Teka Komisji Prawniczej PAN Oddział w Lublinie
vol. XVIII, 2025, no. 2, pp. 575–586
https://doi.org/10.32084/tkp.10205

PROTECTION OF WHISTLEBLOWERS VS. PROTECTION OF PERSONAL DATA*

Doc. JUDr. Peter Varga, PhD.

Trnava University in Trnava, Slovak Republic
e-mail: vargapeter01@hotmail.com; https://orcid.org/0000-0003-4252-6134

Abstract. Directive 2019/1937 on the protection of whistleblowers and Regulation 2016/679 (GDPR) on data protection are key legal instruments safeguarding individual rights within the European Union. Despite their shared objective of protecting individuals, their concurrent application presents practical and legal challenges. To ensure compliance, organizations must adopt integrated mechanisms that reconcile whistleblower protection with data privacy obligations. This article explores the need for a coordinated approach that enables effective implementation of both frameworks, emphasizing the importance of legal clarity and operational balance in practice.

Keywords: GDPR; directive 2019/1937; whistleblower; right to information; right to be forgotten.

1. DIRECTIVE 2019/1937 VERSUS REGULATION 2016/679 – TWO DIFFERENT RIGHTS AND PURPOSES

The adoption of the new Directive 2019/1937 on the protection of persons who report breaches of EU law did not cause the change or demise of older legal regulations. In this context, it is necessary to address the protection of personal data in the current legal regulation within the context of reporting breaches of law and unfair practices [Mičudová 2016]. Even before the adoption of Directive 2019/1937, it was a challenge for many entities to comply with Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. To further complicate this labyrinth of legal regulations and obligations, following the adoption of the

* This article was prepared as an output of the grant project: "Whistleblowing ako prejav etickej spoločnosti alebo aké zlé je byť dobrý?" (English: "Whistleblowing as a Manifestation of an Ethical Society, or How Bad Is It to Be Good?"), which was approved for the research team of the Department of International and European Law at the Faculty of Law of Trnava University in Trnava by the Commission for Economic and Legal Sciences of the Scientific Grant Agency of the Ministry of Education, Research, Development and Youth of the Slovak Republic (VEGA), under project no. 1/0519/22.

ISSN 1899-7694
e-ISSN 2719-7379

Directive, it became necessary to address both the Directive and the GDPR and find mutual symbiosis and balance of rights and obligations set out in the individual legal regulations. Recognizing the mutual overlaps between both legal regulations, the European Data Protection Supervisor (EDPS)[1] adopted Guidelines on the processing of personal data in the context of reporting procedures.[2] These guidelines provide a framework for institutions, bodies, and agencies of the European Union to ensure compliance with data protection obligations during the implementation and execution of whistleblowing procedures. They include specific recommendations aimed at minimizing risks while guaranteeing lawful and secure data processing and offer practical instructions both before and after the introduction of whistleblowing mechanisms, ensuring that data protection obligations are followed [Nechala 2014]. These guidelines may also benefit private entities, as adherence to them can help ensure compliance with the GDPR [Mičudová 2019].

1.1. Purpose of Directive 2019/1937

The main objective of Directive (EU) 2019/1937 of the European Parliament and of the Council on the protection of persons who report breaches of Union law,[3] is to strengthen the protection of whistleblowers. This Directive provides a framework for the protection of individuals who draw attention to illegal or unethical practices in various areas of both the public and private sectors [Križan 2014]. It provides guarantees against retaliation, discrimination, or other negative consequences that might result from their actions.

The text of the Directive itself states that it was adopted with the aim of strengthening the enforcement of EU law and policies in key areas by setting common minimum standards that ensure a high level of protection for persons reporting breaches of EU law. These standards create the basis for a uniform approach by Member States to the protection of whistleblowers and emphasize the need for minimum standards at the national level.

From the perspective of material scope, the Directive includes the protection of persons who report breaches of EU law in specified areas, emphasizing the establishment of a minimum standard of protection. According to Article 6 of the Directive, the reporting person must have reasonable grounds to believe that the information provided was true at the time

---

[1] Wojciech Wiewiórowski is the European Data Protection Supervisor. He was appointed by a joint decision of the European Parliament and the Council on 5 December 2019 for a term of five years. For more information see: https://www.edps.europa.eu/about-edps/members-mission/supervisors/wojciech-wiewi%C3%B3rowski_en [accessed: 21.09.2025].

[2] Available on the website: https://www.edps.europa.eu/sites/default/files/publication/19-12-17_whisteblowing_guidelines_en.pdf [accessed: 21.09.2025].

[3] OJ EU L 305, 26/11/2019, p. 17-56 [hereinafter: Directive].

of reporting and falls within the scope of this Directive. Furthermore, protection applies to various forms of reporting, including internal (Article 6 of the Directive), external (Article 10 of the Directive), and public disclosure of information (Article 15 of the Directive). A specific feature of the Directive is that it works with the concept of public interest, which can be seen as the protection of the well-being of society and the general interest of the EU, especially in areas where legal breaches can seriously harm public interests [Debrecéniová 2008]. This concept is mentioned in the recitals of the Directive (Recitals 13 and 14 of the Directive) and plays a crucial role in its implementation. Unlike the GDPR, whose provisions do not directly include the term public interest, there is an evident difference in the approach of the two legal regulations regarding their purposes.

1.2. Purpose of Regulation 2016/679

Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data[4] aims to ensure the protection of fundamental rights and freedoms of natural persons when processing their personal data. It also aims to establish rules for the processing of personal data with emphasis on adherence to the principles of transparency, lawfulness, and fairness (Article 5(1)(a) GDPR). Since it is an EU legal instrument, last but not least, it aims to guarantee the free movement of personal data within the EU and prevent restrictions on this movement.[5]

Personal data has a broad definition under the GDPR, as personal data is considered to be any information relating to an identified or identifiable natural person.[6] Identification can be carried out directly, for instance, through a name or identification number, or indirectly, through data such as location data, online identifiers, or other attributes specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of the person. The broad definition of personal data ensures that all modern technologies enabling the collection and processing of various types of information are taken into account, thereby providing comprehensive protection in the context of rapid technological progress.

---

[4] OJ EU L 119, 4.5.2016, p. 1-88 [hereinafter: GDPR].

[5] Article 1(3) GDPR: "The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data."

[6] Article 4(1) GDPR: "'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

The primary purpose of the GDPR is the protection of natural persons during the processing of personal data, which is enshrined, among others, in the Charter of Fundamental Rights of the European Union and the Treaty on the Functioning of the European Union. The right to the protection of personal data is recognized as a fundamental right, but it is not an absolute right.[7] When applying it, it is necessary to assess its function in society and find a balance between the protection of personal data and other fundamental rights [Barancová et al. 2019]. This approach is consistent with the principle of proportionality, which requires that data protection does not impede legitimate objectives, such as public interest or security. Naturally, in the context of EU law, an important purpose of the GDPR is also to ensure the free movement of personal data within the EU, or EEA, without restrictions and while maintaining a high level of protection for the data subjects.

Regarding material scope, the GDPR applies to a wide range of processing activities[8] involving personal data, and it is applied to both automated and non-automated processing of personal data. Processing operations include collection, recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure, transmission, dissemination or otherwise making available, as well as erasure or destruction of personal data. Exceptions from the scope of the GDPR are strictly defined in Article 2(2) and concern, for example, the processing of personal data for exclusively personal or household activities.

When applying the GDPR, it is essential to take into account the fundamental principle of EU functioning, which is the principle of proportionality. According to Article 5(4) of the Treaty on European Union (TEU), the content and form of EU action shall not exceed what is necessary to achieve the objectives of the Treaties. This principle of proportionality is crucial in applying the GDPR to ensure that the processing of personal data is appropriate and does not exceed the necessary scope of essential processing. Equally important is the principle of accountability of the controller, who bears objective responsibility for demonstrating compliance with the GDPR. This includes transparency and clarity regarding the processing of personal data. The controller must be able to demonstrate that it complies with all GDPR requirements and that personal data is processed in accordance with applicable laws.[9]

---

[7] Judgment of the Court (Grand Chamber) of 16 July 2020, Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (ECLI:EU:C:2020:559), point 172: "However, the rights enshrined in Articles 7 and 8 of the Charter are not absolute rights, but must be considered in relation to their function in society."

[8] Article 4(2) GDPR: "'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."

[9] Article 5(2) GDPR: "The controller shall be responsible for, and be able to demonstrate compliance with, paragrap. 1 ('accountability')."

1.3. Directive vs. Regulation

These two sources of law are legal instruments pursuing distinct objectives and addressing different legal areas. This disparity, however, raises questions regarding their mutual compatibility and interaction in practical legal application.

However, discrepancies can also be found between the two sources of law due to their pursuit of different purposes. Directive 2019/1937 and the GDPR deal with distinct legal aspects, but they interact in practical application. The Directive explicitly addresses the relationship with the GDPR in Article 17, as it "requires that the processing of personal data in the context of investigations of reported breaches must always be compliant with the rules of the GDPR."[10]

Despite this requirement, difficulties arise in aligning whistleblower protection with the principles of personal data protection. Since these legal regulations protect distinct interests (the Directive focuses on the protection of whistleblowers, and the GDPR prioritizes the protection of personal data against unauthorized processing), these different priorities can lead to conflicts, especially in cases where it is necessary to identify the whistleblower or other involved parties.

The Directive addresses the relationship with personal data protection and the GDPR specifically regarding investigations, where it is essential to ensure that all data processing procedures respect the provisions of the GDPR. This includes minimizing collected data, ensuring its security, and restricting access to it only to necessary entities. The existing legal framework requires simultaneous compliance with the Directive and the GDPR, necessitating careful coordination and thorough assessment of each case. A key aspect is the creation of clear internal policies and procedures that allow the requirements of both legal acts to be met without undermining their objectives.

The Directive and the GDPR represent important tools for the protection of individuals in various areas. However, their simultaneous application requires comprehensive solutions that can align whistleblower protection with data protection rules. In practice, it is essential for organizations to implement mechanisms to balance these two approaches and thus ensure the effective fulfilment of the requirements of both legal frameworks.

To apply the law and resolve conflicts, it is necessary to rely on the basic interpretative methods of EU law, which serve to fill legislative gaps. Interpretative methods are used particularly when there is ambiguity or deficiency in legislation,

---

[10] Article 17(1) of the Directive: "Any processing of personal data carried out pursuant to this Directive, including the exchange or transmission of personal data by the competent authorities, shall be carried out in accordance with Regulation (EU) 2016/679 and Directive (EU) 2016/680. Any exchange or transmission of information by Union institutions, bodies, offices or agencies shall be undertaken in accordance with Regulation (EU) 2018/1725."

and their goal is to ensure the effective application of law and eliminate potential negative consequences arising from a legal vacuum.[11]

In addition to standard interpretative methods, the principle of proportionality is applied in case of conflict between legal norms, which requires that the adopted measures be proportionate to the objective pursued and do not exceed the scope necessary for its achievement. In the context of protecting the fundamental rights and freedoms of natural persons during the processing of personal data, the principle of proportionality plays a key role in finding a balance between data protection and other legitimate interests.[12]

1.4. The role of proportionality

The principle of proportionality is a fundamental concept that governs the exercise of powers by the EU. It requires that interventions by EU institutions do not exceed what is necessary to achieve the objectives set out

[11] It is particularly important to mention the teleological interpretation, which focuses on the purpose and objective of a legal norm. This method is crucial in situations where the legal regulation is not sufficiently clear, such as in the relationship between Directive 2019/1937 and the GDPR. The teleological approach supports the achievement of the goals of the legal regulation and helps to avoid negative consequences that could arise from a literal interpretation of the law. The systematic interpretation examines the legal norm within the broader context of the legal system, serving to understand the mutual interactions between individual legal acts, through which their coherence is to be ensured. The comparative method of legal interpretation involves assessing the influence of various sources of law that deal with the same area, such as the processing of personal data. This approach allows for a broader perspective and helps identify best practices from other legal systems.

[12] Judgment of the Court (Grand Chamber) of 16 July 2020, Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (ECLI:EU:C:2020:559), point 174: "Furthermore, in accordance with the first sentence of Article 52(1) of the Charter, any limitation on the exercise of the rights and freedoms recognised by the Charter must be provided for by law and respect the essence of those rights and freedoms. Under the second sentence of Article 52(1) of the Charter, subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others;" point 176: "Lastly, in order to satisfy the requirement of proportionality according to which derogations from and limitations on the protection of personal data must apply only in so far as is strictly necessary, the legislation in question which entails the interference must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose data has been transferred have sufficient guarantees to protect effectively their personal data against the risk of abuse. It must, in particular, indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary. The need for such safeguards is all the greater where personal data is subject to automated processing (see, to that effect, Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraphs 140 and 141 and the case-law cited)."

in the founding treaties. This means that both the content and form of EU actions must be appropriate to the pursued objective. This principle is explicitly enshrined in Article 5(4) of the TEU. The criteria for its application are specified in Protocol (No. 2) on the application of the principles of subsidiarity and proportionality, which is annexed to the Treaties. The principle of proportionality applies to all areas of EU competence, regardless of their nature (exclusive, shared, or supporting).

In connection with the principle of proportionality, the EU legislator must conduct a test to assess whether the proposed measure meets the following requirements: a) suitability – the measure must be objectively suitable for achieving the intended goal;[13] b) necessity – there must be no other equally effective but less restrictive measure that could achieve the goal;[14] c) proportionality in the strict sense (proportionality *stricto sensu*) – any potential negative effects of the measure must not be disproportionate in relation to the objective pursued.[15] It is therefore necessary to assess whether the benefits of the measure outweigh its impact on the rights or interests of individuals or Member States.

To successfully navigate these conflicts between the GDPR and the Directive, the principle of proportionality is critical. Proportionality requires that any limitation on fundamental rights (such as data protection) must be provided for by law, respect the essence of those rights, and be necessary and genuinely meet objectives of general interest recognised by the EU.

---

[13] Judgment of the Court of 8 June 2010, case C-58/08, The Queen on the application of Vodafone Ltd, Telefónica O2 Europe plc, T-Mobile International AG, Orange Personal Communications Services Ltd v Secretary of State for Business, Enterprise and Regulatory Reform (ECLI:EU:C:2010:321), point 53: "However, even though it has a broad discretion, the Community legislature must base its choice on objective criteria. Furthermore, in assessing the burdens associated with various possible measures, it must examine whether objectives pursued by the measure chosen are such as to justify even substantial negative economic consequences for certain operators."

[14] Ibid., point 61: "As to whether the measure at issue was necessary, it is argued that the said measure goes beyond what is necessary to achieve the objective pursued, given the competitive nature of retail markets. A less intrusive and more proportionate approach would have been to regulate wholesale charges only, while allowing competition in retail markets to bring retail prices down in the normal way, according to the rules of supply and demand, and leaving the NRAs free to intervene in cases where the markets were not functioning properly, on the basis of well-established regulatory criteria."

[15] Ibid., point 70: "Therefore, by adopting, in Article 4 of Regulation No 717/2007, ceilings for retail charges in addition to ceilings for wholesale charges, the Community legislature did not exceed the limits of the discretion it is recognised as having. The same is true of the obligation to provide information laid down in Article 6(3) of that same regulation, given that that provision reinforces the effectiveness of the regulation of retail charges and is therefore justified by the objective of consumer protection."

Furthermore, to satisfy the requirement of proportionality, any limitations on data protection must apply only in so far as is strictly necessary. The legislation that entails such interference must lay down clear and precise rules governing the scope and application of the measure to ensure the interference is limited to what is strictly necessary. This interpretive approach, which includes the teleological[16] and systematic[17] interpretation of EU law, is essential to fill legislative gaps and ensure the effective application and coherence of the two legal acts.

2. ANONYMOUS REPORTING VS. RIGHT TO INFORMATION

2.1. Anonymous reporting

The Directive stipulates that reporting channels must be designed, established, and operated in a secure manner [Hajn and Skupień. 2021]. This manner must ensure the confidentiality of information regarding the identity of the reporting person and any third party mentioned in the report [Olšovská and Hrušovská. 2013]. It must also prevent access to this information by unauthorized employees. This approach is key to ensuring the credibility of reporting channels and protecting whistleblowers against possible retaliatory measures.

---

[16] Teleological interpretation is one of the most important and frequently used methods in the decision-making practice of the Court of Justice of the EU. In interpreting legal norms, it does not limit itself to the wording of the provision but considers its purpose and the objectives pursued by the legislation. This method enables a dynamic interpretation of law, which responds to the needs of the integration process and ensures the effective application of legal rules. See judgment of the Court of Justice of 24 June 2015, C-373/13, H. T. v Land Baden-Württemberg (ECLI:EU:C:2015:413), point 58: "In that context, the meaning and scope of those terms must be determined, in accordance with settled case-law, taking into account both the terms in which the provisions of EU law concerned are couched and their context, the objectives pursued by the legislation of which they form part."

[17] The systematic approach is based on the principle of the unity of the EU legal order. This method examines the position of a specific provision within the entire legal act, its relationship to other provisions, and the context in which the norm is situated. The aim is to ensure internal consistency and the harmonious application of the EU legal order as a whole. See judgment of the Court of Justice of 23 November 1999, C-149/96, Portuguese Republic v Council of the European Union (ECLI:EU:C:1999:574), point 86: "The Court would observe that although it follows from Articles 2 and 3 of the Treaty, and also from Articles 130a and 130e, that the strengthening of economic and social cohesion is one of the objectives of the Community and, consequently, constitutes an important factor, in particular for the interpretation of Community law in the economic and social sphere, the provisions in question merely lay down a programme, so that the implementation of the objective of economic and social cohesion must be the result of the policies and actions of the Community and also of the Member States."

2.2. Right to information

In accordance with the GDPR, individuals have the right to transparent information regarding the processing of their personal data. This information must be provided without undue delay, or within one month, with the possibility of extension by two further months in exceptional cases. According to Article 14(2)(f) of the GDPR, individuals must be informed about the source of their personal data, or whether the data originates from publicly accessible sources.

Article 14(5)(b) of the GDPR sets out exceptions to the duty to inform, if the processing of personal data is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes. These exceptions apply if the obligation to inform individuals is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases, it is essential to demonstrate the public interest in the processing of personal data. The conflict between Directive and the GDPR brings challenges in the area of personal data protection and ensuring the confidentiality of information. Ensuring confidentiality and the protection of personal data is key to the credibility of reporting channels and the protection of whistleblowers. At the same time, it is essential to adhere to the right to information and transparency in accordance with the GDPR, while taking into account exceptions to the duty to inform in cases of public interest.

2.3. GDPR – right to be forgotten

According to Article 17(1)(a) of the GDPR, natural persons have the right to erasure (the "right to be forgotten") of their personal data without undue delay if these data are no longer necessary for the purposes for which they were collected or otherwise processed. This right is crucial for the protection of individuals' privacy and ensures that personal data is not stored longer than necessary. The GDPR also regulates exceptions to the right to erasure of personal data. Furthermore, Article 17(3)(b) of the GDPR sets out exceptions to the right to erasure of personal data. These exceptions apply if the processing is necessary for compliance with a legal obligation under EU or Member State law to which the controller is subject, or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. These exceptions ensure that important data can be retained for purposes that are consistent with the public interest. On the other hand, Directive, in Article 12(1)(b), stipulates that external reporting channels must allow for the permanent retention of information in accordance with Article 18 for the purposes of subsequent investigation. This provision ensures that the information necessary for the investigation is retained for a sufficient period to allow them to be properly reviewed and assessed.

3. THE CONCEPT OF 'PUBLIC INTEREST' AS A KEY TO BALANCING RIGHTS

While Directive and the GDPR address distinct legal aspects and objectives, the concept of public interest serves as a vital tool for finding the necessary symbiosis between them. The Directive explicitly works with the concept of public interest, which is mentioned in its recitals. This public interest can be understood as the protection of the well-being of society and the general interest of the EU, particularly in areas where breaches of law can seriously harm public interests [Pichrt 2013].

The concept is crucial because the right to the protection of personal data, enshrined as a fundamental right, is not an absolute right. Its application requires finding a balance between data protection and other fundamental rights, consistent with the principle of proportionality.

3.1. Public interest and exceptions to the right to information

The core conflict between the Directive and the GDPR often arises concerning confidentiality versus transparency. The Directive mandates that reporting channels must be established and operated in a secure manner to ensure the confidentiality of information regarding the identity of the reporting person and any third party mentioned.[18] This is key to ensuring the credibility of the reporting channels and protecting whistleblowers from retaliation.

Conversely, the GDPR grants individuals the right to transparent information regarding the processing of their personal data, including being informed about the source of their data.

The resolution of this conflict relies on the exceptions provided by the GDPR (Article 14(5)(b)[19]). These exceptions allow the controller to defer

[18] Recital 63 of the Directive 2019/1937: "Lack of confidence in the effectiveness of reporting is one of the main factors discouraging potential whistleblowers. Accordingly, there is a need to impose a clear obligation on competent authorities to establish appropriate external reporting channels, to diligently follow up on the reports received, and, within a reasonable timeframe, give feedback to reporting persons."

[19] Article 14 GDPR establishes the right to information to be provided where personal data have not been obtained from the data subject. This right to information is not applicable if "the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragrap. 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available."

or withhold the duty to inform the data subject if the processing is necessary for purposes of public interest, and if the obligation to inform individuals is likely to render impossible or seriously impair the achievement of the objectives of that processing. Adhering to the right to information and transparency is essential, but must take into account these exceptions in cases where public interest is demonstrated.

3.2. Public interest and exceptions to the right to erasure

A similar conflict occurs regarding data retention. The GDPR grants natural persons the right to erasure (the "right to be forgotten") if their personal data is no longer necessary for the purposes for which it was collected. However, the Directive stipulates that external reporting channels must allow for the durable retention of information for the purposes of subsequent investigation.[20]

The GDPR resolves this tension by stating exceptions to the right to erasure (Article 17(3)(b)[21]). The right to erasure does not apply if the processing is necessary for compliance with a legal obligation under EU or Member State law, or for the performance of a task carried out in the public interest or in the exercise of official authority. These exceptions ensure that crucial data required for proper review, assessment, and investigation purposes related to the public interest can be retained for a sufficient period.

CONCLUSION

The conflict between the Directive and the GDPR presents significant challenges in the area of personal data protection and ensuring information confidentiality. On the one hand, the Directive stipulates that reporting channels must be designed, established, and operated in a secure manner that ensures the protection of the confidentiality of information regarding the identity of the reporting person and any third party mentioned in the report. This approach is key to ensuring the credibility of reporting channels and protecting whistleblowers against possible retaliatory measures.

On the other hand, the GDPR grants individuals the right to transparent information regarding the processing of their personal data. This right also includes the right to erasure of personal data without undue delay if these data

---

[20] For record keeping of records see Article 18 of the Directive 2019/1937.

[21] The right to erasure ("right to be forgotten") shall not apply to the extent that processing is necessary "for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller."

are no longer necessary for the purposes for which they were collected or otherwise processed. The GDPR also sets out exceptions to the right to information and the right to erasure of personal data if processing is necessary for compliance with a legal obligation or for the performance of a task carried out in the public interest.

Ensuring confidentiality and the protection of personal data is key to the credibility of reporting channels and the protection of whistleblowers. At the same time, it is essential to adhere to the right to information and transparency in accordance with the GDPR, while taking into account exceptions to the duty to inform in cases of public interest. This comprehensive approach ensures that personal data is processed in accordance with legal regulations and that the rights of individuals are protected.

REFERENCES

Barancová, Helena, et al. 2019. *Zákonník práce. Komentár*. 2nd ed. Bratislava: C.H. Beck.

Debrecéniová, Janka. 2008. *Antidiskriminačný zákon. Komentár*. Bratislava: Občan a demokracia.

Hajn, Zbigniew, and Dagmara Skupień. 2021. *Ochrona sygnalistów w miejscu pracy w państwach Grupy Wyszehradzkiej, Francji i Słowenii – propozycje zmian*. Łódź: Wydawnictwo Uniwersytetu Łódzkiego.

Križan, Viktor. 2014. "Antidiscrimination law (equality of treatment): introduction." In *Implementation and enforcement of EU labour law in the Visegrad countries*, 31-43. Plomouc: Palacký University.

Nechala, Pavel. 2014. *Chránené oznamovanie (whistleblowing)*. Bratislava: Inštitút pre verejné otázky.

Mičudová, Tatiana. 2016. *Zákon o oznamovaní protispoločenskej činnosti. Komentár*. Bratislava: Wolters Kluwer.

Mičudová, Tatiana. 2019. *Zákon o ochrane oznamovateľov protispoločenskej činnosti. Komentár*. Bratislava: Wolters Kluwer.

Olšovská, Andrea, and Veronika Hrušovská. 2013. "Whistleblowing na pracovisku – právna úprava, teória a prax na Slovensku." In Whistleblowing, 127-43. Praha: Wolters Kluwer ČR.

Pichrt, Jan. (ed.). 2013. *Whistleblowing*. Praha: Wolters Kluwer ČR.