection practices. Such examples underscore the need for regulations that go beyond consent to ensure that organizations are held accountable for their actions, even when individuals are unable to give informed consent or withdraw consent at will (Bardaweel et al., 2021).

The accountability framework has also been tested in practice in other jurisdictions. In Brazil, the Lei Geral de Proteção de Dados (LGPD), which was enacted in 2020, mirrors many of the provisions of the GDPR, emphasizing the need for accountability in data processing activities. Under the LGPD, organizations must designate a data protection officer and conduct data protection impact assessments, similar to the requirements of the GDPR. The LGPD also emphasizes transparency, requiring organizations to provide clear information about their data practices and to notify individuals in the event of a breach. One notable difference, however, is that the LGPD offers more flexibility in terms of consent, allowing organizations to process personal data under a broader range of lawful bases, including legitimate interest, which can be seen as a departure from the strict consent model of the GDPR. Nonetheless, like the GDPR, the LGPD aims to ensure that organizations take proactive measures to protect personal data and are held accountable for any lapses in compliance (Bentotahewa et al., 2022).

In Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) offers a similarly accountability-driven approach to privacy regulation, although it places more emphasis on ensuring organizations have policies and practices in place to protect personal data. While PIPEDA does require organizations to obtain consent for the collection, use, and disclosure of personal data, it also recognizes the importance of accountability by requiring organizations to implement measures to safeguard data, such as setting up data protection policies, training employees, and conducting audits. However, PIPEDA's reliance on consent, rather than solely on accountability mechanisms, continues to reflect the model it was initially based upon, and organizations in Canada are still encouraged to obtain consent before collecting personal data whenever possible (Barati et al., 2020).

Similarly, in China, the Personal Information Protection Law (PIPL), enacted in 2021, has been described as the country's most comprehensive privacy law to date. The PIPL shares many similarities with the GDPR, particularly in its approach to ensuring that organizations are accountable for how they handle personal data. It requires organizations to designate data protection officers and to conduct impact assessments when processing sensitive data. The law also places restrictions on the collection of personal information, and individuals are granted rights to access, correct, and delete their data, in line with the GDPR's provisions. However, the PIPL also includes stricter requirements regarding the transfer of personal data outside China, reflecting the country's unique approach to data governance (Binardy, 2021).

Overall, the shift from a consent-based model to one focused on accountability reflects a growing understanding that privacy protection cannot rely solely on individual actions or consent but must also involve proactive efforts by organizations to ensure responsible data processing. This evolution towards a more robust accountability framework is seen as essential in addressing the complex challenges posed by modern data ecosystems, and its implementation continues to shape the future of privacy regulations across the globe.

5. Challenges in Implementing Data Subject Rights Globally

The implementation of data subject rights globally presents numerous challenges, with enforcement being one of the most significant obstacles. As personal data flows across borders at unprecedented rates, the issue of enforcement has become a complex matter, particularly in jurisdictions with different legal frameworks. Privacy regulations, such as the General Data Protection Regulation (GDPR), have provided a unified approach within the European Union, yet the global landscape remains fragmented. Organizations that operate internationally often encounter difficulties in ensuring compliance with privacy laws due to jurisdictional challenges. In a world where data can easily be transferred between jurisdictions, it is not always clear which regulatory body has the authority to enforce the rules. This can lead to situations where personal data is processed in one country, but the individuals whose data is affected reside in another country, making it difficult for the data subject to assert their rights or for regulators to take action. These jurisdictional issues become even more complicated when a company's operations span multiple countries with different privacy laws, leading to potential conflicts or inconsistencies in the application of regulations. In some cases, companies may be subject to overlapping or contradictory legal requirements, which further complicates enforcement efforts (Barati et al., 2020).

Another challenge lies in the variations in regulatory frameworks between different regions and countries. While certain privacy laws, like the GDPR, have achieved widespread recognition and influence, many countries continue to develop their own frameworks, often with different requirements and definitions of key concepts. For example, some jurisdictions may focus more heavily on data protection from a security standpoint, while others may prioritize individual rights to privacy. This lack of harmonization in privacy laws creates significant challenges for multinational corporations attempting to navigate the complexities of compliance across diverse legal environments. Even when privacy laws are aligned, inconsistencies in enforcement mechanisms and penalties for non-compliance can lead to uneven protection for data subjects across different regions. As such, the global nature of data flows necessitates more robust international cooperation to ensure that data subject rights are upheld universally (Bentotahewa et al., 2022).

The challenge of cultural and regional differences further complicates the global implementation of data subject rights. Privacy is a concept that is deeply embedded in the cultural, social, and political context of a given region. Different countries and regions may have varying attitudes toward privacy and data protection, which in turn influence the design and enforcement of privacy laws. For example, in some cultures, privacy is considered an absolute right, while in others, it may be viewed as a more flexible concept, balanced against other societal interests such as national security or economic development. These cultural variations shape how privacy laws are interpreted and enforced. In countries with a strong tradition of individual rights and freedoms, there may be a greater emphasis on protecting personal data as a fundamental right. In contrast, in countries with more collectivist or security-oriented approaches, the protection of personal data may be seen as secondary to other societal goals. These differences can lead to varying levels of protection for data subjects, depending on the region in which they reside (Beauvais & Knoppers, 2021).

The role of technology in the enforcement of data subject rights is another area where challenges have emerged. The rapid development of technologies such as artificial intelligence (AI), blockchain, and big data has introduced new complexities in

the area of data protection. These technologies often enable the collection, processing, and sharing of personal data at a scale and speed that was previously unimaginable. While they bring significant benefits, including greater efficiencies and more personalized services, they also pose unique challenges to the protection of data subject rights. For instance, AI systems can process vast amounts of data to make decisions about individuals, often without transparency or clear accountability. This raises concerns about how individuals can exercise their right to access or rectify their personal data when it is used in complex algorithmic systems. The opacity of AI decision-making processes means that individuals may not even be aware that their personal data is being processed in this way, making it difficult for them to assert their rights under existing privacy regulations (Barati et al., 2020).

Similarly, blockchain technology presents challenges for data protection, particularly with regard to the right to erasure or the "right to be forgotten." Blockchain operates on the principle of immutability, meaning that once data is recorded on a blockchain, it cannot be altered or deleted. This poses a direct conflict with data subject rights that are enshrined in privacy laws, particularly under the GDPR, which allows individuals to request the deletion of their personal data. While blockchain offers numerous benefits in terms of transparency and security, its inherent characteristics complicate the implementation of data protection laws that are designed to give individuals control over their personal information (Beauvais & Knoppers, 2021). Furthermore, big data presents challenges due to the vast amounts of personal information that are aggregated and processed for analytical purposes. The ability to derive inferences from large datasets, often without clear consent from individuals, raises concerns about the erosion of privacy and the potential for discriminatory outcomes. The use of big data in decision-making processes, such as hiring, lending, or healthcare, also exacerbates issues related to transparency and accountability, as individuals may not have the knowledge or means to understand how their data is being used (Amali, 2022).

In addition to these technological barriers, the rise of data-driven business models presents a fundamental challenge to the implementation of data subject rights. Many organizations, particularly in the digital economy, rely heavily on personal data for their business operations. This includes the use of data for targeted advertising, personalized recommendations, and the development of new products and services. While these business models can bring economic benefits, they often prioritize profit generation over individual privacy, leading to a tension between commercial interests and the rights of data subjects. This dynamic has led to concerns about the commodification of personal data, where individuals' privacy is treated as a resource to be exploited for economic gain. The challenge, then, is to reconcile the commercial interests of organizations with the need to protect individual privacy, while also ensuring that data subject rights are upheld (Bentotahewa et al., 2022).

The convergence of these various challenges—jurisdictional issues, cultural differences, technological advancements, and business interests—creates a complex environment for the effective implementation and enforcement of data subject rights on a global scale. As data flows freely across borders, the protection of personal information requires a multifaceted approach that considers not only legal frameworks but also technological and societal factors. In order to address these challenges, there is a growing call for international cooperation and harmonization of privacy laws, as well as the development of new technologies and mechanisms for ensuring that data subject rights are protected in an increasingly complex digital landscape. At the same time, greater transparency and accountability are needed from organizations handling personal data to ensure that they respect the rights of individuals and are held accountable for any breaches of privacy (Binardy, 2021). Ultimately, the future of data subject rights depends on the ability of regulators, businesses, and individuals to work together to address these challenges and create a system of data protection that is both effective and fair.

6. Future Directions: Enhancing Accountability and Empowering Data Subjects

The future of global privacy regulations is likely to witness significant developments, particularly in the areas of accountability, transparency, and empowerment of data subjects. As privacy concerns continue to evolve alongside technological advancements, legal frameworks are expected to become more robust and adaptable, addressing new challenges that arise in the rapidly changing digital environment. One of the key areas of evolution will be an increased emphasis on accountability. While current regulations, such as the General Data Protection Regulation (GDPR), have established foundational principles of data protection and accountability, the next step in the evolution of privacy laws may involve even stronger mechanisms for ensuring that organizations remain compliant over time. This could include more stringent reporting

and monitoring requirements for businesses, as well as enhanced transparency around how organizations process personal data. The goal would be to create an environment where data subjects are not only aware of their rights but also confident that organizations are continuously held to high standards of accountability in their data handling practices. The evolving nature of digital ecosystems, with new technologies and business models emerging daily, will demand that privacy laws keep pace, creating the need for dynamic regulatory approaches that are capable of addressing the complexities of data processing across diverse contexts.

As privacy regulations become more robust, innovations in enforcement mechanisms will play a critical role in ensuring that data subject rights are respected. Currently, one of the major hurdles to effective enforcement is the complexity and scale of monitoring compliance across borders. With the rise of automated processes, machine learning algorithms, and artificial intelligence (AI), there is potential for these technologies to enhance privacy law enforcement. Automated compliance tools could streamline the process of assessing whether organizations are adhering to data protection requirements in real-time, alerting regulators to any potential violations as they occur. These tools could also allow data subjects to easily exercise their rights, such as accessing or rectifying their personal data, without relying on cumbersome bureaucratic processes. Additionally, AI-driven enforcement could help regulators monitor the activities of multinational organizations and track the movement of personal data across jurisdictions, ensuring that data subject rights are upheld regardless of the location or size of the organization involved. By providing regulators with advanced tools for continuous monitoring and compliance checks, such innovations could significantly improve the effectiveness of data protection laws and increase the accountability of organizations.

Moreover, legal innovations will be necessary to complement technological advancements in the enforcement of privacy regulations. New laws may need to account for emerging issues, such as cross-border data flows, the role of data intermediaries, and the use of blockchain or other decentralized technologies that challenge traditional regulatory models. As organizations adopt more sophisticated technologies to process and store personal data, privacy laws will need to evolve to address potential risks associated with these technologies, while also ensuring that the rights of individuals remain protected. Innovations may also focus on transparency mechanisms, where organizations are required to publicly disclose their data practices and provide regular audits of their compliance with privacy laws. This could include public-facing dashboards that allow data subjects to easily see how their data is being used, the categories of personal data being processed, and the safeguards in place to protect that data. Such transparency measures would not only empower individuals but also put pressure on organizations to operate with a higher degree of accountability.

One of the most ambitious goals for the future of privacy regulation is the possibility of global harmonization of privacy laws. Currently, the lack of alignment between privacy laws in different jurisdictions presents a significant challenge to both organizations and data subjects. As businesses become more globalized and personal data is processed in multiple countries, the variation in privacy regulations creates a fragmented environment in which companies must navigate a complex maze of legal requirements. Achieving greater harmonization in global privacy laws would ensure that data subjects are protected in a consistent manner, regardless of where their data is being processed or stored. This could be accomplished through the establishment of international treaties or agreements that align the key principles of data protection and ensure that the rights of individuals are respected globally. The European Union has made significant strides toward global leadership in this area with the GDPR, but for real harmonization to occur, other major regions, including the United States, Asia, and Latin America, would need to adopt similar frameworks that focus on the core principles of accountability, transparency, and respect for data subject rights. Such harmonization would make it easier for multinational companies to comply with privacy regulations and ensure that data protection practices are consistent worldwide.

Furthermore, harmonized global privacy regulations could encourage the development of international standards for the ethical use of emerging technologies. As new technologies such as artificial intelligence, big data analytics, and blockchain continue to gain prominence, they introduce new risks and challenges to privacy. By adopting common privacy standards, countries could work together to address these challenges, ensuring that individuals' data is protected in a way that reflects universal human rights principles. Global cooperation on privacy issues would not only help to protect individuals but also foster innovation by creating a more predictable and stable regulatory environment for businesses. In this way, the future of privacy regulation could balance the need for robust data protection with the potential for technological innovation, providing a framework in which both individual rights and economic growth can coexist harmoniously.

The future of privacy regulations is poised to address many of the challenges that exist today, including gaps in enforcement, jurisdictional complexities, and the ethical use of emerging technologies. As privacy laws evolve, the focus will likely shift toward greater accountability for organizations, enhanced transparency for data subjects, and a harmonized global framework that ensures consistent protections across borders. These developments will not only empower individuals to control their personal data but also create a more sustainable and responsible data-driven economy.

7. Conclusion

In conclusion, the global landscape of privacy regulations has evolved significantly in recent years, driven by the increasing recognition of the need to protect individuals' personal data in an interconnected, data-driven world. The shift from a traditional consent-based model to one that emphasizes accountability marks a pivotal moment in the development of privacy laws. While consent remains an important element of data protection, it is becoming increasingly clear that accountability mechanisms are essential to ensure that organizations uphold their obligations to data subjects and that individuals are empowered to exercise their rights effectively. The evolution of privacy laws, particularly with the advent of the General Data Protection Regulation (GDPR), has set a global precedent for privacy protection, introducing comprehensive frameworks that focus not only on data subjects' rights but also on the accountability of organizations processing personal data.

The challenges in implementing these legal frameworks globally, however, cannot be understated. Jurisdictional conflicts, variations in regulatory approaches across regions, and differences in cultural attitudes toward privacy complicate the enforcement and consistency of privacy regulations. The complexities introduced by emerging technologies, such as artificial intelligence, big data, and blockchain, further challenge the effectiveness of current privacy laws and highlight the need for continuous innovation in legal frameworks to address new issues. The limitations of the consent model, including difficulties in ensuring informed and voluntary consent and the power imbalances that often exist between individuals and organizations, demonstrate that traditional approaches may no longer suffice in safeguarding personal data in the digital age.

Looking ahead, the future of global privacy regulations will likely involve greater harmonization between regional and national frameworks. While privacy laws such as the GDPR have been a step toward more unified regulations, achieving truly global privacy protection will require international cooperation and collaboration. The continued development of technological solutions, such as AI-driven compliance tools and automated enforcement mechanisms, holds promise for enhancing the enforcement of privacy laws and ensuring that organizations are held accountable for their actions. These innovations could empower data subjects, making it easier for individuals to assert their rights and for regulators to monitor compliance on a large scale.

Moreover, the ongoing evolution of privacy laws will need to strike a balance between protecting individual rights and fostering innovation. As businesses increasingly rely on data-driven technologies, it is crucial that privacy laws are flexible enough to support the growth of emerging industries while ensuring that the fundamental rights of individuals are upheld. This balance will be key in maintaining public trust and confidence in the digital economy.

Ultimately, the protection of data subject rights is an ongoing challenge that requires dynamic, responsive legal frameworks capable of adapting to the ever-changing technological landscape. The emphasis on accountability, transparency, and empowerment of data subjects will continue to guide the evolution of global privacy regulations. As the world becomes more interconnected, the importance of safeguarding personal data will only grow, and the development of effective privacy laws will be critical in ensuring that individuals' rights are respected in the digital age.

Ethical Considerations

All procedures performed in this study were under the ethical standards.

Acknowledgments

Authors thank all participants who participate in this study.

Conflict of Interest

The authors report no conflict of interest.

Funding/Financial Support

According to the authors, this article has no financial support.

References

Adib, A. (2023). Comparative Analysis of Data Protection Laws Among the SAARC Countries: An Appraisal. *Bauet J*, *4*(1). https://doi.org/10.59321/bauetj.v4i1.23

Amali, E. R. T. B. A. (2022). Holistic Approach in Introducing Proper Legal Framework to Regulate Data Protection and Privacy in Sri Lanka. *Vidyodaya Journal of Management*, *8*(I). https://doi.org/10.31357/vjm.v8ii.5608

Barati, M., Rana, O., Petri, I., & Theodorakopoulos, G. (2020). GDPR Compliance Verification in Internet of Things. *IEEE Access*, *8*, 119697-119709. https://doi.org/10.1109/access.2020.3005509

Bardaweel, S. K., AlMuhaissen, S. A., Alkurdi, N. H., & Tayyem, H. H. (2021). Data Privacy and Confidentiality From the Perspectives of General Public and Health Care Providers in Jordan. *International Journal of Clinical Practice*, *75*(6). https://doi.org/10.1111/ijcp.14117

Beauvais, M. J., & Knoppers, B. M. (2021). Coming Out to Play: Privacy, Data Protection, Children's Health, and COVID-19 Research. *Frontiers in Genetics*, *12*. https://doi.org/10.3389/fgene.2021.659027

Bentotahewa, V., Hewage, C., & Williams, J. (2022). The Normative Power of the GDPR: A Case Study of Data Protection Laws of South Asian Countries. *Sn Computer Science*, *3*(3). https://doi.org/10.1007/s42979-022-01079-z

Binardy, Y. A. (2021). Legal Protection Arrangements in Indonesia for Privacy Rights in Cases of Personal Data Leakage. *International Journal of Social Science and Human Research*, *04*(12). https://doi.org/10.47191/ijsshr/v4-i12-56

Gray, C. M., Santos, C., Bielova, N., Toth, M., & Clifford, D. (2021). Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective. 1-18. https://doi.org/10.1145/3411764.3445779

Hou, B. (2021). A Novel Data Governance Scheme Based on the Behavioral Economics Theory. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3773565

Human, S., Pandit, H. J., Morel, V., Santos, C., Degeling, M., Rossi, A., Botes, W., Jesus, V., & Kamara, I. (2022). Data Protection and Consenting Communication Mechanisms: Current Open Proposals and Challenges. 231-239. https://doi.org/10.1109/eurospw55150.2022.00029

Islam, M. T. (2022). An Assessment of Privacy Regime in Bangladesh. *Uum Journal of Legal Studies*, *13*. https://doi.org/10.32890/uumjls2022.13.2.4

Jusić, A. (2022). Privacy Between Regulation and Technology: GDPR and the Blockchain. *Iuslawjournal*, *Vol 1*(No 1), 47-59. https://doi.org/10.21533/iuslawjournal.v1i1.9

Krishnamurthy, V. (2020). A Tale of Two Privacy Laws: The GDPR and the International Right to Privacy. *Ajil Unbound*, *114*, 26-30. https://doi.org/10.1017/aju.2019.79

Lindén, T., Khandelwal, R., Harkous, H., & Fawaz, K. (2020). The Privacy Policy Landscape After the GDPR. *Proceedings on Privacy Enhancing Technologies*, *2020*(1), 47-64. https://doi.org/10.2478/popets-2020-0004

Ribeiro-Navarrete, S., Saura, J. R., & Palacios-Marqués, D. (2021). Towards a New Era of Mass Data Collection: Assessing Pandemic Surveillance Technologies to Preserve User Privacy. *Technological Forecasting and Social Change*, *167*, 120681. https://doi.org/10.1016/j.techfore.2021.120681

Rosenberger, A., Shvartzshnaider, Y., & Sanfilippo, M. R. (2021). Digital Contact Tracing in the <scp>EU</Scp>: Data Subject Rights and Conflicting Privacy Governance. *Proceedings of the Association for Information Science and Technology*, *58*(1), 819-821. https://doi.org/10.1002/pra2.574

Santos, C., & Pandit, H. J. (2023). How Could the Upcoming ePrivacy Regulation Recognise Enforceable Privacy Signals in the EU? https://doi.org/10.31219/osf.io/xvyf3

Teatini, S., & Matinmikko-Blue, M. (2020). Privacy in The 5G World: The GDPR in a Datafied Society. 1-13. https://doi.org/10.1002/9781119471509.w5gref173

Vlahou, A., Hallinan, D., Apweiler, R., Argilés, À., Beige, J., Benigni, A., Bischoff, R., Black, P. C., Boehm, F., Céraline, J., Chrousos, G. P., Delles, C., Evenepoel, P., Fridolin, I., Glorieux, G., Gool, A. J. v., Heidegger, I., Ioannidis, J. P. A., Jankowski, J., . . . Vanholder, R. (2021). Data Sharing Under the General Data Protection Regulation. *Hypertension*, *77*(4), 1029-1035. https://doi.org/10.1161/hypertensionaha.120.16340

Wagner, I. (2022). Privacy Policies Across the Ages: Content and Readability of Privacy Policies 1996--2021. https://doi.org/10.48550/arxiv.2201.08739

Yilmaz, S. S., & Seval, H. D. (2022). Mind Over Matter: Examining the Implications of Machine Brain Interfaces on Privacy and Data Protection Under the GDPR. *European Journal of Privacy Law & Technologies*(2), 342-356. https://doi.org/10.57230/ejplt222ssyhds

Yue, J., & Skiera, B. (2022). How Do Privacy Laws Impact the Value for Advertisers, Publishers and Users in the Online Advertising Market? A Comparison of the EU, US and China. *Journal of Creating Value*, *8*(2), 306-327. https://doi.org/10.1177/23949643221117676