Journal of Law and Administrative Sciences
No.22/2024

SOME JUDICIAL CLARIFICATIONS ON OPERATOR LIABILITY FOR FAILING TO ENSURE PROCESSING SECURITY

Lecturer Dana VOLOSEVICI, PhD.
Petroleum-Gas University of Ploiesti, Romania
dana.volosevici@upg-ploiesti.ro

Abstract
The challenge of implementing technical and organizational measures under the GDPR is multifaceted, requiring a transdisciplinary analysis that encompasses technical, legal, and organizational dimensions. Judicial clarifications from the Court of Justice of the European Union are pivotal in providing a unified and accurate interpretation of GDPR provisions, thereby offering essential guidance to both data controllers and supervisory authorities. This paper examines the scope of the controller's obligation to ensure the security of personal data processing and its liability in the event of breaches of Articles 24 and 32 of the GDPR, with a particular focus on the VB v. Natsionalna agentsia za prihodite case (C-340/21).
Keywords: *GDPR, technical and organisational measures, data, security of processing, burden of proof, liability*

The processing of personal data is carried out within the limits necessitated by ensuring the protection of an individual's fundamental right to the protection of personal data concerning them, as enshrined in Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU). Within this framework, the General Data Protection Regulation (GDPR) requires data controllers to implement technical and organizational measures to safeguard personal data, ensure compliance with legal requirements, protect individual privacy, and enable the secure processing and use of such data.

The precise scope of the obligation to implement appropriate technical and organizational measures to ensure a level of security commensurate with the risk remains the subject of doctrinal and judicial debates, particularly given that Article 32 is among the most frequently violated provisions of the Regulation [1]. Some legal scholars have conducted quantitative analyses [2] of the penalties imposed for non-compliance with the obligation to ensure the security of data processing, while other studies have adopted a qualitative approach [3], utilizing interviews to explore the challenges associated with

implementing security measures. Additionally, certain articles have examined the legal provisions through the lens of legal interpretation tools [4].

A series of rulings by the Court of Justice of the European Union (CJEU) has clarified the interpretation of Articles 24 and 32 of the GDPR, thereby allowing for a more nuanced analysis of these provisions in light of the evolving case law. This article aims to analyze the scope of the controller's obligation to ensure the security of personal data processing and their liability in cases of violations of Articles 24 and 32 of the GDPR, with particular reference to the case of *Natsionalna agentsia za prihodite* (C-340/21) [5].

The obligation of data controllers to implement appropriate technical and organizational measures derives from the "accountability principle" established by Article 5(2) of the GDPR and must be interpreted in light of the risk-based approach that underpins the Regulation [6]. Under this principle, the controller is responsible for adopting suitable, effective, adaptive, and proactive measures to ensure compliance with the principles outlined in Article 5(1) and the Regulation as a whole, as well as for demonstrating such compliance.

Article 24(1) of the GDPR imposes a general obligation on controllers to implement appropriate technical and organizational measures to ensure that processing is carried out in accordance with the Regulation's provisions. These measures must be implemented only after an analysis of the nature, scope, context, and purposes of the processing, as well as an assessment of the risks, including their likelihood and severity, to the rights and freedoms of natural persons. The risk analysis must also establish timelines and/or causes for the review and updating of these measures. The obligation to implement such measures is complemented by the requirement to demonstrate that processing complies with the Regulation's provisions.

Article 24(3) stipulates that adherence to approved codes of conduct or certification mechanisms may serve as evidence of compliance with the controller's obligations.
GDPR codes of conduct are voluntary accountability instruments that establish specific data protection standards for categories of controllers and processors [7]. These codes are developed by associations or other bodies representing categories of controllers or processors, with the aim of specifying how the Regulation should be applied. The content of these codes is varied, as reflected in the non-exhaustive list in Article 40(2) of the

GDPR and may include the measures and procedures outlined in Articles 24 and 25, as well as the security measures specified in Article 32.

Draft codes, or amendments or extensions to existing codes with national applicability, are subject to the review of the supervisory authority, which issues a compliance opinion and approves the draft if it is determined to provide sufficient and appropriate safeguards. Where a draft code of conduct, or amendments or extensions thereto, relates to processing activities in multiple Member States, the competent supervisory authority is required to refer it to the European Data Protection Board (EDPB) before approval. The EDPB's opinion is subsequently transmitted to the European Commission, which may adopt implementing acts to determine that the respective code of conduct has general validity across the Union.

Regarding certification under Articles 42 and 43 of the GDPR, the concept refers to the attestation by a third party concerning the processing operations carried out by controllers and processors [8]. Article 42(5) specifies that certification is issued by an accredited certification body or a competent supervisory authority. The supervisory authority may freely choose one or more of the following options:

- Issue the certification itself, in accordance with its own certification scheme;
- Issue the certification itself, in accordance with its own certification scheme, but delegate the assessment process, in whole or in part, to third parties;
- Develop its own certification scheme and entrust certification procedures to certification bodies authorized to issue certifications; and
- Encourage the market to develop certification mechanisms [9].

As for certification bodies, under Article 43 of the GDPR, Member States must ensure that these bodies can be accredited by the national accreditation body designated under Regulation (EC) No. 765/2008 [10], in accordance with EN-ISO/IEC 17065/2012 standards and additional requirements set by the national supervisory authority. In this regard, Romania's National Authority approved additional requirements for the accreditation of certification bodies under Article 43 of Regulation (EU) 2016/679 through Decision No. 20/2021 [11].

In the specific area of ensuring the security of processing, Article 32(1) of the GDPR provides an illustrative list of technical and organizational measures, stating that

these measures must be evaluated based on several criteria outlined in the Regulation. These criteria include the state of the art, implementation costs, the nature, scope, context, and purposes of the processing, as well as the risk level, considering the likelihood and severity of harm to the rights and freedoms of natural persons.

Paragraph (2) of Article 32 further specifies that the adequacy of the security level must be assessed in light of risks posed by the processing, particularly risks arising from accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or unauthorized access to personal data transmitted, stored, or otherwise processed.
In the context of ensuring processing security, adherence to an approved code of conduct or certification mechanism may also serve as a demonstration of compliance with legal requirements.

The implementation of technical and organizational measures involves an assessment and analysis of risks, which, from a legal perspective, raises the issue of determining the extent of the obligation to ensure the security of data processing. A preliminary observation pertains to the normative source, whether national or European, that must be analyzed to define the scope of this obligation. According to European jurisprudence, the terms of a provision of Union law that do not explicitly refer to the laws of Member States to define its meaning and scope must normally be given an autonomous and uniform interpretation across the Union [12]. Consequently, determining the scope of the obligation to ensure security must be based on the understanding of these terms as interpreted under Union law.

Substantively, it is noteworthy that both Articles 24 and 32 of the GDPR reference the concept of adequacy: “The controller shall implement *appropriate* (emphasis added) technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation” (Article 24(1)); “The controller and the processor shall implement *appropriate* (emphasis added) technical and organizational measures to ensure a level of security appropriate to the risk” (Article 32(1)); “In assessing the *appropriate* (emphasis added) level of security” (Article 32(1)). The use of this concept indicates that the Regulation does not impose an obligation to *eliminate* (emphasis added) risks of personal data security breaches [13] but instead establishes a "risk management regime" [14]. This regime requires that the measures

adopted to protect information systems achieve an “acceptable level” of security [15], both in technical relevance (suitability of measures) and qualitative effectiveness (protection efficiency). European jurisprudence emphasizes that the adequacy assessment must be carried out "concretely," examining whether the measures adopted were implemented “taking into account the various criteria set out in the mentioned articles, the specific data protection needs inherent to the processing, and the risks posed by it” [16]. Similarly, Recital 83 of the GDPR states that “in order to maintain security and prevent processing in breach of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate (emphasis added) those risks,” thereby defining the limits of the obligation based on the concept of mitigation rather than elimination.

Under this legal framework, the measures taken can be highly diverse [17]. Article 32(1) itself provides an illustrative list of measures, including: pseudonymization [18] and encryption of personal data; the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services; the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures to ensure processing security.

It is important to emphasize, as it is relevant for determining the liability of the controller, that the GDPR does not impose a rigid model of processing security requiring the adoption of a predefined set of security measures. On the contrary, it adopts a methodology aligned with international standards for managing information systems risks. An analysis [19] of relevant standards [20] reveals a systematic method comprising the following steps:

- **Step 1**: Identifying risk-based activities across all compared standards (keyword search: “Risk”);
- **Step 2**: Mapping sections/requirements;
- **Step 3**: Describing the relationships or connection points between risk-based activities and their corresponding requirements.

Moreover, the concept of "risk mitigation," explicitly mentioned in Recital 83 of the GDPR, is an integral part of the risk management framework, such as that provided by

ISO 31000, which offers guidelines and best practices in the field. The goal of risk mitigation is to reduce the likelihood and consequences of adverse events. Depending on the specific situation, key strategies for risk mitigation include risk avoidance, risk reduction (whether reducing likelihood or impact), risk sharing, or, in certain cases, risk acceptance [21].

Thus, the scope of the controller's obligation to ensure the security of processing must be assessed with reference to the concept of risk mitigation, rather than risk elimination. In this respect, the Court of Justice of the European Union (CJEU) clarified in Case C-340/21 that unauthorized disclosure of or access to personal data by "third parties" as defined in Article 4(10) of the GDPR is not, in itself, sufficient to conclude that the technical and organizational measures implemented by the controller were not "adequate" under Articles 24 and 32. The controller must be allowed to provide contrary evidence.

To provide contrary evidence, the adequacy of the measures implemented must be established. As outlined earlier, under risk management standards, once a risk analysis is conducted, the controller is afforded a "margin of discretion" [22] to determine the measures to be implemented, provided they are effective in managing the identified risks.

The measures adopted must account for the "state of the art," a phrase that delineates the boundaries of the controller's obligation. At the upper limit, the controller is required to identify all measures available at the time of the risk analysis, with subsequent selection guided by additional criteria outlined in Article 32(1), including implementation costs. Addressing the cost-related considerations, Advocate General G. Pitruzzella highlighted that the adequacy of implemented measures should be assessed through a comparative evaluation that respects the proportionality principle, balancing the data subject's interests (which generally require higher levels of protection) with the economic and technological capacities of the controller (which may at times result in lower levels of protection) [23].

Conversely, the controller's obligation to implement security measures cannot extend beyond the solutions offered by the current state of science, technology, and research. These solutions must be validated by the scientific community and publicly

available. However, it is crucial to note that the concept of "current" evolves rapidly in the field of information technology. Controllers are obligated to review and update the technical and organizational measures in place (Article 24(1), final clause). Consequently, controllers must not only identify adequate measures but also determine the intervals at which these measures should be reviewed and updated based on the risk analysis.

From an analysis of cases sanctioned by supervisory authorities, examples of inadequate measures include insufficient password requirements for user accounts [24], vulnerabilities in encryption mechanisms for banking data [25], and the use of the HTTP protocol, which is susceptible to cyberattacks [26].

When assessing the appropriate level of security, measures must primarily address risks associated with data processing, especially those arising accidentally or unlawfully from destruction, loss, alteration, unauthorized disclosure, or unauthorized access to personal data transmitted, stored, or otherwise processed (Recital 83 and Article 32(2)).

If the risk analysis identifies that one or more types of processing, particularly those based on new technologies, are likely to result in a high risk to the rights and freedoms of natural persons, the controller must conduct a data protection impact assessment (DPIA) before processing begins (Article 35(1) GDPR).

The minimum content of the DPIA is explicitly outlined in Article 35(7) GDPR and must include a systematic description of the proposed processing operations and their purposes, an assessment of the necessity and proportionality of the processing operations in relation to their purposes, an evaluation of risks to the rights and freedoms of data subjects, and the measures envisaged to address the risks, including safeguards, security measures, and mechanisms to ensure compliance with GDPR provisions.

These measures must guarantee the protection of personal data, and the controller must demonstrate compliance with GDPR provisions, taking into account the rights and legitimate interests of data subjects and other interested parties.

If the DPIA concludes that the processing operations pose a high risk that cannot be mitigated through adequate measures in terms of available technology and implementation costs, the controller is required to consult the supervisory authority prior to commencing the processing.

Regarding the evaluation of the measures implemented, European jurisprudence has established that national courts must concretely assess the adequacy of these measures, particularly considering the risks associated with the processing in question. Adopting the specific methodology of risk management, the CJEU has established [27] a two-step procedure for analyzing the adequacy of technical and organizational measures. The first step has two main objectives. First, the risks of personal data security breaches resulting from the processing must be identified. Second, the potential consequences of these risks for the rights and freedoms of natural persons must be evaluated. Both the assessment of risks and their consequences must be conducted concretely, taking into account the likelihood of the identified risks and their severity.

In the second step, it must be verified whether the measures implemented by the controller are tailored to these risks, considering the state of the art, implementation costs, as well as the nature, scope, context, and purposes of the processing.

Thus, national courts must perform a substantive analysis of the measures taken by the controller, with the content of the analysis also established by the CJEU under the GDPR provisions. This analysis should examine the nature of the measures implemented, their specific content, the manner in which they were implemented, and their practical effects on the level of security the controller was obligated to ensure [28].
As for the burden of proof, it is up to the domestic legal order of each Member State to establish the means of proof that allow for the evaluation of the adequacy of the measures implemented by the controller, provided that the principles of equivalence and effectiveness are respected. Procedural modalities under national law must not be less favourable than those applicable to similar situations governed by domestic law, nor should they render the exercise of Union rights practically impossible or excessively difficult [29].

The obligation to conduct a substantive analysis of the measures taken by the controller and the technical specificity of this analysis may lead the court to base its decision on the conclusions of an expert report. Although Article 330(1) of the Code of Civil Procedure provides that, when the court deems it necessary to understand certain factual circumstances, it may appoint one or three experts at the request of the parties or ex officio, in Case C-340/21, the CJEU held that “a judicial expert opinion cannot

constitute a systematically necessary and sufficient means of proof" for assessing the adequacy of security measures implemented by the controller under this article [30].

Regarding the "necessary" nature of such evidence, it was noted that it might be superfluous in light of other evidence available to the court, especially where an independent authority established by law has already conducted a review of the measures' compliance with personal data protection requirements. As for the "sufficient" nature, Advocate General G. Pitruzzella pointed out that the "principle of effectiveness," which implies that an independent court must conduct an impartial assessment, could be undermined if the term "sufficient" were interpreted to mean that the adequacy of the measures taken by the controller could automatically be inferred from an expert opinion. Of course, depending on the circumstances and other evidence available, the court may decide to order expert evidence, but what the Court censured was the expression "a necessary and sufficient means of proof."

As established in case law, a security breach—whether it involves the unauthorized disclosure of personal data or unauthorized access to such data by a third party—cannot be interpreted as evidence that the measures implemented by the controller were inadequate, "without at least allowing the controller to provide contrary evidence" [31]. As previously noted, under the accountability principle set out in Article 5(2) of the GDPR, the burden is on the controller to demonstrate the adequacy of the measures implemented. According to CJEU case law, this burden persists even when the controller is the defendant in litigation. Thus, by exception to civil procedural rules, which stipulate that the party making a claim in court must prove it (Article 249 of the Code of Civil Procedure), in a claim for damages under Article 82 of the GDPR, the burden of proof lies with the controller.

The CJEU's decision is grounded in a combined interpretation of Article 5(2), Article 24(1), and Article 32(1) of the GDPR, as well as the objectives pursued by the Regulation. Advocate General G. Pitruzzella noted that a contrary interpretation would undermine the substance of the right to an effective remedy under Article 82(1). Requiring the claimant to present evidence of the inadequacy of the measures would often be practically impossible, as data subjects generally lack sufficient knowledge to analyze

these measures and have no access to all the information held by the controller, particularly regarding the methods applied to ensure the security of such processing.

Thus, while in a compensation claim under Article 82 the data subject must prove that there has been a breach of the Regulation, that they have suffered damage, and that there is a causal link between the breach and the damage suffered - three conditions that must be cumulatively met [32] - this does not mean the data subject must demonstrate the inadequacy of the technical and organizational measures implemented by the controller.

Another aspect of the evidentiary burden concerns the controller's obligation to prove that they are in no way responsible for the harm caused to the data subject through the unauthorized disclosure of or access to personal data by third parties. Under the definition in Article 4(10) of the GDPR, a "third party" means a natural or legal person, public authority, agency, or body other than the data subject, the controller, the processor, and persons who, under the direct authority of the controller or processor, are authorized to process personal data. Accordingly, the controller does not have any control or oversight over third parties, which could suggest that the controller might be exonerated from liability for their actions. However, Article 82(2), first sentence, of the GDPR establishes the liability of the controller involved in processing operations for any damage caused by processing operations that infringe the Regulation, without distinguishing based on who caused the security breach.

The conditions for the controller's exoneration from liability are explicitly set out in Article 82(3) and require the controller to prove that they are in no way (emphasis added) responsible for the event causing the damage. Thus, even in cases where unauthorized disclosure or access originated from a third party, including a cyberattack, the controller is obligated to prove that there is no causal link between a potential breach of their data protection obligations under the Regulation and the damage suffered by the data subject. It follows that the controller is required to prove both the adequacy of the measures implemented and that the act causing the damage is in no way attributable to them. Naturally, the stronger the evidence of the adequacy of the measures, the more effectively compliance with the GDPR can be demonstrated, particularly the provisions of Article 5(1)(f) and Articles 24 and 32.

Regarding the general conditions for the imposition of administrative fines, the CJEU has held [33] that Article 83 of the GDPR must be interpreted to mean that an administrative fine can only be imposed under this provision if it is established that the controller, as both a legal entity and an enterprise, intentionally or negligently committed an infringement listed in paragraphs (4) to (6) of this article. None of the elements listed within the article mention the possibility of holding the controller liable in the absence of culpable behaviour on their part.

The issue of technical and organizational measures under the GDPR represents a complex challenge, as it requires a multidisciplinary analysis that integrates technical, legal, and organizational aspects. As discussed, the Regulation itself addresses the security of processing from a risk management perspective, which impacts the scope of the controller's liability. In this context, the jurisprudential clarifications provided by the Court of Justice of the European Union play a crucial role in ensuring a uniform and accurate interpretation of the GDPR provisions, offering necessary guidance to both data controllers and supervisory authorities.

The proper and efficient implementation of technical and organizational measures is not only a legal requirement but also a critical element for safeguarding personal data and creating a secure framework in a society increasingly reliant on technology. Simultaneously, clarifying the conditions and extent of liability for parties involved in data processing ensures transparency and predictability, enabling controllers to clearly understand the boundaries of their legal obligations and appropriately adapt the technical and organizational measures they implement.

References:

[1] Barrett, C., *Emerging Trends from the First Year of EU GDPR Enforcement*, Scitech Lawyer 16, 3 (2020), p. 22–35; Ruohonen, J., Hjerppe, K, *The GDPR enforcement fines at glance*, Information Systems 106 (2022), 101876; Marjanov, T., Konstantinou, M., Jozwiak, M., Spagnuelo, D., *Data Security on the Ground: Investigating Technical and Legal Requirements under the GDPR*, Proceedings on Privacy Enhancing Technologies 2023(3), 405–417.

[2] Wolff, J., Atallah. N, *Early GDPR Penalties: Analysis of Implementation and Fines Through May 2020*, Journal of Information Policy 11 (2021), p. 63–103.

[3] Hjerppe, K, Ruohonen, J, Leppänen, V*., The general data protection regulation: requirements, architectures, and constraints*, The 27th International Requirements Engineering Conference. IEEE, Jeju Island, South Korea, 2019, p. 265–275.

[4] Șchiopu, S.-D., *Privire generală asupra măsurilor tehnice și organizatorice necesare pentru implementarea efectivă a Regulamentului general privind protecţia datelor*, Revista Română de Drept al Afacerilor nr. 2/2019, p. 51-58; Lambrinoudakis, C, *The general data protection regulation (GDPR) era: ten*

steps for compliance of data processors and data controllers, International Conference on Trust and Privacy in Digital Business, Springer, Regensburg, Germany, 2018, p. 3–8.
[5] CJEU, Judgment of December 14, 2023, C-340/2021, *VB v. Natsionalna agentsia za prihodite*.
[6] Docksey C., *Article 24. „Responsibility of the controller"*, în Kuner C., Bygrave L.A., Docksey C., Drechsler L., *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, 2020, p. 561.
[7] European Data Protection Board, Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation (EU) 2016/679, Version 2.0 of June 4, 2019, p. 7.
[8] European Data Protection Board, Guidelines 1/2018 on Certification and Identification of Certification Criteria in Accordance with Articles 42 and 43 of the Regulation, Version 3.0 of June 4, 2019, p. 9.
[9] Ibid.
[10] Regulation (EC) No 765/2008 of the European Parliament and of the Council setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93, published in the Official Journal of the European Union L 218/13.08.2008.
[11] Decision No. 20 of June 24, 2021, on the Approval of Additional Requirements for the Accreditation of Certification Bodies under Article 43 of Regulation (EU) 2016/679, issued by the National Supervisory Authority for Personal Data Processing, published in the Official Gazette No. 689 of July 12, 2021.
[12] CJEU, Judgment of June 22, 2021, *Latvijas Republikas Saeima (Penalty Points)*, C-439/19, EU:C:2021:504, para. 81, and Judgment of February 10, 2022, *ShareWood Switzerland*, C-595/20, EU:C:2022:86, para. 21.
[13] M. Gambini, *Responsabilità e risarcimento nel trattamento dei dati personali*, în V. Cuffaro, R. D'Orazio, V. Ricciuto, I dati personali nel diritto europeo, Giappichelli, 2019, p. 1059.
[14] CJEU, Judgment of May 4, 2023, *UI v. Österreichische Post AG*, C-340/21, ECLI:EU:C:2023:986, para. 29.
[15] CJEU, Opinion of Advocate General Giovanni Pitruzzella delivered on April 27, 2023, Case C-340/21, *VB v. Natsionalna agentsia za prihodite*.
[16] CJEU, Judgment of May 4, 2023, *UI v. Österreichische Post AG*, C-340/21, ECLI:EU:C:2023:986, para. 30.
[17] Hagen J, Albrechtsen E., Hovden J., *Implementation and effectiveness of organizational information security measures*, Information Management & Computer Security, 16 (2008): 377-397; 10.1108/09685220810908796.
[18] Hintze, M., & LaFever, G., *Meeting Upcoming GDPR Requirements While Maximizing the Full Value of Data Analytics*, Cybersecurity, 2017, https://doi.org/10.2139/SSRN.2927540.
[19] Barafort, B., Mesquida, A., & Picahaco, A., *Integrating risk management in IT settings from ISO standards and management systems perspectives*, Computer Standards & Interfaces, 54, 2017, pp. 176-185. https://doi.org/10.1016/j.csi.2016.11.010.
[20] The standards underlying the analysis are: *ISO 31000:2009 Risk management – principles and guidelines, ISO Annex SL: high level structure for management system standards, ISO 9001:2015 Quality management systems – requirements, ISO 21500:2012 Guidance on project management, ISO 20000-1:2011 IT service management – service management system requirements, ISO 27001:2013 Information security management*.
[21] Hopkin, P, *Fundamentals of Risk Management*, Kogan Page Ltd, 2021; Hillson, D. (eds), *The Risk Management Handbook: A Practical Guide to Managing the Multiple Dimensions of Risk*, Kogan Page Ltd, 2023.
[22] CJEU, Judgment of December 14, 2023, *VB v. Natsionalna agentsia za prihodite*, C-340/2021, para. 43.
[23] CJEU, Opinion of Advocate General Giovanni Pitruzzella delivered on April 27, 2023, Case C-340/21, *VB v. Natsionalna agentsia za prihodite*, para. 36.
[24] CNIL, Restricted Commitee Deliberation No. SAN-2023-008 of June 8, 2023, concerning the company KG COM; CNIL, Restricted Commitee Deliberation No. SAN-2022-021 of November 24, 2022, concerning the company Électricité de France.
[25] CNIL, Restricted Commitee Deliberation No. SAN-2023-008 of June 8, 2023, concerning the company KG COM.
[26] CNIL, Restricted Commitee Deliberation No. SAN-2023-006 of May 11, 2023, concerning the company Doctissimo.

[27] CJEU, Judgment C-340/2021, para. 42.
[28] Idem, para. 46.
[29] CJEU, Judgment of May 4, 2023, *UI v. Österreichische Post AG*, C-340/21, ECLI:EU:C:2023:986, para. 53; Judgment of December 13, 2017, *El Hassani*, C-403/16, EU:C:2017:960, para. 26; and Judgment of September 15, 2022, *Uniqa Versicherungen*, C-18/21, EU:C:2022:682, para. 36.
[30] CJEU, Case C-340/2021, para. 64.
[31] CJEU, C-340/21, para. 31.
[32] CJEU, Judgment of the Court of September 5, 2019, *European Union v. Guardian Europe* and *Guardian Europe v. European Union* (C-447/17 P and C-479/17), EU:C:2019:672, para. 147; CJEU, Judgment of the Court of October 28, 2021, *Vialto Consulting v. Commission* (C-650/19), EU:C:2021:879, para. 138.; General Court Judgment of January 13, 2021, *Helbert v. EUIPO* (T-548/18), EU:T:2021:4, para. 116.
[33] CJEU, Judgment of December 5, 2023, Case C-807/21, *Deutsche Wohnen SE v. Staatsanwaltschaft Berlin*, ECLI:EU:C:2023:950.