Challenges in the Field of Whistleblower Personal Data Protection in Polish Law Compared to European Solutions

Edyta Bielak-Jomaa[1]
https://doi.org/10.18778/8220-639-5.09

Introduction

The issue of whistleblower protection in the EU has been recognized relatively recently. Until the entry into force of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 of October 2019 on the protection of persons who report breaches of Union law,[2] whistleblower protection had a sectoral nature (it concerned the financial sector). The provisions introducing whistleblower protection in this sector included Regulation (EU) 596/2014 of the European Parliament and of the Council on market abuse (MAR Regulation),[3] and an act issued on the basis of the authorization for the European Commission to issue an implementing act contained in the regulation, i.e. EU Commission Implementing Directive 2015/2392 on Regulation (EU) 596/2014 of the European Parliament and of the Council as regards reporting to competent authorities of actual or potential infringements of that Regulation.[4] Apart from these acts, however, there was no comprehensive whistleblower protection, a situation which exposed them to retaliation.

On the basis of solutions developed in the indicated legal acts and the jurisprudence of the European Court of Human Rights, the Committee of Ministers of the Council of Europe and the Parliamentary Assembly (PACE) began work to develop recommendations aimed at placing the system of protection of persons reporting irregularities in the field of human rights protection in the context of their right to freedom of expression. Moreover, the recommendations assumed that better whistleblower protection would help to combat corruption already at the preventive stage, and would also strengthen the need to build a civil society. The recommendations indicate that an effective reporting process must ensure transparency and anonymity for the person reporting the breach. The fragmentary whistleblower

1 PhD, assistant professor at the University of Lodz.
2 Official Journal of the European Union L 305/17 of 26.11.2019.
3 Regulation 16.04.2014, Official Journal of the European Union L 2014.173.1.
4 MAD Directive, Official Journal of the European Union L 2015.332.126.

protection in the EU so far was the reason why work was commenced to develop a separate, comprehensive act devoted to whistleblowing in the workplace, in the hope to achieve the unification of whistleblower protection standards.

1. Practical problems arising from the lack of regulations regarding the protection of whistleblowers' personal data

There is currently no comprehensive regulation on whistleblower protection in Poland. There are also no provisions relating to the protection of whistleblowers' personal data. The existing sectoral legislation (mainly in the financial sector) protects employees and other whistleblowers from retaliation only to a limited extent. It fails to provide comprehensive regulations regarding the protection of whistleblowers, to define the concept of 'whistleblower' or 'irregularity', to define detailed procedures or mechanisms ensuring safe processing of whistleblowers' personal data. As a result, it should be assumed that whistleblowers in Poland are subject only to the provisions of the General Data Protection Regulation (GDPR) in terms of the protection of their personal data.[5]

In common understanding, a whistleblower is a person who reports or discloses irregularities or ethical doubts regarding behaviour, activities or phenomena occurring in the workplace,[6] a person acting in good will to notify irregularities taking place at the workplace that are detrimental to public interest, and sometimes to the employer,[7] or a person who, acting in good faith and in defence of values that are important from the point of view of social interest, decides to reveal irregularities noticed in the professional environment.[8] A whistleblower is a person who, taking

5 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union, L 119, p. 1.

6 *Sygnalista po polsku – dobre praktyki i rekomendacje wdrożeniowe Budowa systemu zgłaszania nieprawidłowości w oparciu o etykę i wartości*, raport PWC *(The whistleblower in Polish – good practices and implementation recommendations. Building a whistleblowing system based on ethics and values, PWC report)*, https://www.pwc.pl/pl/pdf/sygnalista-po-polsku-poradnik-pwc.pdf, accessed 1/09/2021, E. Andreis, *Towards common minimum standards for whistleblower protection across the EU*, https://www.europeanpapers.eu/en/europeanforum/towards-common-minimum-standards-for-whistleblower-protection-across-eu, accessed 01/09/2021.

7 Online dictionary of new words in Polish, http://nowewyrazy.uw.edu.pl/haslo/ sygnalista.html?pdf=1, accessed 01/09/2021.

8 A. Kobylińska, *Posłańcy złej nowiny. Rola i sytuacja sygnalistów w Polsce i na świecie (Messengers of bad news. The role and situation of whistleblowers in Poland and in the world)*, „Przegląd Antykorupcyjny" 2016, No. 2(7), p. 12.

into account, in particular, the interests of their workplace, and often also the interests of the public, provides (primarily to their superiors, and, in the absence of an appropriate response, also to the relevant law enforcement authorities or the media) information about irregularities that occur in a given workplace.[9] Although the provisions of various acts refer to the issue of whistleblowing, they do not contain a definition of a whistleblower. Likewise, the notion of a whistleblower itself has not been comprehensively regulated in any legal act.

The statutory definition of a whistleblower is included in Article 2 clause 15 of the draft act on transparency in public life, whereby a whistleblower is "a natural person or an entrepreneur whose cooperation with the judiciary consists in reporting information about the possibility of a crime being potentially committed by an entity he or she is bound with by an employment contract, service relationship or other contractual relationship, where this may adversely affect their life, professional and financial situation, and for whom the prosecutor granted the status of a whistleblower." However, this act is currently at the stage of legislative work[10] and neither its final shape nor the date of entry into force are known.

The processing of personal data of whistleblowers who are employees is subject to the data processing rules under GDPR (which indicates the grounds for legalizing data processing, general rights of data subjects, obligations of the data controller, i.e. the employer) and the provisions of the Polish Labour Code, which define the scope of personal data that may be processed on the basis of the need for the employer's execution of the employment relationship. This gap is not filled by the provisions of the Code of Administrative Procedure, which provide public administration bodies with instruments to investigate irregularities reported by persons without disclosing the source of information. Provisions of the Code of Administrative Procedure (Article 61 § 1) enable public administration bodies to investigate such signals by initiating proceedings *ex officio*. Then (pursuant to Article 28 of the Code of Administrative Procedure), only the person against whom the allegations are made becomes a party to it but not the person notifying possible violations. Therefore, the whistleblower is not informed about the course of the procedure and its results, but at the same time their personal data are not disclosed, and thus the whistleblower's privacy is not violated. However, this only applies to administrative proceedings.

The legislation regulating the protection of whistleblowers and their personal data is most fully visible in the Act of 1 March 2018 on counteracting money laundering and financing of terrorism.[11] Pursuant to Article 80 clause 1, the Chief Inspector of Financial Information (Polish: GIFI) is obliged to accept reports of actual or potential violations of provisions on counteracting money laundering and

9 https://poradnikprzedsiebiorcy.pl/-kim-jest-sygnalista-i-jakiej-ochronie-prawnej-podlega, accessed 01/09/2021.

10 https://legislacja.rcl.gov.pl/docs//2/12304351/12465433/12465434/dokument324982.pdf, accessed 01/09/2021.

11 Consolidated text Journal of Laws of 2020, item 971, as amended.

terrorist financing from employees, former employees of obligated institutions or other persons who perform or performed activities for the obligated institutions on a basis other than an employment relationship (whistleblowers). Detailed rules for dealing with whistleblowers' reports are set out in the Regulation of the Minister of Finance of 16 May 2018 on receiving reports of violations of provisions on counteracting money laundering and financing terrorism (Polish Journal of Laws, item 959). The regulation provides for a specific procedure for accepting and handling notifications. First of all, the GIFI is obliged to establish an independent means of communication for the receipt of declarations, separate from the means of communication used in the ordinary activities of the office. The reporting of irregularities is also regulated by the Act of 29 August 1997 – the Banking Law and the Act of 29 July 2005 on Trading in Financial Instruments, both of which require the implementation of procedures for anonymous reporting of violations of the law and ethical procedures and standards applicable in the organization (reporting to a member of the Management Board or a representative of the Supervisory Board) and provide the reporting breaches with protection at least against repressive actions, discrimination or other types of unfair treatment. Such obligations are also provided for in the Regulation of the Minister of Development and Finance of 6 March 2017 on the risk management system and internal control system, remuneration policy and the detailed method of estimating internal capital in banks, and in the Regulation of the Minister of Finance of 29 May 2018 on detailed technical and organizational conditions for investment firms, banks referred to in Article 70 clause 2 of the Act on Trading in Financial Instruments, and custodian banks. The provisions of this act require the institutions (including banks) specified in the Act to develop and implement procedures for anonymous reporting of violations of law by employees and the procedures and ethical standards applicable in these institutions, as well as to ensure that employees can report violations through a special, independent and autonomous communication channel.

As regards other sectoral acts, whistleblower protection is dispersed and fragmented. In the case of whistleblowers who are not employed (officers, persons working under civil-law contracts, interns), it should be noted that such individuals are not covered by any protection against repressive actions. This means that whistleblowers currently have virtually no legal safeguards against potential retaliation, as there is no guarantee of the confidentiality of the whistleblower's data and the persons assisting the whistleblower, or the whistleblower's family.

The lack of a whistleblower protection system raises the question of whether whistleblowers should be protected under the same terms and conditions in the private and public sectors. There is no regulation that would answer the question of whether people from inside or outside of the organization are protected (employees, former employees, collaborators). It is not clear whether whistleblower protection applies only to current violations (or suspected violations) or also to those that occurred in the past. This is important from the perspective of the processing of the employee's personal data because, in the light of the applicable regulations, the

employer may process the employee's personal data on a basis other than the fact of being a former employee, and therefore for a different purpose.

From the point of view of the protection of whistleblowers' personal data, the lack of a whistleblower protection under the Polish law is also serious. The Labour Code does not provide for solutions that would oblige the employer to take any action to protect whistleblowers, nor does it entitle the employer to introduce such solutions in internal regulations (e.g. work regulations). This raises further questions as to where the whistleblower should report irregularities or suspected irregularities and whether the whistleblower should first inform their immediate supervisor (only the superior), who will then forward the information to the employer, or whether the employee can directly notify the employer and how (orally, in writing, electronically, using an internal form) and whether the information should be sent to the indicated department. Failure to indicate the possibilities, channels and methods to signal violations means that it becomes unclear who has access to the whistleblower's personal data in an organization, under what terms, and which whistleblower's data may be processed in connection with irregularity reporting. It should be emphasized that the employer is the controller of the employee's personal data. Neither the immediate superior nor employees of the indicated department may have access to personal data which may need to be processed to report irregularities. There is no indication whether the entity (division, department, indicated person) is supposed to act under a general authorization or a special authorization to process the whistleblower's personal data, and whether this authorizes them to report violations outside the organisation, i.e. to law enforcement agencies, the media, or public opinion.

Another problem that arises in this context is the protection of whistleblowers' personal data and, more specifically: the rules for disclosing personal data, the prohibition of disclosing their personal data to the public, the legal basis to legalize the processing, the place of processing (whether the information signalled by an employee should be stored in employee's personal file or in separate documentation kept for all whistleblowers and reported irregularities), the time of data processing, as well as rules for data removal. The provisions of the Labour Code provide for data retention periods for the purposes of executing an employment relationship or fulfilling obligations arising under specific provisions (e.g. provisions on pursuing claims from an employment relationship, provisions on archiving), but they do not apply to whistleblower data retention. Therefore, it is not clear whether the period of storing the whistleblower's personal data should be related to the period of employment with a given employer (a person providing work on a different basis for the period of work for a specific entity) or to another period, longer than the period of employment.

Another problem directly related to the procedures for reporting breaches and the principles of personal data processing, in particular the principle of data security, is the processing of personal data of job candidates who report irregularities in the recruitment process.

The lack of legal regulations regarding whistleblowers and the protection of their personal data also leads to the lack of guarantees of whistleblowers' rights: the right to access and correct data, and the right to be forgotten.

2. Protection of whistleblowers' personal data in the Directive on the protection of persons who report breaches of Union law

This situation will have to change given the need to implement Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 of October 2019 on the protection of persons who report breaches of Union law, which must be implemented into the Polish legal system by 17 December 2021. The aim of the Directive is to introduce common standards for the protection of persons reporting illegal activities or abuses of law, both in the private and public sectors, who have obtained information on breaches in a work-related context in the following areas (Article 2): public procurement, services, products and financial markets and the prevention of money laundering and terrorist financing, product safety and compliance, transport safety, environmental protection, radiation protection and nuclear safety, food and feed safety, animal health and welfare, public health, protection of consumers, the protection of privacy and personal data and the security of information networks and systems, the financial interests of the Union, breaches of the Union competition rules and state aid, as well as breaches of the internal market in relation to activities which constitute an infringement of corporate tax law or aimed at obtaining a tax advantage contrary to the object or purpose of the applicable provisions on corporate tax. It should be emphasized, however, that the Directive provides for a minimum scope of whistleblower protection, and therefore EU Member States may introduce a broader scope of protection in their national regulations and cover areas and sectors other than those indicated in Article 2 of the Directive.

Directive 2019/1937 states that a whistleblower should be defined as anyone who, while working in the private or public sector, obtains information on breaches in a work-related context, including at least:

- employees (including civil servants and former employees),
- volunteers, interns and other people working with the organization, even if they are not paid,
- self-employed individuals (including people cooperating with the organization on the basis of managerial contracts or B2B contracts),
- shareholders, partners and persons performing functions in the bodies of the organizational unit,

- contractors, subcontractors, suppliers and persons acting under their supervision, i.e. their employees or persons employed by them, whistleblowers should also be understood as persons whose employment relationship with a given employer has already ended or is about to be established (whistleblower protection applies to information obtained in the course of recruitment or negotiations related to the acceptance of a position). The protection provided for whistleblowers will also apply to persons assisting in submitting a report, as well as to those who, although not personally involved, would be exposed to retaliation due to the report.

In order for a person to be considered a whistleblower, it is not enough for them just to report information about irregularities. A person who discloses information about irregularities to the public enjoys the protection under Directive 2019/1937 only if one of the following conditions is met:

a) internal or external reports were made prior to public disclosure and no appropriate timely action was taken as a result of those reports;
b) the person has reasonable grounds to believe that the disclosed breach may constitute a direct or obvious threat to the public interest; or

that they will face the risk of retaliation in case of internal or external reporting; or there is a low probability of effective remedying the breach due to the specific circumstances of the case, such as the possibility of concealing or destroying evidence or the possibility of collusion between the authority and the perpetrator of the breach or the authority's involvement in the breach.

In the light of Article 5 of the Directive, a notification is defined as each communication of information on infringements, both in writing and orally. An oral notification is primarily a telephone notification or notification via other voice telecommunication systems as well as reporting in the course of a previously arranged meeting with persons designated to receive such reports. Reporting includes information about violations, including reasonable suspicion, regarding actual or potential violations that have occurred or are likely to occur in the organization where the reporting person works or worked, or in another organization with which the reporting person maintains or has maintained contact in the context of the work performed, or concerning attempts to conceal such violations.

3. Whistleblower personal data protection: The perspective of Polish law

One of the key concerns regarding whistleblower protection is the protection of their personal data. There is no doubt that the whistleblowing system is a challenge in terms of ensuring the security of the processing of personal data of persons who

report a breach. When implementing a breach, an important aspect is to ensure that the personal data of all participants in the proceedings are protected and that the rights of the data subjects are respected. Since whistleblowers' reporting of breaches by may be open or anonymous, it must be remembered that it is the whistleblower who has the right to decide whether or not they want to disclose their identity when reporting a breach. In this context, the primary duty of the employer is to ensure the confidentiality of the whistleblower's personal data so as to ensure their safety from retaliation. This should be done by defining and implementing procedures for reporting violations, defining the rules of operation for the reporting channels, keeping whistleblowers' personal data confidential, fulfilling the information obligation and ensuring compliance with whistleblowers' rights in terms of personal data protection. The legislator should take into account the means of protection against retaliation available to the whistleblower and other persons protected alongside the whistleblower. For this purpose, it seems necessary to harmonize sectoral regulations, link these provisions with the provisions on the protection of personal data by creating uniform and comprehensive whistleblower protection mechanisms. It is worth noting that the protection of whistleblowers' personal data should include organizational and technical measures.

Therefore, it can be postulated that the Act should set out obligations for employers to introduce procedures specifying the rules for reporting violations, which should be transparently described by employers, available, and presented to employees, associates, contractors and business partners. The employer should develop documents and apply the procedures specified therein: counteracting irregularities, reporting them, and responding to violations. It would also be important to oblige the employer to introduce a policy to manage the occurring violations. Such a policy should regulate the operation of the reporting system, covering, inter alia, specification of the violation or its nature, the person or team responsible for accepting reports, the method of receiving violation reports, confidentiality and personal data protection rules, deadline for deleting personal data, actions taken after notification of violations. Documents developed by the employer should be specific at the level of the organization, define threats in a specific entity, set out a detailed procedure, indicate the tasks and responsibilities of the indicated departments or designated employees to receive whistleblowers' notifications, violation reporting forms, and the deadline for reporting. It would also be important to indicate when, how often and how employers should provide employees with information about the possibility of reporting violations. At the employer's level, the documents and procedures should be clarified, taking into account the singularities of the entity concerned.

3. 1. Channels for reporting violations

Information on breaches may be reported through the internal reporting channels (Article 7 of the Directive), via the external channel (Article 10) or public disclosure

(Article 15). Although the EU legislator does not explicitly indicate that the whistleblower should first use the internal channel for reporting violations, it seems that this is most often the natural way of reporting violations. Prior to public disclosure, the whistleblower should report either internally or externally. If no appropriate action has been taken in a timely manner following these reports, the whistleblower should resort to public disclosure, provided that the breach can be remedied by internal means, rather than disclosing the whistleblower to public authorities.[12] Pursuant to Directive 2019/1937, Member States, and through them private organizations, should encourage people who are aware of breaches to submit internal reports.

3.1.1. Internal channels

The design of internal channels of communication about violations may depend on the employer's size, organizational structure, industry or sector of operation, available financial resources or the level of risk of potential fraud. It seems, therefore, that the situation of employers and, consequently, their obligations in terms of creating and maintaining internal channels may vary. An employer with a more complex structure, employing a large number of employees, cooperating with a larger number of contractors, operating in market segments at risk of breaches, who is a public authority or a critical infrastructure entity, operating in a larger territory, will have to engage more organizational, technical and financial measures to handle a reporting channel than a smaller employer, covering a smaller territory, employing fewer people and operating in an area less exposed to the risk of breaches.[13] An employer with a large and complex organizational structure should introduce solutions consisting in the creation of an internal team (department, division) with specialists in explaining various cases of irregularities. Taking into account the complexity of the structure, e.g. whether the business activity is conducted in the form of a main organizational unit and its subsidiaries, and their location in different countries, the employer will have to develop a methodology of conduct, find out where irregularities are signalled (headquarters or a branch), and decide on an operating procedure. It is permissible for the preliminary procedure, under which the whistleblower reports the violation, to be initiated at the branch, and the remaining parts (clarification, evidence) as well as the decision to be made by the central unit. This solution allows for the concentration of experts in the field of infringements in one place, ensuring that they have access to all information

12 More on the role of social networks in whistleblowing: H. Lam, M. Harcourt, *Whistle-blowing in the digital era: motives, issues and recommendations*, New Technology, Work and Employment, 2019.

13 A. Kantor Kilian, *Organizacja modelu kanałów sygnalizowania nieprawidłowości w świetle dyrektywy 2019/1937 (Organization of the model of whistleblowing channels in the light of Directive 2019/1937)*, [in:] B. Baran, M. Ożóg (eds.), *Ochrona sygnalistów. Regulacje dotyczące osób zgłaszających naruszenia (Whistleblower protection. Regulations concerning persons reporting irregularities),* Wolters Kluwer, Warsaw 2021.

necessary to conduct the proceedings, and ensures efficient cooperation.[14] Therefore, experts should be equipped not only with the knowledge of violations of the law, knowledge of the functioning of the organizational unit, working methods for a given employer, but also the knowledge about the protection of personal data. They should have detailed employer prerogatives, authorizing them to access full documentation, to communicate with all persons whose clarifications may contribute to a fair settlement of the matter within a reasonable time, ensuring cooperation and information exchange. From the point of view of personal data protection, it is extremely important that these persons have specific authorizations to process personal data for the purpose of resolving the signalled case and recognizing that there has been a breach or not, and that they are obliged to ensure special confidentiality of whistleblowers and other persons.

For employers with complex organizational structures, in particular those conducting cross-border activities, the availability of internal signalling may mean not only the possibility of easy transfer of information, in many formats (also going beyond traditional paper), but also the possibility of using a dedicated telephone line, website or e-mail box, and to enable signalling in different languages.

In the case of employers with a less complex organizational structure, or operating in a sector or industry not exposed to the risk of irregularities, or with limited organizational and financial resources, if there is no need or possibility to set up a separate team for internal investigations, these activities may be undertaken by an indicated person. However, it should be emphasized that this person must have appropriate knowledge in the field of dealing with infringements as well as the laws and practices regarding the processing of personal data.

If it is not possible to establish an internal channel, the employer may consider using an external expert or an entity to conduct internal proceedings. This may take place when there is a need to use a consultant's specialist knowledge or experience, in particular when internal resources do not allow certain activities (e.g. data protection and analysis), or when it is not possible to conduct proceedings due to the fact that the reported breach refers to a management team member (a senior manager, a member of the management board or the supervisory board) or it is impossible to ensure the independence or impartiality of the opinion of the person or persons appointed to conduct the proceedings, or to avoid a conflict of interest.[15] It should also be noted that such circumstances should also be provided for in the documentation of internal proceedings. Personal data of an external entity should be processed under an entrustment agreement, specifying the kind of data to be processed and the purpose of processing. The employer who is the data controller should also reserve the possibility for the processor to control and audit the principles of personal data protection.

14 *Ibidem*.

15 D. Tokarczyk, *Whistleblowing i wewnętrzne postępowanie wyjaśniające (Whisteblowing and internal investigation)*, Wolters Kluwer, Warsaw 2020.

3.1.2. External channels

External reporting channels are available for whistle-blowers who do not wish to use internal channels, e.g. for fear of retaliation or where there are no internal reporting channels, e.g. because there are no legal bases to create them or if they are not created by the employer of such a channel. The whistleblower may report the breach to the competent authority if:

- they have reported the breach previously through an internal channel, but the issue is still not resolved,
- there are reasonable grounds to suspect that the whistleblower will suffer retaliation as a result of an internal report, or that the competent authorities would be more appropriate to run an investigation. Member States are required to designate competent authorities to receive reports, provide feedback and follow-up. The reporting procedures in this case should generally meet the same conditions as under internal channels, including the obligation to notify the reporting person of the decision and its justification. The authorities receiving the notification also have the same obligations, e.g. regarding the identification of a procedure to protect against retaliation and the availability of confidential advice to those considering reporting.

3.2. Protection of whistleblowers' personal data confidentiality

The internal channel for reporting violations collects personal data of various people, coming from various sources, such as documents, applications, IT systems, messaging systems, emails, explanatory interviews etc. The personal data processing rules must be observed in the course of the proceedings. This results directly from the provisions of Directive 2019/1937, which obliges Member States to ensure that the implementing provisions provide for the principles of processing and protection of personal data, in accordance with the GDPR provisions (recitals 83–85, Article 13(d) and Article 17). Taking this requirement into account, it should be assumed that the legislator should refer to the provisions of the GDPR, in particular to Article 6 of the GDPR, which defines the conditions for the lawful processing of personal data. Under this provision, the processing of personal data is legal if:

- the data subject has consented to the processing of their personal data for one or more specific purposes,
- processing is necessary to perform a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract,
- processing is necessary to fulfil the legal obligation incumbent on the controller,

- processing is necessary to protect the vital interests of the data subject or another natural person,
- processing is necessary to perform a task carried out in the public interest or in the exercise of public authority entrusted to the controller,
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where these interests are overridden by the interests or fundamental rights and freedoms of the data subject, which require protection of personal data, in particular when the data subject is a child.

In the current legal order, the premise for the processing of whistleblowers' personal data is the fulfilment of the legal obligation incumbent on the controller with regard to the provisions governing mandatory whistleblowing procedures, whereas in other cases it is the existence of a legitimate legal interest, i.e. preventing irregularities at the workplace.

It is worth noting, however, that the employer may also process other types of data, belonging to a specific category of data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and the processing of genetic data, biometric data in order to uniquely identify a natural person or data regarding the health, sexuality or sexual orientation of that person (Article 9(1) of the GDPR). As a rule, the processing of this category of personal data is prohibited, and the conditions of admissibility of their processing are specified in Article 9(2) of GDPR. In explanatory proceedings, the grounds for legalizing data processing may include the consent of the data subject, the need to process such data in order to fulfil the controller's obligation, or the need to process such data in order to establish, assert or defend claims.

From the point of view of the confidentiality of whistleblowers' data, other rules of personal data processing (apart from the lawfulness rule discussed above) are also extremely important. In the light of Article 5 of GDPR, personal data should be processed in a fair and transparent manner for the data subject, collected for specific, explicit and legitimate purposes and not processed further in a manner inconsistent with these purposes.[16] In relation to infringement reporting procedures, the aim is to prevent irregularities from occurring, to reliably establish all circumstances of infringements or potential infringements, and to take measures against persons responsible for infringements. Data processed for the purposes of infringement proceedings must also be adequate, relevant and limited to what is necessary for the purposes for which they are processed. Such data must also be accurate, stored for no longer than necessary, and processed in a manner ensuring

16 P. Drobek, *Komentarz do art. 5 RODO (Commentary on Art. 5 GDPR)*, [in:] E. Bielak-Jomaa, D. Lubasz (eds.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz (GDPR. General Data Protection Regulation. Commentary)*, Warsaw 2018, pp. 326–328.

their appropriate security, including protection against unauthorized or unlawful processing and accidental loss, destruction or damage, and with the use of appropriate technical or organizational measures.

In its capacity of controller, the employer who obtains data from a person should fulfil the information obligation specified in Article 13 of GDPR. In connection with the procedure for reporting a violation or suspecting a violation, the employer is obliged to provide the whistleblower with information, inter alia, on the basis and purpose of processing their data, the processing time and the rights of the whistleblower in the context of processing such data. From the point of view of the whistleblower's personal data protection, the main issue is to ensure confidentiality and the need to maintain anonymity. In this regard, Article 29 Data Protection Working Party stated that anonymity will not prevent effective 'guessing' of the source of the information and will not focus third parties' attention on the substance of the breach reported rather than the potential source of information. Anonymity prevents internal investigators from asking additional questions after receiving information, and fosters bad faith whistleblowing and hampers whistleblower protection, especially when guaranteed by law.[17] In turn, the European Data Protection Supervisor (EDPS), in his recommendations for officials of EU institutions, indicates that maintaining confidentiality and anonymity is a guarantee for the security of signalling through the internal channel and may constitute an incentive for those employees who, fearing retaliation, would not opt for signalling if their data were to be disclosed.[18] According to the position of the EDPS, a whistleblower's data may be disclosed only if the person concerned agrees to that or for the purposes of criminal proceedings resulting from the reported irregularities. The protection related to ensuring confidentiality and anonymity should not extend to those who knowingly provide false information. Even in this case, the personal data of such a person should be protected, at least until it is proved that the information signalled is false (the burden of proof rests with the institution that employs the informant), in order to protect against possible stigmatization among the professional community. One must agree that data protection rules can be used to strengthen whistleblowing procedures, as the application of data protection rules helps to create reliable channels by enhancing the security of whistleblowing procedures.[19]

17 Article 29 Data Protection Working Party, *Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime*, p. 11, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp117_en.pdf, accessed 1/09/2021.

18 EDPS, *Guidelines on processing personal information within a whistleblowing procedure*, p. 6, https://edps.europa.eu/sites/default/files/publication/19-12-17_whisteblowing_guidelines_en.pdf, accessed 1/09/2021.

19 *Ibidem*, p. 5.

Conclusions

As indicated above, there is currently no comprehensive whistleblower protection regulation in Poland. The directive, which aims to unify national systems and introduce minimum standards of whistleblower protection, should be viewed as an opportunity to introduce legal solutions that will ensure genuine whistleblower security. For this purpose, the Polish legislator should create a uniform model of whistleblowing as an institution. It seems that comprehensive whistleblower protection should be regulated in a separate legal act.[20]

It would be reasonable, therefore, at the level of an act of law, following the Directive, to recognize that the protection may cover employees and persons performing work also outside the employment relationship, persons cooperating with the employer, former employees, candidates for employees, and interns.

It is also worth noting that the provisions of the act implementing the Directive introduce and specify the circumstances that allow the use of the external channel for reporting violations, bypassing the internal channel, and designate authorities (e.g. the police, prosecutor's office, tax offices, customs authorities) which are responsible for receiving information from the declarant, confirming their receipt and conducting follow-up activities aimed at solving the reported problem.

The legislator should also introduce solutions that ensure the confidentiality of whistleblowers' personal data and exhaustively indicate the reasons for their disclosure by recognizing that the rule is keep the data secret. Disclosing personal data without the whistleblower's consent could be treated as a retaliatory action. As a general principle, whistleblowing should not be anonymous. Whistleblowers should provide information about themselves in order to ensure effective protection against retaliation and to minimise the potential abuse of whistleblowing procedures. Anonymous signalling could permitted under specific circumstances. The French supervisory authority (CNIL) indicates that anonymous reporting can be processed if: the description of the violation is sufficiently detailed, specific precautions have been taken, such as prior analysis by the first recipient of the report of the legitimacy of its dissemination within the whistleblowing management system.

For this reason, controllers should implement internal notification channels and information protection. The identity of a whistleblower who reports a violation should be treated as confidential in order to protect him against any form of retaliation. From the point of view of the protection of whistleblowers' personal data, it is important to have a functionality in place within the IT system to ensure anonymity of the notification (the system is operated by the IT department responsible for network security, and therefore, even if the name is not provided, employees of this department can identify the whistleblower)[21].

20 H. Szewczyk, *Whisteblowing. Zgłaszanie nieprawidłowości w stosunkach zatrudnienia (Whistleblowing, Disclosing irregularities in employment relationships)*, Scholar, Warsaw 2020, pp. 312–314.

21 H. Jo, J. Nam, S. Shin, *NOSArmot: Building a Secure Network Operating System*, Security and Communication Networks, 2018.

Another element that should be regulated at the level of the act dedicated to the protection of whistleblowers concerns the need to introduce the obligation for the employer and other employees not to retaliate against the whistleblower (e.g. by extending the scope of the premises of employees' organizational liability). Such an obligation would need to be introduced into the Labour Code and regulations governing specific types of employment, e.g. officers or interns[22].

The legislator should also regulate the issues related to the methods of providing feedback to the whistleblower (the manner of providing the information and indicating the person/department/team that provides this information) with the obligation to maintain confidentiality and impartiality. It should be remembered that the contact with the person or persons appointed to conduct the reporting procedure will usually need to occur on more than one occasion. The very notification of a violation or suspected violation will require feedback: confirmation of receipt, information about the initiation of the procedure, request for additional information or clarifications. This means that the smallest possible number of people should communicate with the whistleblower to improve the guaranteed confidentiality of the whistleblower's data.

The provisions of the legal act should oblige employers (employing entities) to develop and implement whistleblower data processing procedures. This can be done, for example, in an annex to the work regulations. A desirable solution would also be to encourage employers to develop and implement codes of conduct / codes of good practice in a given entity, which would provide for specific procedures, indicate the methods and forms of communicating irregularities, indicate the persons responsible for the processing of whistleblowers' personal data, and clearly define the rules for exercising whistleblowers' rights with regard to their personal data and indicate the forms of training, including training in the area of whistleblower personal data[23]. The scope of the procedure must be clear and transparent to avoid abuses when reporting irregularities. The purpose of the whistleblowing procedure must therefore be clearly stated in internal rules and documents. They should clearly set out the circumstances for using different information channels when reporting breaches.

Finally, and importantly, the legislator should oblige the employer to provide reliable and transparent information to whistleblowers about their rights. The requirement of fairness is related to the need for the controller to take into account the interests and legitimate expectations of the data subject. This principle is understood broadly and requires a balance between the right to personal data protection and the interests of data processors (i.e. the whistleblower's right to protect personal data and their confidentiality, and the employer's interest to use this information in order to proceed with infringement. What matters is the principle of transparency: personal data processing operations should be transparent to data subjects. As part of the

22 H. Hassink, M. de Vries, L. Bollen, *A Content Analysis of Whistleblowing Policies of Leading European Companies*, Journal of Business Ethics 75, 2007, pp. 37–40.

23 R. Moberly, *Confidentiality and Whistleblowing*, 96 N. C. L. Rev. 751, 2018, p. 759.

implementation of this principle, the provisions of the regulation significantly expand the obligations regarding the information to be provided to data subjects. Among others, data subjects are enabled to exercise their powers whereas the controller is required to formulate messages addressed to data subjects in clear and plain language.

It is also worth adding that the employer should be obliged to raise employees' awareness of the importance of whistleblowing, the need to report violations, rules of conduct in the event of becoming aware of a potential violation, responsibility for the processing of personal data in the organization and maintaining confidentiality of all information related to the reports that they may come across within individual or team activity.

Abstract

In this chapter, the author presents the problem of the protection of whistleblowers' personal data in the workplace in connection with the processing of their data in the channels for reporting breaches in the context of the transposition of the Directive on the protection of persons who report breaches of Union law into Polish law. The existing regulations ensure limited protection for employees and other individuals against retaliation or violation of privacy. The author postulates the necessity to develop comprehensive whistleblower legislation. The purpose of the legislation will be to oblige the employer to develop and implement solutions that will guarantee genuine confidentiality and protection of whistleblowers' personal data.

Bibliography

Drobek P., *Komentarz do art. 5 RODO (Commentary on Art. 5 GDPR)*, [in:] Bielak-Jomaa E., Lubasz D. (eds.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz (GDPR. General Data Protection Regulation. Commentary)*, Wolters Kluwer, Warsaw2018.

Hassink H., de Vries L. Bollen M., *A Content Analysis of Whistleblowing Policies of Leading European Companies*, Journal of Business Ethics 75, 2007.

Jo H., Nam J., Shin S., *NOSArmot: Building a Secure Network Operating System*, Security and Communication Networks, 2018.

Kantor Kilian A., *Organizacja modelu kanałów sygnalizowania nieprawidłowości w świetle dyrektywy 2019/1937 (Organization of the model of whistleblowing channels in the light of Directive 2019/1937)*, [in:] Baran B., Ożóg M. (eds.), *Ochrona sygnalistów. Regulacje dotyczące osób zgłaszających naruszenia (Whistleblower protection. Regulations concerning persons reporting irregularities)*, WKP, Warsaw 2021.

Kobylińska A., *Posłańcy złej nowiny. Rola i sytuacja sygnalistów w Polsce i na świecie (Messengers of bad news. The role and situation of whistleblowers in Poland and in the world)*, Przegląd Antykorupcyjny No. 2(7), 2016.

Lam H., Harcourt M., *Whistle-blowing in the digital era: motives, issues and recommendations*, New Technology, Work and Employment, 2019.

Moberly R., *Confidentiality and Whistleblowing*, 96 N.C. L. Rev. 751, 2018.

Sygnalista po polsku – dobre praktyki i rekomendacje wdrożeniowe Budowa systemu zgłaszania nieprawidłowości w oparciu o etykę i wartości, raport PWC (The whistleblower in Polish – good practices and implementation recommendations. Building a whistleblowing system based on ethics and values, PWC report), https://www.pwc.pl/pl/pdf/sygnalista-po-polsku-poradnik-pwc.pdf, accessed 01/09/2021.

Szewczyk H., *Whisteblowing. Zgłaszanie nieprawidłowości w stosunkach zatrudnienia (Whistleblowing, Disclosing irregularities in employment relationships)*, Scholar, Warsaw 2020.

Tokarczyk D., *Whisteblowing i wewnętrzne postępowanie wyjaśniające (Whisteblowing and internal investigation)*, WKP Warsaw 2020.