Scientific Papers Series Management, Economic Engineering in Agriculture and Rural Development
Vol. 23, Issue 3, 2023
PRINT ISSN 2284-7995, E-ISSN 2285-3952

MANAGEMENT OF PERSONAL DATA PROCESSING AND PROTECTION

Elena COFAS

University of Agronomic Sciences and Veterinary Medicine Bucharest of Bucharest, 59 Marasti Boulevard, District 1, 011464, Bucharest, Romania, E-mail: cofas.elena@managusamv.ro

Corresponding author: cofas.elena@managusamv.ro

Abstract

This article emphasizes the crucial significance of personal data and the potential dangers arising from its unauthorized processing, which can violate an individual's basic rights and freedoms. To address these worries, the European Union has implemented a comprehensive regulatory structure, widely recognized as the General Data Protection Regulation (GDPR). In the domain of data privacy and security, personal data is defined as encompassing any information with the capacity to identify an individual, whether it be anonymized, encrypted, or pseudonymized data. The regulatory purview of GDPR spans all modes of data processing, automated or manual, and remains indifferent to the storage medium or technology employed. Illustrative examples of personal data comprise an individual's name, identification number (like a CNP), location data (such as GPS coordinates), online identifiers (for instance, specific types of cookies), and a diverse array of attributes pertaining to an individual's physical, physiological, genetic, psychological, economic, cultural, or social identity. This classification also encompasses information such as IP addresses, email addresses, or residential addresses. It is of utmost importance to acknowledge that personal data, whether examined in isolation or in conjunction with other data elements, retains the potential to unveil the identity of an individual. This paper expands the scope of analysis to critically assess the multifaceted implications of GDPR within the contemporary landscape of data privacy and security, with a specific focus on its relevance within the realm of management practices. The examination encompasses an in-depth exploration of the foundational principles of GDPR, its legal framework, and its global impact across businesses, individuals, and regulatory bodies. Additionally, the study delves into the complexities associated with GDPR compliance, illuminating the evolving dynamics of data protection within an increasingly digitized world. It emphasizes the essential role played by effective management strategies in addressing these challenges.

Key words**:** *personal data, GDPR, organization, legality*

INTRODUCTION

The safeguarding of natural persons' personal data processing is a fundamental right protected by Articles 7 and 8 of the Charter of Fundamental Rights of the European Union [1], Article 16 of the Treaty on the Functioning of the European Union (TFEU) [14], and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms [4]. A significant milestone in European data protection regulations occurred in 2016 when the European Parliament and the Council adopted the General Data Protection Regulation (GDPR), which became directly applicable in all European Union member states from May 25, 2018. This regulation was complemented by the Directive on the protection of natural persons in the context of criminal offense prevention, investigation, detection, prosecution, or execution of criminal penalties, ensuring the free movement of such data [3]. In the digital age, the protection of personal data is a serious topic on the agenda of every organization (institution or entity). GDPR, the European regulation that came into effect in Romania on May 25, 2018, provides citizens with increased control over their identifiable data. Since its implementation, several organizations have faced sanctions for illegally processing personal data of natural persons. The National Authority for the Supervision of the Processing of Personal Data (ANSPDCP), as an autonomous central public authority with general competence in the field of personal data protection, represents the guarantor of respect for the fundamental rights to private life and the protection of personal data, stipulated by the

articles mentioned in the first paragraph [9]. Thus, people dissatisfied with the way an organization processes their data have the right to file a complaint with the ANSPDCP (which can also be filed ex officio) and to go to court to obtain compensation.

Protecting personal data is one of the most important responsibilities of an organization or entity, there are many reasons why this responsibility must be taken seriously, including:

✓ *people's trust* – if their data is not properly protected, trust can be lost;

✓ *reputation* – failure to protect personal data can damage the organization's reputation and lead to unpleasant situations for both parties;

✓ *increasing opportunities* – excellent data protection is a way to stand out from the competition;

✓ *prevention of harm* – the misuse of personal data can harm the people involved, this situation can also lead to identity theft or fraud;

✓ *legal compliance* – compliance with privacy and data protection laws is essential in every jurisdiction. Such laws exist globally, but the European Union's General Data Protection Regulation (GDPR) stands out as the most rigorous and intricate regulation in this domain. Neglecting data protection could lead to investigations from regulatory bodies, sanctions (including criminal penalties), or legal action.

✓ *compliance with contractual conditions* – when organizations receive personal data from others, the contracts they have in place may obligate them to ensure the protection of that data.

The primary objective of this academic paper is to conduct a comprehensive and critical analysis of the GDPR concerning contemporary data privacy and security, with a particular emphasis on its relevance within the field of management practices. Enacted in 2018, the GDPR has triggered a significant shift in how organizations gather, process, and safeguard the personal data of European Union citizens.

At the same time, this paper aims to provide a comprehensive grasp of the fundamental principles and legal framework underpinning GDPR, along with its global ramifications for businesses, individuals, and regulatory entities, while underscoring the pivotal role that effective management plays in ensuring compliance and robust data protection. Furthermore, this analysis sheds light on the evolving landscape of data protection in an increasingly digitized world and underscores the essential nature of proficient management strategies in addressing these challenges. By delving into the nuances of GDPR and its implications for management, this paper seeks to offer valuable insights contributing to the ongoing discourse surrounding data privacy, regulation, and the governance of organizations.

MATERIALS AND METHODS

As the General Data Protection Regulation (GDPR) continues to exert its profound influence on the intricate domain of data privacy, it becomes increasingly imperative to embark upon rigorous academic inquiries aimed at comprehending its multifaceted dimensions and rigorously assessing its tangible real-world ramifications.

This scholarly paper endeavors to furnish an exhaustive scrutiny of GDPR compliance, delving into the regulatory framework and its pragmatic consequences. In the pursuit of this scholarly goal, a systematic approach has been embraced, which encompasses a diverse spectrum of sources and research methodologies. The bedrock of this research endeavor resides in the triangulation of primary and secondary sources, thereby ensuring a holistic and comprehensive exploration of the intricate facets inherent to the GDPR.

The following sources were used for the creation of this article:

✓ *Primary sources: this study rests the authoritative text* of the GDPR itself, which is complemented by official documents and guidelines disseminated by data protection authorities and regulatory bodies operating within the European Union. These primary sources serve as the fundamental cornerstone for the analysis of this framework, presenting an unadulterated reflection of the legislative

intent and the operational intricacies underpinning the GDPR.

✓ *Secondary sources*: These sources include academic journals and scholarly volumes authored by experts in the field of data protection law, and reports from esteemed institutions and consulting firms. The insights garnered from these secondary sources, along with the varied perspectives and nuanced interpretations of the GDPR, enhanced the analysis by providing contextual depth to the GDPR's impact across a spectrum of stakeholders.

Moreover, in order to remain attuned to the evolving nature of GDPR and to glean real-time insights, websites have been consistently monitored. Reputable websites, including those maintained by the European Commission, data protection authorities, and reputable news sources, have been regularly consulted for updates, case studies, and relevant reports. These online sources provided critical information to contextualize the analysis within the dynamic landscape of GDPR compliance.

The methodology employed in this study is grounded in the amalgamation of legal analysis and ethical dimensions, thereby establishing a comprehensive framework for the examination of compliance with the General Data Protection Regulation (GDPR).

The management-oriented methodology for GDPR offering pragmatic strategies for organizations to harmonize data management practices with the stipulations of the GDPR. The ethical considerations are intricately interwoven throughout the research process, engaging with salient inquiries pertaining to data privacy, transparency, and societal ethics.

RESULTS AND DISCUSSIONS

A. The fundamental terms of personal data

Personal data can be classified into two categories [10]:

→ ***Personal identification data*** - is information that is related to an identified person or that can be identified with a person, being also called "personal identifiable information". Some examples of personal data are the name and surname of a person, date of birth, home address, e-mail address, telephone number, marital status, photo of the face (image), voice, profession, habits and preferences, identifiers online and any other data related to the physical, physiological, economic, financial, cultural or social identity, which can be used for the direct or indirect identification of a natural person.

→ ***Sensitive data*** - is information that is much more protected than other types of data, which must benefit from special protection.

Sensitive data includes personal information that discloses one's racial or ethnic background, political affiliations, religious or philosophical beliefs, membership in trade unions, genetic details, biometric data for human identification, health-related information, and details about an individual's sexual life or orientation.

In general, the processing of this type of data is prohibited, but it is allowed only in certain exceptional situations, strictly provided by law (for example, when the data is necessary for the conclusion of an employment contract or the provision of medical services).

The following list contains the GDPR - compliant [6] definitions of the phrases used in this paper:

- "personal data" refers to any information related to a natural person, whether identified or identifiable. An identifiable individual is someone who can be directly or indirectly recognized, typically through elements such as a name, identification number, location data, online identifier, or specific physical, physiological, genetic, psychological, economic, cultural, or social characteristics;
- "processing" encompasses any activity conducted on personal data, whether automated or not. This includes actions like gathering, recording, organizing, storing, adapting, modifying, extracting, consulting, using, transmitting, sharing, disseminating, aligning, combining, restricting, deleting, or destroying the data.;
- "*data subject"* is any natural person whose data may be processed;
- "*special categories of data"* are data about the racial and ethnic origin, political opinions, religious or philosophical beliefs, membership in certain organizations, data about criminal

record, or the health and sexual orientation of the data subject;
- "*restriction of processing"* means the marking of stored personal data so as to limit their future processing;
- "*data record system"* means any structured set of personal data accessible according to specific criteria, be they centralized, decentralized, or distributed according to functional or geographical criteria;
- "*data controller*" refers to an individual or legal entity, public authority, agency, or any other organization that, either independently or in collaboration with others, defines the objectives and methods of processing personal data. This term also includes organizations and entities engaged in processing personal data;
- "*data processor*" is an individual or legal entity, public authority, agency, or any other organization that handles personal data on behalf of the data controller;
- "*data protection officer* (DPO)" is the person appointed by the data controller to ensure that the organization complies with relevant data protection laws and regulations;
- "*recipient*" refers to the individual or legal entity, public authority, agency, or any other organization to whom personal data is revealed, regardless of whether they are a third party or not;
- "*third party*" denotes an individual or legal entity, public authority, agency, or organization apart from the data subject, the data controller, the data processor, and individuals authorized by the data controller or data processor to handle personal data under their direct supervision;
- "*transmission*" refers to the disclosure of safeguarded personal data from the accountable entity to a third party;
- "*consent*" from the data subject implies any clear, specific, informed, and voluntary expression of the individual's will, either through a statement or a clear action, indicating acceptance for the processing of their personal data;
- "*breach of personal data security"* means a breach of security that leads, accidentally or unlawfully, to the destruction, loss, alteration, or unauthorized disclosure of personal data transmitted, stored or otherwise processed, or to unauthorized access to them;
- "*genetic data"* means the personal data relating to the inherited or acquired genetic characteristics of a natural person, which provide unique information regarding the physiology or health of that person and which results in particular from an analysis of a sample of biological material collected from the data subject;
- "*biometric data*" refers to personal information obtained through specialized processing methods concerning the physical, physiological, or behavioural traits of an individual. These traits enable or confirm the distinct identification of that person, such as facial images or fingerprint data;
- "*health data*" includes personal information pertaining to the physical or mental well-being of an individual, encompassing the provision of healthcare services. It reveals details about a person's health condition;
- "*enterprise"* means a natural or legal person carrying out an economic activity, regardless of its legal form, including partnerships or associations that regularly carry out an economic activity;
- "*data protection authority (DPA)"* means an independent public body established by a member state that has the responsibility to conduct investigations and take corrective action as necessary to ensure that the data protection rules are being followed.

B. Management of personal data

The management of personal data includes all information related to the rights of data subjects, the principles of the GDPR and the legal grounds on which all operations on personal data must be based.

(a) Rights

GDPR offers the data subject several rights, which can be exercised in relation to the data controller, by submitting a request in this regard [13]. The data controller cannot ignore this request, and it must be solved and answered within the legal term established by GDPR - one month from the receipt of the request, but it can be extended by another two months when the request is complex.

The rights that the data subject has according to GDPR are the following:

the right to be informed which requires individuals to receive information about the data being processed, including details such as what data is involved, the reasons for processing, the intended purposes, recipients of the data, and the individual's rights;

→ *the right of access* which grants individuals the ability to access their data, with the data controller obligated to provide the data subject with this access;

→ *the right to rectification* which enables individuals to correct incomplete or inaccurate information related to them;

→ *the right to erasure ("to be forgotten") which* allows individuals to request the deletion of personal data in certain situations;

→ *the right to restriction of processing* which grants the data subject the ability to request and obtain limitations on personal data processing in specific cases;

→ *the right to data portability* which enables individuals, in certain instances, to request and obtain the transfer of their personal data;

→ *the right to object* which gives individuals the authority to oppose processing when valid grounds exist;

→ *the right not to be subject to an automated decision, including profiling* which allows individuals to avoid being subjected to automated decisions, including profiling. If such a decision significantly affects them, they have the right to challenge it and request human intervention;

→ *the right to lodge a complaint with the national Data Protection Authority* which offers the data subject the possibility to file a complaint with the National Data Protection Authority if they are unhappy with how their data is being processed or if their rights have not been upheld.

→ *the right to take legal action against a company/organisation* where an individual has the right to initiate legal proceedings to seek compensation, both material and moral, for damages incurred due to the unlawful processing of personal data.

(b) GDPR principles

Any organization that processes personal data must comply with the key principles introduced by the GDPR [5]:

The principle of legality, fairness and transparency

This principle dictates that personal data should be processed in a lawful, just, and transparent manner concerning the data subject.

- the principle of legality assumes that the data must be processed in accordance with the law and fall under at least one of the legal grounds for processing from Art. 6 GDPR (consent, contract, legal obligation, vital interest, public interest and legitimate interest). The legality of the processing of special data must comply with certain additional requirements.
- the principle of fairness means that personal data cannot be processed in unfair, immoral ways or in ways that could harm data subjects.
-the principle of transparency means that individuals must know how an organization processes their data. Thus, the data controllers must optimally inform the data subject about how they process his data - prior to data collection - and facilitate the exercise of his rights.

The principle of purpose limitation

The purposes of data collection and processing must be determined, explicit and legitimate. The GDPR prohibits personal data from being processed for other purposes incompatible with the original purposes. In such a situation, being an incompatible purpose, the processing of personal data for the new purpose will not be legal.

The principle of data minimization

This principle assumes that the data controller processes only the minimum amount of data to achieve their goals, i.e. no more data than they need. Indeed, the data should be sufficient, pertinent, and restricted to what is necessary for the intended processing purposes.

The principle of accuracy

Personal data must be precise, comprehensive, and current. Any inaccurate data must be promptly deleted or corrected.

The principle of storage limitations

The data must be stored in a format that permits the identification of data subjects for a

duration not surpassing the period required to fulfill the processing purposes. Any subsequent storage or archiving of this data must comply with legislation, ensuring compatibility with the initial collection purpose and incorporating technical security measures to prevent unauthorized processing.

The principle of integrity and confidentiality

The data must be processed in a way that ensures adequate security of personal data, including protection against unauthorized or unlawful processing and accidental loss, destruction or damage, by taking appropriate technical or organizational measures (for example to put in place measures and protocols to safeguard personal information).

The principle of accountability

The data controller is solely responsible for complying with the above principles and implementing appropriate measures for the protection of personal data, and who can demonstrate this compliance. This implies that the data controller must not only adhere to the GDPR's guiding principles but also be able to prove that he does so. The documentation of these processes is accomplished, for instance, through the implementation of appropriate policies and procedures, such as registers, analyses, agreements, written consents, information notes on the processing of the personal data, etc.

(c) The legal basis

According to Article 6 of the GDPR, personal data can be processed if at least one of the legal grounds is identified and properly documented before processing. All data operations must be lawful, i.e. based on at least one of the following grounds [7]:

- ✓ v*ital interest,*
- ✓ *legal obligation,*
- ✓ *the contract,*
- ✓ *legitimate interest,*
- ✓ *consent and*
- ✓ *the public interest.*

The six grounds listed above are on equal footing. Regardless of the basis, the data controller must comply with the GDPR and implement appropriate data protection policies. In most cases, legal grounds require processing to be "necessary" for a particular and specified purpose. It must be defined before data processing begins, with great care as it will have a significant impact on the processing implementation [2], [11], [12].

Within data processing records, each legal basis should be justified with the proper information. As a result, a compact personal data management system is proposed, presented as an informative decision-making circuit of the logical type, offering YES or NO options [8]. This system aims to facilitate the selection of appropriate legal bases and, in particular, to aid data controllers in making informed choices.

The procedures that are conducted in this informational circuit and that, ultimately, can provide the compliant version concerning the legal grounds, are presented in the following sections.

(1) Vital interest: the processing is necessary in an effort to protect the vital interests of a person (the life or health of the person is protected).

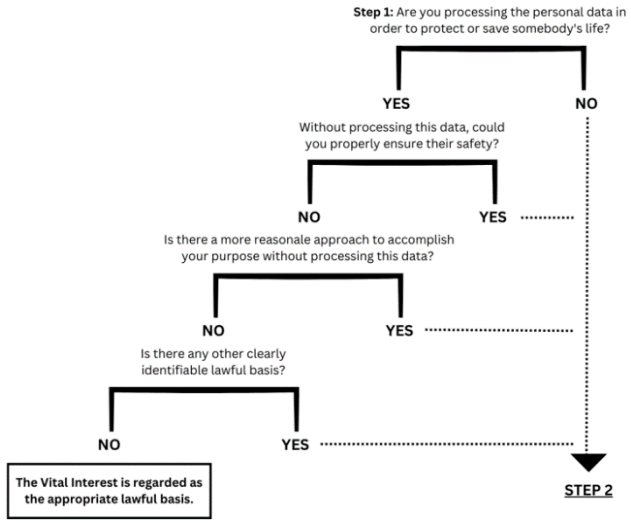

Fig. 1. Verification of vital interest
Source: own contribution.

(2) Legal obligation: the processing is required to uphold the legal responsabilities to which a data controller is subject; the information note must include the applicable legislation, the date and the name of the data subject.

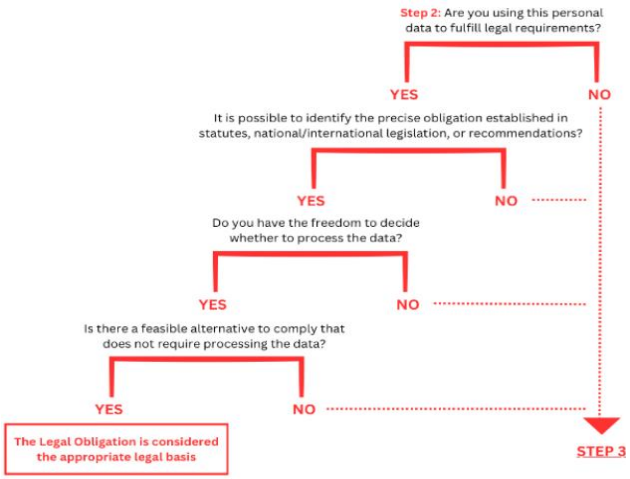

Fig. 2. Verification of legal interest
Source: own contribution

(3) The Contract: processing personal data is considered essential for fulfilling a contract in which the data subject is involved or for carrying out specific measures requested by the data subject before the contract is finalized. In general, in order to draft a contract that is going to be signed by the client, the data controller must handle the personal information of the future client. Such data may only be utilized throughout the duration of the agreement.

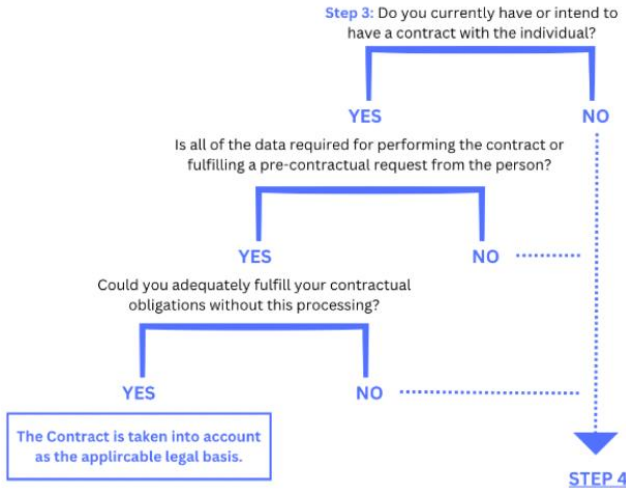

Fig. 3. Verification of the contract
Source: own contribution.

(4) Legitimate interest: can be used with caution as a legal basis following a detailed and well-documented analysis, as long as it does not conflict with the interest of the data subject. In particular, the controller must check that the data subjects' fundamental rights and freedoms are not violated, while ensuring that the reasonable expectations of the data subjects, based on their relationship with the controller, are considered, while also assuring thorough information in regard to this legal basis.

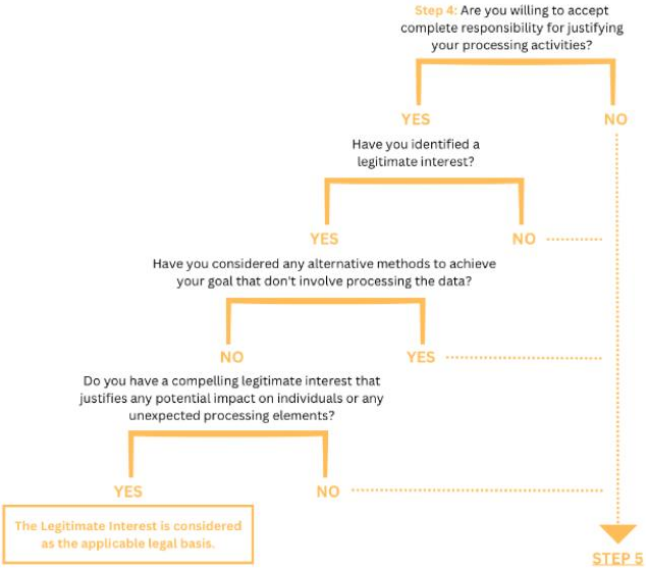

Fig. 4. Verification of the legitimate interest
Source: own contribution.

Additionally, the organisation must demonstrate in writing that their interest outweighs the rights and freedoms of the data subject before using the legitimate interest as a legal basis.

This is typically done through a Legitimate Interest Assessment (LIA), which may be followed by a Data Protection Impact Assessment (DPIA).

(5) Consent: When no other applicable legal basis exists or is mandated by the Regulation, the establishment of this legal foundation is necessary. A comprehensive information note must be provided to the individual, detailing the terms of the permission.

The individual's agreement must be clear, well-informed, and definite to be considered valid. It should be freely given and expressed through a tangible action, like checking a box, signing a document, or verbally confirming agreement. Additionally, the person should have the same ease in withdrawing their consent as they did while giving it, although not necessarily through the same method. According to EU law, the personal data of children under 16 can only be collected and

processed with the consent of a parent or legal guardian.

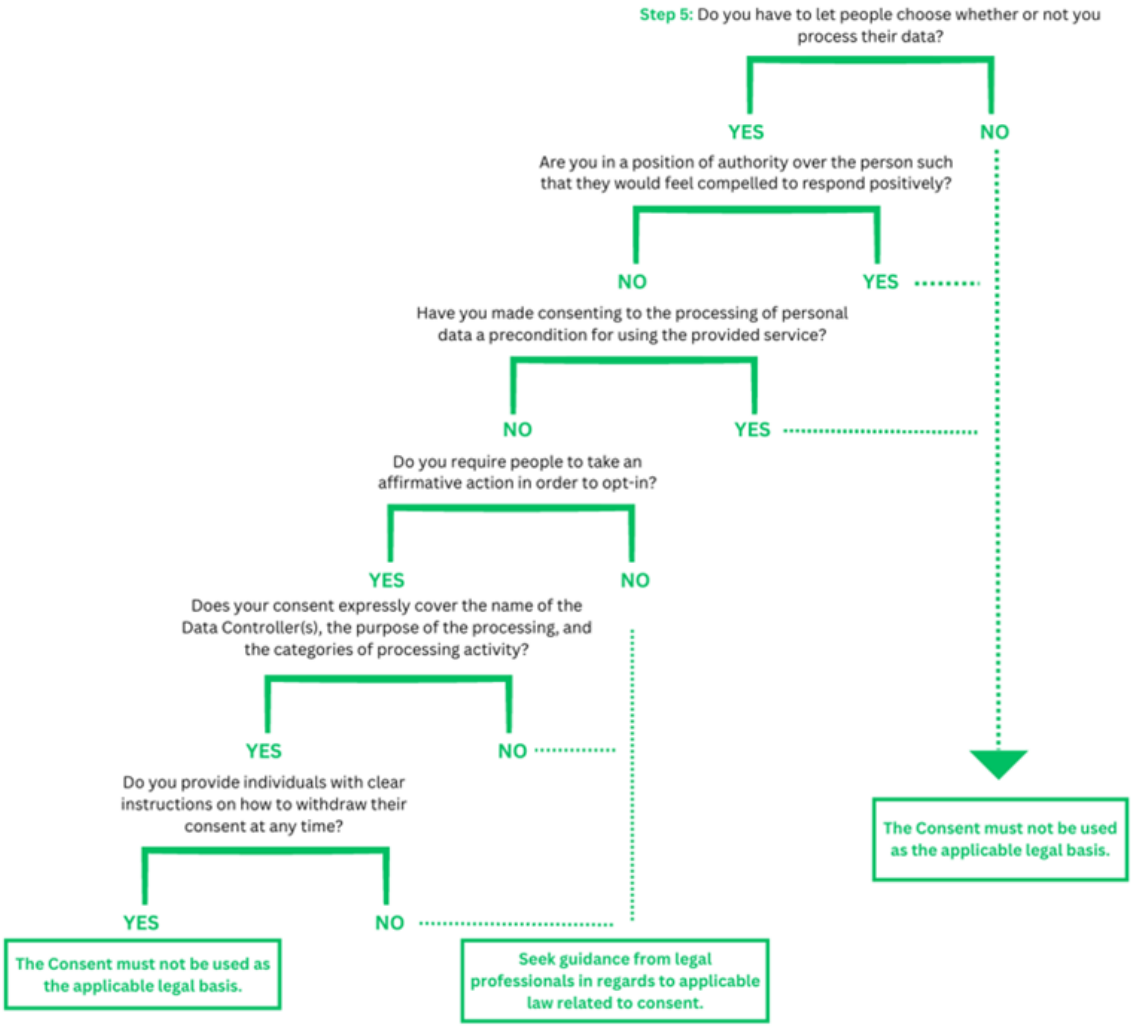

Fig. 5. Verification of consent
Source: own contribution

(6)Public interest: the processing is necessary for the performance of a task carried out in the public interest or the exercise of the official authority vested in the data controller. The use of public interest/task as a legal basis is so specific that it does not require further explanation as to when it applies. This multifaceted approach it was expressly designed to assist institutions/ companies/ organisations in fulfilling legal obligations and realizing efficacious and efficient data protection management that aligns harmoniously with overarching strategic objectives.

The agricultural sector, particularly in rural regions, contends with a distinctive labour landscape characterized by a substantial presence of unregistered or informally employed workers. These individuals, despite constituting an essential component of the agricultural workforce, often lack formal legal recognition, rendering them vulnerable to various forms of labour exploitation and infringements upon their rights and freedoms. In this intricate context, the significance of the General Data Protection Regulation (GDPR) cannot be overstated, due to the fact that it serves as a formidable legal framework with the potential to substantially augment the safeguarding of the rights and liberties of these workers.

Central to GDPR's relevance in this setting is the imperative to establish and maintain comprehensive databases and records that accurately encapsulate the employment status,

wage structures, and prevailing working conditions of agricultural labourers. In aligning with the GDPR's foundational principles of data protection and privacy, the meticulous handling and administration of this data can profoundly ameliorate the predicaments faced by these labourers. This data not only acts as a bulwark against their potential exploitation but also provides a mechanism for effecting equitable remuneration, ensuring occupational safety, and promoting fair labour practices.

The exigency of GDPR becomes more pronounced when contemplating the predicament of Romanian day labourers who seek employment opportunities in other European Union member states, notably Spain and Italy. These migrant labourers, often grappling with linguistic barriers, limited access to legal resources, and susceptibility to discrimination, find themselves ensnared in a particularly precarious position. Within this framework, GDPR-compliant databases emerge as a lifeline for these itinerant labourers. They serve as a conduit for their prospective employers to adhere to the requisite labour norms, thereby effectuating the protection of rights encapsulated within GDPR.

For example, these databases facilitate the meticulous monitoring of work hours, wage disbursements, and the stipulations of employment contracts for Romanian day labourers, thereby ensuring equitable remuneration and lawful safeguarding of their interests while working abroad. Moreover, the steadfast commitment of GDPR to data protection and privacy guarantees the judicious handling of the personal information associated with these labourers, mitigating the risks associated with data breaches and unauthorized data usage.

Therefore, GDPR plays a crucial role in addressing the complex issues faced by the agricultural sector, especially in rural areas where unregistered labour is common. By consistently upholding principles of transparency, accountability, and fairness through compliant databases, GDPR serves as a protector of the rights and liberties of both local and migrant agricultural workers. As a result, it contributes to creating a fairer and more just working environment in Europe and elsewhere, establishing itself as a fundamental element in advancing the principles of social justice and inclusivity within the agricultural sector.

CONCLUSIONS

Personal information, regardless of whether it's in physical form, digital databases, or other formats, must be gathered and managed responsibly. Specific measures are in place to adhere to the Regulation governing the processing and free movement of personal data. In our increasingly data-driven world, where information holds immense value, GDPR's aim is to uphold the confidentiality of personal data.

In adhering to EU privacy regulations for the collection and processing of personal data, it is imperative to establish a robust legal foundation. Consequently, several legal bases underpinning the aforementioned operations encompass:

- the presence of the person’s consent;
- the necessity of executing a contract;
- public interest;
- compliance with legal obligations.

security is everyone's responsibility, as there are dangerous threats that could easily cause damage. It is the role of each individual to implement data security best practices. Thus, it is recommended to:

- lock computers and devices when they are left unattended;
- select strong, long and complex passwords;
- keep data where it belongs;
- dispose of the data properly.

Phishing also involves attempts to trick you into clicking on email links or attachments that contain viruses that might harm your computer system. Beware to never give out your password in response to an email or phone call, and be cautious about the websites you visit and the links you click. One individual making a mistake is all it takes for a hacker to gain access to your computer system or for your data to be lost or stolen. As such, accountability is crucial when it comes to protecting data confidentiality. The

management and usage of personal data can greatly impact an individual's life, which is why it's essential to understand the significance, value, and safeguarding of data in all your actions!

REFERENCES

[1]Charter of Fundamental Rights of the European Union, https://eur-lex.europa.eu/legal-content/RO/ Accessed on July 19, 2023.
[2]Data protection according to GDPR. Requirements and obligations, https://europa.eu/youreurope/ business /dealing-with-customers/data-protection/data-protection-gdpr/index_ro.htm, Accessed on July 10, 2023.
[3]Directive on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data. https://www.dataprotection.ro/servlet/ViewDocument?id=1263, Accessed on July 10, 2023.
[4]European Convention for the Protection of Human Rights and Fundamental Freedoms, https://www.echr.coe.int, Accessed on July 29, 2023.
[5]GDPR principles, https://legalup.ro/principii-privind-prelucarea/, Accessed on July 4, 2023.
[6]General Data Protection Regulation (GDPR) https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=celex:32018R1725, Accessed on July 7, 2023.
[7]Legal basis of data processing, https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data_ro, Accessed on July 19, 2023.
[8]Livovschi, L., 1980, Scheme logice - semnificatie, elaborare, verificare, testare (Logical schemes - meaning, elaboration, verification, testing, technical), Technical Publishing House, Bucharest, pp. 70-95.
[9]National Supervisory Authority for the Processing of Personal Data, https://www.dataprotection.ro/, Accessed on July 10, 2023.
[10]Personal data https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_ro#:~:text =Data cu%20character%20personal, Accessed on July 7, 2023
[11]Procedure for the management of personal data https://dnsc.ro/vezi/document/procedura-pentru-gestionarea-datelor-cu-caracter-personal, Accessed on July 29, 2023
[12]Protection of personal data, http://www.schengen.mai.gov.ro/Documente/Vizite%20de%20evaluare/Protectia%20datelor%20personale.pdf Accessed on July 29, 2023,
[13]The rights of data subjects, https://www.dataprotection.ro/servlet/ViewDocument?id=1298, Accessed on July 10, 2023.
[14]The Treaty on the Functioning of the European Union, https://eur-lex.europa.eu/resource.html, Accessed on July 19, 2023.