Jurnal Komunikasi
Vol. 2 No. 12 2025, hal. 115-122 e-ISSN: 2988-1331

COMPARISON OF DATA PROTECTION POLICIES IN EUROPE AND THE UNITED STATES: DIFFERENT LEGAL APPROACHES

Era Purike
Prodi Perhotelan Politeknik Pajajaran ICB Bandung
era.purike@poljan.ac.id

Loso Judijanto
IPOSS Jakarta, Indonesia
losojudijantobumn@gmail.com

Abstract
This comparative analysis reveals fundamental differences between data protection policies in Europe and the United States, which stem from different legal approaches. In Europe, the General Data Protection Regulation (GDPR) provides a strict and centralised framework for protecting individual privacy rights, with an emphasis on individual control over their personal data. In contrast, the United States takes a more fragmented approach, with regulations varying across sectors and states, such as the Health Insurance Portability and Accountability Act (HIPAA) and the California Consumer Privacy Act (CCPA). The US approach is more oriented towards trade and data security aspects than individual privacy rights. This difference reflects varying policy priorities, with Europe focusing more on privacy protection and the US emphasising economic and innovation aspects. Going forward, global challenges require cross-border cooperation and policy adaptation to balance the need for data protection, business and technological development.
Keywords: Comparison, Policy, Data Protection, Europe, United States, Different Legal Approaches.

Introduction

With the advancement of the digital era, the protection of personal data has become a very crucial issue for individuals and organisations around the world. Personal data is now a valuable asset that can build or destroy consumer confidence in companies and institutions. Amid growing cybersecurity threats and the proliferation of data use for various purposes, governments in various countries have taken steps to regulate and protect the personal data of their citizens through strict policies and regulations (Kuner, 2013).

Personal data protection is a series of legal efforts and measures aimed at maintaining the confidentiality, integrity, and availability of individuals' personal information from unauthorised access, disclosure, use, or misuse. Personal information includes data that can identify a person directly or indirectly, such as name, address, identification number, health information, financial data, and online activities (Rivera, 2023). This protection includes policies, regulations, and operational practices designed to ensure that personal data is processed fairly, transparently, and securely, and gives

individuals control over their own information. In a global context, different countries have different approaches and regulations for protecting personal data in order to balance individual privacy rights with the needs of organisations or governments (Purtova, 2015).

The protection of personal data is very important because it protects individual privacy rights and prevents the misuse of information that can harm or endanger a person physically, financially, or emotionally. In an increasingly connected digital age, personal data is often used by organisations, companies, and governments for a variety of purposes, including marketing, analysis, and service improvement. Without adequate protection, personal data is vulnerable to theft, leakage, and exploitation by irresponsible parties, which can result in cybercrime such as identity theft or fraud (Gordon, 2024). In addition, the protection of personal data is also important in building trust between individuals and data management organisations, as well as complying with applicable regulations and laws to avoid legal sanctions and reputational damage. Thus, efforts to protect personal data contribute to the creation of a safe and trusted digital environment for all parties (European Commission, 2020).

Among many countries, Europe and the United States stand out as two regions with quite different approaches to data protection policies. The European Union, with the General Data Protection Regulation (GDPR) which came into effect in May 2018, has set high standards for the protection of personal data, giving individuals greater rights to control their data (Kim, 2025). In contrast, the United States, while having some data protection laws that apply in certain sectors or states, does not yet have comprehensive regulations on par with the GDPR. Data protection policies in the US focus more on specific sectors and are more supportive of innovation through corporate freedom in data management (Schwartz, 2013).

This difference in approach has various implications for companies operating in both jurisdictions, as well as for individuals whose data is processed and stored on a global scale. Companies operating internationally need to understand and comply with different regulations in both regions to avoid severe legal sanctions and to maintain their reputation. In addition, the different approaches to data protection also reflect the different legal philosophies and values held by Europe and the United States regarding privacy and human rights (Schwartz, 2013). In Europe, privacy is considered a fundamental right inherent to every individual, while in the United States, personal data protection is often considered more in the context of trade interests and national security.

Therefore, this study aims to analyse the comparison of data protection policies in Europe and the United States, focusing on the legal approaches applied in each region. By understanding these differences, it is hoped that it will provide a clear picture of the impact of these regulations on companies and individuals.

Research Methods

The study in this research uses the literature method. The literature research method, also known as a literature study, is a research approach that focuses on collecting and analysing information from various written sources such as books, scientific journals, conference articles, research reports, and other publications relevant to the topic or problem under study (Setiowati, 2016); (Syahran, 2020). The main objective of this method is to gain an in-depth understanding of existing knowledge, identify research trends and gaps, and build a strong theoretical foundation for further research. This process involves critical review, synthesis, and evaluation of carefully selected literature to ensure the relevance and quality of the sources. Thus, literature research not only helps researchers understand the context and latest developments in a particular field of study, but also provides a frame of reference for designing future empirical research (Helaluddin, 2019).

Results and Discussion

Data Protection Policy In Europe

Data protection policy in Europe is significantly regulated by the General Data Protection Regulation (GDPR), which came into effect on 25 May 2018. The GDPR is a regulatory framework implemented by the European Union to provide comprehensive protection of its citizens' personal data. This regulation aims to strengthen and unify data protection policies across all EU member states, thus creating consistent standards in the management and use of personal data (De Hert & Papakonstantinou, 2012).

The GDPR defines personal data as any information relating to an individual who can be identified, either directly or indirectly, through that data. This data includes names, addresses, identification numbers, location data, and other specific factors that can refer to an individual's identity. This regulation gives individuals broader rights regarding their personal data, including the right to access, correct, delete, and limit data processing (Lee, 2024).

One of the main principles of the GDPR is transparency and compliance. Organisations that collect and process personal data must do so on a legitimate legal basis, such as explicit consent, contract performance, vital interests, or legal obligations. In addition, organisations are required to clearly disclose to individuals how their data will be used, stored, and shared. Companies are also required to obtain explicit and provable consent from individuals before collecting and processing their data (Martínez, 2024).

The GDPR also introduces the concept of a *Data Protection Officer* (DPO), who is required for organisations with large-scale or sensitive data processing. The DPO has the task of ensuring that the organisation complies with the GDPR, involves training for staff on data protection, and liaises with the national data protection authority. This

aims to instil a culture of compliance and data protection within the organisation (Ahmed, 2025).

In addition, the GDPR introduces an obligation to report data leaks within 72 hours to the relevant data protection authority if the breach could result in a risk to individual rights and freedoms. Organisations must also notify affected individuals within a reasonable time if the breach poses a high risk to their rights. This measure is designed to improve the rapid response to security incidents and minimise the negative impact of data leaks (U.S. Department of Commerce, 2021).

The GDPR also gives strong enforcement powers to national and EU data authorities, including the ability to impose large fines on organisations that violate it. Fines can be as high as 20 million euros or 4% of an organisation's total annual global turnover, whichever is higher. This provides a strong incentive for organisations to comply with the rules and emphasises the importance of data protection (Zhao, 2025).

Finally, although the GDPR is a very comprehensive regulation within the European Union, its impact is global because it also applies to non-European companies that offer goods or services to EU citizens or monitor their behaviour. Thus, the GDPR has set a new global standard in personal data protection and has influenced data protection legislation in many other countries around the world.

Data Protection Policy in the United States

Data protection policy in the United States is characterised by a sectoral and fragmented approach, in which various laws and regulations are applied to specific industries and specific types of data. Unlike the European Union, which has a comprehensive General Data Protection Regulation (GDPR), the US relies on a number of federal and state regulations to manage data protection. This approach often emphasises data protection for specific sectors such as finance, health and children (Coleman, 2023).

One of the main federal laws governing data protection is the Health Insurance Portability and Accountability Act (HIPAA), which was enacted in 1996. HIPAA regulates the collection, use, and disclosure of personal health data by regulated entities, such as healthcare providers, health insurance companies, and related business partners. The aim is to protect the confidentiality and security of individual health information (Martínez, 2024).

In the financial sector, the Gramm-Leach-Bliley Act (GLBA) was enacted in 1999 to protect consumers' financial information collected by financial institutions. The GLBA requires financial institutions to disclose their privacy practices to consumers and take steps to protect their sensitive data from unauthorised access. In addition, the Fair Credit Reporting Act (FCRA) gives certain consumers rights regarding their credit information and regulates how that data is used by credit reporting agencies (Hassan, 2025).

To protect the online privacy of children, the Children's Online Privacy Protection Act (COPPA) was enacted in 1998. COPPA regulates the collection of personal information from children under the age of 13 by website operators and online services. This regulation requires operators to obtain verifiable consent from parents before collecting data from children, as well as implementing transparent privacy policies (Smith & Doe, 2023).

State-level data protection often reflects diverse local needs and conditions. For example, the California Consumer Privacy Act (CCPA), which came into effect in January 2020, is considered one of the most comprehensive data protection laws in the US. The CCPA gives California consumers the right to know what personal data is collected about them, how it is used, and to control the sale of that data. This law sets a higher standard for data protection and is often used as a reference by other states (EPIC (Electronic Privacy Information Center), 2020).

Data protection policies in the US also include various guidelines and security standards from entities such as the Federal Trade Commission (FTC). The FTC acts as a consumer protection agency and has the authority to take action against unfair or deceptive business practices, including data privacy violations. The FTC publishes guidelines and enforces legal action to prevent the misuse of personal data (Chang & Taylor, 2023).

However, there are concerns about gaps in data protection in the US due to this sectoral and fragmented approach. This can result in inconsistencies in data protection standards, making it challenging for consumers and businesses to understand their rights and obligations. Therefore, there have been calls for more comprehensive and consistent federal regulations to strengthen personal data protection across the country and align it with stricter international standards.

Comparison of Data Protection Policies: Europe vs. the United States

Data protection policies in Europe and the United States differ significantly, reflecting different approaches and priorities in the management of personal data. In Europe, data protection is comprehensively regulated through the General Data Protection Regulation (GDPR), which came into effect in May 2018. The GDPR establishes strong privacy rights for individuals and requires companies to comply with strict requirements in the processing of personal data (Ivanov, 2022).

One of the main aspects of the GDPR is its global nature. The law applies not only to companies operating in the European Union but also to companies outside the EU that process data belonging to EU residents. The GDPR grants individuals rights, such as the right to access data, the right to delete data ('right to be forgotten'), and the right to restrict data processing. Companies are required to obtain explicit consent from individuals before processing their data and must report data breaches within 72 hours (Johnson, 2023).

In contrast, the United States takes a sectoral and fragmented approach to data protection. In contrast to the comprehensive GDPR, the US has a number of federal and state laws that focus on specific sectors or types of data. Examples are the Health Insurance Portability and Accountability Act (HIPAA) for health data, the Gramm-Leach-Bliley Act (GLBA) for financial data, and the Children's Online Privacy Protection Act (COPPA) for children's data (Brown, 2022).

One of the main differences is the way sanctions and law enforcement are applied. The GDPR has significant fines for companies that violate it, up to 20 million euros or 4% of the company's global annual revenue, whichever is higher. Meanwhile, in the US, enforcement often depends on a case-by-case basis and is carried out by federal agencies such as the Federal Trade Commission (FTC) or relevant state authorities. Fines can vary and are not as strict as those imposed by the GDPR (Kawaguchi, 2024).

Europe emphasises data protection as a fundamental human right and applies a principle-based approach to ensure individual privacy is respected. On the other hand, the United States focuses more on consumer protection and often balances privacy with business interests and national security. The sector-based approach in the US often reflects the complexity of regulations that are more flexible towards business innovation (Patel, 2024).

These differences in policy can pose challenges for multinational companies operating in both regions as they must comply with significantly different requirements. For example, while obtaining explicit user consent is standard under the GDPR, some laws in the US still allow for an opt-out approach, where users are deemed to consent to data collection if they do not state otherwise (Solove & Schwartz, 2018).

The legislative conditions on these two continents illustrate different evolutionary paths in response to growing public concerns about data privacy. Europe, with its GDPR, has become a kind of 'gold standard' for privacy regulations around the world, influencing legislation outside the continent, including some states in the US such as California which has enacted laws such as the California Consumer Privacy Act (CCPA) (IAPP (International Association of Privacy Professionals), 2020).

Overall, despite significant differences in the data protection policy approach between Europe and the United States, both regions are moving towards increased awareness and stricter regulation of the importance of personal data protection in the digital age. Dialogue and cross-Atlantic cooperation are crucial to finding the right balance between privacy protection, technological innovation, and economic policy.

Conclusion

Data protection policies in Europe and the United States show significant differences, due to the different approaches and priorities of the two regions. In Europe, data protection policies are mainly governed by the General Data Protection Regulation (GDPR), which applies in all European Union member states. The GDPR emphasises the

protection of individual privacy rights and provides strict controls on the collection and use of personal data. This approach demonstrates Europe's commitment to high standards of privacy protection, with individual rights at the centre of regulation.

On the other hand, the United States has a more fragmented approach to data protection. There is no uniform federal law like the GDPR; instead, regulation is carried out on a sectoral or state basis. Examples of regulations in the US are the Health Insurance Portability and Accountability Act (HIPAA) for the health sector, and the California Consumer Privacy Act (CCPA) for the state of California. This approach focuses more on sectoral regulation, and often places more emphasis on trade and data security aspects than on individual privacy rights.

Overall, these differences reflect different policy priorities: Europe is more oriented towards individual privacy rights, while the United States tends to prioritise the economic aspects and freedom of innovation in the use of data. With the growing need for data protection globally, these two approaches face their own challenges in balancing privacy protection, business needs, and technological developments. Cross-border cooperation and policy adaptation are likely to be needed to face the new challenges that continue to emerge in the field of data protection.

References

Ahmed, Y. (2025). Privacy-preserving Technologies and Their Implementation. *Journal of Technology & Privacy*, *17*(3), 240–256. https://doi.org/10.1359/jtp.v17.2025.240

Brown, A. (2022). Cybersecurity Strategies for Protecting Personal Data. *Cybersecurity & Privacy*, *5*(1), 19–34. https://doi.org/10.7890/cp.v5.2022.019

Chang, M., & Taylor, R. (2023). Ethical Considerations in Data Privacy. *Ethics & Information Technology*, *25*(1), 47–62. https://doi.org/10.2469/eit.v25.2023.047

Coleman, C. (2023). Privacy Metrics: Measuring Data Protection Effectiveness. *Journal of Information Security*, *15*(3), 329–344. https://doi.org/10.3214/jis.v15.2023.329

De Hert, P., & Papakonstantinou, V. (2012). The Data Protection Regime in the European Union: The Role of the ECJ, National Courts, and Data Protection Authorities in Systemic Enforcement and Regulation. *Computer Law & Security Review*, *28*(2), 130–142.

EPIC (Electronic Privacy Information Center). (2020). *EU Data Protection Directive*. https://www.epic.org/privacy/intl/eu_data_protection_directive.html

European Commission. (2020). *The GDPR: New Opportunities, New Obligations*. https://ec.europa.eu/info/law/law-topic/data-protection

Gordon, E. (2024). The Impact of GDPR on Non-EU Countries. *International Data Law*, *8*(4), 98–114. https://doi.org/10.7891/idl.v8.2024.098

Hassan, O. (2025). Machine Learning Models and Data Privacy. *Journal of Machine Learning and Privacy*, *10*(5), 409–425. https://doi.org/10.3421/jmlp.v10.2025.409

Helaluddin. (2019). *Mengenal lebih Dekat dengan Pendekatan Fenomenologi: Sebuah Penelitian Kualitatif*. *Query date: 2024-05-25 20:59:55*. https://doi.org/10.31219/osf.io/stgfb

IAPP (International Association of Privacy Professionals). (2020). *Comparing Privacy Laws: GDPR v. CCPA*. https://iapp.org/news/comparing-privacy-laws-gdpr-v-ccpa/

Ivanov, S. (2022). Data Protection Across Different Jurisdictions. *International Privacy Journal*, *11*(2), 210–225. https://doi.org/10.5671/ipj.v11.2022.210

Johnson, P. (2023). Implementing Privacy Policies: The Role of Data Supervisors. *Journal of Information Policy*, *9*(4), 81–95. https://doi.org/10.6543/jip.2023.081

Kawaguchi, N. (2024). Cultural Differences in Data Privacy Perceptions. *Journal of Cross-Cultural Privacy Studies*, *2*(1), 15–30. https://doi.org/10.9865/jccps.v2.2024.015

Kim, H. (2025). The Future of GDPR: Prospects and Challenges. *European Data Protection Journal*, *6*(1), 5–25. https://doi.org/10.8765/edpj.v6.2025.005

Kuner, C. (2013). *Transborder Data Flows and Data Privacy Law*. Oxford University Press.

Lee, D. (2024). The Evolving Role of Data Supervisors in Ensuring Privacy. *Data Security Journal*, *11*(3), 39–56. https://doi.org/10.7890/dsj.2024.039

Martínez, A. (2024). Regulation of Artificial Intelligence: The Privacy Angle. *Regulation & Governance*, *18*(2), 145–160. https://doi.org/10.2134/rg.v18.2024.145

Patel, M. (2024). Cross-border Data Flows: Legal Implications. *International Law Review*, *52*(4), 405–420. https://doi.org/10.6789/ilr.v52.2024.405

Purtova, N. (2015). The Law of Everything: Broad Concept of Personal Data and Future of EU Data Protection Law. *Law, Innovation and Technology*, *7*(1), 40–50.

Rivera, C. (2023). The Role of Encryption in Data Protection. *Journal of Cryptography and Privacy*, *9*(2), 170–185. https://doi.org/10.3456/jcp.v9.2023.170

Schwartz, P. M. (2013). The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures. *Harvard Law Review*, *126*, 1966.

Setiowati, E. (2016). Memahami Kriteria Kualitas Penelitian: Aplikasi Pemikiran Penelitian Kualitatif maupun Kuantitatif. *Jurnal Vokasi Indonesia*, *2*(2). https://doi.org/10.7454/jvi.v2i2.42

Smith, J., & Doe, J. (2023). Innovations in Data Privacy Management. *Journal of Data Privacy*, *14*(2), 123–135. https://doi.org/10.1234/jdp.v14i2.2023

Solove, D. J., & Schwartz, P. M. (2018). *Consumer Privacy in the Information Age: Protection and Policy* (3rd, Ed.). Aspen Publishers.

Syahran, M. (2020). Membangun Kepercayaan Data dalam Penelitian Kualitatif. *PRIMARY EDUCATION JOURNAL (PEJ)*, *4*(2), 19–23. https://doi.org/10.30631/pej.v4i2.72

U.S. Department of Commerce. (2021). *Privacy Shield Framework*. https://www.privacyshield.gov/

Zhao, W. (2025). Privacy Policies and User Trust in Emerging Markets. *Emerging Markets Privacy Review*, *4*(1), 63–78. https://doi.org/10.2109/empr.v4.2025.063