Volume **14** / **2026** ISSN 2344-102X
Issue **2** ISSN-L 2344-102X

FROM CORRECTIVE ORDER TO DOCUMENTED CLOSURE: PUBLIC EVIDENCE FROM ROMANIAN GDPR ENFORCEMENT AND IMPLICATIONS FOR NIS2

Ion BURLUI
Ștefan cel Mare University of Suceava, 720229, Romania
ionburlui@yahoo.com
Ionel BOSTAN
Ștefan cel Mare University of Suceava, 720229, Romania
ionel_bostan@yahoo.com
ORCID: 0000-0002-7653-7192

Abstract
Corrective measures imposed after GDPR infringements or cybersecurity incidents have limited practical value unless their implementation is documented and subsequently verified. To analyse this, we studied the most important European and Romanian laws, public reports and press releases of the competent authorities, as well as other relevant documentation and sources. We conclude that aggregate reporting of post-deadline compliance checks and repeated findings would facilitate the assessment of the effectiveness of subsequent administrative actions.

Keywords: GDPR; NIS2; Romania; ANSPDCP; DNSC; corrective measures; post-deadline verification

JEL Classification: *H83; D73; L86; O33*

Received on*:* April 21, 2026 **Accepted on:** July 21, 2026 **Published on:** July 23, 2026

INTRODUCTION

We begin with a 2022 ANSPDCP notice concerning a bank document sent via WhatsApp to the wrong recipient. The authority required the controller to restrict the use of personal devices and unauthorised messaging services and to train its staff. Another notice, issued after a publisher's customer database became publicly accessible and was followed by a ransomware incident, required changes to security measures and internal procedures. In 2025, a further notice concerning V-RO required periodic testing and evaluation of technical and procedural controls (ANSPDCP, 2022a, 2022b, 2025b). We observe that the three notices describe the changes that had to be made but do not report the results of subsequent checks. Sanctioning and implementation are distinct stages. Although the decision may target the legal representative, compliance often depends on technical staff, contractors, procurement, and available funding (Voss & Bouthinon-Dumas, 2021; Zaguir et al., 2024). Romanian cybersecurity legislation has changed rapidly, with Law No. 362/2018 belonging to the former NIS1 regime. Government Emergency Ordinance No. 155/2024, approved with amendments by Law No. 124/2025, now constitutes the main national NIS2 framework. DNSC Orders Nos. 1 and 3/2025 regulate registration and subsequent supervision, verification, and control activities, while Law No. 123/2026 introduced a consultation requirement and a cause excluding criminality where the statutory conditions for vulnerability research and reporting are cumulatively met (Romanian Government, 2024; Romanian Parliament, 2018b, 2025, 2026; DNSC, 2025c, 2025d). We therefore examined a narrow component of implementation: the transition from an official finding to the organisational action it requires. The analysis was guided by two questions. What do Romanian sources say about the actor responsible for remediation? What do they reveal about verification of the measure after the deadline? Importantly, the article does not construct a national maturity score or compare Romania with other Member States.

I. METHODOLOGY AND SOURCES

The documentary research was initially conducted during the first half of 2026 and the legal framework was last verified on 6 July 2026. Annual reports, implementing orders, and case notices were obtained from ANSPDCP (2022a, 2022b, 2023, 2024, 2025a, 2025b) and DNSC (2025a, 2025b, 2025c, 2025d);; ENISA, the European Commission (2020), the OECD, and relevant academic studies provided context. Figure 1 outlines the

DOI: 10.4316/EJAFB. 2026.14204

Volume **14** / **2026** ISSN 2344-102X
Issue **2** ISSN-L 2344-102X

procedure. For the three selected notices, ANSPDCP public notices and annual reports available up to the same date were searched for later documents reporting verification, closure, or recurrence.

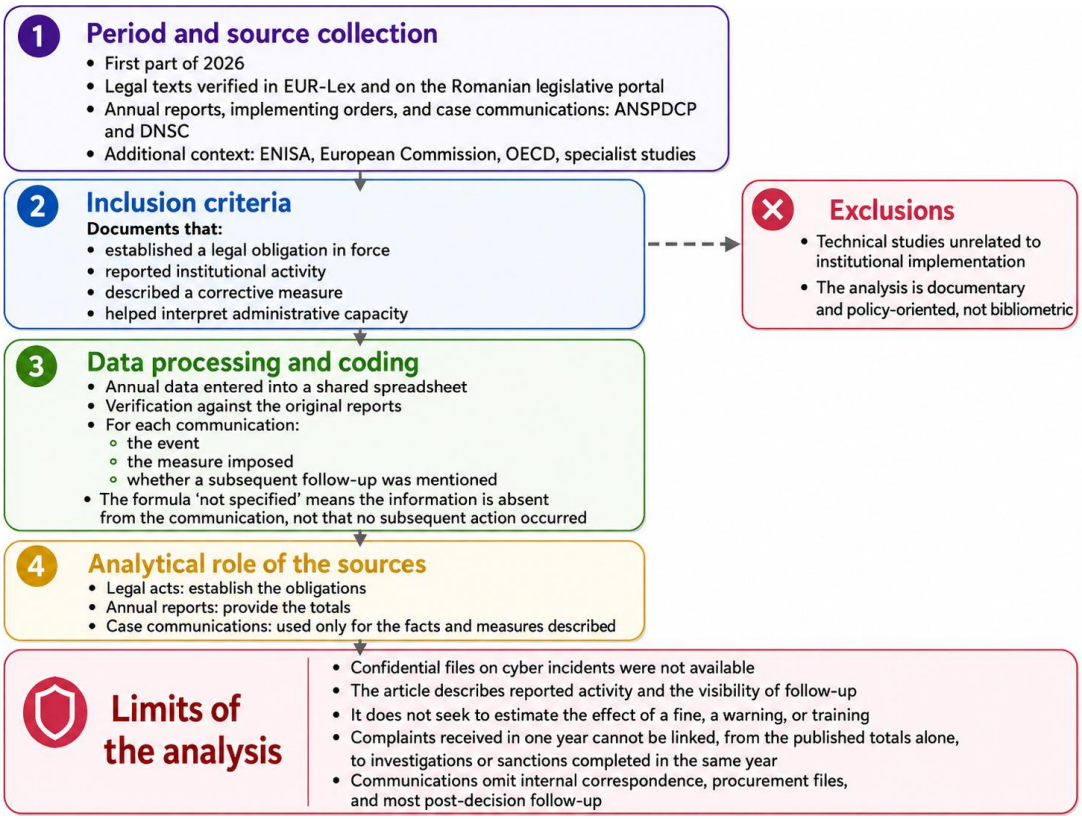

Figure 1. Documentary analysis workflow Source: Authors' own elaboration based on the reviewed literature.

Confidential cybersecurity incident files were unavailable. We therefore describe reported activity and the visibility of follow-up rather than estimating the effect of a particular fine, reprimand, or training measure. Further information limitations arise because complaints received in one year cannot be matched, from the published totals, to investigations or sanctions completed in the same year. Moreover, all notices omit internal correspondence, procurement files, and most post-decision control activities.

II. LEGAL AND INSTITUTIONAL FRAMEWORK

3.1. GDPR supervision and organisational remediation

The GDPR requires controllers to show that safeguards work in practice (Voigt & von dem Bussche, 2017). In Romania, Law No. 190/2018 and ANSPDCP's Article 58 powers translate this duty into concrete measures such as staff guidance, access controls, recovery procedures, and testing, consistent with CJEU case law emphasising effective protection and active supervision (European Parliament and Council, 2016; Romanian Parliament, 2018a; Court of Justice of the European Union, 2014, 2020).

3.2. NIS2 rules currently in force

At EU level, Directive (EU) 2022/2555 (NIS2) establishes measures for a high common level of cybersecurity across the Union and provides the legal basis for the national framework examined below (European Parliament and Council, 2022). The national framework examined here includes the applicable laws and certain orders issued by the heads of the institutions involved. For every regulated entity, these instruments determine whether it falls within the scope and must submit registration data, identify the management personnel who bear responsibility, review risk-management measures, and ensure incident reporting. The DNSC NIS2 legislation portal was consulted to identify and cross-check the national legal and administrative instruments applicable to the cybersecurity component of the study (DNSC, 2025b). The current framework therefore extends beyond Law No. 362/2018 and the original version of Government Emergency Ordinance No. 155/2024. In Romania, Law No.

DOI: 10.4316/EJAFB. 2026.14204

Volume **14** / **2026** ISSN 2344-102X
Issue **2** ISSN-L 2344-102X

362/2018 transposed the first NIS Directive, whereas Government Emergency Ordinance No. 155/2024 replaced that framework for the national civilian cyberspace and was approved with amendments by Law No. 124/2025. DNSC Order No. 1/2025 then introduced registration notification requirements, while Order No. 3/2025 established the rules on supervision, verification, and control and the risk-based prioritisation methodology. More recently, Law No. 123/2026 introduced paragraph (1¹) into Article 36 and Article 365¹ into the Criminal Code (Romanian Government, 2024; Romanian Parliament, 2018b, 2025, 2026; DNSC, 2025c, 2025d). The supervision rules adopted in December 2025 specify how DNSC may verify these mechanisms.

3.3. Who implements a corrective measure

Corrective measures usually require coordination among the data protection officer, IT staff, contractors, procurement, and management, with additional authorities involved when essential services are affected (Romanian Government, 2021; OECD, 2023). Effective implementation depends on assigning the finding to those with the technical, contractual, and financial authority to act and document compliance. Figure 2 summarises the operational sequence from the identification of a finding to the assignment of responsibility, preparation of the remedial plan, submission of evidence, post-deadline verification, and subsequent closure or reopening of the measure.

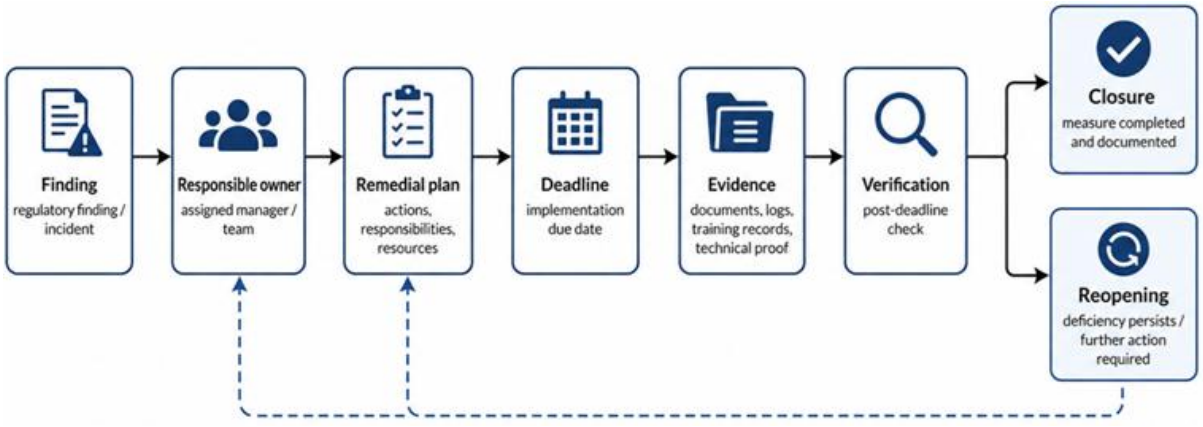

Figure 2. Corrective-measure follow-up workflow from finding to closure or reopening. Source: Authors' own elaboration.

Corrective measures generate lasting effects only when responsibilities are assigned, deadlines are monitored, implementation evidence is documented, and compliance is subsequently verified. Effective compliance depends on clear rules, assigned responsibilities, adequate resources, reliable information systems, and proper documentation from initiation to closure.

III. EVIDENCE ON IMPLEMENTATION IN ROMANIA

4.1. What the annual reports record

The ANSPDCP reports cover distinct activities rather than a single enforcement process. The combined annual number of complaints, referrals and personal-data-breach notifications increased from 4,260 in 2022 to 5,354 in 2024, while investigations declined and corrective measures peaked in 2024. Table 1 presents the published figures separately, without combining them into a performance index.

Table 1. ANSPDCP activity reported for 2022–2024.

ANSPDCP indicator	2022	2023	2024
Complaints, referrals and personal data breach notifications	4,260	4,772	5,354
Investigations reported	629	548	476
Fines imposed	69	73	83
Total value of fines	RON 1,058,863	RON 2,348,265	RON 1,855,907
Reprimands	134	186	161
Corrective measures	93	138	180
Requests for interpretative opinions	948	970	882
Opinions on draft legal acts	107	103	99

DOI: 10.4316/EJAFB. 2026.14204

Volume **14** / **2026** ISSN 2344-102X
Issue **2** ISSN-L 2344-102X

ANSPDCP indicator	2022	2023	2024
Court files managed	108	155	173

Source: Authors' transcription of ANSPDCP reports (2023, 2024, 2025a).

These indicators should be interpreted separately, as cases may extend across reporting years and a single investigation may result in several measures. The reports also provide no data on time to implementation, post-deadline checks, or repeated deficiencies involving the same controller.

4.2. Corrective action in selected published notices

Table 2 brings together three notices selected because they describe the required remedy more clearly than the financial sanction; they do not constitute a representative sample. The AB-RO case concerned personal devices, messaging services, and training. The CVP-RO notice required safeguards and procedures to be revised following two security events, while the V-RO notice required the establishment of a periodic testing and evaluation mechanism. In the public sources searched up to 6 July 2026, no subsequent document was identified that reported verification, closure, or recurrence of the deficiencies described in these notices (ANSPDCP, 2022a, 2022b, 2023, 2024, 2025a, 2025b).

Table 2. Published corrective measures and publicly identifiable follow-up status.

Case / notice date	Incident and corrective action	Implementation deadline stated	Subsequent public sources searched	Public follow-up and status
AB-RO 29 August 2022	A document was sent through WhatsApp to the wrong recipient; four data subjects were affected. Instructions against personal devices and unauthorised chat services; staff training.	Not stated in the notice.	ANSPDCP public notices and annual reports; cut-off: 6 July 2026.	No separate public follow-up document identified; verification, closure, or recurrence not publicly identifiable.
CVP-RO 21 September 2022	A file containing data on 10,739 clients was posted on a public forum; a separate ransomware event affected about 100 persons. Review and update of technical and organisational measures and procedures; additional security solutions.	Not stated in the notice.	ANSPDCP public notices and annual reports; cut-off: 6 July 2026.	No separate public follow-up document identified; verification, closure, or recurrence not publicly identifiable.
V-RO 23 June 2025	Unauthorised disclosure and access affected customer identification, contact, and payment data. A mechanism for periodic testing, evaluation, and assessment of technical and procedural measures.	Not stated in the notice.	ANSPDCP public notices and annual reports; cut-off: 6 July 2026.	No separate public follow-up document identified; verification, closure, or recurrence not publicly identifiable.

Source: Authors' analysis of ANSPDCP notices, annual reports, and public materials available up to 6 July 2026 (ANSPDCP, 2022a, 2022b, 2023, 2024, 2025a, 2025b).

4.3. A similar issue under NIS2

Over time, NIS2 continues to expand the number and diversity of organisations required to perform core cybersecurity functions. A large operator may distribute this work among legal, security, audit, and procurement teams. A municipality, by contrast, may rely on a single IT employee, an external provider, and a data protection officer who also performs other duties. Nevertheless, the DNSC rules on registration and supervision still require systems to be identified, responsibility to be assigned by name, risk-management measures to be implemented, and incidents to be reported (DNSC, 2025c, 2025d). Public incident descriptions, however, are usually too brief to reconstruct the subsequent administrative file. They are therefore used here only to identify recurrent pressures such as privileged access, staff behaviour, asset inventories, and recovery (ENISA, 2024; Zamfiroiu & Sharma, 2022).

IV. DISCUSSION

In the context examined, risk-based verification is essential and should focus on serious incidents, repeated findings, essential services, and missed deadlines rather than reopening every file. Clear operational guidance can reduce uncertainty, while standard templates may help smaller institutions define responsibility, escalation

DOI: 10.4316/EJAFB. 2026.14204

Volume **14** / **2026** ISSN 2344-102X
Issue **2** ISSN-L 2344-102X

procedures, and the evidence needed to close a measure (Clim et al., 2023; Stan & Titirisca, 2025). Documentary information is most complete up to the point at which a measure is ordered. It generally identifies the rule, the authority, the infringement, and the action required; thereafter, the available information becomes sparse. By the research cut-off date, no subsequent public document was identified that reported a post-deadline check or stated whether the same deficiency had recurred. This finding concerns the publication of information, not the authority's or controller's non-public activities. We argue that even a small set of aggregate indicators would make it easier to assess the final stage. We consider that ANSPDCP could report, for example, the "typical period between ordering and closing a measure" or the "proportion of selected measures checked after the deadline and the number of repeated findings". Additional data could supplement the already published numbers of complaints, investigations, and sanctions with evidence on implementation, if DNSC were to publish comparable information on completed post-incident assessments and remedial actions. Table 3 synthesises these reporting and verification requirements.

Table 3. Corrective-measure follow-up and post-deadline verification (Conceptual synthesis of the discussion on GDPR–NIS2 coordination).

Dimension	Problem / gap	Proposed response	Indicator or intended outcome
Risk-based verification	Reopening every file would disperse resources and treat cases with different risk levels identically.	Prioritise serious incidents, repeated findings, essential services, and overdue deadlines.	Proportionate control; resources concentrated on cases with high impact and likelihood.
Post-decision traceability	Publicly available enforcement materials describe the rule, infringement, and measure ordered, but rarely show what happened after the deadline.	Separate the stages: measure ordered, check conducted, remediation evidenced, and file closed.	Visibility of the full pathway without confusing the absence of public information with the absence of administrative action.
ANSPDCP reporting	Complaints, investigations, and sanctions indicate the volume of activity, not the completion of corrective measures.	Introduce a limited set of follow-up indicators in annual reports.	Time to closure; proportion of measures checked after the deadline; open measures; repeated findings.
DNSC reporting	Public data do not allow comparable tracking of post-incident assessments and remediation.	Publish comparable indicators while protecting sensitive technical information.	Completed post-incident assessments; remediated actions; overdue deadlines; recurrent vulnerabilities.
GDPR–NIS2 coordination	The same incident may trigger different obligations and authorities without a common operational sequence.	An integrated working file for notification, evidence preservation, communication, task assignment, and case closure.	Reduced overlap and uncertainty while keeping the two legal regimes distinct.
Support for small entities	Limited staffing and dependence on providers hinder escalation, documentation, and closure of the measure.	Procedural templates identifying the decision-maker, escalation path, and required evidence.	More consistent implementation and sufficient documentation of remediation (Clim et al., 2023; Stan & Titirișcă, 2025).

Source: Authors' own elaboration.

In addition, we consider that certain IT clauses in procurement contracts should regulate logging, access, incident assistance, data return, and cooperation during subsequent checks.

V.A BRIEF OVERVIEW OF THE LATEST LEGISLATIVE DEVELOPMENTS IN THE FIELD

Since July 2026, Romanian law has expressly recognised and protected certain good-faith activities aimed at identifying and reporting vulnerabilities affecting ICT products and services (Romanian Government, 2024; Romanian Parliament, 2026; Cybershield.org, 2026). Law No. 123/2026 introduces paragraph (1^1) into Article 36 of Government Emergency Ordinance No. 155/2024 and Article 365^1 into the Criminal Code. The main purpose of this reform is to distinguish legitimate cybersecurity research from conduct directed against information systems for unlawful purposes. However, the protection offered by the new rules is limited and conditional. It does not constitute a general decriminalisation of unlawful access to or interference with information systems. It applies only if all legislative conditions are met. Research is considered to be conducted in good faith when it is carried out exclusively for the purpose of contributing to improved cybersecurity and in compliance with the applicable legal requirements. Such research must not involve unlawful actions such as unauthorised access to or copying of

DOI: 10.4316/EJAFB. 2026.14204

Volume **14** / **2026** ISSN 2344-102X
Issue **2** ISSN-L 2344-102X

file contents, modifying or deleting data, using malware, bypassing security measures through brute-force techniques or social engineering, or compromising the availability or functioning of ICT services. The application of this legal protection is contingent upon the cumulative fulfilment of the applicable requirements, including reporting the vulnerability to DNSC within 48 hours, and the vulnerability must not be publicly disclosed, either before or after reporting, without DNSC's agreement. Good faith is determined on the basis of the researcher's specific conduct, the extent of the access to information obtained, and the manner in which the reporting procedure before DNSC is followed. The new paragraph (1^1) requires DNSC, in fulfilling Article 36(1), to consult a consultative committee without legal personality, composed of the authorities specified by law and operating under a statute drawn up by DNSC and endorsed by the member authorities. Under the coordinated vulnerability disclosure framework already established by Government Emergency Ordinance No. 155/2024, DNSC, in its capacity as Romania's national CSIRT, coordinates the vulnerability disclosure process and facilitates interaction between researchers, affected entities, producers or service providers, and the competent public authorities. This role is essential in cases involving information security breaches with implications for sensitive personal data, financial operations, critical infrastructure, and essential services that require collaboration between multiple public authorities. By alleviating the legal uncertainty under which good-faith researchers currently operate, this legislative framework is expected to promote early notification and a closer partnership between the cybersecurity community and organisations managing information systems. However, the actual effectiveness of the new legal regime depends on its uniform application, consistent procedures, a robust confidentiality framework, the prompt and effective functioning of the relevant institutional arrangements, and the timely remediation of identified vulnerabilities.

VI. CONCLUSIONS

Romania's current legal framework combines the NIS2 regime with established GDPR supervisory practice. Our analysis shows that ANSPDCP's annual data confirm substantial activity, while the selected notices illustrate that corrective measures address key staff rules, security procedures, and technical testing. Nevertheless, they do not support a conclusion about the durability of the changes. The most useful additional information would concern the implementation of measures after the deadline and the recurrence of previously identified deficiencies.

Our conclusions are limited to the materials published by the institutions whose activities were examined. Annual totals cannot be linked to individual case cohorts, and we had no access to internal correspondence, procurement files, or confidential incident records.

Future studies should therefore track a number of measures from notification to documented closure in organisations of different sizes.

Acknowledgments: Not applicable.

Funding: This research received no external funding.

Conflicts of interest: The authors declare no conflict of interest.

Ethics statement: This study is based exclusively on publicly available legal, institutional, policy and secondary academic sources. It does not involve human participants, interviews, surveys, experiments, personal data collection or clinical/biomedical material. Therefore, formal ethical approval was not required.

REFERENCES

1. ANSPDCP/Autoritatea Nationala de Supraveghere a Prelucrarii Datelor cu Caracter Personal (2022a). Sanction for the breach of the GDPR – AB-RO. https://www.dataprotection.ro/index.jsp?lang=en&page=Comunicat_Presa_29_08_2022.
2. ANSPDCP/Autoritatea Nationala de Supraveghere a Prelucrarii Datelor cu Caracter Personal (2022b). Sanction for the breach of GDPR – CVP-RO. https://www.dataprotection.ro/index.jsp?lang=en&page=Comunicat_Presa_21_09_2022.
3. ANSPDCP/Autoritatea Nationala de Supraveghere a Prelucrarii Datelor cu Caracter Personal (2023). Raport anual al ANSPDCP pe 2022. https://www.dataprotection.ro/index.jsp?lang=ro&page=Comunicat_Presa_21.09.2023.
4. ANSPDCP/Autoritatea Nationala de Supraveghere a Prelucrarii Datelor cu Caracter Personal (2024). Raport anual al ANSPDCP pe 2023. https://www.dataprotection.ro/?lang=ro&page=Comunicat_Presa_09_12_2024.
5. ANSPDCP/Autoritatea Nationala de Supraveghere a Prelucrarii Datelor cu Caracter Personal (2025a). Raport anual al ANSPDCP pe 2024. https://www.dataprotection.ro/?lang=ro&page=Comunicat_Presa_11.08.2025.
6. ANSPDCP/Autoritatea Nationala de Supraveghere a Prelucrarii Datelor cu Caracter Personal (2025b). Sanction for infringing the GDPR – V-RO. https://www.dataprotection.ro/?lang=en&page=Comunicat_Presa_23_06_2025.
7. Cybershield.org (2026). România oferă, în sfârșit, un cadru legal cercetătorilor în securitate cibernetică. https://www.cybershield.org/legea-123-2026-romania-ofera-in-sfarsit-un-cadru-legal-cercetatorilor-in-securitate-cibernetica
8. Clim, A., Toma, A., Zota, R. D., & Constantinescu, R. (2023). The need for cybersecurity in industrial revolution and smart cities. Sensors, 23(1), Article 120. doi: 10.3390/s23010120.

Volume **14** / **2026** ISSN 2344-102X
Issue **2** ISSN-L 2344-102X

9. CJEU/Court of Justice of the European Union (2014). Case C-131/12. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ0131.
10. CJEU/Court of Justice of the European Union (2020). Judgment of 16 July 2020, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, Case C-311/18, ECLI:EU:C:2020:559.
11. DNSC/Directoratul National de Securitate Cibernetica (2025a). Raport anual de activitate 2024. https://www.dnsc.ro/vezi/document/dnsc-raport-anual-2024.
12. DNSC/Directoratul National de Securitate Cibernetica (2025b). Legislatie NIS2. https://www.dnsc.ro/pagini/legislatie-nis2.
13. DNSC/Directoratul National de Securitate Cibernetica (2025c). Order No. 1/2025 approving the requirements concerning notification for registration and the method for transmitting information. Official Gazette of Romania, No. 776 of 20 August 2025. https://legislatie.just.ro/Public/DetaliiDocumentAfis/301473.
14. DNSC/Directoratul National de Securitate Cibernetica (2025d). Order No. 3/2025 approving the rules on supervision, verification and control and the risk-based prioritisation methodology. Official Gazette of Romania, No. 1149 of 11 December 2025. https://legislatie.just.ro/Public/DetaliiDocument/305129.
15. ENISA/European Union Agency for Cybersecurity (2024). ENISA threat landscape 2024. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.
16. European Commission (2020). The EU's Cybersecurity Strategy for the Digital Decade. https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0.
17. European Parliament and Council (2016). Regulation (EU) 2016/679 of 27 April 2016 (General Data Protection Regulation). Official Journal of the European Union, L119, pp. 1-88.
18. European Parliament and Council (2022). Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union, L333, pp. 80-152.
19. OECD/Organisation for Economic Co-operation and Development (2023). Digital government review of Romania: Towards a digitally mature government. OECD Publishing. doi: 10.1787/68361e0d-en.
20. Romanian Government (2021). Government Decision No. 1321/2021 approving the Cybersecurity Strategy of Romania for 2022-2027 and the action plan for its implementation. Official Gazette of Romania.
21. Romanian Government (2024). Government Emergency Ordinance No. 155/2024 on establishing a framework for the cybersecurity of networks and information systems in the national civilian cyberspace. Official Gazette of Romania, No. 1332 of 31 December 2024.
22. Romanian Parliament (2018a). Law No. 190/2018 on measures for the implementation of Regulation (EU) 2016/679. Official Gazette of Romania.
23. Romanian Parliament (2018b). Law No. 362/2018 on ensuring a high common level of security of networks and information systems. Official Gazette of Romania.
24. Romanian Parliament (2025). Law No. 124/2025 approving Government Emergency Ordinance No. 155/2024. Official Gazette of Romania, No. 638 of 7 July 2025.
25. Romanian Parliament (2026). Law No. 123/2026 supplementing Article 36 of Government Emergency Ordinance No. 155/2024 and the Criminal Code. Official Gazette of Romania, No. 550 of 3 July 2026.
26. Stan, G., & Titirişcă, C. (2025). Guarantees of the rule of law in Romania in the digital age, cybersecurity and the processing of personal data. In R. Arnold & J. Cremades (Eds.), Rule of Law, Technology and Environment (pp. 3–17). Springer. doi: 10.1007/978-3-031-76349-6_1.
27. Voigt, P., & von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A practical guide. Springer. https://doi.org/10.1007/978-3-319-57959-7.
28. Voss, W. G., & Bouthinon-Dumas, H. (2021). EU General Data Protection Regulation sanctions in theory and in practice. Santa Clara Computer and High-Technology Law Journal, 37(1), pp. 1-96.
29. Zaguir, N. A., de Magalhaes, G. H., & Spinola, M. M. (2024). Challenges and enablers for GDPR compliance: Systematic literature review and future research directions. IEEE Access, 12, pp. 81608-81630. doi: 10.1109/ACCESS.2024.3406724.
30. Zamfiroiu, A., & Sharma, R. C. (2022). Cybersecurity management for incident response. Romanian Cyber Security Journal, 4(1), pp. 69-75. doi: 10.54851/v4i1y202208.

DOI: 10.4316/EJAFB. 2026.14204