Overview of GDPR and Its Enforcement Mechanisms

Destiny Hale

CYSE 425W

Professor Aslan

February 22, 2026

Introduction

In the world today, since technology has advanced throughout the years, data privacy has become a frequent topic that is addressed in cybersecurity and governments, regarding the security and safety of user data. Although most regulations set rules governing how organizations and companies gather and collect data, some fail to uphold the principles of protecting personal data and user privacy. However, in May 2018, a regulation upheld these principles by its strict responsibilities and enforcement mechanisms. This regulation was the General Data Protection Regulation (GDPR), which has become the strongest and most impactful data protection law in cybersecurity policy. This has also reshaped how global organizations and governments govern personal data.

What is the GDPR?

Li et al. (2019) describe the GDPR under simplistic terms as a data protection law that " lays down rules for processing, storing, managing data from people who are currently within the European Union". Some qualities of this law include that it holds companies accountable for personal data and establishes clear rules in the collection of data to reduce the risks of data being misused and unauthorized access. A few other qualities that this legislation includes are user rights, such as the right to be forgotten, access to data, data portability, etc (Li et al., 2019). All these rights give the user control over their data that companies legally hold. According to Axinte et al. (2018), the structure of the regulation comes with 272 paragraphs; half of the regulation includes the Directive's documentation, 11 chapters, and 16 sections. The layout of this regulation not only covers the overall principles of data privacy, but also specifies

responsibilities for companies to adhere to and comply with in processing personal data. By combining user rights and company responsibilities, this regulation creates a balanced framework that strengthens accountability while emphasizing the importance of data security.

Development of the GDPR

Before the GDPR came into full effect, there was a regulation called the European Data Protection Directive (DPD). This regulation was adopted in October 1995 and was developed for the protection of "individuals with regard to the processing of personal data and on the free movement of such data" (European Data Protection Supervisor, n.d.). This was the predecessor of the current law. Also, this is considered the first international data protection law (Bu-Pasha, 2017). A key characteristic of this law was that it also granted a few user rights, such as the right to know the data controller, the option to withhold data use in some circumstances, and to have inaccurate data rectified (Epic.org, n.d). It also had enforcement mechanisms, such as banning, order blocking, and destruction of data (Epic.org, n.d.). However, there were implications regarding how this legislation was practiced.

According to Bu-Pasha (2017), this regulation faced challenges regarding national implementation, legal issues, and addressing cross-border issues. For example, the article highlights the complexities of transactional data flow between third-world countries and how data is handled between the controllers, revealing the gap between the provisions of the DPD and enforcement in a global digital environment. In addition, most users had limited knowledge about where their data was being stored and how it was used (Smirnova & Travieso-Morales, 2025). When the GDPR came into effect, it reduced concerns through its strict requirements and strong security, and it replaced the legislation in its entirety, creating "a single, harmonised legal framework across the EU, raising the bar for how organisations manage personal data"

(Smirnova & Travieso-Morales, 2025). Additionally, it also has a few enforcement mechanisms such as fines, investigative powers, and lawsuits. These mechanisms were developed to establish a high standard of data protection and ensure that companies comply with these regulations.

The Application

The GDPR and its enforcement mechanisms are applied to every European company that collects and gathers data from its customers. Not only does this apply to just companies in Europe, but to companies in other countries that process personal data or sell goods and services to European Union residents (Wolford, n.d.). How this works for non-European Union companies is that they must comply with these three requirements, such as data minimization, legal basis, and implementation of security. According to Psomiadi (2025), data minimization requires data that is only collected and processed for specific uses. It is for the companies to ensure that only relevant data is gathered and stored to prevent excessive data collection. This also prevents the risk of data breaches. The processing of data also comes with legal bases, such as obtaining consent from the users and providing safeguards for vital interests (Psomiadi, 2025). These companies must document every legal basis and inform every user regarding their data. Lastly, security is highly essential for data protection, as it prevents unauthorized access from malicious actors. For non-European Union companies, they must implement security measures such as encryption, access controls, security assessments, and more (Psomiadi, 2025).

As for enforcement mechanisms, these are applied when companies fail to comply with the regulations. One enforcement mechanism is fines, which DPAs or Data Protection Authorities regulate. According to Bahr (2025), there are two severity levels of fines, such as 2% and 4% of the company's global turnover. The first level involves the company's violation of records or failure to notify data breaches, while the second level involves violation of users'

rights and unlawful data processing. These penalties can also include temporary or permanent bans, depending on the levels. Klar (2020) provides an example of how this was executed in U.S. companies. In the article, French DPAs issued a 50 million euro fine to Google for the lack of transparency and lawful processing violations. This reflects the second level of fines described by Bahr (2025) and demonstrates that non-European companies are also subject to GDPR enforcement just as European Union-based companies.

Another enforcement is investigative powers, such as the Data Protection Authorities (DPA) and Data Protection Officers (DPO). The DPA's role is to oversee compliance and enforcement in each European Union state. They have the power to investigate, restrict, and impose corrective measures (Bahr, 2025). As for DPOs, they are responsible for informing their clients and users of obligations under the data protection law (European Commission, n.d.). They also conduct audits, monitor the compliance of the organizations, and have awareness training for processing operations. Both powers are responsible for companies adhering to the GDPR requirements and protecting user data.

One other enforcement is lawsuits. Users have the right to sue if any company violates their GDPR rights. According to True Vault (n.d.), these legal lawsuits are based on three articles, such as articles 79, 80, and 82. In article 79, users have rights to a judicial remedy for the infringement of their rights. In article 80, users can mandate non-profit organizations to litigation on their behalf and file complaints with DPAs (True Vault, n.d). Lastly, in article 82, users can earn compensation for any infringement of both non-material and material damage. In all, these enforcement mechanisms enhance the effectiveness of the GDPR by ensuring that companies are held accountable for any misuse of data and giving users power over their data.

National & International Implementation

The GDPR and its enforcement serve as a role model in national and international cybersecurity policies by unifying data protection standards that extend beyond the European Union. This law encouraged and influenced other governments and global organizations to adopt similar and stronger data protection practices into their frameworks. In the U.S., numerous privacy laws have been passed in 29 states since the GDPR was adopted (Klein, 2023). A few states, such as California, Virginia, and Connecticut, have set and put their laws into effect from 2023 to this current year. As a result of this law, the U.S. has reconsidered its data-gathering processes and adopted stronger approaches to data privacy and cybersecurity policies.

In other countries, such as Indonesia, they have implemented this regulation into their privacy laws. Their law, called the Personal Data Protection (PDP) law, came into effect in October 2021 (Calais et al., 2023). This law has introduced a new authoritative matter over data protection and shifted how businesses, public institutions, and individuals operate in Indonesia. Similarly, with its investigative powers like the GDPR, the PDP has also implemented these powers with the PDP Authorities. They report any type of data collection to the president and oversee personal data. Overall, this highlights the impact of the GDPR in shaping national and international approaches to data privacy and cybersecurity policies.

Conclusion

The GDPR represents one of the most effective and influential data protection laws in modern cybersecurity policy. Through its strict rules, defined user rights, and enforcement mechanisms such as fines, investigative powers, and lawsuits, this regulation ensures that companies are held accountable for how they collect users' personal data. By replacing its

predecessor, the European Data Protection Directive, the GDPR has reduced the implications, such as national implementation, legal issues, and addressing cross-border issues that the Data Protection Directive failed to protect, by creating a unified legal framework across the European Union. This regulation also serves as a role model for national and international cybersecurity policies, encouraging other countries to adopt similar, stronger data privacy practices in their frameworks. In the end, this legislation meets new privacy challenges as digital advancements continue to develop.

References

Bu-Pasha, S. (2017). Cross-border issues under EU data protection law with regards to personal data protection. *Information & Communications Technology Law*, *26*(3), 213–228. https://doi.org/10.1080/13600834.2017.1330740

Calais, S., Ng, S., Thanachoksopon, P., & Kwok, S. (2023, May 24). *How has GDPR influenced the evolution of data protection in APAC?* Aoshearman.com; A&O Shearman. https://www.aoshearman.com/en/insights/how-has-gdpr-influenced-the-evolution-of-data-protection-in-apac

Epic.org. (n.d.). *EU Data Protection Directive*. EPIC - Electronic Privacy Information Center. Retrieved February 17, 2026, from https://epic.org/eu-data-protection-directive/

European Commission. (2023). *What are the responsibilities of a Data Protection Officer (DPO)?* European Commission. https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/obligations/data-protection-officers/what-are-responsibilities-data-protection-officer-dpo_en

European Data Protection Supervisor. (n.d.). *The History of the General Data Protection Regulation | European Data Protection Supervisor*. European Data Protection Supervisor. Retrieved February 15, 2026, from https://www.edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

Klar, Manuel. (2020). Binding effects of the european general data protection

regulation (gdpr) on u.s. companies. Hastings Science and Technology Law Journal, 11(2), 101-154.

Klein, J. (2023, May 17). *How the GDPR has shaped U.S. privacy regulation and cyber risk management | Lockton*. Lockton. https://global.lockton.com/us/en/news-insights/how-the-gdpr-has-shaped-u-s-privacy-regulation-and-cyber-risk-management

Li, H., Yu, L., & He, W. (2019). The impact of GDPR on global technology development. *Journal of Global Information Technology Management*, *22*(1), 1–6. https://doi.org/10.1080/1097198X.2019.1569186

Psomiadi, A. (2025, January 24). *How GDPR Applies to Non-EU Businesses*. Pandectes. https://pandectes.io/blog/how-gdpr-applies-to-non-eu-businesses/

Smirnova, Y., & Travieso-Morales , V. (2025, August 1). *Why is GDPR compliance still so difficult? - LSE Business Review*. LSE Business Review. https://blogs.lse.ac.uk/businessreview/2025/08/01/why-is-gdpr-compliance-still-so-difficult/

True Vault. (n.d.). *The GDPR's Private Right of Action*. True Vault. Retrieved February 15, 2026, from https://www.truevault.com/learn/gdpr-private-right-of-action

Wolford, B. (n.d.). *Does the GDPR apply to companies outside of the EU?* GDPR.eu. Retrieved February 15, 2026, from https://gdpr.eu/companies-outside-of-europe/