European Journal of Law and Public Administration
ISSN: 2360-6754 | e-ISSN: 2559-7671
Covered in: Erih Plus; HeinOnline; CEEOL; RePEc; CrossRef; Google Scholar; KVK; WorldCat; ICI Journals Master List - Index Copernicus; EBSCO.

2025, Volume 12, Issue 2, pages: 121-137 | https://doi.org/10.18662/eljpa/12.2/269

The Ethical Dimension of the Principle of Responsibility Regarding the Right to the Protection of Personal Data

Andreea BURUIANĂ (RUSU) [1]

[1] "Ştefan cel Mare" University of Suceava, Romania; andreea.rusu@fdsa.usv.ro

Abstract: *The principle of responsibility, enshrined in Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data, holds a central place in the conceptual framework of data protection in contemporary society. Beyond its legal and operational role, this principle expresses a profound ethical dimension, which calls for a reconceptualization of the relationship between the controller and the data subject. Responsibility is not limited to mere formal compliance with legal requirements, but involves a real, active, and demonstrable commitment to all measures adopted in the data processing activities, aimed at respecting the fundamental rights and freedoms of the individual. In this context, responsibility becomes the expression of an organizational conduct that reflects integrity, transparency, and a commitment to fundamental ethical values such as dignity, autonomy, and informational self-determination of the individual. Therefore, a shift is required from a reactive and minimal approach, focused on formal obligations, to a vision based on the internalization of ethical principles in everyday decision-making practices. This transition presupposes the existence of an organizational culture in which data protection is not treated solely as a legal or technical issue, but as an ongoing commitment to respecting the human person. The present article offers a theoretical reflection on the ethical dimension of the principle of responsibility, without aiming to conduct empirical research. Its purpose is to highlight the importance of a coherent ethical perspective in the application of personal data protection rules. In conclusion, it argues that responsibility should be understood not only as a mechanism of legal traceability, but as a form of moral commitment to a fundamental right, in a digital context marked by complexity, automation, and systemic risks.*

Keywords: *responsibility; applied ethics; data protection; personal data processing; GDPR; fundamental rights.*

How to cite: Buruiană (Rusu), A. (2025). The ethical dimension of the principle of responsibility regarding the right to the protection of personal data. *European Journal of Law and Public Administration, 12*(2), 121-137. https://doi.org/10.18662/eljpa/12.2/269

©2025 Published by In Manifest Network in partnership with LUMEN Publishing. This is an open access article under the CC BY-NC-ND license http://creativecommons.org/licenses/by-nc-nd/4.0/

Introduction

In today's information society, where the circulation and processing of personal data have become ubiquitous phenomena, the protection of privacy and personal data has acquired a distinct significance, both legally and ethically. Although often addressed together in public discourse and various regulations, the right to respect for private life and the right to the protection of personal data are two distinct rights, with different origins, formulations, and scopes of application. As emphasized in the specialized literature, the right to privacy has a longer-standing recognition in international human rights law and essentially refers to the prohibition of unjustified interferences in an individual's personal sphere (European Union Agency for Fundamental Rights, 2018). By contrast, the protection of personal data emerged as a response to technological developments and the new risks associated with the automated processing of information. In the European context, this distinction has been acknowledged and strengthened through the establishment of a specific legal framework dedicated to data protection, with its own features and enforcement mechanisms, which do not necessarily depend on the existence of a violation of private life. Data protection has a broader scope of application, as it applies to any data processing activity, regardless of whether it involves an interference with private life. This aspect is essential for understanding the autonomous and proactive nature of the right to data protection, which entails not only the safeguarding of the intimate sphere of the individual, but also the application of principles and safeguards covering the entire personal data processing cycle (collection, storage, use, transfer of personal data, etc.) (Cireaşă, 2021). From this perspective, it is important to note that data protection is not limited to preventing potential intrusions into privacy, but rather aims to establish a framework of balance between the legitimate interests of data processing actors and the rights of the data subjects. Therefore, although the two rights - closely connected through their shared focus on the individual and their dignity - are complementary in function, they rest on distinct legal foundations. As stated in the Handbook on European data protection law, published by the European Union Agency for Fundamental Rights (2018), data protection must be understood as an autonomous normative instrument, applicable in any situation involving the handling of personal information, and not merely as a modern extension of the traditional right to privacy (European Union Agency for Fundamental Rights, 2018). This conceptual separation between the two rights does not diminish their functional interdependence. Both seek to safeguard individual autonomy and

to ensure a space in which persons can act freely, think, and communicate without unjustified constraints. At the same time, the differences between them become legally and practically relevant, especially when analyzing the implications of each right on the institutional framework and on the responsibilities of those who process data (Terec-Vlad, 2022). Exploring these differences - without losing sight of the convergences between the two rights - is essential for understanding the complex nature of personal protection in the digital age.

It should be noted that the right to the protection of personal data is not absolute, but is subject to limitations, such as those provided by:

- **Charter of Fundamental Rights of the European Union (the Charter), Article 52(1)**: „ *(1) Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.*" (Charter of Fundamental Rights of the European Union, 2016).
- **General Data Protection Regulation, Article 23**: „ *(1)Union or Member State law to which the data controller or processor is subject* ***may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5*** *in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:*
  (a) national security;
  (b) defence;
  (c) public security;
  (d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
  (e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security;
  (f) the protection of judicial independence and judicial proceedings;
  (g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
  (h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);
  (i) the protection of the data subject or the rights and freedoms of others;

(j) the enforcement of civil law claims.

2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to:

(a) the purposes of the processing or categories of processing;

(b) the categories of personal data;

(c) the scope of the restrictions introduced;

(d) the safeguards to prevent abuse or unlawful access or transfer;

(e) the specification of the controller or categories of controllers;

(f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;

(g) the risks to the rights and freedoms of data subjects; and

(h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction." (Regulation (EU) 2016/679).

- **Judgment of the Court (Grand Chamber) of 9 November 2010: Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen**: In the Schecke case, the Court of Justice emphasized that European institutions cannot rely on the principle of transparency in abstract or general terms to justify an interference with the fundamental rights to privacy and data protection. A responsible approach on the part of the legislator would have required the definition of precise and specific objectives - these being the only ones that allow for a rigorous assessment of the necessity and proportionality of a legislative measure. The Court annulled the scheme for publishing the recipients of agricultural subsidies precisely because the institutions failed to provide a coherent explanation of the intended purpose, shifting inconsistently between macro-transparency aimed at budgetary control and micro-transparency aimed at preventing individual fraud. This lack of clarity demonstrated that a proper balance between public interests and individual rights had not been achieved, turning the annulment of the regulation into a form of sanction against a legislator that had not adequately substantiated its decisions. Moreover, the application of the principle of responsibility requires that any limitation of rights pass the necessity test, which obliges authorities to demonstrate that they have considered less intrusive alternatives to achieve the intended objective. In this case, the Court noted that there was no evidence that the Council or the Commission had considered publication methods that would have affected private life to a lesser extent - such as limiting the disclosure of names based on the periods in which aid was received or the amounts involved. The conclusion is that transparency cannot be granted automatic precedence over data protection; rather, it

must be actively supported as a morally and legally grounded practice, where each instance of data processing is justified by concrete evidence of necessity and by a careful assessment of the impact on the individual. (Court of Justice of the European Union, 2010; Bobek, 2011).

- **European Convention on Human Rights, Article 8(2)**: „*(2)There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*" (Council of Europe, 1950).
- **Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, article 11**: „ *1. No exception to the provisions set out in this Chapter shall be allowed except to the provisions of Article 5 paragraph 4, Article 7 paragraph 2, Article 8 paragraph 1 and Article 9, when such an exception is provided for by law, respects the essence of the fundamental rights and freedoms and constitutes a necessary and proportionate measure in a democratic society for:*
  a. the protection of national security, defense, public safety, important economic and financial interests of the State, the impartiality and independence of the judiciary or the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties, and other essential objectives of general public interest;
  b. the protection of the data subject or the rights and fundamental freedoms of others, notably freedom of expression.
  2. Restrictions on the exercise of the provisions specified in Articles 8 and 9 may be provided for by law with respect to data processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes when there is no recognisable risk of infringement of the rights and fundamental freedoms of data subjects.
  3. In addition to the exceptions allowed for in paragraph 1 of this article, with reference to processing activities for national security and defense purposes, each Party may provide, by law and only to the extent that it constitutes a necessary and proportionate measure in a democratic society to fulfill such aim, exceptions to Article 4 paragraph 3, Article 14 paragraphs 5 and 6 and Article 15, paragraph 2, litterae a, b, c and d.
  This is without prejudice to the requirement that processing activities for national security and defense purposes are subject to independent and effective review and supervision under the domestic legislation of the respective Party." (Council of Europe, 2018).

- **Hotărârea CEDO [MC] în cauza S. şi Marper/Regatul Unit, nr. 30562/04 şi 30566/04, 2008**:„ I. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION
  58. The applicants complained under Article 8 of the Convention about the retention of their fingerprints, cellular samples and DNA profiles pursuant to section 64(1A) of the Police and Criminal Evidence Act 1984 (PACE). Article 8 provides, in so far as relevant, as follows:
  "1. Everyone has the right to respect for his private ... life ...
  2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society ... for the prevention of disorder or crime ..."
  FOR THESE REASONS, THE COURT UNANIMOUSLY
  1. Holds that there has been a violation of Article 8 of the Convention; [...]" (European Court of Human Rights, 2008)

Key aspects regarding compliance with the principle of accountability

It must be noted from the outset that the wording of the legal provision governing this principle is extremely succinct: "(2) The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')." (Regulation (EU) 2016/679, 2016). In practice, this provision often raises questions from controllers who, when faced with the obligation to demonstrate compliance with legal requirements, turn to consultants or data protection officers for clarification: "What exactly are we supposed to do? What does it concretely mean to demonstrate that we comply with this obligation?" (Cireaşă et al., 2021). Thus, the difficulty lies not only in achieving actual compliance, but especially in identifying appropriate means of demonstrating it, within a regulatory context that imposes results but does not always specify the steps or reference standards[1] (European Union Agency for Fundamental Rights, 2018).

Compliance with the accountability requirement can be achieved by controllers through a series of concrete measures, adapted to the specificities of each data processing activity. Among the methods recognised as relevant is the maintenance of detailed records of processing activities[2]. These records must be available for submission to the supervisory authority when a request is made in this regard (Simionovici et al., 2020). The practice of documenting processing activities is not merely a formal exercise; it reflects the controller's ability to continuously monitor and control compliance with

[1] The burden of proof lies with the controllers.
[2] GDPR, art. 30.

legal requirements. In certain cases, controllers are required to appoint a Data Protection Officer (DPO), who must be involved in all matters related to the protection of personal data within the respective entity (Cireaşă, 2020). The role of this person is essential in supporting a compliant organisational culture (Burch & Burch, 2025) and in the ongoing supervision of compliance with applicable requirements[3]. For processing operations likely to result in high risks to the rights and freedoms of natural persons, impact assessments must be carried out[4]. These assessments provide a preventive analysis of the potential consequences of processing operations and contribute to the substantiation of risk mitigation measures. In addition to these measures, data protection must be integrated from the design stage of processes and systems involving data processing, as well as through the implementation of data protection by default - such as limiting data collection and processing to what is strictly necessary[5]. Another important element is the establishment of effective procedures by which data subjects can exercise their rights provided by data protection legislation. Controllers must create the necessary conditions for such requests to be handled promptly and appropriately (Ploeşteanu, 2019). Moreover, adherence to approved codes of conduct or recognised certification mechanisms may serve as an additional method for demonstrating compliance and strengthening trust in processing activities (European Union Agency for Fundamental Rights, 2018).

Although the principle of accountability is not directly addressed to processors, they nevertheless have a series of obligations arising from applicable legal provisions. These include, among others, the obligation to keep records of processing activities carried out on behalf of the controller, as well as the designation of a data protection officer when required by the nature of the operations (Şandru, 2018). Processors also have the duty to ensure that the necessary data security measures are effectively implemented. The relationship between the controller and the processor must be governed by a binding contract that includes clear provisions regarding cooperation to ensure compliance. This contract may, for example, stipulate that the processor must assist the controller in carrying out data protection impact assessments or notify the controller without undue delay of any data breaches of which it becomes aware (European Union Agency for Fundamental Rights, 2018). These aspects are consistent with the recommendations formulated by the Organisation for Economic Co-

[3] *Ibidem*, art. 37-39.
[4] *Ibidem*, art. 35.
[5] *Ibidem*, art. 25.

operation and Development (OECD), which, as early as 2013, in its privacy guidelines, emphasized the importance of controller accountability in the effective implementation of substantive data protection principles. According to these guidelines, each data controller must be accountable for implementing the necessary measures to ensure compliance with these principles: "*Accordingly, the accountability principle requires data controllers to demonstrate compliance proactively, without waiting for data subjects or supervisory authorities to raise concerns.*" (European Union Agency for Fundamental Rights, 2018).

The ethical dimension of personal data protection in the context of technological transformations

In the context of rapid technological transformations and the proliferation of increasingly complex digital practices, the European Data Protection Supervisor (EDPS) has expressed ongoing concern about the impact of emerging technologies on fundamental rights, particularly the right to privacy and the protection of personal data. This concern materialized in a significant and strategic initiative with the adoption, on 3 December 2015, of the decision to establish an external advisory group on the ethical dimensions of data protection - known as the "Ethics Advisory Group" (European Data Protection Supervisor, 2016). The establishment of this group represents a key step in strengthening the European mechanisms for protecting data subjects by adding an ethical and reflective dimension to existing legal and technical regulations. The European Data Protection Supervisor recognized that recent technological developments - such as big data analytics, machine learning algorithms, and artificial intelligence - enable massive and opaque processing of personal data, posing serious risks to human dignity, freedom, and individual autonomy. Therefore, effective data protection in the digital age can no longer be conceived solely in terms of legal compliance; it requires a broader approach that integrates ethical principles and considerations related to social justice, fairness, and transparency (European Data Protection Supervisor, 2016). The Ethics Advisory Group was designed as a multidisciplinary forum for reflection, aimed at supporting the EDPS in anticipating and understanding the ethical challenges raised by new data processing practices. Through its work, the group contributes to the development of independent and informed recommendations, offering guidance on sensitive areas such as health, security, artificial intelligence, or algorithmic governance. Additionally, the group is tasked with drafting public reports, proposing research directions, and consulting with informed audiences, with the goal of grounding ethical

reflection in practical reality. The composition of the group reflects its independent and academic character: it consists of up to six distinguished experts, selected based on their competence and experience in analyzing the ethical dimensions of data protection. Members act in their personal capacity, without representing institutional interests, and are bound by strict rules of impartiality and confidentiality. Through this initiative, the EDPS demonstrates that the protection of data subjects cannot be ensured solely through legal instruments, but also requires a deep understanding of the moral and social implications of emerging technologies. It is, thus, an example of mature institutional evolution, acknowledging the need for proactive protection grounded in ethical vigilance and public responsibility, in an era where personal data has become both a critical resource and a zone of vulnerability (European Data Protection Supervisor, 2016).

In an increasingly complex and pervasive digital landscape, the initiative of the European Data Protection Supervisor (EDPS) on digital ethics represented a crucial intervention aimed at anchoring emerging technologies in the fundamental values of dignity and human rights. Officially launched in June 2018 through a public consultation, the initiative was part of a broader framework of reflection that began three years earlier, in 2015, with the publication of the opinion "*Towards a New Digital Ethics: Data, Dignity and Technology*" (European Data Protection Supervisor, 2018). This opinion served as a wake-up call, suggesting that technological development should not be left solely in the hands of economic actors or technical innovators, but requires a value-based framework to guide innovation toward the common good. The 2018 consultation was conceived as a moment of openness to society, offering individuals and institutions the opportunity to express their concerns, anxieties, and hopes in the face of an accelerated digital transition (European Data Protection Supervisor, 2018). This exercise in collective listening and deliberation represented a rare occasion in which ethics was treated not as a marginal consequence of technology, but as the possible foundation of a just digital society. A defining feature of the consultation was its transdisciplinary and inclusive character. The 76 contributions received reflected a remarkable diversity of perspectives, originating not only from the private sector, but also from healthcare, education, public administration, civil society, and even from individual citizens, artists, or religious organisations. This diversity enabled a more accurate understanding of how digital transformations permeate all aspects of social and personal life. Contributions came from numerous European countries, as well as from Australia and the United States, highlighting the global nature of the ethical challenges posed by technology (Trifu et al., 2017). Thus, the consultation was not merely a

technocratic exercise, but a genuine deliberative platform through which the EDPS invited society to participate in shaping normative and philosophical responses to contemporary dilemmas. Most of the questions posed were open-ended, deliberately avoiding restrictive or binary formulations, in order to stimulate critical thinking and authentic argumentative input (European Data Protection Supervisor, 2018). The deeper motivation behind this consultation was not only to anticipate future risks but also to acknowledge present-day concerns: the emergence of phenomena such as invasive profiling, behavioural manipulation, algorithmic opacity, or automated discrimination. These are no longer hypothetical threats, but already documented realities in various contexts, from recruitment and criminal justice to healthcare and education. For this reason, participants in the consultation emphasised that legislation, while necessary, is not sufficient. Law merely outlines the minimum threshold of acceptability, whereas decisions about what is "just," "humane," or "respectful" of autonomy and privacy belong to the ethical sphere. Consequently, the consultation called for a rethinking of the relationship between technology, law, and values - not as a hierarchical structure, but as an interdependence that must be managed deliberatively and democratically. The EDPS initiative thus positioned itself within a horizon of normative rigor and collective responsibility, calling both institutions and citizens to engage in reflection (European Data Protection Supervisor, 2018).

A particularly important aspect highlighted during the consultation was the recognition that technology shapes not only behaviours, but also structures of thought and social perception. Participants identified subtle yet profound risks, such as the naturalisation of inequalities through seemingly neutral algorithms, or the transfer of moral decision-making from the human to the technical system. A relevant example was that of autonomous vehicles, which may alter their route automatically without adequately informing the user, thereby raising questions about both human autonomy and responsibility for the consequences of the action (European Data Protection Supervisor, 2018). Such cases require a rethinking of ethics as a form of active protection of dignity, not merely as a reaction to the violation of a right. At the same time, the consultation revealed concerns about the opacity of artificial intelligence systems, stressing the need for decision-making processes to be understandable and for accountability to be ensured. In the absence of these conditions, the foundations are laid for a crisis of trust in technology, with serious implications for social cohesion and the functioning of democracy. Beyond critical observations, the consultation also had a constructive dimension, offering concrete proposals for integrating ethics into digital governance. Most participants advocated for an

active role of public authorities in defining and applying ethical standards, not just legal ones (European Data Protection Supervisor, 2018). According to the data collected, 86% of respondents believe that state institutions should lead the effort to establish ethical regulation, in order to protect the public interest and prevent commercial interests from dominating the public sphere. In addition, many organisations stated that digital ethics is not merely an option, but a fundamental condition for the legitimacy and sustainability of their activities. This consensus provided important support for the EDPS in the lead-up to the 2018 International Conference of Data Protection and Privacy Commissioners, an event intended to conclude the initiative through an open and transdisciplinary international debate. Here, the reflection on ethics was not treated as an appendix to legal norms, but as a foundational dimension of life in the digital age (European Data Protection Supervisor, 2018).

The EDPS initiative on digital ethics and the related public consultation represented a model of democratic, reflective, and participatory engagement with technological transformation. In an era where technical decisions tend to escape public deliberation, such processes bring back to the forefront the idea that technology is, above all, a human construct - one that must be guided by values, not merely by efficiency or profit. The fact that the initiative brought together a wide range of actors - from experts to ordinary citizens - enabled the articulation of a pluralistic yet coherent normative framework capable of guiding European public policy toward a more "human" digital future. Digital ethics is not a normative luxury, but a practical necessity in the face of accelerating innovation. Consequently, the dominant conclusion of the consultation was that the European digital future must rest on an inseparable triad: technology, rights, and moral responsibility. Only in this way can we hope for a digital society that not only functions, but also thrives (European Data Protection Supervisor, 2018).

The responses received during the EDPS consultation on the question regarding ethical challenges addressed by organisations revealed an almost exclusive focus on issues arising from digital technologies, despite the broad wording of the question. Although it aimed to identify various types of ethical challenges, not limited to technology, all responses revolved around the impact of digitalisation (European Data Protection Supervisor, 2018). Among the most frequently mentioned topics were the fair processing of personal data, the valid collection of consent, and compliance with the General Data Protection Regulation (GDPR). Participants emphasised the difficulties of balancing the legitimate interests of economic operators with the fundamental rights of data subjects, especially in relation

to the extensive use of data for commercial, predictive, or marketing purposes. In this context, ethics is viewed not merely as a supplementary tool for legal compliance, but as an indispensable normative resource for understanding the limits and responsibilities toward individual autonomy, dignity, and freedom. This exclusive focus on the technological dimension of ethical challenges also reflects a broader trend of redefining organisational ethics through the lens of digital risks, even when the wording of the questions allows for more diverse answers (European Data Protection Supervisor, 2018). Beyond data protection, contributions highlighted a wide range of ethical risks associated with digitalisation: from the non-transparent functioning and lack of reproducibility of AI-based systems, to algorithmic discrimination, fake news, online fraud, or harassment in digital spaces.

Significantly, some participants mentioned the difficulty individuals face in benefiting from the data they generate themselves, as well as more structural issues such as unequal access to new technologies or the imbalanced distribution of the benefits of digitalisation. These themes go beyond the classic relationship between controller and data subject, raising systemic questions about social justice in the digital age (European Data Protection Supervisor, 2018). Additionally, several formulations express a deep concern for the value-based dimension of digitalisation: "ensuring dignity and privacy," "fair and respectful treatment of each client," or the recognition that individuals should "understand and want" the services offered to them. Such expressions do not merely indicate formal compliance, but reflect a genuine intention to reposition technology in relation to fundamental human values. Overall, the results point to a growing willingness to discuss digitalisation not only in terms of efficiency and innovation, but through a language grounded in rights, ethics, and responsibility (European Data Protection Supervisor, 2018).

Compliance with the principle of accountability, enshrined in Article 5(2) of the General Data Protection Regulation (GDPR), entails not only a legal obligation to comply, but also a profound ethical commitment on the part of controllers toward data subjects and society at large. In a strictly legal sense, accountability means that the controller not only complies with the data processing principles, but can also demonstrate such compliance at any time - including lawfulness, fairness, transparency, data minimisation, accuracy, storage limitation, and integrity. However, beyond this formal framework lies an essential ethical dimension concerning how these obligations are understood, assumed, and applied in practice - not merely checked off in a compliance list. Ethically, respecting the principle of accountability implies, first and foremost, genuine transparency - meaning

clear, complete, and accessible information provided to data subjects about what data is being collected, for what purposes, to whom it is disclosed, and how long it is retained. An ethics of accountability does not tolerate deliberate ambiguities, opaque language, or communication strategies designed to discourage the exercise of rights. Secondly, it involves the fairness of internal processing operations - such as avoiding unnecessary data collection, preventing erroneous duplication or profiling, and periodically updating data to avoid unfair outcomes for individuals. Truly respecting this principle means avoiding any form of instrumentalisation of the person - treating data not as mere anonymised resources, but as extensions of human beings worthy of respect. From an ethical standpoint, accountability also entails a genuine - not merely declarative - respect for the rights of data subjects: the rights to access, object, rectify, erase, and port data. A responsible approach requires that these rights are not obstructed through abusive bureaucratic procedures or delayed responses, but are actively supported through efficient and user-friendly infrastructures that demonstrate respect for each individual's dignity and autonomy. Finally, the ethical dimension of accountability is also reflected in how an organisation responds to security incidents: to act ethically means not to hide, minimise, or cover up breaches, but to take responsibility promptly, to inform the competent authority and affected individuals accurately, and to learn from each incident to prevent recurrence. Thus, accountability under the GDPR is not merely a compliance obligation, but a continuous exercise in institutional integrity. The ethics of this principle lies precisely in internalising these requirements into the organisational culture, not just embedding them in written policies (Burch & Burch, 2025). Being accountable in data processing means acting with honesty, openness, and respect for people - even when they do not see, do not ask, and do not complain.

Conclusions

The principle of accountability enshrined in the GDPR acquires a profound ethical significance when analysed beyond the letter of the legal norm and in relation to the concrete effects of data processing on the individual. From this perspective, accountability can no longer be reduced to a procedural obligation of documentation, audit, or formal demonstration of compliance - it becomes a moral assumption of the informational power held by the controller. Every processing activity involves a structural imbalance between the entity that collects, stores, and analyses the data and the data subject, who typically remains in a vulnerable position. The ethics of accountability demands awareness of this imbalance and its transformation

into a central decision-making criterion: not just "is it legal?" but also "is it fair?", "is it proportionate to its impact on the individual?", "does it respect autonomy and self-determination?" In this sense, accountability becomes the expression of a moral relationship between the organisation and the individual - not merely a defensive mechanism against sanctions.

Practically speaking, the ethical dimension of accountability manifests in how internal data processing procedures are designed and implemented. An ethically responsible organisation does not limit itself to drafting standardised policies or using inaccessible legal jargon, but actively invests in genuine transparency that is comprehensible to data subjects. This entails clear, structured, and honest notifications that do not conceal risks, do not downplay consequences, and do not turn consent into a formal act devoid of substance. Moreover, ethical accountability requires the material fairness of data - not merely its technical accuracy: avoiding excessive profiling, preventing automated decisions with discriminatory effects, and promptly correcting errors that may cause real harm. To respect accountability in this sense means treating data as bearing moral consequences, not merely as inputs in an automated system.

An essential dimension of the ethics of accountability also lies in how organisations respond to security incidents and to the inherent risks of processing. From a legal perspective, the obligation to notify is clearly regulated. Ethically, however, the stakes are far broader: institutional honesty and a deliberate refusal to hide, downplay, or postpone accountability. An organisation that truly respects the principle of accountability does not treat an incident as a reputational failure to be managed strategically, but as an event that affects real people and demands a prompt response, empathy, and genuine corrective measures. In this framework, accountability is not reactive, but proactive - oriented toward prevention, continuous risk assessment, and institutional learning, even when the law does not explicitly impose specific actions.

Ultimately, ethical compliance with the principle of accountability requires its internalisation within organisational culture, not its exclusive delegation to legal departments or formal compliance roles. Accountability thus becomes an institutional virtue that shapes daily decisions, strategic priorities, and the organisation's relationship with the human person. In a society dominated by automation and large-scale data processing, this ethical approach is the only one capable of preventing the reduction of the individual to an object of algorithmic governance. Respecting accountability in the deeper sense of the GDPR therefore means recognising that technological progress is legitimate only insofar as it remains subordinated to

the dignity, autonomy, and freedom of the person (Terec-Vlad, 2021). Only through such constant moral commitment can a sustainable digital ecosystem be built - one in which technology, rights, and moral responsibility coexist in authentic balance.

AI Tools Use Statement |No AI-assisted technologies were used in the writing, editing, or data analysis for this manuscript. All work is original and completed solely by the listed authors.

References

Bobek, M. (2011). Joined Cases C-92/09 and C-93/09, Volker und Markus Schecke GbR and Hartmut Eifert, judgement of the Court of Justice (Grand Chamber) of 9 November 2010 N.Y.R. *Common Market Law Review, 48*(6).

Burch, G. F., & Burch, J. (2025). Creating a compliant and accountable data culture. *ISACA Journal, 5*. https://www.isaca.org/resources/isaca-journal/issues/2025/volume-5/creating-a-compliant-and-accountable-data-culture

Charter of Fundamental Rights of the European Union. (2016). Official Journal of the European Union, C 202, 389–405. https://eur-lex.europa.eu/eli/treaty/char_2016/oj/eng

Cireaşă, D. (2020). Responsabilul cu protecţia datelor personale la un an şi jumătate de aplicare a GDPR [The data protection officer one and a half years after the application of the GDPR]. *Revista Română pentru Protecția și Securitatea Datelor cu Caracter Personal, 1*, 106–108. Universul Juridic

Cireaşă, D.-I. (2021). Principiile GDPR - de la teorie la practică [The principles of the GDPR – from theory to practice]. *Curierul judiciar, 4,* 189–193. C.H. Beck.

Cireaşă, D.-I., Simionovici, D., & Dumitrescu, M. (2021). Obligaţiile operatorilor de date cu caracter personal în aplicarea GDPR [The obligations of personal data controllers in the application of the GDPR]. *Curierul judiciar, 4*, 194–200

Council of Europe. (1950). Convention for the Protection of Human Rights and Fundamental Freedoms [European Convention on Human Rights]. https://www.echr.coe.int/documents/d/echr/convention_ENG

Council of Europe. (2018). Modernised convention for the protection of individuals with regard to the processing of personal data (Convention 108+), adopted at the 128th Session of the Committee of Ministers, Elsinore, Denmark, 17–18 May 2018. https://search.coe.int/cm?i=090000016807c65bf

Court of Justice of the European Union. (2010). Judgment of the Court (Grand Chamber) of 9 November 2010: Volker und Markus Schecke GbR (C-

92/09) and Hartmut Eifert (C-93/09) v Land Hessen. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62009CJ0092

European Court of Human Rights. (2008). Judgment of the Grand Chamber in the case of S. and Marper v. the United Kingdom (nos. 30562/04 and 30566/04), 4 December 2008. https://hudoc.echr.coe.int/fre?i=001-90051

European Data Protection Supervisor. (2016). European Data Protection Supervisor decision of 3 December 2015 establishing an external advisory group on the ethical dimensions of data protection ('the Ethics Advisory Group') (2016/C 33/01). https://www.edps.europa.eu/sites/default/files/publication/15-12-03_ethical_dimensions_en.pdf

European Data Protection Supervisor. (2018). Public consultation on digital ethics: Summary of outcomes. https://www.edps.europa.eu/sites/default/files/publication/18-09-25_edps_publicconsultationdigitalethicssummary_en.pdf

European Union Agency for Fundamental Rights. (2018). Handbook on European data protection law: 2018 edition. https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition

Finn, R. (2019). *Cultivating a culture of data protection within your organisation*. Trilateral Research. https://trilateralresearch.com/data-protection/cultivating-a-culture-of-data-protection-within-your-organisation

Ploeşteanu, N.-D. (Coord.). (2019). *Ghid practic pentru conformare cu Regulamentul General privind Protecția Datelor: Instrument de audit [Practical guide for compliance with the General Data Protection Regulation: Audit tool]*. Universul Juridic.

POEU (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) (OJ L 119 04.05.2016, p. 1. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679

Şandru, D. M. (2018). Principiile protecţiei datelor - de la teorie la practică [Principles of data protection – from theory to practice]. *Curierul Judiciar, 364*.

Simionovici, D., Cireasă, D.-I., Pantilimon, C., & Dan, M.-F. (2020). *GDPR aplicat: Instrument de lucru pentru implementarea Regulamentului (UE) 679/2016 [Applied GDPR: Working tool for the implementation of Regulation (EU) 679/2016]*. Wolters Kluwer

Terec-Vlad, L., (2021). Meanings of the Autonomy concept. *European Journal of Law and Public Administration 8*(1). 114-120.

Terec-Vlad, L., (2022). General considerations on International Human Rights Law in the context of new technologies. *Journal of Social Media Inquiry, 4*(1). 41-47.

Trifu, A., Juravle A.I., Terec-Vlad L., (2017). The economic and philosophical implications of the concept of responsibility. *Ecoforum Journal, 6*(1).