ISSN 2706-6827 Vol. 7, Issue 3: 67-73, DOI: 10.25236/IJFS.2025.070310

The Role of GDPR in Strengthening Personal Data Security

Yuan Li

Faculty of Law & Justice, University of New South Wales, Sydney, New South Wales 2052, Australia
leali23ly@outlook.com

Abstract: *This essay will argue that the European Union's General Data Protection Regulation is effective in strengthening the protection of personal data, especially in the context of increasing globalization and digitalization. Since the birth of Internet technology, electronic data and network information flow rapidly, and personal information security problems are gradually exposed. Therefore, the European Union to implement the General Data Protection Regulation came into being. Through the analysis of three key legal cases, This essay demonstrates how GDPR effectively protects the security of personal information in specific cases. GDPR still faces the contradiction between the inherent lag of laws and institutions and technological progress in the digital realm. The GDPR needs to be constantly adjusted to keep pace with technological innovation.*

Keywords: *Personal Privacy Data Protection, GDPR, Information Security*

1. Introduction

In the age of digital globalization, data privacy and protection have become critical issues, which prompted the European Union to implement the General Data Protection Regulation in 2018. GDPR is widely considered the nice standard on regulations related to personal data protection.[13] This legislation has a significant impact on the legal practice of personal privacy data protection, and its ultimate aim is to protect personal information. However, the GDPR faces significant challenges in fully achieving its legislative purpose, especially due to the contradiction between the inherent lag of the law and the rapid development of technological advances in the digital sphere, which means that the GDPR will have difficulties adapting to new technologies during the implementation process. If a law is difficult to enforce, it is hard to be a real law.

The GDPR seeks to ease the complex conflict between the need for personal data protection in the Internet age and the dependence of businesses and governments on personal data. Its core principles and regulations are embodied at the level of directly restricting the collection and use of personal data, which lays the foundation for preventing the theft of personal information. Since its implementation, GDPR has played a key role in broadening the path of data protection practices, not only within the EU, but also in other countries and regions around the world, influencing the way organizations handle personal information.

However, with the continuous development of technology, the law related to private data and information security is increasingly tested. This lag between technological innovation and the application of the law creates potential gaps in the field of data protection. This issue also plays out in the application and implementation of GDPR, particularly with regard to the leakage of personal information.

Through case studies, this paper analyzes how GDPR deals with practical problems in legal practice, including the ways and limitations of dealing with the problem of lag. For example, the case 'Google LLC v CNIL' highlights the geographical limitations to which GDPR applies. British Airways (BA) Data Breach Incident and the 'Irish Data Protection Commission v Meta Platforms Ireland Limited' case demonstrates the impact of GDPR on the data-processing practices of companies.

Finally, the article will discuss its practical role in protecting personal data, deepening the understanding of GDPR in protecting personal data in a digital, informational world.

ISSN 2706-6827 Vol. 7, Issue 3: 67-73, DOI: 10.25236/IJFS.2025.070310

2. GDPR Overview

GDPR applies to all processing of personal data about the EU citizens. This deliberately broad definition establishes awareness of the importance of the privacy of EU citizens' personal data, its processing, usage, and sharing. It makes a preliminary judgment on the protection of personal privacy security in the information age.

As a pioneer in personal data protection, GDPR covers a very broad scope and generally applies to all businesses and various organizations that receive personal data. Large data collectors must adapt to and comply with GDPR to reduce long-term legal liability risks while ensuring the security of personal data.[11]

Because individuals naturally have perpetual ownership and control over their personal data, they inherently have the right to publish their information on the internet. GDPR enshrines key 'privacy rights', allowing individuals to exercise ongoing 'boundary control' by requiring explicit and continuous consent, which data collectors must respect.[13]

Although data security is sometimes considered separate from privacy, it is closely related. Accessing data without an individual's consent violates their ownership and control over data access and usage, leading to potential personal information leaks and subsequent security issues such as identity theft.

3. Case studies on the specific role of GDPR in protecting personal information

3.1 Google LLC v CNIL (Court of Justice of the European Union, Case C-507/17, 24 September 2019)

3.1.1 Brief introduction of the case

French National Commission on Informatics and Liberty (CNIL) ordered Google to remove users' requests from search results worldwide, that is, to enforce the 'right to be forgotten' on all of its domain name extensions. Google argues that such a global deletion obligation goes beyond the provisions of the GDPR, arguing that such a right should apply to domain names in EU member states.[6]

The court ruled that under the GDPR, Google must delete content related to domains within EU member states.

3.1.2 Focus of dispute

The 'right to be forgotten' at the heart of this case is an important right under the GDPR, reflecting advances in data protection law in the digital age. This right gives great respect to individuals, clarifies the right to create their own data subjects, and gives individuals the right to delete personal data on the Internet. This right increases the subjective control of the individual over the data and has a profound impact on the protection of personal privacy.

This case underscores the importance of protecting individuals' right to privacy. Search engine companies are not unrelated subjects and should also have some obligations when processing personal information. This means that large search engine companies like Google are required by law to support users' requests to delete personal information. Offer some help when necessary. This legal provision not only gives individuals more control over their online information, but also clarifies the scope of responsibility of search engine companies and other data controllers.

3.1.3 Application and challenge analysis of GDPR

In the European Union, the right to forget is effective in matters of information control and protection. When personal information is obtained illegally on the Internet, it is often used for various fraud activities. Individuals can now request the deletion of various types of personal or important information, such as personal phone numbers, home addresses, financial information, and workplace. The implementation of this right is important to reduce the risk of personal data stolen. Because in most cases, law enforcement is as helpless in responding to personal data stolen.[5]By allowing individuals to remove sensitive information from publicly accessible online resources, the 'right to be Forgotten' effectively reduces the amount of personal data that could be exploited by potential identity thieves.

By giving individuals more control over their online data and information, the right to be forgotten provides an important legal tool to prevent personal data stolen under the GDPR framework. A primary

ISSN 2706-6827 Vol. 7, Issue 3: 67-73, DOI: 10.25236/IJFS.2025.070310

effect of data breach laws should be the reduction of the incident of personal data stolen, as well as a mitigation of its impact, via better precaution.[10]

It reflects how data protection laws are struggling to adapt to the demands of the digital age, while also highlighting the complexity of enforcing such rights in a global internet environment.

Over time, the implementation and impact of the 'right to be forgotten' will continue to be an important topic in data protection and privacy discussions.

The ruling also indicates that in the context of globalization, the GDPR's jurisdiction over personal information is currently limited to the EU region. The 'extraterritoriality' of EU data protection legislation, or rather its territorial extension, risks conflicts with non-EU countries.[4]They may have different data protection standards. The GDPR faces implementation challenges in a globalized context, making it difficult to effectively protect personal data on a global scale.

But the scope of the GDPR is not limited. The GDPR's reach is far wider, which means almost all the institution anywhere in the world that provides services into the EU that involve processing personal data will have to comply.[1]

This case reflects the limitations of legal provisions in addressing complex and evolving situations within the global internet environment. In a diverse setting, the law is always lagging, and there is a conflict between the borderless nature of the internet and the territoriality of legal frameworks.

3.2 Analyzing the British Airways (BA) Data Breach Incident

3.2.1 Brief of the case

In June 2018, British Airways (BA) experienced a major data breach due to security vulnerabilities in their website and mobile application, resulting in the exposure of personal data of approximately 500,000 customers, including names, addresses, payment card information, and login details. In June 2019, the UK's Information Commissioner's Office (ICO) fined British Airways £183 million under GDPR regulations, but the final amount was set at £20 million. ICO investigators found that BA did not detect the June 22, 2018, attack on their own, but rather received a third-party alert on September 5, more than two months later. Upon realizing this, BA immediately took action and notified the ICO. The ICO determined that British Airways failed to implement adequate technical and organizational measures to protect users' personal data, thereby violating relevant provisions of the GDPR.

3.2.2 Application of GDPR

The leakage of personal data often results in a series of issues, including privacy violations. Large-scale data breaches involve not only well-known enterprises but also government agencies and other public institutions. Such incidents severely impact the reputation of companies and the credibility of governments.

From the perspective of the GDPR, personal data stolen typically occurs when data is out of control, meaning that data may be stolen or accidentally lost when the technical protections for data processing are insufficient. According to the GDPR, the processing of personal data should pay attention to legality, transparency, data minimization, and security. In the event of a data breach, the controller should promptly report this to the supervisory authority and, where appropriate, no later than seventy-two hours after becoming aware of it, unless the data breach poses a minor risk to the rights and freedoms of the individual. The ICO determined that BA's response was untimely and inappropriate, and did not achieve the desired effect, leading to the decision to impose a penalty.

3.2.3 The effectiveness of GDPR in protecting personal data

Although the ICO's penalty for British Airways took into account the force majeure factor of COVID-19, the final penalty is also very high. This serves as a warning to all businesses that use user data to take data security more seriously and push them to improve their personal data protection.

The data breach in this case included payment card information, a type of personally identifiable information that can easily be used for criminal offenses such as identity theft and financial fraud. Many consumers said that they avoid making purchases online because of concern that their important information may be stolen.[7] Effective data protection measures and severe penalties for breaches help to increase consumer trust in companies' data processing capabilities and security.

The law is now a useful method. The ICO's punitive measures against BA underscore the

ISSN 2706-6827 Vol. 7, Issue 3: 67-73, DOI: 10.25236/IJFS.2025.070310

importance it attaches to personal information.

3.2.4 The contradiction between new technology and legal lag

Although new technology continue to be an invaluable resource, they also form the basis of a unique medium for someone by providing unlimited opportunities to engage in personal data stoling.[9] With the development of new technologies, cyber attack methods are also continuously advancing. In this case, the attackers carried out multiple acts of information theft. Since the attack, British Airways has made significant improvements to the security of its IT systems. Companies need to continually update their security measures to counter new threats, which may result in them suffering losses from being unable to cope with these new technologies while also facing penalties under GDPR. The law finds it challenging to anticipate such situations. This could place greater pressure on companies, potentially resulting in outcomes contrary to the original intentions.

3.3 Irish Data Protection Commission v Meta Platforms Ireland Limited

3.3.1 Brief of the case

The Irish Data Protection Commission (DPC) conducted an investigation into Meta Platforms Ireland Limited (Facebook Ireland Ltd), focusing on the legality of Meta Ireland's transfer of EU user data to the United States. This case spanned over ten years. The incident was exposed in 2013 by people familiar with the matter. In 2015, the European Court of Justice invalidated the 'Safe Harbor agreement'. In 2020, the 'Privacy Shield agreement' was declared invalid. In August 2020, the Irish Data Protection Commission (DPC) began an investigation. Finally, in May 2023, the DPC released the final results of the investigation. They found Meta Ireland in violation of the GDPR, ordered it to stop the transfer of personal data and imposed a fine of 1.2 billion euros.

The DPC also required Meta to cease transferring EU user data to the United States within five months and to ensure that its processing operations comply with GDPR requirements within 6 months.

3.3.2 Application of GDPR

The DPC mainly based its decision on Article 46(1) of the GDPR, which means in the absence of an adequacy decision, data controllers or processors must provide appropriate method. These measures for the protection of personal data are quite comprehensive and include obtaining approval through professional certification bodies and procedures, obtaining the explicit consent of the data subject for the data transfer and informing them of the risks that may be involved in the transfer. Additionally, the use of standard contractual clauses, approved by regulatory authorities as part of the data transfer agreement, ensures that the data recipient provides adequate protection.

Article 58 of the GDPR grants corrective powers to supervisory authorities, including the ability to suspend data flows and impose fines. Article 83 outlines the conditions for imposing fines. Articles 44-49 address the transfer of personal data to third countries. Therefore, the DPC sanctioned Meta Ireland based on the relevant laws.

These articles collectively form the regulatory framework for cross-border data transfers. In the context of the internet, the transmission and processing of data are analogous to the trade of physical goods in the real world. However, the boundaries and scope are much more complex than in the physical world. The transmission of personal data is more frequent, and regulations on data vary between countries and regions, with some even lacking such regulations. The purpose of the GDPR is to ensure that the personal data of EU citizens are adequately protected during transmission.

3.3.3 The effectiveness of GDPR

The GDPR requires an assessment of third-country laws to ensure that they can provide adequate protection for personal data. Additionally, the law grants supervisory authorities investigative and enforcement powers, providing institutional and legal safeguards for enforcement, which makes personal data protection more systematic.

In this case, the DPC conducted a detailed assessment of U.S. laws, found that they could not provide a level of protection equivalent to EU laws, and took decisive action.

3.3.4 Challenges to the GDPR

Data transfer is already common. Reliance on the Internet has changed the way individuals interact, conduct business, stay in touch with others, and collect and disseminate information.[9] In the context

ISSN 2706-6827 Vol. 7, Issue 3: 67-73, DOI: 10.25236/IJFS.2025.070310

of globalization, implementing and enforcing regulations in coordination with the legal systems of other countries or regions is extremely challenging. In the digital age, there are complex contradictions between legal and technological developments, as well as between commercial and trade demands. In this case, the GDPR addresses these conflicts arising from mismatches and lack of coordination by suspending the transfer of personal data if adequate protection is not ensured.

4. Summary of how the GDPR protects personal privacy

The GDPR plays a crucial role in protecting personal information. This regulation has established a comprehensive framework for personal data protection within the EU, and its impact is like a drop in the ocean, creating ripples that affect the entire world. Under the framework of the GDPR, the core of data protection includes main principles of data protection such as lawful processing, fair processing, and accountability of data controllers.[2]

The GDPR covers a wide range of subjects, from institutions to individuals. Institutions and organizations that hold personal information are required to obtain the explicit and affirmative consent of individuals before collecting or processing personal data. It requires the collection and processing of only necessary personal data, thereby reducing the risk and potential impact of data breaches. In this case, the data collector may only collect the necessary data for a specific purpose and delete it immediately after completing the specific purpose.

The GDPR grants individuals a wide range of rights, such as the 'right to access', 'right to redress' and 'right to be forgotten'. The GDPR regulates the ability of individuals to manage their digital identities and online traces in a way that affirms rights. The GDPR enforces strict data protection standards, creates a more secure environment for personal data, and helps prevent malicious cybersecurity incidents.

The GDPR also includes detailed provisions for regulatory authorities. In the event of a data breach, the organization must report it to the regulatory authorities within 72 hours of discovery. Additionally, the GDPR advocates for privacy by design, requiring the integration of data protection measures into the development of business processes for products and services. The case of the Irish Data Protection Commission against Meta Platforms Ireland Limited highlights the GDPR's stringent requirements for international data transfers. This case emphasizes the need for adequate safeguards in third countries and demonstrates the far-reaching impact of the GDPR on global data flows. Both this case and the British Airways data breach case underscore the crucial role of supervisory authorities in protecting personal data.

The GDPR strengthens data security through three main avenues: strict punitive measures, such as hefty fines, for tech companies and organizations that handle personal data;[12] a focus on protecting relatively vulnerable individuals; and an emphasis on the importance of regulatory authorities. The regulation also raises public awareness of personal data privacy, encouraging individuals to be more cautious with their personal information.

5. Reflections on the GDPR dilemma and Where will the laws protecting personal data head?

5.1 Reflections on the Dilemmas and Challenges of GDPR Implementation

In the digital age, rapid advances in technology often outpace existing legal frameworks, leading to potential gaps in protection measures. The EU's General Data Protection Regulation (GDPR) has significantly enhanced the protection of personal data in the EU region. The GDPR provides a solid foundation for addressing privacy issues in the digital age through comprehensive measures, and it has a significant effect on personal data protection in the EU. However, the implementation of GDPR on a global scale still faces certain challenges, especially in countries with different data protection standards, which makes its theoretical extraterritorial effect impossible to truly implement in legal practice.

The continuous application of GDPR marks the EU's achievements in protecting personal data privacy. Its core lies in increasing transparency and user autonomy, ensuring the transparency and legality of data processing, but also introduces new responsibilities and potential transaction costs for users. These measures have already achieved remarkable results within the EU, with companies and organizations significantly improving their compliance in data processing, personal data breaches

ISSN 2706-6827 Vol. 7, Issue 3: 67-73, DOI: 10.25236/IJFS.2025.070310

effectively curtailed, and citizens' privacy rights better protected. For example, the high fines against large technology companies such as Facebook and Google show the severity and effectiveness of the GDPR in the enforcement process. These companies need to pay attention to how users handle personal data and their privacy policies, and strengthen data protection measures to avoid another huge fine.

The implementation of GDPR on a global scale faces difficulties due to the complexity of data transfers. There are significant differences in data protection standards across countries, and domestic laws vary in their severity regarding personal data issues. Some countries impose civil penalties, while others consider it a criminal offense, and some lack regulations entirely. However, the flow of personal data does not depend on these legal provisions. Companies outside of the GDPR geographic area are still required to comply in some sense with the regulation.[3] But even if GDPR has extraterritorial effects, in countries where data protection laws are weak or poorly enforced, it is difficult for GDPR to achieve its primary purpose.

Apart from the British Airways Data Breach Incident, where BA's official system encountered technically sophisticated information theft,[8] the rapid development of emerging technologies such as artificial intelligence, blockchain, and big data has brought unprecedented challenges to data protection. While the GDPR was developed with the impact of technological developments in mind, its provisions are inevitably lagging in the face of a rapidly changing technological environment. For example, the powerful capabilities of AI technology in data processing and analysis make the protection of personal data more complex and difficult.

5.2 The future of personal data protection law

Personal data protection have become global challenges. With the rapid development of emerging technologies, traditional legal frameworks struggle to address these issues effectively.

Firstly, revising the laws themselves is essential to ensure they can effectively address personal data privacy issues brought about by emerging technologies. This requires close collaboration among stakeholders, including technical experts, industry representatives, and consumer rights protection organizations. By deeply understanding the characteristics of new technologies and their potential impact on personal data protection, laws can be crafted to protect individual rights without hindering technological innovation.

At the same time, international cooperation is an important way to solve this problem.[2]Through cooperation with data protection authorities in other countries and regions, a number of personal data protection organizations can be established, and each country and region can reach an agreement. Gradually, these common principles were incorporated into domestic law. This will facilitate the creation of laws related to the protection of personal data on a global scale.

In this context, GDPR is undoubtedly a landmark legal document. As a forward-looking data protection law, GDPR sets a new standard for data privacy protection in the digital age. It not only establishes uniform data protection rules within the EU, but also has a profound impact on global data protection practices through its extraterritorial effects. The GDPR introduces innovative concepts such as data portability and the right to be forgotten, strengthening the control of individuals over their own data, while also placing higher data processing requirements on enterprises. With the continuous development of technology and the strengthening of international cooperation, GDPR can continue to optimize and improve in the future, and make some new legal exploration for data privacy protection around the world.

While it is impossible to completely eliminate the risk of personal data problems, a combination of legal and technical measures can significantly reduce their frequency and impact. National supervisory authorities should have the capacity to ensure effective enforcement.[12] With the continuous development of the digital economy, protecting personal data will remain crucial issues that require ongoing attention and innovative solutions.

How to effectively protect personal data while promoting the full release of data value will continue to be an important issue that requires continuous attention and exploration of innovative solutions from all sectors of society. This is not only about individual rights, but also about the healthy and sustainable development of the digital economy.

ISSN 2706-6827 Vol. 7, Issue 3: 67-73, DOI: 10.25236/IJFS.2025.070310

6. Conclusion

The GDPR is regarded as an important legal attempt to protect personal data, and it has shown some effectiveness. With the rapid development of information and communication technology, GDPR is facing more challenges. The inherent lag of legal provisions and the complex realities of current demands are becoming increasingly apparent.

The three cases analyzed in the article illustrate both the strengths and inherent limitations of the GDPR. In the future, the evolution of personal data protection laws may involve several aspects like promoting international cooperation to tackle global challenges. But the current core challenge lies in keeping a balance between personal data protection, technological innovation, and economic interests. As the continuous upgrading of network technology, legal frameworks and protective mechanisms must advance to make sure individual privacy rights in the digital age.

References

[1] A. Roos, "The European Union's General Data Protection Regulation (GDPR) and its Implications for South African Data Privacy Law: An Evaluation of Selected 'Content Principles.' " The Comparative and International Law Journal of Southern Africa,2020, pp. 3-30.
[2] C. Kuner, "International Organizations and the EU General Data Protection Regulation" International organizations law review, 2019, pp.183.
[3] C. Laybats and J Davies, "GDPR: Implementing the Regulations" Business information review , 2018, pp. 82.
[4] C. Ryngaert, and T. Mistale, "The GDPR as Global Data Protection Regulation?" AJIL unbound 5, 2020, pp. 8.
[5] D. Reynolds, "Decisions, Decisions: An Analysis of Identity Theft Victims Reporting to Police, Financial Institutions, and Credit Bureaus" Victims & offenders, 2023,pp. 1394.
[6] Google LLC v. CNIL, Case C-507/17, ECLI:EU:C:2019:772 (Court of Justice of the European Union, September,2019,24.
[7] K. B. Anderson, D. Erik and S.A. Michael A, "Identity Theft," The Journal of economic perspectives, 2008, pp. 181.
[8] M.N. Lintvedt, "Putting a Price on Data Protection Infringement" International data privacy law, 2022, pp.12.
[9] P.Q. Brady, R. Ryan and B.W. Reyns, "From WWII to the World Wide Web: A Research Note on Social Changes, Online "Places," and a New Online Activity Ratio for Routine Activity Theory" Journal of contemporary criminal justice , 2016,pp. 130.
[10] S. Romanosky, T. Rahul and A. Alessandro, "Do Data Breach Disclosure Laws Reduce Identity Theft?" Journal of policy analysis and management,2011, pp. 262.
[11] S. Sharma and M. Pranav, "Data Privacy and GDPR Handbook," John Wiley & Sons, 1st edition, 2020, pp. 45.
[12] T.F. Walree and P.T.J Wolters, "The Right to Compensation of a Competitor for a Violation of the GDPR" International data privacy law, 2020, pp. 351.
[13] T. Tony Ke and K. Sudhir, "Privacy Rights and Data Security: GDPR and Personal Data Markets." Management Science,2023, pp. 4389.