Proceedings of the 3rd International Conference on Management Research and Economic Development
DOI: 10.54254/2754-1169/178/2025.22770

Research on CSRD and the Protection of Enterprise Data Privacy Rights

Ziyue Huang

Institute of Civil Law, China University of Political Science and Law, Beijing, China
210201372@cupl.edu.cn

Abstract: This study explores the relationship and potential conflicts between the Corporate Sustainability Reporting Directive (CSRD) and data privacy protection. As a key EU regulation promoting corporate sustainability and transparency, the CSRD mandates extensive disclosure of environmental, social, and governance (ESG) information. Such disclosures create significant personal data protection challenges and may conflict with privacy regulations like the General Data Protection Regulation (GDPR). The requirement of detailed cybersecurity reports may expose technical vulnerabilities, thereby elevating data breach risks. The directive may lead to potential over-collection of data that violates the GDPR's principle of data minimization. Disclosing information about upstream and downstream supply chains may potentially infringe upon the personal information rights of both employees and end-users. Through comparative legal analysis, the study reveals how these regulatory tensions disproportionately impact high-risk sectors such as finance and digital platforms, where the common practice of centralized data storage significantly amplifies the potential consequences of security breaches. To comply with the directive while safeguarding data privacy, enterprises should integrate cybersecurity and data protection into their corporate social responsibility (CSR) framework and strengthen data security measures. Establishing cross-departmental collaboration mechanisms and comprehensive risk assessment systems is also essential to ensure compliance. This study provides theoretical support and practical guidance for enterprises to strike a balance between sustainability reporting requirements and data privacy protection.

Keywords: CSRD, sustainable reporting, data privacy protection, GDPR

1. Introduction

The Corporate Sustainability Reporting Directive (CSRD) is a regulation enacted by the European Union in 2022 and stands as one of the EU's core legislative measures in advancing green transition and sustainable development. The objective is to ensure that companies provide more detailed, transparent, and consistent information in the areas of environmental, social, and governance (ESG) performance. Against the backdrop of frequent human rights and environmental incidents in global supply chains, the previous Non-Financial Reporting Directive (NFRD) proved inadequate in coverage and allowed companies to voluntarily choose reporting standards and frameworks issued by international professional organizations, leading to insufficient comparability and reliability in corporate sustainability disclosures.

DOI: 10.54254/2754-1169/178/2025.22770

The CSRD replaces the non-financial reporting obligations under the NFRD and introduces a more detailed regulatory framework, mandating companies to prepare sustainability reports that include both backward-looking and forward-looking metrics based on financial and non-financial materiality [1]. The scope of the CSRD has been expanded to cover all large companies operating in the EU that meet specific thresholds in terms of employee numbers, turnover or assets including those not listed, EU-listed small and medium-sized enterprises, as well as large non-EU multinational corporations operating in the EU market. Notably, the CSRD for the first time requires non-EU companies operating in Europe to comply simultaneously, aiming to establish a "level playing field" for European businesses [2].

The CSRD elevates sustainability reporting to a level equivalent to financial reporting [3]. The directive emphasizes the principle of double materiality, requiring companies to disclose not only factors affecting their financial performance but also the impacts of their operations on the external environment and society. To ensure the comparability and consistency of disclosed information, companies are required to prepare their reports in strict compliance with the European Sustainability Reporting Standards (ESRS). Moreover, all sustainability reports must undergo independent third-party audits to enhance their reliability and credibility. Furthermore, the CSRD mandates that enterprises submit their reports in a machine-readable digital format and aggregate the information in the European Single Access Point (ESAP), significantly enhancing accessibility for both the public and investors.

Under the CSRD, sustainability reporting has a recent trend toward mandatory rather than voluntary reporting worldwide through the ESRS [4]. The directive mandates companies to disclose over 1,100 data points spanning all ESG dimensions, including sustainability risks throughout their value chains which simultaneously amplifies potential data infringement risks. While the current text of the CSRD has not made explicit provisions specifically addressing corporate data security, its implementation necessitates alignment with existing EU regulations such as the GDPR and ESRS. Notably, when data security and privacy protection constitute material impacts for either the company or its stakeholders, such matters should be incorporated into disclosures. If data security and privacy protection are material to the company or its stakeholders, they should be included in disclosures. This paper examines how companies can comply with the CSRD while adhering to data security and cybersecurity requirements under the GDPR, integrating compliance practices and risk management into sustainability or ESG disclosures.

2. Potential conflicts between the CSRD and data privacy protection

2.1. General principles of EU data protection

The EU primarily regulates corporate data protection through legislation such as the GDPR. Hailed as one of the strictest and most protective data privacy laws globally, the GDPR adopts a fundamental rights approach to personal data protection, providing clear rules for organizations and reducing regulatory fragmentation [5]. The GDPR changed the way companies tackle privacy protection and data security [6], applying only to data involving identifiable natural persons and excluding non-personal information. The regulation permits the disclosure of personal data in cases involving consumer protection, public safety, law enforcement, rights enforcement, cybersecurity, and fraud prevention. Article 32 of the GDPR outlines security requirements for data processing, allowing companies discretion in selecting measures but mandating risk assessments based on the nature, scope, context, and purpose of data processing, as well as the state of technology and implementation costs [7]. The GDPR does not prescribe specific security measures but provides a non-exhaustive list of minimum requirements. Overall, the GDPR offers flexible yet accountable rules for personal data protection, with national courts determining whether measures are adequate and imposing penalties

DOI: 10.54254/2754-1169/178/2025.22770

for misuse. While the GDPR benefits citizens and SMEs in principle, its high compliance costs have inadvertently favored established players, as smaller firms struggle to meet the requirements and may exit the market [8].

2.2. Conflicts between the CSRD and EU data privacy protection

The CSRD requires enterprises to disclose ESG-related data, including greenhouse gas emissions, labor rights, supply chain transparency, and anti-corruption measures. The requirement for a large amount of data disclosure may help improve transparency for businesses, but it may also conflict with data privacy protection.

2.2.1. Disclosing security measures may expose sensitive information

The development of the internet has created new opportunities for corporate growth and expansion. However, networks and information systems cannot fully guarantee the security of data and systems. Issues such as data breaches occur frequently, leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data that is transmitted, stored, or otherwise processed [9]. These incidents not only violate customer privacy rights but also negatively impact corporate performance. Prior to the implementation of the CSRD, disclosures regarding cybersecurity information were primarily voluntary [10]. The ESRS, as the specific technical standards under the CSRD, requires companies to assess and disclose risks associated with data collection, processing, and storage. They must also provide detailed descriptions of security measures implemented to prevent cybersecurity incidents such as data breaches and unauthorized access. While such disclosures demonstrate a company's capability to withstand cyberattacks and maintain operations and profitability, excessively detailed revelations of technical specifics or customer information may inadvertently expose system vulnerabilities and security weaknesses. This could provide opportunities for malicious actors such as hackers, thereby compromising consumer or user privacy. For instance, some companies may publicly disclose specific cases of personal data handling as evidence of compliance with privacy requirements, inadvertently creating privacy risks for users.

2.2.2. Excessive disclosure

Under the requirements of CSRD and ESRS S4, enterprises are compelled to collect large sets of data to meet the disclosure obligations. During data processing, if companies misinterpret or improperly execute these requirements, they may disclose excessive specific details about users' personal data. When processing user data, if the anonymization or de identification process is not rigorous, the processed data may still indirectly identify the user's identity through certain means, which may lead to the leakage of user profiles, location information, and other content. According to the data minimization principle and purpose limitation of the GDPR, companies should only collect necessary data. However, the mandatory disclosure requirements of the CSRD may force enterprises to collect excessive information, potentially resulting in over-collection or even unlawful data gathering during the collection phase. Some platforms or businesses, in pursuit of more accurate user profiling, may collect large amounts of user data unrelated to their operations, including sensitive information such as users' health status, home addresses or even credit card numbers. Disclosure of such information would severely compromise user privacy. Furthermore, the mandatory disclosure requirements may lead companies to centralize the storage of the massive data. For high-risk sectors like internet companies and financial institutions, falling victim to data attacks can lead to disproportionately severe breach consequences. In practice, a large number of companies have suffered data leaks due to internal mismanagement or systemic vulnerabilities.

DOI: 10.54254/2754-1169/178/2025.22770

2.2.3. Implementation of the "double materiality" principle

The predecessor of CSRD, the NFRD limited the scope of mandatory disclosure to the environmental and social impacts on communities where companies operate [11]. The CSRD widens the spectrum of risks companies must assess, mandating that companies conduct a double materiality assessment, requiring disclosures on both:

(1) Impact Materiality: How the company's operations affect the environment, society, and consumers (outside-in perspective);

(2) Financial Materiality: How sustainability-related risks and opportunities influence the company's financial performance (inside-out perspective).

Companies must consider not only impacts on themselves, but also the effects of their operations on the environment, society and throughout their supply chains. Firstly, to comply with CSRD requirements, companies must establish ESG systems to give an account of relevant supply chain information, including measures to reduce carbon emissions and achieve carbon neutrality, resource efficiency, impacts on biodiversity and ecosystems, and strategies for minimizing environmental impacts throughout the supply chain. Companies are also required to report information about working conditions and employee rights protection. Such data may involve personal information of employees, customers or other individuals. For example, when revealing labor rights data in supply chains, companies may need to provide basic employee information such as age, gender, working hours and so on. If not handled properly, such data processing activities could violate employee privacy rights. Additionally, disclosed supply chain data may contain customer-related sensitive data, particularly personal information collected during service provision, which could lead to privacy breaches without adequate protection.

Secondly, the CSRD's carbon emission disclosure requirements necessitate the inclusion of environmental performance across the entire supply chain. To collect the information, companies must share data with all supply chain participants, relying on data provided by upstream and downstream partners. Certain suppliers, primarily small and medium-sized enterprises, frequently fail to implement adequate data protection systems. As a result, data transmissions through these channels may create security vulnerabilities that could lead to breaches or unauthorized processing. The CSRD requires disclosure of water usage, pollutant emissions, energy consumption, and other environmental data. While these constitute environmental data, when combined with other information, they may reveal trade secrets or sensitive personal information. Furthermore, enterprises are required to evaluate and disclose how sustainability-related matters may impact their operations, financial performance, and future cash flows. For instance, environmental or social issues among suppliers, disruptions in raw material supply, and downstream consumer demands regarding product safety and sustainability could all directly affect a company's profitability and financial stability.

3. Data privacy compliance recommendations for EU enterprises under the CSRD framework

While the CSRD aims to enhance corporate transparency in sustainability, its mandatory disclosure requirements—particularly concerning supply chain and employee privacy data—raise significant data privacy concerns that cannot be overlooked. For EU companies, the strengthening of corporate social responsibility (CSR) regulations directly links disclosure obligations to sustainability performance, which in turn influences investor and consumer evaluations, ultimately affecting access to financial resources and long-term growth potential. Concurrently, compliance with the GDPR's stringent data protection framework remains equally critical. Thus, reconciling CSRD disclosure mandates with GDPR requirements presents a key compliance challenge for enterprises. In practice, however, achieving alignment between these two regulatory frameworks is demonstrably feasible.

DOI: 10.54254/2754-1169/178/2025.22770

3.1. Integrating data protection into Corporate Social Responsibility (CSR) frameworks

Undoubtedly, future markets will be sustainability-oriented. Given the relative stability of legislation and rapid technological advancement, not all corporate activities are ethical or beneficial to society and individuals [12]. Therefore, companies must treat data protection and cybersecurity as both assets and ethical imperatives. Since its implementation, the GDPR has faced significant compliance challenges, with less than half of companies fully adhering to the regulation due to high compliance costs and discretionary enforcement practices. Paradoxically, risks such as identity theft and cyber fraud have increased rather than decreased under this framework. This demonstrates that mere legal compliance cannot adequately protect fundamental rights or address risks from new technologies and economic models. Robust data protection and cybersecurity compliance have been proven to enhance ESG ratings. In fact, ESG rating agencies frequently incorporate cybersecurity and privacy into their "ESG scores" [13]. As operational entities, companies should not view data protection and cybersecurity merely as legal obligations but as opportunities to improve ESG ratings and corporate image. Thus, companies can adopt frameworks like UM-DPCSR, incorporating ethical principles into data disclosure practices and making data protection an integral part of CSR and ESG strategies [14].

3.2. Implementing specific, auditable technical and organizational controls

Companies should establish concrete technical controls internally to prevent data leaks and excessive disclosure. First, they must strengthen the implementation of data minimization, anonymization, and pseudonymization measures throughout all stages of data collection, processing, and storage. Effective risk-balancing mechanisms are needed to reconcile transparency requirements with data security. For instance, companies should implement systematic risk assessment processes to evaluate security and privacy risks during data processing, conduct dual materiality assessments, and establish continuous monitoring and internal review mechanisms to promptly identify and mitigate potential threats. Additionally, to comply with the CSRD's stringent data authenticity requirements, enterprises must implement control measures that accommodate third-party audit obligations. The measures should include conducting regular risk assessments and security audits to enhance both transparency and security in data processing activities. Special industries, particularly internet-based enterprises, must emphasize privacy protection measures during data sharing, collection, storage, and processing, adopting stricter technical measures to prevent leaks and misuse of personal data.

Moreover, companies should establish cross-departmental governance teams to ensure organization-wide implementation of data protection policies, with clear responsibility allocation and oversight mechanisms at the governance level [14]. These teams should specialize in preventing and monitoring cyberattacks, as well as responding to and managing incidents promptly. Through internal governance and continuous risk assessments, companies can ensure proper implementation of data protection measures, meeting legal requirements while preventing sensitive information leakage. The systematic approach helps prevent corporate infringement risks and reduces unnecessary financial losses from compensation obligations.

3.3. Employee training and supply chain risk management

Pursuant to ESRS S4 Appendix A, Article 1, companies shall disclose in their sustainability reports any material impacts that their operations may have on consumer and user privacy, including but not limited to scenarios involving large-scale data breaches. Following CSRD implementation, significant amendments were made to accounting directives regarding non-financial information disclosure. Article 29 requires large enterprises to expand reporting scope, disclosing not only parent company risks but also consolidated risk profiles of subsidiaries and entire groups. The provisions do not restrict subsidiaries by geographic location. Where the operations or risks of overseas subsidiaries

DOI: 10.54254/2754-1169/178/2025.22770

have a material impact on the group's overall financial performance and sustainability, such risks must also be included in the disclosure scope. Therefore, companies must strengthen internal training across their groups, enhancing all employees' data protection awareness through regular programs. It must be acknowledged that data misuse is inevitable during operations, necessitating a top-down organizational culture of data security supported by incentive and disciplinary measures. This initiative also helps build corporate image, increasing trust from regulators, investors, and consumers in companies' data processing practices.

4. Conclusion

The adverse effects of cybersecurity incidents have brought increasing attention to data privacy rights. This paper first reviewed CSRD's background and its crucial role in enhancing corporate ESG disclosure transparency, noting that CSRD requires disclosure of extensive financial and non-financial data based on the double materiality principle while significantly expanding disclosure scope to include upstream and downstream supply chain information. The paper examined data privacy risks introduced by CSRD, particularly how excessive information disclosure may lead to sensitive data leaks, cybersecurity vulnerabilities, and improper data governance. Research indicates that while CSRD implementation helps improve overall corporate transparency and sustainable development, its mandatory requirements also pose severe challenges to data security and privacy protection. Moving forward, while enhancing ESG disclosure transparency, companies must pursue technological innovation, leveraging big data, AI, and other advanced technologies to strengthen data encryption, anonymization, and real-time risk monitoring, thereby elevating overall data security. Companies should also establish comprehensive data security management frameworks, enhance cross-departmental collaboration and employee training, and foster a top-down security culture to effectively manage data risks while fulfilling ESG reporting requirements.

References

[1] *Directive (EU) 2022/2464 of the European Parliament and of the Council of 14 December 2022 amending Regulation (EU) No 537/2014, Directive 2004/109/EC, Directive 2006/43/EC and Directive 2013/34/EU, as regards corporate sustainability reporting. Official Journal of the European Union, L 322, 16.12.2022, 15–80.*

[2] *European Commission (2021b) Title of Document. Publication Office of the European Union, p.11.*

[3] *Lámfalusi, I., Hámori, J., Rózsa, A., Hegyi, J., Kacz, K., Miklósné Varga, A.,Gombkötő, N. (2024). Evaluation of sustainability reporting of the food industry in Hungary from an EU taxonomy perspective. Quality & Quantity, 58(5), 4479-4504.*

[4] *Hummel, K., and Jobst, D. (2024). An overview of corporate sustainability reporting legislation in the European Union. Accounting in Europe, 21(3), 320-355.*

[5] *European Commission. Protection of your personal data.Retrieved from https://europa.eu/info/law/law-topic/data-protection-eu_en.2025-04-05.*

[6] *Sirur, S., Nurse, J. R., and Webb, H. (2018). Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR). Proceedings of the 2nd international workshop on multimedia privacy and security, 88-95.*

[7] *Porcedda, M. G. (2023). Cybersecurity, Privacy and Data Protection in EU Law, 1-352.*

[8] *Layton, R. and Elaluf-Calderwood, S. (2019) A social economic analysis of the impact of GDPR on security and privacy practices. 2019 12th CMI Conference on Cybersecurity and Privacy (CMI), 1-6.*

[9] *GDPR, Article 4(12).*

[10] *Eijkelenboom, E. V. A., Nieuwesteeg, B. F. H. (2021). An analysis of cybersecurity in Dutch annual reports of listed companies. Computer Law & Security Review, 40, 105513.*

[11] *Arena, C., Catuogno, S., Lamboglia, R., Silvestri, A., Veltri, S. (2022). The disclosure of non-financial risk. The emerging of cyber-risk. Non-financial Disclosure and Integrated Reporting, 29-60.*

[12] *Baldini, D.,Francis, K. (2024) AI Regulatory Sandboxes between the AI Act and the GDPR: the role of Data Protection as a Corporate Social Responsibility. CEUR Workshop Proceedings, 3731.*

[13] *Balboni, P.,Francis, K. E. (2024). Data ethics and digital sustainability: Bridging legal data protection compliance and ESG for a responsible data-driven future. Journal of Responsible Technology, 100099.*

DOI: 10.54254/2754-1169/178/2025.22770

[14] Balboni, P.,Francis, K. (2023). Data protection as a corporate social responsibility. Edward Elgar Publishing.