THE GENERAL DATA PROTECTION REGULATION BETWEEN NORMATIVE EVOLUTION AND DATA GOVERNANCE MANAGEMENT

Claudia Pau *, Mihaela Martin, Alina Stancovici

Babeș-Bolyai University, UBB Center from Reșița, Faculty of Political, Administrative and Communication Sciences
Traian Vuia Square, no. 1-4, Reșița, Caraș-Severin, România
* Corresponding author. E-mail: claudia.pau@ubbcluj.ro

Abstract. The General Data Protection Regulation (GDPR) represents the central pillar of European data governance, instituting the transition from a formal–procedural compliance approach to a model based on accountability, transparency and continuous risk assessment. Its evolution reflects a progressive normative consolidation at the level of the European Union, yet the published literature highlights the persistence of notable differences in effective implementation, generated by uneven organizational capacity and divergent maturity levels of managerial practices. The relevance of the GDPR becomes particularly evident in the domain of data protection incidents, where the convergence between the legal dimension and the managerial one is most visible. In this sense, the value of the GDPR is not conferred solely by its normative texture, but by the internalization of data protection as an anticipatory strategic function, embedded within organizational processes of detection, reporting and remediation. Thus, incident management represents the operational indicator of GDPR maturity in practice.
Keywords: digital governance, incident management, information risk, transparency, organizational resilience.

1. Introduction

Data protection management in the logic of the GDPR represents a continuous process of internal governance that transforms organizations from mere collectors of personal data into responsible actors, required to demonstrate at any moment that they comply with the principles of protection, security and ethical processing of personal data. The GDPR shifts responsibility from the state (the supervisory authority) to the controller, in the sense that it is no longer the authority that "authorises" processing, but the controller that designs the internal protection system, while the supervisory authority merely verifies ex post. The contribution of this article consists in conceptualising incident management as an operational indicator of GDPR implementation maturity, through the triangulation of the normative framework, post-2018 scientific literature and comparative data concerning incident notifications. The recent body of literature on this topic has been advanced, inter alia, by Finck [7], Voigt & von dem Bussche [8], Kloza et al. [9], Mildebrandt [10] and Kaminski & Malgieri [11].

The protection of personal data has become a constitutive dimension of the European digital ecosystem, and the General Data Protection Regulation (GDPR) represents the central normative instrument through which the European Union has attempted to respond to these transformations. Adopted in 2016 and applicable since 2018, the GDPR has redefined the architecture of data governance by shifting from a static, procedural compliance model to a dynamic one focused on accountability, transparency, risk analysis and internal audit. At the same time, recent doctrinal observations indicate that, with the acceleration of digitalization, the legal regime is inseparable from the organizational capacity to manage complex data flows, automated processes and distributed processing systems, including in cross-border contexts [1]. In this logic, the data protection incident becomes an empirical test of GDPR maturity: not only from the perspective of legal notification obligations, but from the perspective of the actual production of managerial capacity (detection, response, remediation). For this reason, the current literature insists on integrating incident management into organizational culture and on institutionalizing data protection as a continuous function — not as a post-factum corrective measure [2].

Subsequently, against the background of the increasing volume of security incident notifications, the literature has advanced towards an approach based on organizational maturity and internal capabilities, arguing that the GDPR cannot be interpreted exclusively as a legal framework, but as a normative–managerial framework in which processing is embedded within complex operational architectures [5]. In parallel, European research derived from EDPB, ENISA and CJEU reports has consolidated a direction in which the data protection incident is used as a "proxy indicator" for assessing real-world implementation: where

institutionalized instruments for detection, reporting and remediation exist, the protection function is effectively internalized [6]. Through this repositioning, the GDPR becomes an instrument of institutional governance rather than a mere regulatory norm, which requires analysis to be situated at a systemic level, not merely at a procedural one.

The current trend in European literature is therefore one of transition towards anticipatory governance models, in which data protection is analyzed in correlation with organizational resilience, dynamic compliance processes and the integration of risk analysis as a strategic — rather than procedural — mechanism of data management. Consequently, the risk dimension does not represent a static category, but a dynamic organizational construction dependent on the technological environment, system architecture, data volumes and the nature of processing. From this perspective, the GDPR becomes a governance instrument that internalizes data protection into organizational strategic design rather than treating it as a mere administrative checklist exercise.

2. Methodological Approach

The methodological approach adopted in this study is analytical documentary in nature, grounded in the triangulation of the published literature with normative analysis and the secondary examination of publicly available empirical data concerning notified data protection incidents in EU Member States. In the epistemic logic of applied legal research, the methodology does not seek statistical exhaustiveness, but rather the operationalization of relevant juridical-managerial concepts for assessing the maturity of GDPR implementation in practice.

The selection of sources was carried out according to criteria of thematic relevance, currency and academic validity, with a particular emphasis on peer-reviewed scientific journals and official documents issued by European institutions. The analysis was guided by the central research question: to what extent can incident management be used as an organizational maturity indicator for GDPR implementation? Through this approach, the study enables the articulation of a coherent interpretation of the evolution of the normative framework and the performativity of internal organizational mechanisms, without transferring conclusions into the domain of statistical causality but maintaining anchoring in the conceptual–operational evaluation paradigm. This selection is supported by the European literature that treats the GDPR as a managerial rather than exclusively legal framework, especially in the area of accountability, impact assessments and risk governance, as highlighted in recent studies published in indexed journals [7], [8], [9], [10], [11].

3. Strategic, Anticipatory, and Risk-Based Approach

In the context of the accelerating process of digitalization at global level, the protection of personal data has become one of the most prominent themes of contemporary societal debate. Whether it concerns the use of social networks, interactions with public institutions or online commercial relations, individuals are constantly required to provide personal data, sometimes without clearly understanding how such data are collected, processed and protected. In this context, ensuring confidentiality, security and integrity of personal data is no longer merely a technical or legal concern, but becomes a fundamental component of human rights in the digital era [7].

The European Union identified early the need for an appropriate legislative framework for data protection, acting in the direction of coherent and harmonized regulation adapted to new technological realities. Thus, in 2016, Regulation (EU) 2016/679 of the European Parliament and of the Council — known as the General Data Protection Regulation (GDPR) was adopted. This normative act, applicable since May 2018 in all Member States, represented a fundamental step in strengthening the right to personal data protection and established clear and strict rules for both data controllers and national supervisory authorities [3].

The strategic, anticipatory and risk-based approach represents the dimension through which data protection shifts from an exclusively normative register to a functional instrument of organizational governance. Recent literature emphasizes that GDPR implementation maturity is not visible in the mere presence of formal procedures, but in the capacity of organizations to anticipate incidents, to design early-detection mechanisms and to internalize risk assessment as a cyclical process rather than as a singular administrative act. In this sense, the role of Data Protection Impact Assessments (DPIA) becomes central, as they integrate data protection already at the stage of operational design, not only ex-post at the stage of compliance. In this paradigm, risk does not represent a static category, but a dynamic organizational construction, dependent on the technological environment, system architecture, data volumes and the nature of processing. Consequently, data protection becomes part of integrated information governance, which includes mechanisms of continuous monitoring, internal audit, decision documentation and scalable response capacity. The anticipatory approach creates a logic in which the incident is not merely a disruptive event, but a systemic feedback indicator that enables the recalibration of internal processes, the optimization of controls and the updating of protection measures. As a result, risk analysis becomes the nodal element through which the transition is made from minimalist compliance to substantive protection oriented towards

organizational resilience. The main purpose of the GDPR is to guarantee individuals real control over the collection and use of their personal data, while at the same time encouraging the accountability of the organizations that process them. It establishes a series of extended rights for data subjects, such as the right of access, rectification, erasure, portability and objection, and sets concrete obligations for controllers, including the obligation to notify security breaches, to conduct impact assessments and to designate a Data Protection Officer.

Nevertheless, the implementation of the GDPR is not free from challenges. One of the most significant difficulties lies in the disparity between organizations in terms of resources, technical expertise, organizational culture, the internal maturity of risk management procedures and the capacity to operationalize accountability in practice. Although the regulatory framework is unified at the EU level, the organizational reality is heterogeneous, and discrepancies persist not only between Member States, but also between organizations within the same country, depending on sector, size, education, personal experience and professional context.

4. Legislative Developments

4.1. Recent European-Level Evolutions

Regulation (EU) 2023/2854 – Data Act was adopted on 13 December 2023 by the European Parliament and the Council and represents a key component of the EU's digital regulatory architecture. The Data Act expands the structural logic of data governance beyond personal data alone, consolidating rules on access, sharing and control over data generated in various economic and social contexts. From the perspective of GDPR relevance, the Data Act reinforces the requirement for organizations to develop coherent internal data governance mechanisms capable of ensuring that the processing of personal data remains aligned with the principles of accountability, transparency and risk-based management. It thus complements the GDPR by imposing strategic requirements on the capacity of organizations to operate data protection and to manage associated risks.

Other related initiatives include guidelines on the use of artificial intelligence systems in the context of data protection, such as those issued by the European Commission for the implementation of the Artificial Intelligence Act. Thus, the European framework is evolving towards a stronger synergy between data protection, data governance and the digital economy: regulations no longer concern only consent or transparency, but also data access, interoperability, data sharing between entities, and accountability for automated instruments.

4.2. Romania-Specific Developments

In Romania, the GDPR application framework has continued to be complemented through repeated sanctioning decisions issued by the National Supervisory Authority for Personal Data Processing (ANSPDCP). Specialised websites have recorded a constant flow of sanctions for violations of the GDPR or related legislation.

Furthermore, Romania is actively engaged in adopting new legislative initiatives, for example, a draft law (PL-x no. 385/2025) aiming at protecting minors under the age of 18 from harmful online content (the European Commission has issued warnings concerning delays in meeting the implementation deadline).

In addition, the active monitoring of incidents and notifications by the ANSPDCP indicates increasing pressure on organizations to institute internal incident management processes. Even if no radical legislative amendments specific to the GDPR have yet been adopted, the regulatory landscape is becoming increasingly dynamic.

It is also important to note that Law no. 190/2018 for the implementation of the GDPR continues to represent the national legislative basis and remains subject to interpretation and practical decisions.

4.3. Implications for Incident Management and Data Governance

The introduction of the Data Act at European level implies that organizations within the EU, including Romania, must integrate not only GDPR compliance procedures, but also mechanisms that cover: data sharing, cross-border interoperability, and risk assessment concerning the use of data generated by connected products/services.

In Romania, the increasing pressure exerted by the supervisory authority regarding sanctions suggests that incident management is becoming a key operational element: entities that cannot demonstrate adequate procedures for response, notification and remediation risk higher sanctions and reputational loss.

Consequently, legislative developments create an extended framework of accountability, in which compliance alone is no longer sufficient, proactive governance, continuous risk assessment, internal audit and rapid reaction capacity in case of incidents being required. This methodological structure does not aim at statistical exhaustiveness, but at the operationalization of GDPR governance mechanisms. Therefore, the results should not be interpreted in a causal sense, but as a conceptual–operational assessment of implementation maturity.

5. Challenges and Limitations

Despite the consolidation of the European normative framework, GDPR implementation faces a series of structural challenges and systemic limitations that influence the performance of data protection in practice. First, the literature highlights the persistence of an institutional capacity deficit, particularly in small and medium-sized organizations, where dedicated human resources and technical expertise are insufficient. For example, in the annual EDPB reports it has been observed that a significant number of controllers submit notifications late or incorrectly, not out of bad faith, but due to their inability to understand legal notification thresholds and impact assessment criteria.

Secondly, the heterogeneity of interpretations at Member State level, visible in divergent sanctions for comparable situations (e.g., differences between decisions in Germany, Ireland and France regarding cookie-based tracking), introduces a degree of legal uncertainty. Two organizations using similar profiling mechanisms may receive significantly different sanctions depending on jurisdiction, which partially contradicts the objective of harmonization.

From a technological perspective, the emergence of generative models and machine learning systems trained on massive datasets creates additional challenges regarding traceability and explainability, as not all AI architecture allow granular mapping of personal data flows. In practice, many organizations continue to operate under a "checkbox compliance" logic, maintaining formal documentation, but without integrating continuous risk auditing into the operational cycle. This structural dissonance largely explains why security incidents remain under-reported or treated exclusively as isolated episodes, without systemic feedback value.

6. Analysis of Implementation and Challenges Encountered in Two Member States

The application of the GDPR exhibits significant differences between Member States, generated not only by local market particularities, but also by institutional architecture and by the economic role assigned to data protection. In Ireland, where most European headquarters of large digital platforms are established (Meta, Google, TikTok, Apple), the national supervisory authority (Data Protection Commission – DPC) has become a central actor in GDPR enforcement. However, the literature reveals structural difficulties: the complexity of cross-border procedures, disproportionate institutional workload, and lengthy investigation timelines. For example, major cases concerning profiling practices or cookie-based tracking have recorded analysis periods exceeding two years, which has led to the perception that the high degree of technological sophistication of controllers exceeds the supervisory authority's capacity to deliver rapid procedural response.

The graphical visualisations used in the analytical section are intended to represent structural evolutions and functional differences and are integrated as interpretative support rather than as exhaustive statistical datasets.

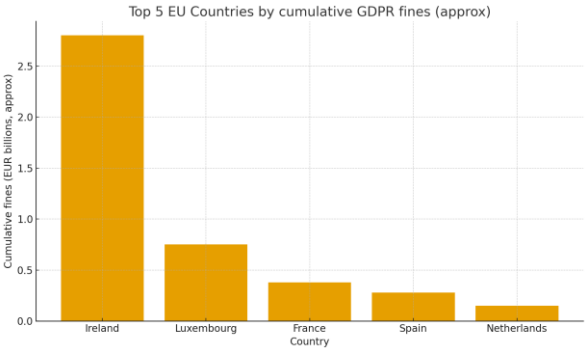

Fig. 1. Analytical operationalization of incident data Top 5 EU countries by estimated cumulative GDPR fines - *Note: values reflect estimated cumulative enforcement levels consolidated at EU level; comparative purpose only. Source: own elaboration based on EDPB Annual Reports (2020–2023) and ENISA Overview Reports.*

This chart highlights the structural concentration of GDPR fines in a few key jurisdictions, particularly Ireland. The central argument is systemic rather than incidental: Ireland hosts the European headquarters of major global platforms (Meta, Google, TikTok, Apple), which means that most globally relevant cases are processed by the Irish authority (DPC). In contrast, Luxembourg and France appear in the top for different reasons: Luxembourg due to its financial–digital corporate ecosystem, and France due to the activity of the CNIL, one of the most assertive authorities in the EU. Therefore, the chart demonstrates that the distribution of fines reflects the economic geography of digital platforms, not strictly normative differences.

In Romania, the challenges are of a different nature. The National Supervisory Authority (ANSPDCP) does not handle the litigation of global platforms, but faces challenges associated with the low level of organizational maturity: numerous entities report incidents late, there is confusion regarding notification thresholds, and internal audit mechanisms are rarely institutionalized. Moreover, many organizations adopt a reactive compliance model, in which GDPR documentation is produced formally through legal outsourcing, without the operational integration of risk management.

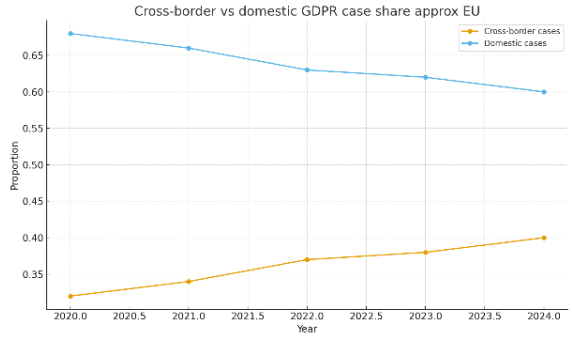

Fig. 2. Share of cross-border vs. domestic GDPR cases in the EU (comparative trend representation) *Note: classification based on case typology; indicative functional segmentation. Source: own elaboration based on cross-border case typology reported by EDPB Annual Reports (2020–2024).*

The chart illustrates the percentage evolution of GDPR cases at European level, distinguishing between: domestic cases (processed entirely within a single Member State) cross-border cases (involving multiple Member States or controllers established in one Member State and users in others). The trend highlighted is structural and highly relevant for assessing GDPR maturity:

- the share of domestic cases gradually decreases from ~0.68 in 2020 towards ~0.60 in 2024, meaning that national authorities are proportionally handling fewer "purely national" cases.
- the share of cross-border cases increases steadily from ~0.32 in 2020 to ~0.40 in 2024, indicating that data processing is becoming increasingly transnational

This chart shows that as the digital economy becomes platform-centric, incidents and complaints are no longer local phenomena, but systemic phenomena, structurally connected to multinational business models.

This also explains why Ireland is the "node" of European enforcement (because Big Tech headquarters are located there), why there is institutional pressure for a GDPR Procedural Regulation, and why incident investigation is slower in "hub" jurisdictions.

The chart demonstrates the transformation of the GDPR from a national administrative regime into a real European coordination mechanism, in which the data protection incident becomes cross-border by the nature of the digital ecosystem, and not by exception.

Therefore, the Ireland–Romania contrast demonstrates that GDPR enforcement challenges are not uniform: in "high-tech" jurisdictions the major challenge is volume and complexity (overload), while in states with emerging institutional infrastructures the primary barrier remains the absence of strategic integration.

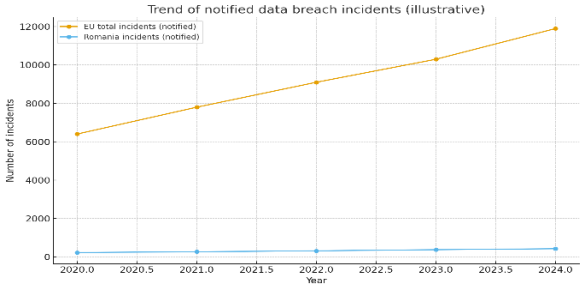

Fig. 3. Trend of notified data breach incidents in the EU and Romania (illustrative trend representation) *Note: representation aims to reflect directional evolution, not statistical exhaustiveness. Source: own elaboration based on ANSPDCP public reporting (Romania) and EU-level aggregate trends (EDPB).*

The chart illustrates the evolution of personal data breach incident notifications over the period 2020–2024, comparing the EU aggregate level with the situation in Romania. The constant upward trend at European Union level (from ~6,400 incidents in 2020 to almost ~12,000 in 2024) confirms the central observation from recent European literature: digitalization and the densification of data flows generate a continuous increase in operational risk and greater visibility of reported incidents. This increase reflects not only the intensification of risks, but also the consolidation of reporting mechanisms.

In Romania, the trend is likewise upward, but at significantly lower values (~250–450 annually). The difference should not be interpreted exclusively as a lower risk, but as an indicator of lower organizational maturity and capacity limitations on the part of controllers in documenting and reporting incidents. Thus, lower reporting may represent an effect of under-reporting, not superior security.

Therefore, the chart supports two relevant conclusions:

• at European level, the GDPR becomes more "visible" in practice through the annual increase in notifications.

• in Romania, the problem is not the absence of incidents, but the variable level of internal detection, assessment and reporting mechanisms, which remain insufficiently consolidated.

This indicator reinforces the argument that incident management is a robust proxy of GDPR implementation maturity.

7. Conclusions

The future trajectory of the GDPR is strongly associated with its evolution from a compliance-centered legal instrument into a proactive governance framework integrated into organizational risk management. Given the structural rise of cross-border processing, platform-based data ecosystems and AI-

enabled automated decision-making, the regulation is likely to evolve procedurally rather than conceptually: we can expect the forthcoming GDPR Procedural Regulation to act as a harmonization amplifier, particularly in cross-border enforcement coordination, case timelines and evidentiary standards. In parallel, sector-specific regimes (e.g. EHDS for health data, Data Act for industrial/mixed data, and the AI Act for high-risk systems) will progressively complement GDPR and drive it towards a more interoperable multi-regulation model. Consequently, GDPR's future will be less about refining principles, and more about operational integration, procedural acceleration and risk-based enforcement maturity.

8. Recommendations

To institutionalize continuous risk assessment, the DPIA must evolve from a static document into a periodic evaluative cycle, one that aligns with business changes, emerging data flows, and system updates.

To strengthen incident intelligence, breach notifications should be leveraged analytically, not just treated as administrative formalities. Each incident must inform and refine governance design, rather than serving solely as a trigger for sanctions.

Mandatory organizational learning loops should be enforced by regulators, requiring demonstrable evidence of post-incident remediation maturity (not only evidence of notification).

Cross-regulation alignment requires organizations to integrate the GDPR with the Data Act, EHDS, and AI Act, moving beyond the outdated "single-regulation silo" approach.

Support for SMEs by simplifying procedural templates and shared compliance infrastructures. These could help reduce the asymmetry between large platforms and smaller national operators. Future research directions could empirically assess whether the volume of incident notifications correlates with the density of internal risk management processes, rather than merely with the market's level of digitalization.

All things considered, the future of GDPR will not depend primarily on additional rules, but on the capacity of organizations to integrate data protection into strategic governance and continuous operational resilience.

9. References

[1] European Data Protection Board: "Annual Report 2023", EDPB Publications Office -used as basis for trend representation, 2024.

[2] ENISA: Data breach notifications in the EU: Overview Report. European Union Agency for Cybersecurity - used as basis for trend representation, 2023.

[3] Court of Justice of the European Union: "Key GDPR jurisprudence" – Case Law Digest, 2022.

[4] European Commission, "GDPR Procedural Regulation Proposal – COM", 728 final, 2023.

[5] European Commission: "Data Act – Regulation (EU) 2023/2854 Summary Note", 2024.

[6] European Commission, "European Health Data Space Regulation – Official Journal", 2025.

[7] Finck M.: "GDPR and the Internet of Things: A New Regulatory Model for Data Protection?" Computer Law & Security Review, 2020.

[8] Voigt P., von dem Bussche, A.: "The Concept of Accountability under the GDPR". International Data Privacy Law, 2018.

[9] Kloza D. et al.: "Data Protection Impact Assessments: Features, Roles and Management Expectations under GDPR", Computer Law & Security Review, 2021.

[10] Mildebrandt M.: "Data protection as a risk governance tool in the European Digital Ecosystem", Law, Innovation & Technology, 2022.

[11] Kaminski M.E., Malgieri G. :"Algorithmic Impact Assessments under EU Data Protection: From Principle to Practice. Yale Journal on Regulation", 2020.