

Data protection officer The new guarantor of freedom in the digital era

*Cristian Gabriel Nicolae Coman**

Abstract

In a digital landscape increasingly shaped by data-driven surveillance, the protection of fundamental rights is undergoing a systemic reconfiguration, with the Data Protection Officer (DPO) emerging as a key figure of resilience and institutional balance. This paper examines the evolution of the DPO role from a purely compliance-oriented function into a strategic pillar for safeguarding human dignity within public administration. Building on the DPO's duty to monitor compliance with data protection law and relevant standards, the paper explores how the DPO operationalizes rights protection through assessment mechanisms such as DPIA, PIA, and LIA. These instruments function as safeguards designed to ensure that no administrative procedure unlawfully infringes or restricts citizens' rights and freedoms. The study highlights the importance of the DPO's independence, including a direct reporting line to senior management, as an essential condition for objective and impartial oversight. It also analyses the DPO's advisory and training mission, aimed at embedding privacy and personal data protection values within the institution as intrinsic components of human rights protection. The findings suggest that, by liaising with supervisory authorities and overseeing information security, the DPO acts as an architect of modern public administration, in which technology both serves and protects human rights.

Keywords: DPO, digital freedom, human rights, DPIA, information security, strategic independence, GDPR compliance.

Introduction

In an era defined by unprecedented technological expansion, the traditional concept of protecting fundamental human rights is undergoing a phase of systemic reconfiguration. The transition from analog interaction to a complex digital identity has shifted the center of gravity of individual freedoms from the simple right to be "left alone" to the imperative need to control one's own informational flows. „Artificial Intelligence (AI) is influencing almost every area of modern life from entertainment, commerce, and healthcare to organizations internal processes operations”¹ and, within this hyper-connected landscape, personal data no longer represent

* National University of Political Studies and Public Administration / Faculty of Public Administration / Doctoral Studies / Bucharest, Romania; cristian-gabriel-nicolae.coman.25@drd.snsa.ro

¹ C. Vrabie, „Artificial Intelligence Promises to Public Organizations and Smart Cities”, 14th PLAIS EuroSymposium on Digital Transformation (PLAIS), 2022, DIGITAL TRANSFORMATION 465, pp.3-14

mere technical attributes but have become digital extensions of human dignity. At the same time, the subject addressed herein constitutes a critical dimension of the in-depth research conducted within my doctoral thesis entitled "Algorithmic Governance in Public Administration: Managerial Constraints and Impact on Human Resources."

While the thesis examines the way in which the automation of decision-making processes reconfigures public management and the accelerated dynamics of human capital, the present article focuses on the protection mechanisms required within this ecosystem, especially since algorithmic governance, by its very opaque and automated nature, is liable to significantly affect human rights, generating risks of discrimination, profiling errors, or the erosion of citizens' decisional autonomy.

Under these circumstances, this paper argues that the function of the Data Protection Officer (DPO) represents the institutional pillar capable of operationalizing the new configuration of fundamental rights protection in the face of algorithms that are increasingly present in everyday life. Beyond being a simple compliance requirement, the DPO acts as a guarantor of digital ethics and as a mediator between algorithmic efficiency and individual freedoms, introducing an active practice of auditing and prevention so that the implementation of algorithmic governance in public administration does not take place to the detriment of the fundamental values of the rule of law. In the words of Jacques Chevallier *„at the heart of the theory of the rule of law lies the principle according to which the various organs of the state may act only by virtue of a legal authorization: any use of material force must be founded on a legal norm; the exercise of authority is transformed into a competence, established and framed by law. To the extent that the organs of the state are thus required to comply with higher legal norms, the rule of law tends to present itself under the formal aspect of the hierarchy of norms”*².

The digital transformation of public administration has accelerated the collection, analysis, and sharing of data about citizens, particularly through integrated platforms, interconnected registries, and online public services. Although this development brings real benefits, such as speed and reduced bureaucracy, it also entails structural risks: the expansion of administrative surveillance, opacity in decision-making, errors propagated through interoperability, and potential discrimination in automated processes.

The independence of the dpo in the architecture of algorithmic governance

From a theoretical perspective, the Data Protection Officer (DPO) is frequently perceived as holding a compliance function, and precisely for this reason the present paper proposes a paradigm shift: the DPO can become an institutional

² Jaques Chevallier, *„Statul de drept”*, Editura Universitaria, Craiova, 2012, p.70 și urm

guarantor of freedom in the digital era, insofar as this function protects citizens' autonomy against excessive processing and supports a model of administration that is responsible, transparent, and open to challenge.

The role of the DPO in monitoring the impact of algorithms on citizens

Within algorithmic governance, the impact of automation extends beyond the sphere of administrative efficiency, reaching the very core of fundamental human rights. The DPO does not merely exercise compliance control but becomes a direct critical observer of the way in which systems using predictive algorithms or models based on artificial intelligence affect citizens through automated administrative decisions. In a data-driven public administration, the DPO has the mission of identifying the risk of bias, also addressed in Article 10(2)(g) of the AI Act³, and of preventing the transformation of algorithmic error into a violation of rights. Thus, the role of the Data Protection Officer is to ensure that the "intelligence" of systems does not suppress the mechanisms for the protection of human rights.

Specialized literature notes that "the data protection officer has a status similar to that of an auditor,"⁴ which once again underlines the importance attached to this role by allocating the necessary resources and providing the independence without which its activity could not yield consistent results. Some scholars argue that „the adoption of AI and algorithmic governance represents a paradigm shift in public administration, necessitating a re-evaluation of institutional frameworks to balance technological efficiency with human-centric values and accountability”⁵, which provides an additional argument in favor of the idea that the DPO is the one who ensures this balance.

DPO vs. Traditional guarantors: a comparative study in the defense of fundamental rights

The protection of human rights is achieved in a democratic society through multiple mechanisms precisely because of the complexity of the subject. Among these, I have selected what are perhaps the most representative roles involved in guaranteeing and ensuring respect for fundamental rights.

Thus, the prosecutor is directly involved in protecting citizens' freedoms, having the role of safeguarding the rule of law and defending the general interests of society, while exercising a coercive and repressive role against criminal offences. At the same time, the prosecutor acts as a filter of legality within criminal proceedings,

³ EU Artificial Intelligence Act, „appropriate measures to detect, prevent and mitigate possible biases identified”

⁴ C.Coman, GDPR în administrația publică, Manual, Editura Economică, București, 2025, p.143

⁵ A. Alakoum, E. Nica și M. Abiad, „AI and Algorithmic Governance in Public Administration: Implications for Faculty Satisfaction, HR Strategies, and Performance Systems in Higher Education”, Administrație și Management Public, nr. 44, 2025, p. 7

ensuring that investigative procedures comply with the fundamental guarantees owed to the persons concerned. In the digital environment, the intervention of the prosecutor is essential for combating cybercrime, including unlawful data processing that reaches the criminal threshold, functioning as a deterrent force against serious abuses capable of destabilizing the security of citizens' digital identity. Also, within the sphere of administrative protection, though in a more specific sense, the Ombudsman has the role of mediating the relationship between citizens and public authorities, with the purpose of correcting bureaucratic dysfunctions without resorting to the coercive force of the courts. Through reports and recommendations issued following complaints, this institution identifies systemic deficiencies and administrative abuse produced ex post, promoting transparency and good administration. In the context of algorithmic governance, the Ombudsman acts as a mechanism of moral and political oversight, drawing attention to cases in which excessive automation leads to the dehumanization of administrative action or to the restriction of citizens' rights through opaque procedures.

The supreme form of jurisdictional protection is vested in the judge, who is the guarantor of the legality and proportionality of any interference by the state in a citizen's private life. By exercising ex post judicial review, the judge has the authority to annul arbitrary administrative acts and to sanction abuses of power, issuing enforceable decisions that restore the rule of law. In the context of the digital era, this role is being reconfigured by the need to interpret classical legal norms in relation to new technological realities, while guaranteeing all citizens equal and effective access to justice and ensuring that the use of automated systems does not violate the right to a fair trial or the principle of non-discrimination. Within the democratic architecture of the protection of fundamental rights, the function of the Data Protection Officer reconfigures the mechanisms of protection by complementing traditional guarantors with a preventive and technological dimension that is indispensable to algorithmic governance. Thus, while the judge represents the supreme guarantor by offering executive jurisdictional protection and ex post legality review, and while the Ombudsman intervenes administratively to correct institutional abuses that have already occurred, the DPO acts proactively and from within the system, operating as an anticipatory barrier against risks, whether physical or digital. Unlike the prosecutor, who exercises a coercive function, the DPO uses auditing and advisory instruments to ensure the compliance of automated processes before they generate harm, thereby providing an opinion that prevents algorithmic opacity from turning into judicial or administrative litigation.

It is precisely this preventive action that highlights how the protection of human rights is being reconfigured, not by replacing the classical figures, but by adding a layer of „by design“ (*„Companies and organizations are encouraged to implement technical and organizational measures from the earliest stages of designing processing operations, in order to guarantee the principle of confidentiality and data*

protection from the outset ("data protection by design"). By default, companies and organizations should ensure that personal data are processed with the highest level of protection - meaning only necessary data, for a short storage period, with limited accessibility - so that, by default, personal data cannot be accessed by an unlimited number of persons ("data protection by default")⁶. This is a layer of protection that neither the prosecutor, nor the judge, nor the Ombudsman can ensure from outside the system.

CRITERION	JUDGE	PROSECUTOR	OMBUDSMAN	DPO
Type of action	Jurisdictional (settles disputes)	Coercive (repressive/prosecutorial)	Administrative (recommendatory)	Audit, advisory, and monitoring
Moment of intervention	Ex post (after the dispute arises)	Ex post (after the act is committed)	Ex post (following a complaint of abuse)	Ex ante and in itinere (preventive)
Positioning	Impartial third party, outside the parties	Party in criminal proceedings (state representative)	Autonomous external institution	Within the organization, but independent
Source of independence	Constitutional	Hierarchical (limited)	Constitutional	Regulatory (GDPR)
Main objective	Application of the law	Limiting criminality	Correcting state abuses	Protecting data and privacy
Relationship with technology	Assesses digital evidence	Identifies cybercrime	Analyses bureaucratic abuses	Architect of Privacy by Design
Triggering of action	Formal (strict procedures)	Ex officio or upon complaint	By petition (free of charge)	Directly (point of contact for citizens)
Role in algorithmic governance	Assess the legality of the final decision	Prosecutes digital fraud	Verifies the transparency of the process	Monitors the risk and impact of algorithms

The autonomy of the DPO as a barrier against external influences

The autonomy of the Data Protection Officer (DPO) represents the foundation upon which the defense of human rights is reconfigured within the architecture of algorithmic governance. In a public administration often subjected to "managerial constraints," such as the need to reduce operational costs through automation or political pressure for the rapid implementation of monitoring systems, the DPO must act as a barrier of integrity. Independence is not merely a legal requirement of the Regulation (*The controller and processor shall ensure that the data protection*

⁶ https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_ro - accesat la 16.03.2026

officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalized by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor”)⁷, but a condition for the survival of human dignity in the face of technological efficiency; without autonomy, the DPO would risk being transformed into an instrument for the formal validation of algorithms that may, by design, be intrusive or discriminatory.

To effectively counteract both external and internal influences, the positioning of the DPO must be insulated from classic hierarchical pressures, allowing this officer to issue negative opinions on projects of algorithmic governance without fear of professional reprisals. In this context, direct reporting to the highest level of management becomes a mechanism for the protection of the citizen, so that the risks identified in triage or profiling processes are addressed at a strategic rather than merely technical level, thereby transforming compliance from an administrative cost into a guarantee that digitalization is not achieved through the sacrifice of fundamental freedoms. While management is oriented toward quantifiable results and performance indicators, the DPO evaluates the impact of those indicators, protecting citizens against the invisible errors of opaque algorithms. Structural independence is what gives the DPO function a force similar, in spirit, to that of traditional guarantors, yet with immediate and technical applicability within the digital “engine” of the new public governance.

There are scholars who consider that “this independence is necessary in order for the DPO to be able to provide objective recommendations and assessments, without the risk of being constrained by the commercial or political interests of the entity within which he or she operates.”⁸. For this very reason, Article 38(3) GDPR provides that *„the controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalized by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor”*⁹

Instruments for the reconfiguration of protection

The reconfiguration of the protection of human rights in the era of algorithmic governance cannot be reduced to mere declarations of principle; rather, it requires a set of technical and legal instruments that function as filters of ethics and legality.

⁷ 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), Art.38, alin.3

⁸ C.Coman, „GDPR în administrația publică, Manual”, Editura Economică, București, 2025, p.143

⁹ <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>

The DPO is not merely a data expert, but a true “architect of digital ethics,” whose independence and instruments (DPIA, LIA, PIA) guarantee that the transition toward an intelligent public administration is not achieved through the sacrifice of fundamental freedoms, but through their consolidation in a form adapted to contemporary technological developments.

The central instrument is the Data Protection Impact Assessment (DPIA), which must not be seen as a bureaucratic document, but as a process for auditing the “morality” of technology. Through the DPIA, the DPO analyses the origin of the data, the logic of the algorithm, and the probability that it may generate discriminatory decisions. It is absolutely necessary to identify the “breaking points” at which the state’s interest in optimizing resources through technology begins to infringe individual autonomy, with the aim of creating a rigorous methodology for mitigating risks before the system is implemented. The reconfiguration of protection through the specific instruments of the DPO responds to a profound transformation in public administration.

As institutions evolve toward “system-level bureaucracies,” traditional forms of control centered on the official become insufficient. As Bovens and Zouridis (2002) emphasize, we are witnessing a mutation of constitutional control: *the focus of constitutional and administrative control shifts from the individual official to the system. In system-level bureaucracies, it is no longer the street-level bureaucrat who should be the primary object of legal and democratic control, but the system of rules and the technical infrastructure that produces the decisions.*¹⁰

In this new context, instruments such as the Data Protection Impact Assessment (DPIA) are no longer mere compliance procedures, but become the mechanisms through which this “system of rules” and the technical infrastructure are examined from the perspective of respect for fundamental rights. By using these instruments, the DPO reconfigures the defense of the citizen by shifting legality review from the phase of execution of the administrative act directly into the algorithmic architecture of the system.

The need to make processes more efficient may lead to the rapid introduction of predictive algorithms. Unfortunately, without sufficient analysis of the way in which these algorithms may determine the making of a decision, they constitute a major risk factor, whether of discrimination or error of judgment, most often due to the way AI systems have been trained.

Complementarily, the Legitimate Interest Assessment (LIA) becomes an exercise in balancing the efficiency of algorithmic governance against the citizen’s fundamental rights, because it enables the DPO to identify those “breaking points” at which the state’s interest in optimizing resources through technology begins to

¹⁰ M. Bovens și S. Zouridis, *From Street-Level to System-Level Bureaucracies: How ICT is Transforming Administrative Discretion and Constitutional Control*, *Public Administration Review*, vol. 62, nr. 2, 2002, p. 20

infringe individual autonomy, thus offering the opportunity to mitigate risks before the system is implemented.

Faced with opaque “black box” systems, the protection of human rights is reconfigured through the imposition of an obligation to explain the logic of decision-making, the role of the DPO being to guarantee the citizen the right to understand how a decision concerning him or her was generated, so that the individual does not remain merely a passive subject of a computerized outcome.

The integrity of fundamental rights is inseparably linked to information security, which transforms the monitoring of security management systems from a technical task into a form of protection of digital identity. In this context, the Data Protection Officer becomes the key actor who must design the flows through which citizens’ data do not become vulnerable to unauthorized access or abusive use - a true protective “shield” that allows the right to private life to exist within the digital ecosystem of intelligent public administration.

Moreover, digital integrity presupposes a convergence between cybersecurity and the ethics of processing, where continuous monitoring operates as a mechanism for auditing the “health” of public governance. In an administrative ecosystem defined by interoperability and massive data flows, any security breach may generate a domino effect upon the autonomy of the data subject, leading to insidious forms of exclusion or algorithmic discrimination. Consequently, the DPO reconfigures the protection of human rights by transforming security standards into norms of ethical conduct, while also constantly verifying that the institution is capable of resisting internal or external pressures that might compromise the confidentiality and availability of data.

Conclusions

Given the increasingly accelerated evolution of technologies, the reconfiguration of the protection of human rights in the twenty-first century depends directly on the effectiveness of the DPO function within the new forms of algorithmic governance. The DPO is not merely a data expert, but a genuine “architect of digital ethics,” whose independence and instruments (DPIA, LIA) prepare the transition toward an intelligent public administration not by sacrificing fundamental freedoms, but by consolidating them in a new form adapted to contemporary technological developments.

Human oversight is absolutely necessary, and *„the power of algorithmic systems to shape human behavior and social outcomes demands a robust framework of accountability, ensuring that such regulation remains subject to human oversight and democratic contestation”*¹¹. The Data Protection Officer therefore represents the

¹¹ L. Andrews, B. Benbouzid, J. Brice, L. A. Bygrave, et al., *„Algorithmic Regulation”*, Discussion Paper No. 85, Centre for Analysis of Risk and Regulation, London School of Economics and Political Science, 2017, p. 14

necessary “human factor” through which algorithmic governance may remain compatible with the values of democracy and the protection of fundamental rights.

Ultimately, the present research underlines that the success of the transition toward an intelligent public administration depends on the institutional capacity to maintain a fragile balance between innovation and ethics. As substantiated in the JuLIA Project Handbook (2025), the central challenge in the implementation of AI by public authorities is to ensure that the efficiency of processes does not undermine the citizen’s fundamental guarantees, since: *„the core challenge in the deployment of AI by public administrations is to ensure that the pursuit of efficiency does not override the fundamental right to good administration, which requires that every person has the right to have his or her affairs handled impartially, fairly and within a reasonable time by a human-led oversight mechanism.”*¹²

Therefore, the reconfiguration of the protection of human rights through the DPO function is not merely a technical option of compliance, but an imperative democratic necessity. The DPO thus becomes a guarantor of the protection of fundamental human rights, operating as a critical barrier against the risk that algorithmic governance may become arbitrary or unjust due to the lack of adequate human control over automated systems and their decisions.

The effectiveness of the DPO function in intelligent public administration goes beyond the sphere of legal compliance, becoming an essential pillar for maintaining citizens trust in institutions. In an environment governed by automated processes, the legitimacy of the state is reconfigured through the way these systems are supervised. As Parviainen et al. (2025) observe, the foundations of institutional trust have shifted from the sphere of service quality to the sphere of algorithmic ethics: *„in the era of algorithmic governance, institutional trust is no longer solely based on the quality of public services, but increasingly on the transparency, fairness, and accountability of the automated systems that mediate the relationship between the citizen and the state.”*

The role of the DPO in ensuring the transparency and accountability of algorithmic systems does not merely protect personal data; it protects the very democratic relationship between citizen and state. Without the auditing and control mechanisms exercised by the DPO, algorithmic governance risks eroding the capital of trust necessary for the proper functioning of modern public administration and may ultimately lead to an institutional deadlock that is difficult to manage.

¹² A. Colombi Ciacchi, M. L. Flórez Rojas, L. Lane și T. Nowak (eds.), „JuLIA Handbook. AI and Public Administration: The (legal) limits of algorithmic governance”, Proiect JuLIA (Justice, Fundamental Rights and Artificial Intelligence), 2025, p. 115.

Bibliography

Specialized Literature

Chevallier, Jaques, *Statul de drept*, Editura Universitaria, Craiova, 2012;

Coman, Cristian, *GDPR în administrația publică, Manual*, Editura Economică, București. 2025

Studies and Articles

Alakoum, Alice, Nica, Elvira și Abiad, Mohammad, *AI and Algorithmic Governance in Public Administration: Implications for Faculty Satisfaction, HR Strategies, and Performance Systems in Higher Education*. *Administrație Și Management Public*, nr. 44, 2025;

Andrews, Leighton, Benbouzid, Bilel, Brice, Jeremy, Bygrave, Lee A., et al. *Algorithmic Regulation*. Discussion Paper No. 85, Centre for Analysis of Risk and Regulation, London School of Economics and Political Science, 2017, 49 pp. ISSN: 1740-164X

Bomvens, Mark și Zouridis, Stavros, *From Street-Level to System-Level Bureaucracies: How ICT is Transforming Administrative Discretion and Constitutional Control*. *Public Administration Review*, vol. 62, nr. 2, 2002;

Colombi Ciacchi, Aurelia, Florez Rojas, María Lorena, Lane, Lottie și Nowak, Tobias (eds.). *JuLIA Handbook. AI and Public Administration: The (legal) limits of algorithmic governance*. Proiect JuLIA (Justice, Fundamental Rights and Artificial Intelligence), European Union's Justice Programme, 2025

Vrabie, Cătălin, *Artificial Intelligence Promises to Public Organizations and Smart Cities*, 14th PLAIS EuroSymposium on Digital Transformation (PLAIS), 2022, DIGITAL TRANSFORMATION 465, pp.3-14

Web Resources

<https://artificialintelligenceact.eu/>

https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_ro

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679>

<https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>