ISSN 2029-1701
ISSN 2335-2035 (Online)

Research Journal
PUBLIC SECURITY AND PUBLIC ORDER
2021 (26)

ASSURANCE OF THE RIGHT TO PRIVACY AND THE PROTECTION OF PERSONAL DATA IN LABOUR RELATIONS

Eglė ŠTAREIKĖ
Mykolas Romeris University
Maironio st. 27, LT 44211 Kaunas
E-mail egle.stareike@mruni.eu
ORCID ID: 0000-0001-7992-991X

DOI: 10.13165/PSPO-21-26-26

Abstract. *Daily work activities of employees and performance of their job functions are inseparable from ensuring the right to privacy and the protection of personal data. The recent era and adaptation to new working conditions such as remote work, difficulty of separating corporate and private life, and use of new IT tools pose new challenges to employee privacy and protection of personal data. Monitoring of employees, checking of correspondence, collecting information about employees, storage of such information, and its transfer to third parties concern both the right to privacy of employees and protection of their personal data.*
Object of the article – assurance of employee rights to privacy and protection of personal data.
The purpose of the article is to analyse the content of employee right to privacy and protection of personal data and to identify the main problems related to violations of these rights in order to properly understand and comply with the legal framework.
The relevance of this research paper is linked with the assurance of the employee right to personal data protection and privacy requirements, appropriate personal data processing of employees, identification of the nature of violations, and provision of recommendations seeking to avoid them.

Keywords: *right to privacy, protection of personal data, labor relations, GDPR.*

Introduction

Numerous everyday tasks of employees such as performance and fulfilment of work functions and duties pertain to data protection and processing and simultaneously encompass the right to private life. Employee data are often processed in the course of labour relations and quite often before they even start – during recruitment and sometimes even after the labour relations have ended. Covid-19 pandemic, globalisation processes, development of information technologies and new data processing methods, spreading of remote work as a work organisation form, and blurring of boundaries between professional and personal life pose new challenges to the right of employees to privacy and implementation of personal data protection assurance.

From the European perspective, there are no specific mandatory legal acts that would entrench particularly the protection of employee‘s privacy and personal data in labour relations. Breach of the right to personal data protection simultaneously results in the breach of the person’s privacy. Personal data processing at workplaces and the right of employees to privacy are applied the general data processing rules and principles provided for in the legal framework of the European Union and of the Council of Europe, when employees have the same rights as those guaranteed for the data subjects. More specific rules governing personal data protection in the context of labour relations have to be sought in national legal acts as well as recommendations and guidelines of the European Union and of the Council of Europe.

It is noteworthy that the legal governance of both the European Union and Council of Europe (encompassing both the binding legislation and the rules of recommendatory nature) represent two separate legal frameworks that are nonetheless closely interrelated and

supplement each other in order to establish and ensure the employee right to privacy and personal data protection.

The relevance of this research paper is linked with the assurance of the employee right to personal data protection and privacy requirements, appropriate personal data processing of employees, identification of the nature of violations, and provision of recommendations seeking to avoid them. Object of the article – assurance of employee rights to privacy and protection of personal data. The purpose of the article is to analyse the contents of employee right to privacy and the protection of personal data and to identify the main problems related to violations of these rights in order to properly understand and comply with the legal framework.

In the research paper, the following theoretical and empirical methods have been used: comparative analysis, logical-analytical method, and system analysis. The comparative analysis method was applied seeking to compare the contents and legal regulation of the employee right to personal data protection and the right to privacy. Logical-analytical method was used to analyse the requirements posed to employee personal data processing seeking to ensure the employee privacy. The same method was also invoked for the analysis of principles for the processing of employees' personal data as manifestation of the right to privacy. The logical-analytical method and system analysis method were used for disclosure of the relationship between the legal acts and legal doctrine, and different legal rules, for the summing up of the research paper, disclosure of the key problems, provision of recommendations, and formulation of conclusions.

Legal regulation context ensuring the employee right to personal data protection and privacy

Common legal acts of the European Union applied for the personal data protection in labour relations include the Charter of Fundamental Rights of the European Union and General Data Protection Regulation (hereinafter – GDPR).

Article 7 of the Charter of Fundamental Rights of the European Union (*Charter of Fundamental Rights of the European Union* (CFR), OL 7.6.2016, C 202/391) accentuates a person's right to private and family life stating that everyone has the right to respect for their private and family life, inviolability of their home and secrecy of correspondence. Article 8 of the same enshrines the protection of personal data where everyone has the right to the protection of personal data concerning them, whereas such data must be processed appropriately and used only for specified purposes and only with the consent of the person concerned or on other legitimate grounds laid down by the law (Article 8 of the CFR).

As of 25 May 2018, European Union member states started applying the GDPR that has repealed Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data that had been used as the basis for personal data processing in the EU member states. The objective of GDPR to ensure real personal data protection, to protect the rights of individuals in the digital space, and to reinforce the fight against crimes is cited as an incentive to have a uniform and updated legal act in all European Union member states for the governing of personal data protection. The key goals of the personal data protection reforms included strengthening the rights of the data subjects, including employees, establishing the responsibility of data processors and subprocessors, and ensuring transparent and reliable personal data regulation and processing (*Štareikė, Kausteklytė-Tunkevičienė*, 2018).

Besides the general data protection provisions, article 9(2) of the GDPR embeds a possibility for the employer to process special data of the employees when processing is

necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services. Article 88 of the GDPR prescribes that member states may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context (*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* (GDPR)).

Furthermore, although the explanations of the Article 29 Working Party, replaced following the coming into force of GDPR by the European Data Protection Board, laid down in the Opinion 2/2017 on data processing at work are not binding, they are, nonetheless, important. This opinion supplemented earlier publications of the Article 29 Working Party – Opinion 8/2001on the processing of personal data in the employment context (*Article 29 Working Party – Opinion 8/2001 on the processing of personal data in the employment context*, 5062/01/EN/Final, WP 48, 2001 (Article 29 Working Party – Opinion 8/2001)) and Working Document on the surveillance of electronic communications in the workplace (*Article 29 Data Protection Working Party, Working Document on the surveillance of electronic communications in the workplace*, 5401/01/EN/Final, WP 55, 2002 (Article 29 Working Party – WP 55)).

Protection of employee data and the right to privacy are also governed by the European Union legal acts and documents of recommendatory nature. Among the most important of them is the European Convention for the Protection of Human Rights and Fundamental Freedoms (*European Convention for the Protection of Human Rights and Fundamental Freedoms* (ECHR), Council of Europe, Rome, 1950). Article 8 of the ECHR embeds the individual‘s right to the respect for private and family life: (i) everyone has the right to respect for his private and family life, his home and his correspondence; (ii) there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Another important international document, the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108), was opened for signature yet back in 1981, well before the era of internet and electronic communications. The development of technologies and globalisation of information posed new tasks and highlighted the existing problems in the field of personal data protection. In 2018, the modernised Convention (i.e. Convention 108 modified by the amending Protocol) has a uniform scope of application for all Parties to the Convention, without the possibility to fully exclude sectors or activities from its application. It thus covers all types of data processing under the jurisdiction of the Parties, in both the public and private sectors.

The amending Protocol significantly increases the level of data protection afforded under Convention 108. Notably, the modernised Convention further specifies the principle of lawful processing, further strengthens the protection of special categories of data and also strengthens the rights of the data subjects, especially with regard to transparency and access to data (*Proposal for a Council Decision authorising Member States to ratify, in the interest of the European Union, the Protocol amending the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (ETS No. 108), 2018).

The Council of Europe Modernised convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data with the amendments adopted by the Committee of Ministers of the Council of Europe (*Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data*, 128th Session of the Committee of Ministers, Elsinore, Denmark 17-18 May 2018 (Convention 108+)) is a legally binding multilateral agreement in the field of personal data protection. The aim of the Convention is the protection of the right to privacy when processing personal data automatically, respect for the rights of each individual, simultaneously those of employees, and fundamental freedoms in the territories of all states, irrespective of their nationality and place of residence, regulation of international data transmission and, most importantly, assuring the right of the individuals to privacy.

European Social Charter (revised) (*European Social Charter (revised),* Strasbourg, 1996 (ESC)) is yet another important legal regulation document of the Council of Europe. It establishes the rights of employees, including the right to information and consultation (Article 21 of ESC).

Noteworthy are other documents of the Council of Europe that have no binding legal power. Recommendation CM/Rec(2015)5 on the processing of personal data in the context of employment (*Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment* (Recommendation CM/Rec(2015)5)) defines specific rules for data processing in the context of employment relations. Moreover, Recommendation No R(86) 1 on the protection of personal data (*Recommendation No. R (86) 1 of The Committee of Ministers To Member States on the Protection of Personal Data Used for Social Security Purposes*) used for social security purposes establishes the respect for the privacy of individuals when collecting, using, transferring, and storing personal data used for social security purposes. It also prescribes appropriate controls sufficient for assuring data protection in each social security institution.

The Law on Legal Protection of Personal Data of the Republic of Lithuania (hereinafter – LLPPD) (*Official Gazette* 1996, No. 63-1479), is one of the most important national legal acts in the field of data protection. Article 5 establishes the criteria for the processing of personal data pertaining to labour relations. First, it prohibits the processing of personal data relating to the record of conviction or criminal acts of a candidate applying to the position or function, or those of employee, except in the cases where such personal data are necessary in order to verify that the person satisfies the requirements for the position or function provided for in the laws and implementing legislation. The law also establishes that a prospective employer or company may collect the personal data of a candidate applying to the position or function pertaining to their qualification, professional skills, or work-related personal qualities from former employers after notifying the candidate and from the current employer – only with the candidate's consent (Article 5 of LLPPD). State Data Protection Inspectorate also draws up numerous helpful recommendations in the context related to labour relations, for instance, the recommendation on personal data processing of employees when organising remote work.

Article 27 of the Labour Code of the Republic of Lithuania (hereinafter – LC) ((*Official Gazette*, 2016, No. 2016-23709). provides for the duty of the employer to respect the employee's right to privacy and ensure protection of their personal data.

In summary, it can be concluded that the right of employees to personal data protection and privacy in the context of labour relations is governed by the general legal acts of the European Union and Council of Europe. The frameworks of both the Union and Council of Europe contain special non-binding documents (rules, opinions, and recommendations)

governing exclusively the rights of employees. Naturally, the right to privacy and personal data protection in the context of labour relations is further specified in national legal acts.

Principles for the processing of personal data as expression of the employee‘s right to privacy in the context of labour relations

The right of employees to privacy and the right to personal data protection are closely interrelated and even overlap; however, these are not identical rights (despite them defending similar values – employee dignity, right to personal and family life privacy etc.). According to the ECHR, the right to personal data protection is an expression of the right to privacy. However, the scope, possibilities for restriction, and supervision authorities of the right of employees to privacy and of the right to personal data protection differ.

According to T. Bagdanskis and P. Sartatavičius (2012), an employee has the right to inviolability of their privacy encompassing:

1. Informational privacy which in the labour context can be described as knowing what information gathered about employee by the employer is being used and where;
2. Physical privacy (includes bodily integrity – it is forbidden to perform medical or scientific experiments without the consent of the subject);
3. Communicational privacy – in labour context it means that employee’s right to communicate with others not associated with labour relations must be respected;
4. Territorial privacy (inviolability of personal integrity and private territory).

In the meantime, the right of employees to personal data protection includes and protects the personal data associated with any information about the natural person who has been or could be directly or indirectly identified, 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 right to employee‘s personal data protection is exercised immediately, as soon as personal data processing starts, irrespective of what these are (given name, surname, bank card number, telephone number, residential address, email address etc.) and whether they belong to the data of special categories (membership in trade unions, biometrical data, health data etc.). Undeniably, unlawful processing of employee personal data might disclose information about their family and personal lives and simultaneously breach the person’s right to privacy. Consequently, a breach of employee’s personal data protection results in a breach of their right to privacy. ECHR explained in the case of Niemietz v. Germany that it is not necessary to try to define the notion of private life comprehensively. Respect for personal life also includes the right to build and develop relations with other people. Moreover, there are no grounds to infer why the perception notion of private life should not include professional or business activities. After all, in their working lives, the majority of people have a significant if not greatest opportunity to build relations with the outer world. The court clarified that the word "domicile" has a broader connotation than the word "home" and may extend, for example, to a professional person’s office (*Decision of the European Court of Human Rights* of 16 December 1992, Case of Niemietz V. Germany).

When analysing the employee‘s right to data protection it should be emphasised that an employee is equated with a data subject, whereas the employer is the data controller. The General Data Protection Regulation has established seven key rights of the data subjects also held by every employee in the field of data protection. Four of those had been known and were regulated yet before the Regulation came into force (and were eventually transposed to the

Regulation), including the right to be informed, the right of access, the right to rectification, and the right to object to processing. Furthermore, three entirely new rights for the data subjects were established, namely: the right to erasure ("the right to be forgotten"), the right to restrict processing, and the right to data portability (*Štareikė, Kausteklytė-Tunkevičienė*, 2018). The employer must ensure that the personal data of employees should be processed seeking for the development of normal labour relations and business, and for the balance of interests between the private interests of employees and legitimate interests of employer.

Article 88 of the General Data Protection Regulation states that Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the following purposes:

1. recruitment;
2. employment contract performance;
3. management, planning and organisation of work;
4. equality and diversity in the workplace;
5. health and safety at work;
6. protection of employer's or customer's property;
7. for the purposes of the exercise and enjoyment, on an individual basis, of rights and benefits related to employment;
8. termination of the employment relationship (*Article 29 Data Protection Working Party, Opinion 2/2017 on data processing at work,* WP249, 2017 (Article 29 Data Protection Working Party, Opinion 2/2017)).

In line with Artcile 88(2) of the GDPR, those rules shall include suitable and specific measures to safeguard the employee's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity, and monitoring systems at the work place (Artcile 88(2) of the GDPR). Employee as a person has the right to private life and a reasonable expectation that this right will not be breached even in their workplace. However, there are numerous reasons forcing the employers to monitor and control the employees in their workplace via information technologies. Scientific literature identifies the following key reasons: 1) striving to ensure work procedure and discipline of employees; 2) striving to improve the employee productivity and effectiveness; 3) striving to save employer's financial resources; 4) striving to protect employer's good reputation; 5) striving to meet the requirements for computer system safety and efficiency (*Lukacs*, 2020).

However, employers' lawlessness has been restricted and they are obliged to process the personal data of employees following the data processing principles embedded in Article 5 of the GDPR: process the data lawfully, fairly and in a transparent manner in relation to the employee; collect the employee data for specified, explicit and legitimate purposes and not further process them in a manner that is incompatible with those purpose; implement the data minimisation principle; ensure that the data are accurate and, where necessary, kept up to date; take every reasonable step to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay; implement the storage limitation principle; ensure that the personal data of employees are processed in a manner that ensures appropriate security of the personal data, including assurance of suitable personal data security, using appropriate technical or organisational measures. Further, the key principles of personal data processing are discussed in the context of labour relations.

Principle of lawfulness, fairness and transparency

First, personal data must be processed lawfully, fairly and in a transparent manner in relation to the employee (principle of lawfulness, fairness and transparency). Lawfulness in the context of labour relations is understood as proportionality and necessity of employee's personal data processing, for example, when data are processed on the basis of employment contract or law (when a duty is prescribed for the employer to submit data to the State Tax Inspectorate, State Social Insurance Foundation Board etc.). Opinion 2/2017 on data processing at work of the Article 29 Working Party (WP29) recommends that consent should not be treated as legal grounds in labour relations due to the subordination between the employer and employee. Attention is drawn to the fact that employees almost never have any possibilities to give, refuse or withdraw consent voluntarily, seeing the relations of employer and employee determine dependency. Due to the imbalance of power, employees are capable of giving consent voluntarily only under exceptional circumstances, when the employees do not experience any consequences pertaining to the acceptance or rejection of an offer (*Article 29 Data Protection Working Party*, Opinion 2/2017).

Guidelines 05/2020 on consent under Regulation 2016/679 of the European Data Protection Board dated 4 May 2020 uphold the same position and emphasise that the imbalance of power appears in the context associated with employment relations. Due to the dependency inherent to the relations of employer and employee, it is not likely that an employee might be able to refuse consent to their employer to process their data without fear or real risk of experiencing negative effects due to their objection. It is likely that an employee would be unable to refuse to give consent of their free will, when their employer asks for it, for instance, to object to the use of surveillance systems in the workplace without feeling any pressure associated with negative consequences, if they object. The European Data Protection Board emphasised that the employer' basing on consent for the personal data processing of current or prospective employees poses problems seeing that consent of such nature would not be given of their own free will. Due to the nature of the employer's and employee's relations, in many cases of such data processing at work, the consent of employees could not and should not comprise legitimate grounds for employee data processing at work (*Guidelines 05/2020 on consent under Regulation 2016/679 of the European Data Protection Board*, 2020). This notwithstanding, if the consent comprises legitimate grounds for employee data processing, it should be given of employee's own free will, informed, specific and unambiguous, while no negative consequences may arise to the employee due to their objection.

Article 5 of the Law on Legal Protection of Personal Data of the Republic of Lithuania also embeds the principle of lawfulness, by committing the employer to collect the personal data of candidates applying to the position or function pertaining to the qualification, professional skills, or work-related personal qualities from former employers after notifying the candidate and from the current employer – only with the candidate's consent (Article 5 (2) of LLPPD).

State Data Protection Inspectorate of the Republic of Lithuania also emphasized the importance of principle of lawfulness, fairness and transparency in their recommendation on personal data processing of employees when organising remote work that organisation of remote work per se does not imply the duty for the employer to assume the employee surveillance measures (e.g. monitor the correspondence by email, record calls etc.), but it also does not mean that such measures are necessary or proportionate. Although surveillance of the acts of employees carried out using the resources provided by the employer during the working time should not be treated as a breach per se, it should be carried out in line with the GDPR

requirements. European Court of Human Rights noted, that ECHR Member States must be granted a wide margin of appreciation in assessing the need to establish a legal framework governing the conditions in which an employer may regulate electronic or other communications of a non-professional nature by its employees in the workplace. Nevertheless, the discretion enjoyed by States in this field cannot be unlimited. The domestic authorities should ensure that the introduction by an employer of measures to monitor correspondence and other communications, irrespective of the extent and duration of such measures, is accompanied by adequate and sufficient safeguards against abuse (*Decision of the European Court of Human Rights of* 5 September 2017, Case of Bărbulescu v. Romania). Before starting the surveillance of any specific employee, the employer should:

(i) Assess the proportionality of the employee surveillance to the objectives sought and determine whether the interests of employer override the employee's interests and fundamental rights and freedoms. Following Article 6(1(f) of the GDPR, the condition of lawful data processing obliges the data controller to perform a test of interest balance and to assess whether his interests override the interests and fundamental rights and freedoms of the employee.

(ii) The employer has to perform an assessment of the impact on data protection when the employees' personal data are processed for the purposes of employee surveillance or control (processing of video and audio personal data in the workplace and in the employer's premises or territories, where his employees work; processing of personal data related to the surveillance of employees, communication, behaviour, location, or movement). If upon completion of the assessment of the impact on data protection it is concluded that data processing would pose a high risk unless the employer assumed measures to reduce it, the employer should apply to the State Data Protection Inspectorate for a prior consultation.

(iii) The employer has to draw up a procedure for the surveillance of employees and familiarise the employees obtaining signatures corroborating the familiarisation. The procedure must be clear, i.e. employees should understand the scope and consequences of processing of their data in the employer's activities so that eventually the ways their personal data are used would not be unexpected for them, thus ensuring proper implementation of the transparency principle (*Recommendation for employee data management by remote working*, 2020).

Purpose limitation principle in employee data processing

Purpose limitation principle obliges to collect the personal data of employees for the specified, explicit and legitimate purposes and not further process them in a manner that is incompatible with those purposes. Consequently, the personal data processing of employees when the purposes are not specified or not limited or collection of data expecting that various information and data about the employee will come handy in the future are unlawful. The employer must be frank and clearly state the purposes for which the personal data of employees are processed (*Personal Data Protection Guidelines for Startups*, 2019).

Article 5(3) of the Law on Legal Protection of Personal Data of the Republic of Lithuania establishes that the processing or video and/or audio data in the workplace and employer's premises or territories where his employees work, and processing of personal data pertaining to the surveillance of employee behaviour, location, or movement require informing them thereof with signature to confirm it or in another way corroborating the fact of informing providing them with information specified in parts 1 and 2 of Article 13 of Regulation (EU) 2016/679 (Article 5(3) of LLPPD). It is important to note that the purpose of employee personal data processing must be legitimate; the method for future data processing, for instance, video surveillance, must be necessary for attaining legitimate interests of the employer. The use of

information technologies allowing for monitoring, surveillance and collection of information about the employee violate their privacy and shape the appropriate behaviours of employees, prevent them from relaxing and exert pressure to comply with requirements, so that no things are detected that could be perceived as abnormalities (*Article 29 Data Protection Working Party*, Opinion 2/2017). Considering the above, proper balance between the legitimate interests of employer and fundamental rights and freedoms of employees (*Decision of the European Court of Human Rights of* 5 October 2010, Case of Köpke v. Germany) should be ensured and employee privacy should be protected. The progress of technologies should be also emphasised, when threat arises that the employees may not be aware altogether of them being subjected to surveillance or which personal data are processed and for what purposes.

A flawed practice should be mentioned when due to the possibility to correspond and gain free access to employee profiles in social networks, as the new analytical technologies develop, the employers have the technical opportunity to constantly check on their employees collecting information about their family members, relatives or friends as well as opinions, beliefs, interests, habits, location, attitude, and behaviour, thus recording their data, including sensitive data about the employee's private and family life.

Although social profiles of employees should not be checked in the context of labour relations, even more so, the employer should not request access to information shared by the employees with other persons in social networks, however, certain clauses are established for the employers, when the purpose of collecting such information can be justified: for example, upon conclusion of an additional agreement on non-competition. During the agreement validity period, the employer is provided an opportunity to monitor, for instance, the LinkedIn profile of their former employee (considering that this is one of the most popular social networks in the context of labour relations). The objective of such monitoring should pertain only to the information how the employee complies with the terms of the agreement on non-competition.

Data minimisation objective in labour relations

This principle states that the personal data of employees should be processed using the appropriate measures only when the purpose of personal data processing cannot be attained through other measures. If the employer reasonably cannot achieve the purpose without processing the personal data of employees, then he should select the least quantity of personal data necessary for the attainment of the purpose sought. To make sure that the personal data are adequate, suitable and non-redundant, the employer should assess the purpose sought through the processing of the employee personal data and determine the specific personal data required to attain it (*Personal Data Protection Guidelines for Startups*, 2019).

In its decision adopted on 02-04-2020, the Supreme Administrative Court of Lithuania examined whether the collection of biometrical data of employees was compatible with the data minimisation principle and noted that the necessity and proportionality of the data processed must be rigorously assessed as well as the possibility to attain the planned purpose by measures that are less-restrictive to privacy. When assessing the proportionality of the biometrical system installed in the workplace, the first thing that needs to be taken into account is whether the system is indeed necessary to meet the identified need. In other words, it is necessary to assess whether the system is essential for meeting the need and not selected due to convenience or cost-efficiency. Furthermore, it is important to assess whether the loss of employee privacy will match the benefit planned to receive. If the benefit is not particularly substantial and rather pertains more to greater convenience for the employer or small savings of funds, then the loss of privacy is not acceptable. Moreover, when assessing the suitability of the biometrical system,

it has to be considered whether the desired objective could be reached by means less limiting the employee privacy. For this purpose, the employer should determine whether the data processing and its mechanisms, categories of data to be collected and processed, and transfer of the information contained in the database are necessary and unavoidable (*Decision of the Supreme Administrative Court of Lithuania* of 2 April 2020).

Another example to mention, the Hamburg Commissioner for Data Protection and Freedom of Information imposes a 35.3 million euro fine for data protection violations at H & M's Service Center after violations related to improper processing of employees' personal data and violation of the right to privacy were identified. The investigation showed that the surplus data of employees were collected without a specific purpose, as well as special categories data were collected about the employees health condition, illness, vacation, family, religious beliefs (*European Data Protection Board*).

One more example deals with the processing by employer of special category data of employees, such as health data. The employer should take into account and collect only the necessary data. If the employee got ill (e.g. coronavirus infection) and that threatens the safety of health of other employees, the employee should inform the employer of having this disease and only notify the employer of the fact of illness. In order words, to comply with the data minimisation principle, the employer is provided only the information that would oblige the employer to enable the employee to work remotely. By submitting a suggestion to perform the working functions remotely, the employer should not specify the disease of the employee as the cause of such work mode. Quite the opposite, the employer should specify and disclose a cause that violates the employee privacy to a lesser extent, for instance, ensuring health protection for other employees (*Processing of employee health data following the entry into force of the amendments to the Labour Code concerning quarantine,* 2020). To sum up, when processing the employee data, especially those ascribed to special categories, the employer should only process the necessary data of employees seeking to implement the data minimisation principle.

Principle of accuracy

The implementation of the principle of accuracy in the context of labour relations requires that the personal data are accurate and brought up-to-date, if appropriate. The employer should assume all reasonable measures to ensure that that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (*Personal Data Protection Guidelines for Startups,* 2019). The GDPR obliges the employer to assume reasonable measures to ensure that the personal data are accurate, and to set the terms for deletion or revision of personal data. For instance, upon determining, that the data of former employees are no longer necessary, the employer should take all reasonable measures to ensure that such personal data are deleted. Article 5 of the Law on Legal Protection of Personal Data of the Republic of Lithuania also prohibits to process the personal data relating to the record of conviction or criminal acts of a candidate applying to the position or function, or those of employee, except in the cases where such personal data are necessary in order to verify that the person satisfies the requirements for the position or function provided for in the laws and implementing legislation (Article 5 of LLPPD).

Principle of storage limitation

The principle of storage limitation establishes that the personal data should be processed and stored no longer than necessary for the purposes for which they are being processed. Hence,

when implementing this principle, the employer has to ensure a minimum retention period of employees' personal data. The employer should take into account the personal data processing purpose, seeing as it will determine the types of personal data processed by the employer and the requirements of the national legislation stipulating the storage periods of specific data, i.e. personal data processing of employees is also governed by legal acts of other domains establishing specific periods for retention of documents and simultaneously personal data.

It has already been discussed that numerous everyday tasks of employees such as performance and fulfilment of work functions and duties pertain to data protection and processing and simultaneously concern the right to privacy. However, also relevant is the fact that the personal data processing of employees does not start after agreeing on the essential terms of employment and concluding an employment contract; it also includes pre-contractual labour relations, i.e. recruitment. It is important that the data collected in the course of recruitment process should be generally deleted as soon as it becomes clear that a job offer will not be made or the person does not accept it (*Article 29 Data Protection Working Party*, Opinion 2/2017). The individual concerned should also be duly informed of such data processing before starting to participate in the recruitment process. In the cases when the employer wishes to retain the data in order to have the opportunity to offer the candidate a vacancy later, as the position becomes vacant, the candidate should be properly informed and provided the opportunity to object to such further data processing; in this case, the data should be erased (*Recommendation CM/Rec(2015)5*).

Principle of integrity and confidentiality

The principle of integrity and confidentiality obliges the employer to process the employee data in such a way that the appropriate technical or organisational measures applied ensured adequate security of personal data, including protection against unauthorised or unlawful data processing and against accidental loss, destruction, or damage This principle obliges the employer to introduce appropriate safety measures to protect the personal data being processed.

Recommendations for data processing in the context of labour relations seeking to avoid violations

As already mentioned, seeing that unlawful processing and storage of personal data simultaneously violates the employee right to private life, each time when starting to process the personal data of employees the employer should provide for appropriate and specific measures to avoid violations and protect the human dignity, legitimate interests and fundamental rights of employees, in particular focusing on the following:

(i) legitimate interest in processing the personal data of employees; considering the subordination between the employer and employee inherent to the labour relations, the employer should not use the employee consent as legal grounds for processing their personal data;

(ii) transparency of employee data processing, especially by informing the employees that the workplace or equipment provided by the employer contain surveillance (video and audio, car tracking or location) systems as well as performing an assessment of the impact on data protection to determine whether the use of such measures is lawful and based on the balance of interests of the employer and employee. The employer should also inform the

employees if their emails and other correspondence tools (for instance, Teams, Hangout, Zoom, Telegram etc.) are monitored and inform them about consequences for inappropriate use of such tools etc.;

(iii) principle of data storage limitation, for example, by drawing up the rules for the processing of personal data of employees and familiarising the employees with them;

(iv) minimisation and proportionality of personal data of employees, by not collecting redundant data about the employees, especially those pertaining to special categories: health, biometrical data, information about the person's sexual orientation, religious or philosophical attitudes, data about personal or family life, opinions, statements in social networks etc. The employer should take into account that data processing at work should be a proportionate response to the hazards experienced by the employer. For example, instances of inappropriate use of the internet can be detected not necessarily by identifying the contents of websites, where the inappropriate use could be prevented by installing internet filters;

(v) principle of integrity and confidentiality of the personal data of employees, by obliging the employer to introduce appropriate technical or organisational safety measures to protect the personal data of employees being processed against unauthorised access, accidental loss, destruction, or damage.

Conclusions

The right of employees to personal data protection and privacy in the context of labour relations is guaranteed by the general legal acts of the European Union and Council of Europe, which ensures the protection of fundamental human rights. The frameworks of both the Union and Council of Europe contain special non-binding documents governing exclusively the rights of employees. The right to privacy and personal data protection in the context of labour relations is further specified in national legal acts.

The right of employees to privacy and the right to personal data protection are closely interrelated and even overlap. However, these are not identical rights. According to the ECHR, the right to personal data protection is an expression of the right to privacy. However, the scope, possibilities for restriction, and supervision authorities of the right of employees to privacy and of the right to personal data protection differ. The right of employees to privacy encompassing informational privacy, physical privacy, communicational privacy and territorial privacy. Meanwhile, the right of employees to personal data protection includes and protects the personal data associated with any information about the natural person who has been or could be directly or indirectly identified.

The right of employees to personal data protection includes these aspects in the labour context: recruitment; employment contract performance; management, planning and organisation of work; equality and diversity in the workplace; health and safety at work; protection of employer's or customer's property; purposes of the exercise and enjoyment, on an individual basis, of rights and benefits related to employment.

The key principles which must be taken into account by the employer in order to ensure employees' personal data processing and right to privacy in the context of labour relations are: principle of lawfulness, fairness and transparency; purpose limitation principle; data minimisation objective principle; principle of accuracy; principle of storage limitation; principle of integrity and confidentiality.

References

1. Article 29 Data Protection Working Party, Opinion 2/2017 on data processing at work, WP249, 2017. Available at https://ec.europa.eu/newsroom/article29/items/610169 (Accessed: 20 April 2021).
2. Article 29 Data Protection Working Party, Working Document on the surveillance of electronic communications in the workplace, 5401/01/EN/Final, WP 55, 2002. Available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp55_en.pdf (Accessed: 20 April 2021).
3. Article 29 Working Party – Opinion 8/2001 on the processing of personal data in the employment context, 5062/01/EN/Final, WP 48, 2001. Available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf (Accessed: 11 April 2021).
4. Asmens duomenų apsaugos gairės startuoliams [Personal Data Protection Guidelines for Startups] Solving Privacy Paradox Project, 2019. Available at str https://vdai.lrv.lt/uploads/vdai/documents/files/03%20SolPriPa%20Asmens%20duomenu%20apsaugos%20gaires%20STARTUOLIAMS%202020-02-20.pdf (Accessed: 30 April 2021).
5. Bagdanskis, T., Sartatavičius, P. Workplace Privacy: Different Views and Arising Issues, Jurisprudence, p. 697–713, 19(2), 2012, Available at https://www3.mruni.eu/ojs/jurisprudence/article/view/56/51 (Accessed: 15 April 2021).
6. Charter of Fundamental Rights of the European Union, OL 7.6.2016, C 202/391. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12016P/TXT&from=EN (Accessed: 20 April 2021).
7. Decision of the European Court of Human Rights of 5 October 2010, Case of Köpke v. Germany, Application no. 420/07. Available at http://www.bailii.org/eu/cases/ECHR/2010/1725.html (Accessed: 22 April 2021).
8. Decision of the European Court of Human Rights of 5 September 2017, Case of Bărbulescu v. Romania, Application no. 61496/08, Available at https://hudoc.echr.coe.int/spa#{%22itemid%22:[%22001-177082%22]} (Accessed: 25 April 2021).
9. Decision of the Supreme Administrative Court of Lithuania of 2 April 2020, administrative case, No. A-3345-822/2020.
10. Darbuotojų sveikatos duomenų tvarkymas, įsigaliojus Darbo kodekso pataisoms dėl karantino [Processing of employee health data following the entry into force of the amendments to the Labour Code concerning quarantine], 2020. Available at https://vdai.lrv.lt/uploads/vdai/documents/files/DK%20pataisos%20del%20darbuotoju%20sveikatos%20duomenu%20tvarkymo%20%202020-04-14.pdf (Accessed: 30 April 2021).
11. European Convention for the Protection of Human Rights and Fundamental Freedoms, Council of Europe, Rome, 1950. Available at https://www.echr.coe.int/documents/convention_eng.pdf (Accessed: 11 April 2021).
12. European Data Protection Board. Hamburg Commissioner Fines H&M 35.3 Million Euro for Data Protection Violations in Service Centre. Available at https://edpb.europa.eu/

news/national-news/2020/hamburg-commissioner-fines-hm-353-million-euro-data-protection-violations_en (Accessed: 30 April 2021).

13. European Social Charter (revised), Strasbourg, 1996. Available at https://rm.coe.int/168007cf93 (Accessed: 25 April 2021).
14. Guidelines 05/2020 on consent under Regulation 2016/679 of the European Data Protection Board dated 4 May, 2020. Available at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_lt_0.pdf (Accessed: 30 April 2021).
15. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas, Valstybės žinios. 1996. Nr. 63-1479. [The Law on Legal Protection of Personal Data of the Republic of Lithuania]. (Official Gazette, 1996, No. 63-1479).
16. Lietuvos Respublikos darbo kodekso patvirtinimo, įsigaliojimo ir įgyvendinimo įstatymas, Valstybės žinios. 2016. Nr. 2016-23709. [The Labour Code of the Republic of Lithuania). (Official Gazette, 2016, No. 2016-23709).
17. Lukacs, A. Protection Of Employees' Right To Privacy And Right To Data Protection On Social Network Sites – With Special Regard To France And Hungary, Doctoral (PhD) dissertation, 2020. Available at https://core.ac.uk/download/pdf/333872675.pdf (Accessed: 29 April 2021).
18. Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, 128th Session of the Committee of Ministers, Elsinore, Denmark 17-18 May 2018 (Convention 108+), Available at https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf (Accessed: 17 April 2021).
19. Proposal for a Council Decision authorising Member States to ratify, in the interest of the European Union, the Protocol amending the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), 2018. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018PC0451&from=LT (Accessed: 14 April 2021).
20. Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment (Adopted by the Committee of Ministers on 1 April 2015, at the 1224th meeting of the Ministers' Deputies) Available at https://www.conjur.com.br/dl/conselho-europa-internet-trabalho.pdf (Accessed: 29 April 2021).
21. Recommendation No. R (86) 1 of The Committee of Ministers To Member States on the Protection of Personal Data Used for Social Security Purposes, Council of Europe Committee of Ministers, 1986. Available at https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016804dd352 (Accessed: 29 April 2021).
22. 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). Available at https://eur-lex.europa.eu/eli/reg/2016/679/oj (Accessed: 9 April 2021).

23. Rekomendacija dėl darbuotojų duomenų tvarkymo nuotolinio darbo metu [Recommendation for employee data management by remote working] 2020). Available at https://vdai.lrv.lt/uploads/vdai/documents/files/Rekomedacija%20del%20darbuotoju%20duomenu%20tvarkymo%20nuotolinio%20darbo%20metu%202020-04-09.pdf (Accessed: 17 April 2021).

24. Štareikė, E; Kausteklytė-Tunkevičienė, S. Pagrindinės duomenų subjekto teisės ir jų užtikrinimas pagal ES Bendrąjį duomenų apsaugos reglamentą [The main rights of the data subject and their enforcement in accordance with the EU General Data Protection Regulation] Public Security and Public Order, 2018 (20), ISSN 2335-2035 (Online). Available at https://ojs.mruni.eu/ojs/vsvt/article/download/5597/4793 (Accessed: 11 April 2021).