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.

2024, Volume 11, Issue 2, pages: 15-22 | https://doi.org/10.18662/eljpa/11.2/227

Personal Data Protection in the Digitalization Process of the Public Administration

Andreea BURUIANĂ (m. RUSU) [1]

[1] PhD candidate Titu Maiorescu Doctoral School of Law of Bucharest, Romania; Assistant Professor, Stefan cel Mare University of Suceava, Faculty of Law and Administrative Sciences. ORCID iD: https://orcid.org/0009-0000-1535-7270

Abstract: *Regulation (EU) 2016/679 on the safeguarding of personal data and the free flow of such information, applies not only to organizations in the digital sector but also to public authorities, which must comply with it. Currently, the flow of data between public authorities is continuously increasing, presenting new challenges in managing this data. One of the main difficulties faced by public authorities is the inability to store and process large amounts of data, which leads them to collaborate with private companies. While it is possible that the data is protected, there is no guarantee that the measures taken by private companies are sufficient to ensure complete protection.*

Keywords: *principle of transparency, eGovernment, public authorities, protection, personal data.*

How to cite: Buruiană, A. (2024). Personal data protection in the digitalization process of the public administration. *European Journal of Law and Public Administration, 11*(2), 15-22. https://doi.org/10.18662/eljpa/11.2/227

©2024 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

Data processing is the cornerstone of the working apparatus of the central public administration. Public administrations must collect all the data necessary in the cumbersome process of issuing decisions and legislative documents, which must be at the same time correct from the information point of view but also from a legal perspective. The lack of data leads to incorrect and erroneous decisions and the processing of invalid documents. In this context, administrative authorities sometimes collect and manage an infinite number of data necessary for the preparation and processing of documents.

These data processed, transferred, and held by the authorities fall into the category of personal data and implicitly under the incidence of legislation specific to this field. The holders of these data are central or local public administrations, which manage them for specific administrative procedures and institutional purposes, even in the absence of a defined procedure for their use. For instance, public administrations collect and retain health and tax data, even if no complaint or appeal has been filed regarding such information. A similar approach applies to spatial data, which encompasses any type of information directly or indirectly connected to a specific location or geographical area. Public administrations gather this data as part of their evaluation and monitoring of activities involving satellites and spacecraft operated by various states.

With the entry into force of Regulation (EU) 2016/679 in 2018, concerning the protection of individuals regarding the processing of personal data and the free movement of such data, it was established that its scope extends beyond private organizations collecting personal data. In addition to the private sector, the regulation also applies to public administration, namely public institutions of the state. Thus, public authorities are obliged to comply with the new regulations, given that the flow of data between them is constantly expanding.

Although data protection regulations apply to both public administrations and private entities and individuals, the primary purpose of public administrations to protect the general interest justifies the right to data protection. This requires an analysis of the specific compatibility with other rights and legal situations, in particular when public administrations communicate or disseminate information, given their obligation of transparency.

One of the biggest challenges in the collection and transfer of data by public authorities is the difficulties of storing and processing it, which leads to collaborations with private companies to support these processes.

This raises the question of whether a private company can collect, store and transfer personal data from public authorities and, more importantly, whether this data is adequately protected. The answer is yes, but we cannot say with certainty that the data is effectively protected, as the current guarantees are not robust enough to cover legislative gaps or vulnerabilities to cyberattacks.

Challenges of the GDPR regulation in the public sector

The management of information between the institutions, bodies, offices, and agencies of the European Union, on one side, and the authorities of the Member States, on the other, has led to an increasing number of information exchange networks within the field of public administration.

With regard to the challenges faced by the public administration of the Member States or of the European Union (Law no. 190 from 18 july 2018), it is important to underline that public authorities have both rights and specific obligations conferred by the GDPR, which may differ from those applicable to private entities.

In the public sector, the responsibility is much greater, given the need to store personal data, but also their transfer. In addition, there is also specific legislation of each Member State that must be aligned with the principles of the GDPR (Bieker et al. 2024, 69).

The implementation and compliance with the GDPR in the public sector generates a number of specific challenges, due to the complexity of the activities of public authorities and the nature of the data processed. Here are some of the most important challenges:

Managing large volumes of personal data

Public authorities process a significant amount of personal data, including sensitive data, to perform their functions and provide services to citizens. In this context, implementing data protection measures effectively and in accordance with the GDPR can be challenging, especially in terms of: • Storing and managing data in a secure manner. • Ensuring controlled access to data. • Implementing procedures for archiving and deleting data in accordance with the terms regulated by the GDPR.

The need to respect the principles of transparency and information

The GDPR imposes on public authorities the obligation to clearly inform citizens about how their data is collected, processed and stored. This can be complicated, especially when there are multiple databases or integrated services, and communication with the public must be clear, accessible and easy to understand for all categories of citizens.

In the European Union, Directive 2003/98/EC on the reuse of public sector information and Regulation (EU) 2016/679 on personal data protection (GDPR) play a crucial role in ensuring transparency and access to accurate information. At the national level in Romania, Law No. 544/2001 on free access to public interest information establishes citizens' rights to request and obtain information from public institutions.

Respecting the principle of transparency and information in public administration is essential for strengthening the democratic system and for ensuring public control over the activity of authorities. The correct implementation of these principles not only supports good governance, but also contributes to the development of a climate of trust between citizens and state institutions.

Consent and legitimation of data processing

While consent may serve as a valid basis for data processing, in the public sector, other legal grounds are more commonly relied upon to legitimize the processing of personal data. These include fulfilling a legal obligation or acting in the public interest, as outlined in Article 6(1)(c) and (e) of the Regulation.This raises difficulties in the correct application of the regulation, especially in establishing the correct legal grounds for processing different types of data (Suksi, 2023, 34-36).

According to the GDPR, data processing in the public sector is typically justified by one of the following legal grounds: 1) the performance of a task in the public interest or based on public authority (Article 6(1)(e) GDPR). This is by far the most common reason for data processing in the public sector, where public authorities may process citizens' personal data for law enforcement, the administration of public services, or the management of administrative procedures, without the need for explicit consent from individuals; 2) the fulfillment of a legal obligation (Article 6(1)(c) GDPR), as many public authorities have legal duties to collect and process personal data, such as tax obligations, social security requirements, or public health protections. These obligations are set by law and do not require consent from citizens; 3) the protection of vital interests of the data subject or others (Article 6(1)(d) GDPR), which refers to situations where

data processing is necessary to safeguard someone's health or fundamental rights, such as in medical emergencies; 4) the legitimate interests of the public authority or a third party (Article 6(1)(f) GDPR), where public authorities may process data to achieve legitimate purposes, as long as these interests do not outweigh the fundamental rights and freedoms of the individuals whose data is being processed.

Public institutions are required to ensure that the processing of personal data is conducted securely, safeguarding it against unauthorized or unlawful access, as well as accidental loss, destruction, or damage. This can be achieved through the implementation of suitable technical and organizational measures designed to protect the data effectively.

Cybersecurity challenges

Public authorities are frequently targets of cyberattacks and other security incidents. Implementing effective technical and organizational measures to protect data is crucial, though it can be challenging due to limited resources or the complexity of IT infrastructure in the public sector. Some public agencies also face outdated IT infrastructures, which can make implementing the GDPR requirements more difficult.

Insufficient resources and training

Many public authorities, especially at local level, have limited financial and human resources to fully implement the measures required by the GDPR. Public sector staff may also not be sufficiently trained on GDPR requirements, and continuous training and specialization are essential to ensure compliance.

Coordination between institutions and authorities

The public sector often involves multiple entities that process data collaboratively, such as ministries, government agencies, local authorities and education or health institutions at Member State level as well as at EU central public authorities. Coordination between these entities to ensure GDPR compliance can be a complex process, especially when data is shared between different public entities.

Conflicts between data protection and government transparency

In the public sector, there is often a conflict between the requirements of the GDPR and the principle of government transparency. For example, some information that should be accessible to the public (according to the legislation on access to information in the public interest)

may contain personal data protected by the GDPR, which requires authorities to find a balance between the principle of transparency and data protection (Pasquier & Acatrinei, 2018).

Data Protection Impact Assessment (DPIA)

Public authorities must carry out Data Protection Impact Assessments (DPIA) for certain data processing activities. These assessments can be complex and time-consuming, especially when public authorities implement large projects involving the collection and processing of sensitive data.

Respect for citizens' rights

The GDPR regulation grants citizens several rights, including the right to access their data, the right to correct or delete it, and the right to data portability. In the public sector, handling requests for these rights can be complex, particularly when authorities process large volumes of personal data across multiple systems.

Digitalization and integration of new technologies the biggest challenge of the public domain

The public sector is currently undergoing digitalization and the integration of new technologies, such as big data and artificial intelligence, which pose new challenges in the area of personal data protection. The implementation of these technologies must align with the principles of the GDPR and ensure a high level of data security, requiring advanced technical expertise.

A crucial aspect of the streamlining process in public institutions is digitalization. In public administration, digitalization offers numerous advantages that should be incorporated into institutional strategies and actively promoted by leadership. On the one hand, it streamlines institutional operations, resulting in more efficient resource use, cost reductions, and the institution's contribution to technological and socio-economic progress. On the other hand, digitalization creates new opportunities by leveraging institutional capabilities to provide citizens with innovative public services.

It is essential for public authorities to pay close attention to individuals' requests regarding access to their personal data. According to the General Data Protection Regulation (GDPR), individuals have the right to contact public administrations to exercise their rights to access, rectify, erase, restrict processing, object, and the right not to be subject to automated decision-making (Regulation (EU) 2016/679).

Individuals also have the right to object to the processing of their data by public authorities, even if the processing is based on a public interest. In such cases, the individual must provide specific reasons justifying their request. The public administration may continue processing the data and reject the request only if it can demonstrate that there are legitimate and compelling reasons for the processing, which outweigh the individual's rights and interests, or if the data are necessary for defending a right in court.

For example, when a company processes an individual's personal data using automated means, based on consent or a contract, the individual may request that the data be transferred directly to another company, as long as it is technically feasible. However, this right does not apply when the data are necessary for the performance of a legal obligation by public authorities or other organizations acting in the public interest. For instance, when an individual provides data to apply for social benefits or a building permit, they cannot request the public authority to transmit the same data to another entity. (Baltac, 2024)

As regards the response time, the public administration is obliged to respond to requests from individuals without undue delay and, as a general rule, within one month of receiving the request. It may request additional information to verify the identity of the applicant. In the event of a refusal, the individual must be informed of the reasons behind the rejection of the request and their right to lodge a complaint with the National Data Protection Authority (DPA) or to take legal action.

The digitalization of public administration, with its intricate data management networks, holds great promise for increasing the efficiency of public services and improving service delivery to citizens. However, this development also presents challenges related to confidentiality and data protection.

Conclusions

The GDPR is a directly applicable legal instrument, intended to establish in detail the rights of the natural persons concerned and the obligations of data controllers, regardless of whether this concerns the private or public domain. The main purpose being to prevent national legislators from interpreting and reinterpreting legal texts in order to interpretively align administrative procedures with the provisions of the regulation. At the same time, the GDPR provides for minimum guarantees for automated administrative procedures by indicating their content and direction.

More than 6 years after the application of the General Data Protection Regulation in Romania, public authorities and institutions have made progress in implementing and enforcing the rules. However, there is a lack of official statistics or concrete measures from the National Supervisory Authority for the Processing of Personal Data. Difficulties still persist regarding the grounds for processing, especially when the principle of data minimization is invoked.

Adapting administrative law to the needs inevitably implied by the digitalization of public authorities and the use of new technologies would be a response to the issue of implementing the provisions of the GDPR regulation in the field of public administration. For instance, the management and exchange of information during the initial phase of an administrative procedure must take into account that today, this information is no longer stored in physical files held by public administrations, but on electronic platforms, which may sometimes be managed by private entities. Thus, national databases can end up sharing personal data outside the national jurisdiction in order to fulfill administrative duties. Hence the issue of data transfer between different entities or different jurisdictions.

References

Baltac, V. (2024). *Transformarea digitală a administraţiei publice.Strategii de eGuvernare*, Editura Excell Book

Bieker F., Schiering I., Jensen M., Gruschka N., Conca S. (2024). *Privacy and Identity Management. Sharing in a Digital World.* Springer Nature, 69. https://link.springer.com/book/10.1007/978-3-031-57978-3

Law No. 190 of July 18, 2018 on the implementation measures of Regulation (EU) 2016/679 of the European Parliament and the Council of April 27, 2016. https://legislatie.just.ro/Public/DetaliiDocument/203151

Law No. 544 of 12 October 2001 regarding the free access to information of public interest. Official Gazette of Romania No. 663 of 23 October 2001. http://www.madr.ro/docs/english/law_544.pdf

Pasquier, M., Acatrinei, N. (2018). *Comunicarea Organizaţiilor Publice*, Editura Universităţii din Bucureşti. 75-76. https://editura-unibuc.ro/comunicarea-organizatiilor-publice/

Regulation (EU) 2016/679 on the protection of individuals with regard to the processing of personal data and the free movement of such data. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

Suksi M. (2023). *The Rule of Law and Automated Decision-Making.Exploring Fundamentals of Algorithmic Governance*. Springer International Publishing.