sciendo

Human Resources and GDPR Compliance: Lessons from Romanian Data Protection Case Law on Workplace Privacy

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

Abstract. *The General Data Protection Regulation (GDPR) has been in force since May 2018, yet its implementation in employment relationships continues to present compliance challenges. This study examines the intersection of data protection and labor law by analyzing how the Romanian Data Protection Authority (DPA) interprets and enforces GDPR principles in workplace settings. The research is based on an empirical analysis of decisions issued by the Romanian DPA, offering insights into common compliance failures and risk mitigation strategies.*

The study identifies two primary categories of GDPR breaches in employment contexts. The first includes direct violations committed by employers, such as unauthorized data collection, failure to ensure transparency, and excessive monitoring through video surveillance or electronic tracking. The second category consists of violations formally attributed to employers but triggered by employee actions, highlighting the importance of internal safeguards and employee training. The research further demonstrates that non-compliance extends beyond employer-led processing to include unauthorized disclosures, misuse of biometric data, and failures in data retention policies.

Findings reveal that many breaches result from the inability of employers to justify legitimate interests, failure to consult employees before implementing monitoring systems, and inadequate security measures. The study underscores the necessity of a structured compliance framework in human resource management, advocating for transparent monitoring policies, strict access controls, and periodic security assessments.

By integrating legal analysis with human resource management principles, this research contributes to the broader discourse on GDPR compliance in employment relations. It highlights the importance of interdisciplinary approaches in shaping data protection strategies and reinforces the need for organizations to adopt risk-based methodologies to mitigate regulatory exposure.

Keywords: GDPR, employment relationships, workplace surveillance, data protection, human resource management, regulatory compliance.

Introduction

Since its enforcement in May 2018, the General Data Protection Regulation (GDPR) has established a comprehensive framework for data protection across the European Union. However, despite seven years of legal applicability, significant uncertainties remain regarding its practical implementation and compliance requirements. This issue is particularly critical in the context of employment relationships, where legal clarity is essential given the vast number of individuals engaged in the workforce. The intersection of data protection and labor law necessitates a thorough analysis of how GDPR principles are interpreted and applied in employment-related scenarios.

Against this backdrop, this study seeks to identify and clarify the key considerations that employers must take into account when evaluating risks associated with the processing of personal data in the workplace. To achieve this objective, the research conducts a systematic examination of the interpretative approach adopted by the Romanian Data Protection Authority (DPA) in cases involving employment-related data processing. The study relies on primary data, specifically decisions issued by the Romanian DPA, which are analyzed from both a legal perspective and a

DOI: 10.2478/picbe-2025-0332

human resource management standpoint, facilitating an interdisciplinary approach to compliance and risk mitigation.

Through this analysis, the study aims to identify patterns and common pitfalls in the application of data protection rules within human resource management. It also seeks to identify systematic guidelines that can support organizations in ensuring compliance with personal data processing requirements. This study makes three key contributions to literature. First, it provides an empirical analysis of how the Romanian DPA interprets both the GDPR principles of personal data processing in employment relations and the concept of appropriate measures. By adopting a data-driven approach, the study examines fines imposed by the Romanian DPA in cases where GDPR breaches arose in the context of employment relationships, offering an empirical foundation for understanding the complexity of legal compliance in this domain.

Second, the findings of this study have significant implications for human resource management, as they demonstrate that data protection risks are not solely associated with processing activities carried out by employers but may also arise from employees' actions and conduct. This approach, which represents a novel perspective in the legal analysis of personal data processing within employment relationships, is likely to enable HR managers to develop more comprehensive risk mitigation strategies when they are required to contribute to the establishment of appropriate measures for ensuring the lawful processing of personal data by employees.

Finally, this study goes beyond the mere analysis of GDPR infringements in the field of human resources and the sanctions imposed. It demonstrates that examining cases in which a regulatory authority interprets legal provisions can contribute to the advancement of disciplines beyond the legal field — in this case, human resource management. Once again, this confirms that progress in both research and managerial practices must be grounded in transdisciplinary approaches in order to achieve a comprehensive understanding of the applicable issues.

Literature review

The interplay between data protection and employment law has been a subject of increasing academic and legal scrutiny, particularly following the implementation of the GDPR. Scholars and regulatory bodies have emphasized the challenges of applying GDPR principles in workplace settings, where power imbalances between employers and employees complicate traditional notions of lawful data processing, consent, and privacy protection (Article 29 WP, 2018; Ebert et al., 2021; Kuner et al., 2021). The legal asymmetry inherent in employment relationships necessitates a rigorous examination of compliance obligations, particularly concerning the use of monitoring technologies, biometric data collection, and surveillance mechanisms (Ogriseg, 2017).

Research has shown that GDPR compliance in employment contexts is primarily assessed through the principles of necessity, proportionality, transparency, and accountability (Bodie, 2022). While the regulation provides a general framework for data protection, national authorities (DPAs) play a pivotal role in interpreting and enforcing these principles. Studies on regulatory enforcement have underscored the importance of national DPAs in shaping GDPR compliance through case law and administrative decisions (Kamarinou & Van Alsenoy, 2020; de Hert & Papakonstantinou, 2016).

A central issue identified in prior literature concerns the limitations of consent as a legal basis for processing employee data. Given the inherent imbalance of power in the employment relationship, scholars argue that employee consent cannot be freely given, making it an unreliable legal ground for processing personal data (Article 29 WP, 2017; Edwards & Veale, 2017). Instead, employers must justify data processing through alternative legal bases, such as legitimate interest

or compliance with a legal obligation (Spiecker genannt Döhmann, 2021). However, case law suggests that many employers struggle to meet the burden of proof required to justify these legal bases, particularly in cases of employee monitoring and surveillance (Volosevici, 2018).

Additionally, research on GDPR enforcement in workplace surveillance highlights recurring compliance failures related to video surveillance, GPS tracking, and biometric data collection (Ball, 2022). Aloisi & De Stefano (2022) signal that employers frequently fail to inform employees about surveillance practices, justify the necessity of monitoring, or implement proportionate security measures. These shortcomings have resulted in substantial fines and highlight the need for risk-based compliance strategies.

The study builds on existing literature by providing an empirical assessment of GDPR enforcement in employment settings, focusing on decisions issued by the Romanian DPA. By analyzing legal interpretations, regulatory sanctions, and risk mitigation strategies, this research contributes to a growing body of work on data protection in human resource management. Additionally, it reinforces the argument that data protection compliance requires an interdisciplinary approach, integrating legal analysis, risk management (Merrick & Ryan, 2019), stakeholder theory (Isbasoiu, 2023) and organizational governance (Seerden et al., 2018) to develop effective and sustainable privacy strategies in the workplace.

Methodology

This study employs a qualitative research design to analyze the intersection of GDPR compliance and human resource management in Romania. The analysis is based on enforcement decisions issued by the Romanian DPA. The data collection process involved an in-depth examination of GDPR provisions related to employment relationships, workplace surveillance, and employer responsibilities. Romanian national legislation, including Law No. 190/2018, which adapts GDPR to the national context, was also reviewed alongside guidance documents issued by the European Data Protection Board and Article 29 Working Party regarding workplace data processing.

A systematic review of all publicly available GDPR-related enforcement decisions from the Romanian DPA between June 27, 2019, and February 10, 2025, was conducted. Each decision was classified based on the nature of GDPR violations, responsible entities, and imposed sanctions. Annotation of these decisions was performed to capture key legal and procedural factors, including the legal basis for data processing, type of violation, and organizational measures taken.

A structured coding framework was employed to systematically analyze the collected data. The methodological approach involved the classification of GDPR violations, distinguishing between employer-led infractions and those triggered by employee actions. High-risk data processing activities, such as video surveillance, biometric data collection, and electronic employee monitoring, were also identified.

Thematic analysis was used to examine common patterns in enforcement decisions, highlighting key compliance failures and best practices that may be built based on the Romanian DPA's interpretation of GDPR provisions. Special attention was given to assessing how HR management practices influence compliance outcomes and the role of internal safeguards in mitigating risks. The analysis also explored how regulatory interpretations may shape organizational approaches to GDPR adherence in workplace settings.

This research adheres to ethical standards in legal and social sciences research. The study relies exclusively on publicly available data and does not involve human subjects or confidential information. Additionally, efforts were made to maintain neutrality and objectivity in assessing GDPR compliance trends.

Results and discussions

The comprehensive analysis of the cases has allowed us to establish a primary classification based on the party responsible for the actual GDPR violation. Notably, in all instances, the employer was the entity held liable and subjected to fines. However, a closer examination of the actual perpetrator of the violation reveals two distinct categories.

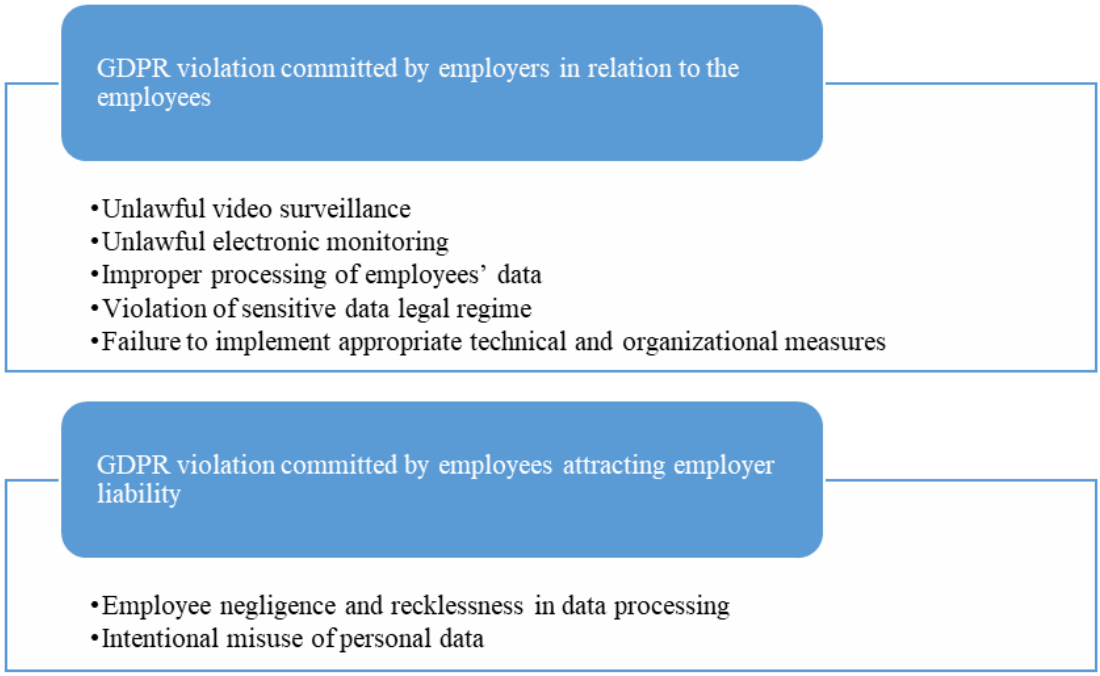

Figure 1. Categories of GDPR violations

Source: Author's own research.

The first category of cases comprises sanctions resulting from direct violations of the GDPR committed by employers in the context of employment relationships. These breaches occur both during the execution of the employment contract and after its termination. This category aligns with the standard approach found in the specialized literature when discussing the processing of personal data in employment contexts. It includes infractions such as unlawful collection, processing, or retention of employees' personal data, as well as failures to ensure data security and compliance with transparency obligations. Given the direct link between these violations and employment relationships, this category is frequently analyzed in academic and legal discussions concerning workplace data protection.

The second category consists of sanctions formally imposed on employers in their capacity as data controllers; however, these penalties were, in practice, triggered by actions or omissions committed by their employees. While the legal connection between these violations and employment relationships may appear less direct than in the first category, this aspect remains highly relevant from a human resource management perspective. These cases highlight specific employee behaviors that resulted in GDPR breaches, allowing organizations to identify recurring patterns of non-compliance. Consequently, this category provides valuable insights into risk

management strategies by helping to define preventive measures and internal controls aimed at reducing the likelihood of such incidents.

GDPR violations committed by employers in relation to their employees

The employment relationship is characterized by the legal inequality between the parties, as explicitly stated in the legal definition of the employment contract under Article 10 of the Labor Code, which specifies that the employee is in a subordinate relationship with the employer. Certain measures implemented by employers directly impact the execution of the employment relationship, such as the inspection of personal data (ID card or fingerprint) for workplace access, the installation of video surveillance equipment in the workplace, or the deployment of electronic performance monitoring tools. Given that employees often have limited control over how their personal data is processed in such contexts, employers have a heightened duty of care regarding data protection and compliance.

This legal context has direct consequences for the application of the GDPR in employment relationships. Specifically, one of the six lawful bases for processing personal data, as outlined in Article 6 of the GDPR - consent - is generally not considered a valid legal basis in employment relationships except in exceptional circumstances. Due to the inherent power imbalance between employers and employees, consent cannot be freely given, making it an unreliable legal ground for processing personal data in most workplace scenarios. Consequently, employers must rely on alternative legal bases for data processing, such as the necessity of processing data in pursuit of their legitimate interest (Article 29 WP, 2017).

Furthermore, due to the nature of the employment relationship, employers routinely process a significant volume of employees' personal data, including health records, financial information, disciplinary records, and, in some cases, even biometric data. Any failure to comply with GDPR requirements does not merely affect a single individual but has the potential to impact the entire workforce, amplifying both the legal risks and operational consequences of non-compliance.

Workplace monitoring

A significant number of sanctions are related to the video surveillance of employees. According to Law No. 190/2018, the processing of employees' personal data through workplace video surveillance is permitted only if the employer can justify that its legitimate interests outweigh employees' rights and freedoms. Additionally, employees must receive clear and explicit prior notification, and the employer is required to consult the trade union or employee representatives before implementing monitoring measures. Monitoring should only be used if less intrusive alternatives have proven ineffective, and data retention must be proportionate to its purpose, not exceeding 30 days unless legally justified.

An analysis of case law reveals that employer violations frequently stem from failure to inform employees about the processing of personal data/images through video surveillance systems (Uttis Industries SRL, 2019; Iamsat Muntenia SA, 2022), as well as the installation of audio-video surveillance cameras in employees' offices, locker rooms, cafeterias, and smoking areas (Tip Top Food Industry SRL, 2021; Mayr Melnhof Packaging Romania SRL, 2022). In several cases, employers failed to demonstrate a legitimate interest that outweighed employees' fundamental rights and freedoms, did not consult trade unions or employee representatives, and could not prove that less intrusive methods had been considered and found ineffective (Entirely Shipping & Trading SRL, 2020; Denmar Nacrut SRL, 2022).

In another set of cases, video surveillance was coupled with audio recording through an integrated audio-video system (capturing both image and sound), without the employer providing

evidence of compliance with the legal grounds for processing as required under Article 6(1) of the GDPR (Entirely Shipping & Trading SRL, 2020; Glove Technology SRL, 2021; Concordia Capital IFN SA, 2022). A particularly concerning case involved direct employee monitoring, where audio-video surveillance cameras were installed inside vehicle cabins, directed at the driver, and allowing for online remote monitoring. While the vehicles were used for public transportation, the processing of personal data violated fundamental GDPR principles, including lawfulness, legitimacy, and necessity in relation to the stated purpose. Furthermore, the DPA found that the images and audio recordings captured by the surveillance cameras were used for purposes beyond those originally stated, including in disciplinary investigations and sanctions against employees (Compania de Transport Public Cluj-Napoca SA, 2024).

In a case, an employer notified the Romanian DPA that it had discovered 135 unauthorized surveillance cameras connected to unofficial systems, beyond the official security system. These cameras, which were not configured according to internal policies, were predominantly placed within the production area (Continental Automotive Romania SRL, 2022). The DPA found that the employer had failed to implement appropriate technical and organizational measures, did not conduct regular assessments of its security measures, and had not ensured adequate safeguards to prevent unauthorized data processing, thus violating both internal security policies and GDPR compliance requirements.

The fines imposed ranged from €1,000 to €5,000. However, at the European level, non-compliance with legal provisions governing workplace video surveillance can lead to significantly higher penalties. For example, a substantial fine of €10.4 million was imposed after the data protection authority emphasized that companies must recognize the severe impact of extensive video surveillance on employees' rights (LfD, 2021).

In the same area of workplace monitoring, employers must ensure the protection of employee rights when implementing surveillance through electronic communication systems, as Law No. 190/2018 establishes an equivalent legal framework for electronic monitoring in the workplace as it does for video surveillance. The Romanian DPA has addressed several cases related to the GPS tracking of company vehicles assigned to employees, identifying serious compliance violations.

A recurring issue involved employees not being informed about GPS tracking (Tehnoplus Industry SRL, 2023; Global Ports's Services SRL, 2024), as well as cases where monitoring continued after the termination of the employment contract or even during annual leave periods (Global Ports's Services SRL, 2024; Up România SRL, 2024). In these instances, the processing of location and identification data lacked a valid legal basis, violating fundamental data processing principles such as lawfulness, transparency, and data minimization. In a particularly concerning case, an employer was sanctioned for processing personal data for purposes other than those originally specified, further demonstrating the risks of non-compliance with GDPR transparency obligations (Tehnoplus Industry SRL, 2023).

Another violation sanctioned by the DPA was the unjustified retention of GPS tracking data beyond the legally permitted 30-day period (Global Ports's Services SRL, 2024; Up România SRL, 2024). Similar to video surveillance, fines were imposed on employers who failed to demonstrate that they had exhausted less intrusive alternatives before implementing continuous GPS tracking (Tehnoplus Industry SRL, 2023; Global Ports's Services SRL, 2024). The fines in these cases ranged from €2,000 to €5,000, reinforcing the need for strict compliance with GDPR retention and proportionality requirements.

At the European level, the most significant fine issued to date for employee monitoring through both electronic tracking and video surveillance was €32 million, imposed on Amazon Logistique France (2023). This case highlights the heightened regulatory scrutiny applied to workplace surveillance practices, emphasizing the need for transparent policies, lawful processing grounds, and strict adherence to data protection principles to avoid substantial penalties.

Given the legal and regulatory challenges associated with employee monitoring, human resource management must adopt a structured and compliant approach to ensure that surveillance practices align with GDPR requirements and fundamental employee rights. Case law analysis has demonstrated that common violations include insufficient employee notification, failure to justify legitimate interests, lack of consultation with employee representatives, and the absence of adequate security measures. To mitigate these risks, human resources managers must implement clear policies and procedural safeguards.

A fundamental measure is ensuring transparency in monitoring practices, requiring employers to provide explicit and prior notification regarding how surveillance is conducted, the purpose of data collection, and the duration of data retention. Monitoring should only be carried out if less intrusive alternatives have been evaluated and deemed ineffective. Moreover, consultation with trade unions or employee representatives should be conducted prior to implementing new surveillance systems to ensure compliance with labor laws and collective agreements.

Additionally, human resources management must establish a clear legal basis for data processing, ensuring that the employer's legitimate interests do not override employees' fundamental rights and freedoms. Employers should also restrict surveillance to necessary areas, avoiding excessive monitoring in private spaces such as offices, cafeterias, or locker rooms. The retention period of recorded data should be proportionate to its intended purpose and should not exceed 30 days, unless a longer retention period is legally justified.

To prevent unauthorized surveillance, human resources management should implement periodic audits and security assessments to ensure that all monitoring systems comply with internal policies and data protection regulations. The discovery of unauthorized surveillance cameras, as seen in previous case law, underscores the importance of strong internal controls and employee training on GDPR compliance.

Finally, non-compliance with legal provisions regarding workplace surveillance has led to significant financial penalties, both at the national and European levels. To mitigate legal and reputational risks, human resources management must work alongside data protection officers and legal advisors to develop a monitoring framework that balances security needs with employee rights, ensuring compliance with GDPR and national labor laws.

Sensitive data

Another category of violations concerns the use of employees' biometric data. In one case, an employer implemented fingerprint-based access control for restricted areas (Entirely Shipping & Trading SRL, 2020). However, the DPA ruled that the processing of biometric data through this access control system was neither appropriate nor necessary, as it failed to meet the principles of adequacy, relevance, and data minimization in relation to the stated purpose of processing.

It is important to note that, under Article 9 of the GDPR, biometric data used for the unique identification of an individual falls under a special category of personal data, whose processing is generally prohibited unless specific legal conditions are met. As a result of non-compliance, the employer was fined €5,000. This highlights the need for employers to carefully assess the necessity

and proportionality of using biometric data in workplace monitoring and to consider less intrusive alternatives to ensure compliance with data protection regulations.

The personal numerical code (*codul numeric personal*, CNP) is also classified as a special category of personal data, subject to enhanced protection under data protection legislation. Law No. 190/2018 establishes that the processing of national identification numbers, including the collection or disclosure of documents containing them, must comply with Article 6(1)(f) of the GDPR, which permits processing based on the legitimate interests of the data controller or a third party, provided that adequate safeguards are in place.

To ensure compliance, organizations must implement technical and organizational measures that adhere to data protection principles, particularly the data minimization principle, while guaranteeing security and confidentiality in data processing, as required by Article 32 of the GDPR. Where applicable, organizations must appoint a Data Protection Officer (DPO) to oversee the lawful handling of personal data and ensure compliance with regulatory requirements. Additionally, well-defined data retention policies must be in place, specifying storage durations based on the nature and purpose of the data, along with procedures for periodic review and deletion to prevent unnecessary data retention.

Given the sensitivity of national identification numbers, organizations must also invest in regular employee training and awareness programs to ensure that individuals handling such data understand their responsibilities and comply with relevant data protection obligations. By integrating these safeguards, organizations can process national identification numbers in a lawful, secure, and proportionate manner, minimizing risks related to unauthorized access, excessive data retention, and regulatory violations.

The Romanian DPA has sanctioned employers for failing to comply with legal protections for employees' national identification numbers (CNPs). One case involved Uttis Industries SRL (2019), where the employer disclosed employees' CNPs by posting a personnel training report for ISCIR-certified staff on the company notice board. The document contained several personal details, including employees' national identification numbers, thus violating confidentiality and data protection regulations.

Another violation was identified at Compania Națională Poșta Română S.A. (2023), where the employer pre-filled Form 230 with employees' personal data, including full names and CNPs, to redirect 3.5% of their annual income tax to a foundation affiliated with the company. The investigation found that in January 2023, the employer had partially completed these forms without a legal obligation and failed to meet any of the legal conditions required under Article 6(1) of the GDPR. The €5,000 fine imposed in this case highlights the seriousness of processing personal data without a lawful basis, constituting a violation of Article 5(1)(a) and (2) in conjunction with Article 6(1) of the GDPR.

Further breaches occurred through unauthorized sharing of identity documents. In the case of World Class România SA (2021), the employer posted an employee's resignation request in a company WhatsApp group, granting all group members unauthorized access to personal data, including name, address, identity card details, CNP, and employment termination information. Similarly, Profi Rom Food SRL (2024) was found to have shared copies of employees' identity documents with an external service provider without legal grounds, leading to unauthorized access to names, CNPs, identity card numbers, addresses, gender, nationality, place of birth, and photographs.

Fines imposed in these cases ranged between €1,500 and €10,000, highlighting the importance of strict access controls, data-sharing policies, and employee training in preventing unauthorized disclosure of sensitive personal data.

Improper processing of employees' personal data

A key consideration in employee data processing is ensuring that all data processing activities cease upon the termination of the employment contract, except for the retention of data that employers are legally obligated to keep (Iamsat Muntenia SA, 2022; Unicredit Consumer Financing IFN SA, 2024). Throughout employment and even after its termination, employees maintain the right to access their processed personal data, as outlined in Article 15 of the GDPR. In one case, an employer delayed responding to an employee's access request by redirecting it to an internal department. The Romanian DPA determined that the employer had failed to properly uphold the right of access, thereby violating Articles 12(2), (3), and (4) in conjunction with Article 15(3) of Regulation (EU) 2016/679 (Fan Courier Express S.R.L., 2024).

Another frequently identified violation pertains to the unauthorized transfer of employee personal data to third-party contractors, conducted without adherence to the principles of data minimization and lawful processing. Several instances of such breaches have already been discussed in the section addressing the unlawful processing of sensitive data. Additionally, specific cases highlight instances where employers disclosed employee data to external entities without a legitimate legal basis (Condor SA, 2022) or utilized personal data for unauthorized administrative purposes, such as completing various forms. For example, in one case, an employer processed an employee's personal data without obtaining prior consent, registering them on the national COVID-19 vaccination platform without lawful justification (Wabag Water Services SRL, 2022). Another notable infringement involved the unauthorized use of an employee's email address without their knowledge or explicit consent, in the absence of prior notification or a valid legal basis (Entirely Shipping & Trading, 2020).

Failure to implement appropriate technical and organizational measures

A further issue identified in sanctioned cases relates to employers' failure to implement appropriate technical and organizational measures to ensure a sufficient level of data security. Such failures often result in unauthorized access, accidental or unlawful destruction, loss, modification, or disclosure of personal data, whether in physical or electronic formats. In one case, a binder containing personnel files for 12 employees was stolen (Bristol Logistics SA, 2023), underscoring the need for security measures that extend beyond electronic data processing. Nevertheless, the majority of cases involve unauthorized access to electronic records (Ana Hotels SRL, 2024; Constanța South Container Terminal SRL, 2024), emphasizing the urgent need for robust cybersecurity measures to protect employee personal information.

By analyzing these cases, it becomes evident that ensuring compliance with GDPR in employee data processing requires a multi-layered approach that includes data minimization, lawful processing, employee awareness, and stringent security protocols. Organizations must not only implement clear internal policies but also actively monitor their compliance to mitigate risks associated with data breaches, unauthorized access, and regulatory sanctions.

Employer liability for GDPR violations committed by employees

A distinct set of cases emerging from the analysis of Romanian DPA decisions involves situations where GDPR violations are legally attributed to the employer, despite the material actions being carried out by employees. The DPA's case law includes numerous instances where employers failed to implement adequate safeguards to ensure that individuals acting under their authority processed

personal data exclusively under employer instruction. In many cases, employers were also found to have neglected the implementation of appropriate technical and organizational measures, thereby failing to maintain an adequate level of security and risk assessment for data processing activities.

From a legal and managerial perspective, these cases fall into two major categories, each with implications for data security measures and HR management strategies related to workplace discipline.

Employee negligence and recklessness in data processing

In the first category, employees violate internal data protection policies and procedures without a direct intention to cause harm. The liability in these cases is based on negligence or recklessness, where employees either fail to anticipate the consequences of their actions or consciously accept the risk without actively seeking to cause harm. While these acts constitute disciplinary offenses, their gravity is mitigated by the absence of malicious intent.

However, from the perspective of employer liability, such violations remain severe, as reflected in the higher fines imposed in these cases. For example, in a recent case involving Vodafone (2025), the DPA found that the company failed to ensure confidentiality in handling customer data, including names, email addresses, national identification numbers (CNPs), customer codes, and residential addresses. The breach resulted from employee non-compliance with internal data handling policies, leading to incidents such as: unauthorized transmission of customer invoices via WhatsApp to third parties; failure to use the bcc function in emails, exposing recipient addresses; sharing screenshots of customer data through messaging applications, and incorrectly sending invoices to unintended recipients. The employer was fined €15,000, underscoring the importance of enforcing strict compliance with data handling protocols and ensuring continuous employee training.

Other similar cases involved Hora Credit IFN SA (2023), which was fined €20,000 for sending documents containing a client's personal data to another customer via email, and Artima SA (2023), where employees misused the video surveillance system, recorded footage using personal phones, and disseminated images on social media. The latter case resulted in an €8,000 fine, reinforcing the need for stricter access controls and employee awareness programs regarding confidential data processing.

The most severe penalty in this category was imposed on Banca Transilvania (2020), amounting to €100,000. In this case, an internal customer declaration on intended use of withdrawn funds was improperly shared among employees via corporate email. Subsequently, one employee printed the document, another photographed it with a mobile phone and shared it via WhatsApp, and eventually, the document was posted online and widely distributed on Facebook and other websites due to its humorous content. This case illustrates how employee failure to recognize the sensitivity of data can lead to significant reputational and financial consequences for the employer.

Intentional misuse of personal data by employees

The second category consists of cases where employees deliberately misuse personal data with fraudulent intent, typically for financial gain or other unauthorized purposes. Unlike the previous category, where employees acted recklessly or negligently, these cases involve direct intent to exploit customer data for illicit activities.

For instance, multiple cases involved employees of financial institutions misusing customer data to obtain fraudulent loans (Raiffeisen Bank SA, 2019; Raiffeisen Bank SA, 2022; Raiffeisen Bank SA, 2024). Similarly, in Rompetrol Downstream SRL (2023), employees disclosed customer

data to facilitate unauthorized loan applications with non-banking financial institutions. The DPA imposed a fine of €110,000, reflecting the serious nature of fraudulent data misuse.

It is important to note that in most such cases, employee misconduct qualifies as a criminal offense, potentially leading to legal liability not only for the individuals involved but also for their employer. If damages result from the misuse of personal data, the employer may be held jointly liable with the employee for compensating the victims, further emphasizing the need for stringent internal controls and compliance measures to prevent such violations.

Conclusion

The analysis of case law issued by the Romanian Data Protection Authority reveals that the application of personal data protection provisions in the context of employment relationships can generate various types of risks. The first category of violations concerns decisions taken by the employer regarding different aspects of the employment relationship, in which the employer deliberately assumes non-compliance with the GDPR. These cases have taken various forms, as evidenced by the analysis, such as implementing identity verification systems using fingerprint scanning, installing video cameras in restricted areas or in the canteen, or monitoring employees via GPS. In our view, these represent the most serious category of cases, as they are based on a conscious decision by the employer to unlawfully process employees' personal data.

Another category of violations stems from the negligence of employees whose job responsibilities involve processing a significant amount of personal data, primarily human resources staff. Their actions are, in most cases, the result of negligence rather than direct intent. Nevertheless, these actions lead to violations of the rights of data subjects, i.e., the employees. Such incidents include the display of employee data without respecting the principle of data minimization, sending emails containing employee information to incorrect recipients without encrypting or password-protecting the attached documents, and continuing to process personal data after the termination of the employee's contract. This category of violations clearly highlights the need to implement HR procedures that contain explicit rules for the processing of personal data, as well as the necessity of establishing a comprehensive training system, especially for HR personnel, regarding data protection.

However, not only HR staff may pose risks related to personal data processing. As shown by the cases analyzed, the negligence of employees from other departments, such as finance or customer relations, has also led to significant fines being imposed on employers.

Finally, employees' criminal activities—difficult to control and monitor by the employer—constitute a serious source of legal risk, particularly when the acts committed amount to criminal offenses. Employers must therefore develop procedures that address not only employee negligence but also intentional misconduct, including through the implementation of periodic checks on employees' professional activities.

Based on the case law analysis and the variety of identified cases, it becomes evident that ensuring GDPR compliance in employment relationships requires a multi-faceted approach. Employers must not only adopt clear internal policies and procedural safeguards, but also invest in continuous employee training, periodic security assessments, and proactive compliance monitoring. We believe that the adoption of risk-based data protection strategies, including consultation with employee representatives prior to the implementation of monitoring systems and the integration of multidisciplinary tools such as Fault Tree Analysis (Isbasoiu, 2024), is essential to reducing legal exposure.

While this research provides valuable insights into GDPR compliance in employment relationships, several limitations must be acknowledged. One limitation stems from the reliance on publicly available decisions issued by the Romanian DPA. The study does not include an analysis of case law from Romanian courts, which may offer additional perspectives on GDPR enforcement and legal interpretation.

Furthermore, this study is confined to the Romanian jurisdiction, which limits the broader applicability of its conclusions to other European legal frameworks where interpretations of GDPR provisions and enforcement mechanisms may vary. A key challenge in the implementation of the GDPR across the European Union lies in the divergence of regulatory interpretations and the inconsistency in the severity of fines imposed by national Data Protection Authorities. Such discrepancies may contribute to a phenomenon of regulatory arbitrage, wherein companies strategically adjust their compliance practices in response to the relative stringency of enforcement and sanctioning policies adopted in different member states.

Another constraint relates to methodological reliance on DPA jurisprudence. Although case law analysis offers valuable empirical insights, it does not provide a complete picture of organizational compliance efforts, or the challenges faced by employers in implementing GDPR requirements. The absence of direct engagement with corporate compliance officers, HR managers, or employees means that the study does not account for internal perspectives on data protection strategies, workplace monitoring policies, and risk mitigation practices.

Despite these limitations, the research provides a structured analysis of GDPR enforcement trends and highlights critical areas where employers must strengthen their data protection measures. Future studies could expand on these findings by incorporating comparative analyses of enforcement practices in multiple European jurisdictions, conducting interviews with compliance professionals or HR managers, or integrating quantitative assessments of GDPR-related fines and corrective actions. Such extensions would contribute to a deeper understanding of workplace privacy challenges and enhance the development of more effective regulatory and managerial compliance strategies.

References

Article 29 Data Protection Working Party. (2017). *Opinion 2/2017 on data processing at work (WP249)*. European Commission.

Article 29 Data Protection Working Party. (2018). *Guidelines on consent under Regulation 2016/679*. Adopted on November 28, 2017. Revised and adopted on April 10, 2018.

Aloisi, A., & De Stefano, V. (2022). Essential jobs, remote work and digital surveillance: Addressing the COVID-19 pandemic panopticon. *International Labour Review*, *161*(2), 289-314.

Ball, K. (2022). Surveillance in the workplace: Past, present, and future. *Surveillance and Society*.

Bodie, M. T. (2022). The law of employee data: privacy, property, governance. *Ind. Lj*, *97*, 707.

de Hert, P., & Papakonstantinou, V. (2016). The new general data protection regulation: Still a sound system for the protection of individuals. *Computer Law and Security Review*, *32*, 179–194.

Ebert, I., Wildhaber, I., & Adams-Prassl, J. (2021). Big Data in the workplace: Privacy Due Diligence as a human rights-based approach to employee privacy protection. *Big Data & Society*, *8*(1), 20539517211013051.

Edwards, L., & Veale, M. (2017). Slave to the algorithm? Why a "right to an explanation" is probably not the remedy you are looking for. *Duke Law & Technology Review, 16*, 18-84.

Isbasoiu, G. D. (2023). Tourists as stakeholders: For a better tourist involvement in promoting sustainable tourism. *Jus et Civitas, 10*, 41.

Isbasoiu, G. D. (2024). From blame to prevention: The role of just culture and fault tree analysis in managing human errors. *Jus et Civitas, A Journal of Legal Studies, 11*(1), 19-28. https://doi.org/10.51865/JETC.2024.1.03

Kamarinou, D., & Van Alsenoy, B. (2020). Data protection law in the EU: Roles, responsibilities, and liability. *International Data Privacy Law, 10*(4), 395–398. https://doi.org/10.1093/idpl/ipaa014

Kuner, C., Bygrave, L. A., Docksey, C., Drechsler, L., & Tosoni, L. (2021). *The EU General Data Protection Regulation: A commentary/update of selected articles.* SSRN. https://doi.org/10.2139/ssrn.3839645,

Law No. 190 of July 18, 2018, on measures for the implementation of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC (General Data Protection Regulation). (2018). *Official Gazette of Romania*, No. 651, July 26, 2018.

Ogriseg, C. (2017). GDPR and personal data protection in the employment context. *Labour & Law Issues, 3*(2), R. 1–24. https://doi.org/10.6092/issn.2421-2695/7573

Merrick, R., & Ryan, S. (2019). Data privacy governance in the age of GDPR. *Risk Management*, *66*(3), 38-43.

Seerden, X., Salmela, H., & Rutkowski, A. F. (2018). Privacy governance and the GDPR: How are organizations taking action to comply with the new privacy regulations in europe. In *ECMLG 2018 14th european conference on management, leadership and governance* (p. 371).

Spiecker genannt Döhmann, I. (2021). The legal framework for access to data from a data protection viewpoint – Especially under the GDPR. In *Data access, consumer interests, and public welfare* (pp. 175–198). German Federal Ministry of Justice and Consumer Protection (Bundesministerium der Justiz und für Verbraucherschutz), Max Planck Institute for Innovation and Competition (Max-Planck-Institut für Innovation und Wettbewerb), Nomos. https://doi.org/10.5771/9783748924999-175

Volosevici, D. (2018). Some considerations on video-surveillance and data protection. *Jus et Civitas: A Journal of Social and Legal Studies, 69*(2), 7-14.

Appendix

List of cases

Amazon Logistique France. (2023). Employee monitoring: French SA fined Amazon France Logistique €32 million. *European Data Protection Board.* Retrieved from https://www.edpb.europa.eu/news/national-news/2024/employee-monitoring-french-sa-fined-amazon-france-logistique-eu32-million_en

Ana Hotels SRL. (2024). Press release of the National Authority for the Supervision of Personal Data Processing in Romania. National Authority for the Supervision of Personal Data Processing. Retrieved from https://www.dataprotection.ro/?page=Comunicat_Presa_20.08.2024&lang=ro

Artima SA. (2023). Press release of the National Authority for the Supervision of Personal Data Processing in Romania. National Authority for the Supervision of Personal Data Processing. Retrieved from

https://www.dataprotection.ro/?page=Comunicat_Presa_15.06.2023
Banca Transilvania. (2020). Press release of the National Authority for the Supervision of Personal Data Processing in Romania. National Authority for the Supervision of Personal Data Processing. Retrieved from https://www.dataprotection.ro/?page=Comunicat_17_12_2020&lang=ro
Bristol Logistics SA. (2023). Press release of the National Authority for the Supervision of Personal Data Processing in Romania. National Authority for the Supervision of Personal Data Processing. Retrieved from https://www.dataprotection.ro/?page=Comunicat_Presa_12_01_2023
Compania de Transport Public Cluj-Napoca SA. (2024). Press release of the National Authority for the Supervision of Personal Data Processing in Romania. National Authority for the Supervision of Personal Data Processing. Retrieved from https://www.dataprotection.ro/?page=Comunicat_Presa_12.12.2024
Compania Națională Poșta Română S.A. (2023). Press release of the National Authority for the Supervision of Personal Data Processing in Romania. National Authority for the Supervision of Personal Data Processing. Retrieved from https://www.dataprotection.ro/?page=Comunicat_Presa_16.05.2023
Concordia Capital IFN SA. (2022). Press release of the National Authority for the Supervision of Personal Data Processing in Romania. National Authority for the Supervision of Personal Data Processing. Retrieved from https://www.dataprotection.ro/?page=Comunicat_Presa_04_05_2022
Condor SA. (2022). Press release of the National Authority for the Supervision of Personal Data Processing in Romania. National Authority for the Supervision of Personal Data Processing. Retrieved from https://www.dataprotection.ro/?page=Comunicat_Presa_28_03_2022
Constanța South Container Terminal SRL. (2024). Press release of the National Authority for the Supervision of Personal Data Processing in Romania. National Authority for the Supervision of Personal Data Processing. Retrieved from https://www.dataprotection.ro/?page=Comunicat_Presa_17.09.2024
Continental Automotive Romania SRL. (2022). Press release of the National Authority for the Supervision of Personal Data Processing in Romania. National Authority for the Supervision of Personal Data Processing. Retrieved from https://www.dataprotection.ro/?page=Comunicat_Presa_30_06_2022
Denmar Nacrut SRL. (2022). Press release of the National Authority for the Supervision of Personal Data Processing in Romania. National Authority for the Supervision of Personal Data Processing. Retrieved from https://www.dataprotection.ro/?page=Comunicat_Presa_09.08.2022_2
Entirely Shipping & Trading SRL. (2020). Press release of the National Authority for the Supervision of Personal Data Processing in Romania. National Authority for the Supervision of Personal Data Processing. Retrieved from https://www.dataprotection.ro/?page=O_noua_sanctiune_pentru_incalcarea_RGPD_2020_3&lang=ro
Fan Courier Express S.R.L. (2024). Press release of the National Authority for the Supervision of Personal Data Processing in Romania. National Authority for the Supervision of Personal Data Processing. Retrieved from https://www.dataprotection.ro/?page=Comunicat_Presa_23_12_2024

Glove Technology SRL. (2021). Press release of the National Authority for the Supervision of Personal Data Processing in Romania. National Authority for the Supervision of Personal Data Processing. Retrieved from https://www.dataprotection.ro/?page=Comunicat_Presa_21.10.2021_2&lang=ro

Global Ports's Services SRL. (2024). Press release of the National Authority for the Supervision of Personal Data Processing in Romania. National Authority for the Supervision of Personal Data Processing. Retrieved from https://www.dataprotection.ro/?page=Comunicat_Presa_02.10.2024&lang=ro

Hora Credit IFN SA. (2023). Press release of the National Authority for the Supervision of Personal Data Processing in Romania. National Authority for the Supervision of Personal Data Processing. Retrieved from https://www.dataprotection.ro/?page=Comunicat_Presa_07_12_2023

Iamsat Muntenia SA. (2022). Press release of the National Authority for the Supervision of Personal Data Processing in Romania. National Authority for the Supervision of Personal Data Processing. Retrieved from https://www.dataprotection.ro/?page=Comunicat_Presa_22_02_2022_1

LfD Niedersachsen. (2021). *LfD Niedersachsen verhängt Bußgeld über 10,4 Millionen Euro gegen notebooksbilliger.de*. Retrieved from https://www.lfd.niedersachsen.de

Mayr Melnhof Packaging Romania SRL. (2022). Press release of the National Authority for the Supervision of Personal Data Processing in Romania. National Authority for the Supervision of Personal Data Processing. Retrieved from https://www.dataprotection.ro/?page=Comunicat_Presa_17_05_2022

Profi Rom Food SRL. (2024). Press release of the National Authority for the Supervision of Personal Data Processing in Romania. National Authority for the Supervision of Personal Data Processing. Retrieved from https://www.dataprotection.ro/?page=Comunicat_Presa_23_10_2024

Raiffeisen Bank SA. (2019). Press release of the National Authority for the Supervision of Personal Data Processing in Romania. National Authority for the Supervision of Personal Data Processing. Retrieved from https://www.dataprotection.ro/?page=Comunicat_Presa_09_10_2019&lang=ro

Raiffeisen Bank SA. (2022). Press release of the National Authority for the Supervision of Personal Data Processing in Romania. National Authority for the Supervision of Personal Data Processing. Retrieved from https://www.dataprotection.ro/?page=Comunicat_Presa_16_11_2022

Raiffeisen Bank SA. (2024). Press release of the National Authority for the Supervision of Personal Data Processing in Romania. National Authority for the Supervision of Personal Data Processing. Retrieved from https://www.dataprotection.ro/?page=Comunicat_Presa_20_11_2024

Rompetrol Downstream SRL. (2023). Press release of the National Authority for the Supervision of Personal Data Processing in Romania. National Authority for the Supervision of Personal Data Processing. Retrieved from https://www.dataprotection.ro/?page=Comunicat_Presa_13_11_2023

Tehnoplus Industry SRL. (2023). Press release of the National Authority for the Supervision of Personal Data Processing in Romania. National Authority for the Supervision of Personal Data Processing. Retrieved from https://www.dataprotection.ro/?page=Comunicat_Presa_23.03.2023

Tip Top Food Industry SRL. (2021). Press release of the National Authority for the Supervision of Personal Data Processing in Romania. National Authority for the Supervision of Personal Data Processing. Retrieved from https://www.dataprotection.ro/?page=Comunicat_Presa_15_/04/_2021&lang=ro

Unicredit Consumer Financing IFN SA. (2024). Press release of the National Authority for the Supervision of Personal Data Processing in Romania. National Authority for the Supervision of Personal Data Processing. Retrieved from https://www.dataprotection.ro/?page=Comunicat_Presa_17_12_2024

Up România SRL. (2024). Press release of the National Authority for the Supervision of Personal Data Processing in Romania. National Authority for the Supervision of Personal Data Processing. Retrieved from https://www.dataprotection.ro/?page=Comunicat_Presa_13_11_2024

Uttis Industries SRL. (2019). Press release of the National Authority for the Supervision of Personal Data Processing in Romania. National Authority for the Supervision of Personal Data Processing. Retrieved from https://www.dataprotection.ro/?page=A_patra_amenda&lang=ro

Vodafone. (2025). Press release of the National Authority for the Supervision of Personal Data Processing in Romania. National Authority for the Supervision of Personal Data Processing. Retrieved from https://www.dataprotection.ro/?page=Comunicat_Presa_20_01_2025

Wabag Water Services SRL. (2022). Press release of the National Authority for the Supervision of Personal Data Processing in Romania. National Authority for the Supervision of Personal Data Processing. Retrieved from https://www.dataprotection.ro/?page=Comunicat_Presa_09.08.2022

World Class România SA. (2021). Press release of the National Authority for the Supervision of Personal Data Processing in Romania. National Authority for the Supervision of Personal Data Processing. Retrieved from https://www.dataprotection.ro/?page=Comunicat_07_/05/_2021&lang=ro

Acknowledgements: This research was supported by a grant from the Petroleum-Gas University of Ploiesti, Romania, project number GO-GICS-30813/11.12.2024, within the Internal Grant for Scientific Research.