Economic Insights – Trends and Challenges	Vol.VI(LXIX) No. 4/2017	65 - 72

Considerations on the Processing of Personal Data in the Employment Context

Dana Volosevici

Petroleum-Gas University of Ploieşti, Bd. Bucureşti 39, 100680, Ploieşti, Romania
e-mail: dana.volosevici@vplaw.ro

Abstract

Rapid technological developments and globalisation have brought new challenges for the protection of employees' personal data. The protection of natural persons in relation to the processing of personal data is a fundamental right in the European Union and, since the execution of employment relationship requires the processing of personal data, each employer should ensure adequate level of protection of its employees' rights. The paper summarizes the main aspects related to the processing of personal data in employment context in the light of the Regulation 2016/679 that shall enter into force on May 25, 2018. The Regulation aims to ensure a consistent level of protection for natural persons throughout the Union and to prevent divergences hampering the free movement of personal data within the internal market.

Keywords: *employment; data protection*

JEL Classification: *K31; K38*

The protection of natural persons in relation to the processing of personal data is a fundamental right in the European Union, express legal provisions, Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU), stating that everyone has the right to the protection of personal data concerning him or her. In the same time, the right to the protection of personal data is not an absolute right and it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.

The execution of employment relationship requires the processing of personal data; thus each employer should ensure adequate level of protection of its employees' rights as well as an effective framework which guarantee that its employees comply with the specific legal regime applicable to the personal data processed by the employer. The processing of personal data should also be adapted to the employer structure; employers that are part of a group of undertakings or institutions affiliated to a central body may have a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes, including the processing of employees' personal data.

As any other controller, the employer shall observe the principles and the derived provisions of the Regulation 2016/679 (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), published in the Official Journal of the European Union L 119/ 4.5.2016), but also specific provisions issued by the Member States or agreed by negotiation between the social partners. Thus, Member State law or collective agreements may provide for specific rules on the processing of employees' personal data in the employment context, „in particular for the conditions under which personal data in the employment context may be processed on the basis of the consent of the employee, the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship" (Article 88 of the Regulation 2016/679).

When processions personal data in the employment context, at least one of the criteria set out in the Article 6 of the Regulation 2016/679 has to be satisfied:

a) the employee has given consent to the processing of his or her personal data for one or more specific purposes;
b) processing is necessary for the performance of a contract to which the employee is party or in order to take steps at the request of the data subject prior to entering into a contract;
c) processing is necessary for compliance with a legal obligation to which the employer is subject;
d) processing is necessary in order to protect the vital interests of the employee or of another natural person;
e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the employer;
f) processing is necessary for the purposes of the legitimate interests pursued by the employer or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

The criteria regarding the protection of the vital interests of the employee and the performance of a task carried out in the public interest are less likely to be relevant in the employment context and are limited to the protection of safety and public health. As regards the other criteria stated by the Article 6, some further discussions are necessary.

Employee Consent

The employee's consent is the basis for the entire employment relationship. The employment contract is executed based on the parties' consent, and any amendment to the employment contact should be subject to an addendum mutually agreed, except where such a change is expressly provided for by law or the applicable collective labour agreement (Article 17 Para (5) of the Romanian Labour Code, Law nr. 53/2003 republished in the Official Gazette no. 345/18 May 2011, as further amended). According to the Regulation, 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Since the employment relationship is characterized by the imbalance between the employer and the employee, the later undertaking to perform the work for and under the authority of the employer, Working Party 29 outlined that "where as a necessary and unavoidable consequence of the employment relationship an employer has to process personal data, it is misleading if it

seeks to legitimize this processing through consent. Reliance on consent should be confined to cases where the worker has a genuine free choice and is subsequently able to withdraw the consent without detriment" (WP29, 2001, p.23).

Where the employer can prove that the employee's consent was freely given, the consent shall be unambiguous and comprehensive. For example, the consent to use a vehicle which has a GPS tracking system, may not be considered as a consent to allow processing on location data. Moreover, if the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. The employee shall be informed that he/she has the right to withdraw his or her consent at any time. However, the withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

Performance of a Contract

Performance of a contract is the legal ground for any data processing based on the obligations that the employer has under the employment contract. Moreover, employment, fiscal and H&S regulations and law provisions are applicable to the employer, generating the obligation to process employees' personal data. Performance of a contract (Article 6 (a)) and legal obligations (Article 6 (b)) constitute valid legal basis for data processing, even cases of special categories of personal data. As a rule, Article 9 Paragraph (1) of the Regulation 2016/679 provides that processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited. Derogating from the prohibition on processing special categories of personal data is be allowed when processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.

As regards data concerning health, the processing may interfere with the right to private life, interference which will contravene Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms as well as the Regulation 679/2016. The employer has the right to process data concerning health in connection with pay during sickness, meeting health and safety requirements, providing insurance or pension benefits, but the data processing should remain under the limits of the fundamental rights.

Thus, in Radu v. Republic of Moldova, the applicant, a lecturer at the Police Academy, complained about a State-owned hospital's disclosure of medical information about her to her employer. The President of the Police Academy requested information from the hospital in connection with the applicant's medical leave. In particular, he asked who had ordered her hospitalisation, when she had been hospitalised, what had been the initial and final diagnoses, and what treatment she had received. The hospital disclosed to the applicant's employer detailed medical information: that the applicant had been hospitalised on account of an increased risk of miscarriage, that this was the applicant's first pregnancy and that she was carrying twins; that the pregnancy had resulted from artificial insemination and that the applicant had hepatitis B. The letter further mentioned that the applicant had obstetrical complications and that she had a negative blood type. A copy of the applicant's medical file from the hospital where she had been hospitalised, containing a detailed description of all the medical procedures she had undergone and of all the medical analyses, was annexed to the letter.

The applicant initiated civil proceedings against the hospital and the employer and claimed compensation for a breach of her right to private life. She argued, *inter alia*, that her employer had had sufficient information as to the reasons for her medical leave and had not been entitled to seek further details of such a private nature. Moreover, the information had not been kept confidential but had been disclosed to everyone at her workplace. According to the applicant, the disclosure had caused her serious stress and anxiety.

The Court assessed that the disclosure by the hospital to the applicant's employer of such sensitive details about the applicant's pregnancy, her state of health and the treatment received constituted an interference with her right to private life. An interference will contravene Article 8 unless it is "in accordance with the law", pursues one or more of the legitimate aims referred to in paragraph 2 of that Article, and furthermore is "necessary in a democratic society" in order to achieve the aim. The Court noted that all the relevant domestic and international law expressly prohibits disclosure of such information to the point that it even constitutes a criminal offence and Court therefore found that there had been a violation of Article 8 of the Convention in respect of the applicant's right to respect for her private life.

Legitimate Interest

A more sensitive legal ground for data processing is the legitimate interest (Article 6 (f)), since this criterion requires a fine balance between the interests of the employer and the rights and interests of the employee.

In Bărbulescu v. Romania, the Grand Chamber held that there had been a violation of Article 8 of the Convention, finding that the Romanian authorities had not adequately protected the applicant's right to respect for his private life and correspondence. They had consequently failed to strike a fair balance between the interests at stake, namely Mr Bărbulescu's right to respect for his private life and correspondence, on the one hand, and his employer's right to take measures in order to ensure the smooth running of the company, on the other. The case concerned the decision of a private company to dismiss an employee after monitoring his electronic communications and accessing their contents.

The Regulation 2016/679, Paragraph (47) states that at any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the employee could in particular override the interest of the employer where personal data are processed in circumstances where employees do not reasonably expect further processing.

When invoking the legitimate interest, a number of cumulative conditions must be met (WP29, 2017a). Firstly, the purpose of the processing must be legitimate and proportionate to the business needs. The method or the technology used for the processing must be adequate for the legitimate interest of the employer and should constitute the least intrusive manner possible.
WP29 (WP29, 2001) recommends that specific mitigating measure should be present to ensure a proper balance between the legitimate interest of the employer and the fundamental rights and freedoms of the employees. Such measures could include geographical, data-oriented or time-related limitations on monitoring so as to guarantee that the employee's privacy is not violated.

In Bărbulescu v. Romania, the Grand Chamber assessed that Contracting States must be granted a wide margin of appreciation in evaluating 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, but they 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.

The Grand Chamber specifies the criteria to be applied by the national authorities when assessing whether a given measure is proportionate to the aim pursued and whether the employee concerned is protected against arbitrariness. The paragraph 121 of the judgment enumerates the criteria to be applied by the national authorities when assessing whether a measure to monitor employees' communications is proportionate to the aim pursued and whether the employee concerned is protected against arbitrariness:

- whether the employee has been notified of the possibility that the employer might take measures to monitor correspondence and other communications, and of the implementation of such measures. The notification should be clear about the nature of the monitoring and be given in advance;
- the extent of the monitoring by the employer and the degree of intrusion into the employee's privacy. In this regard, a distinction should be made between monitoring of the flow of communications and of their content. In order to establish the extent of the monitoring, the following aspect should be also analysed: whether all communications have been monitored, whether the monitoring was limited in time and the number of people who had access to the results;
- whether the employer has provided legitimate reasons to justify monitoring the communications and accessing their actual content;
- whether it would have been possible to establish a monitoring system based on less intrusive methods and measures than directly accessing the content of the employee's communications;
- the consequences of the monitoring for the employee concerned and the use made by the employer of the results of the monitoring operation, in particular whether the results were used to achieve the declared aim of the measure;
- whether the employee has been provided with adequate safeguards, especially when the employer's monitoring operations are of an intrusive nature.

Whenever the employer relies on the Article 6 (f), the employee retains the right to object to such processing on compelling legitimate grounds. In such case, the employer shall no longer process the personal data unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the employee or for the establishment, exercise or defence of legal claims.
Any processing shall comply with the principles stated by the Article 5 of the Regulation 2016/679, principles which have already been promoted by the Directive 96/46/EC (Beaugrand et al., 2017). Based on the principle of accountability, the employer shall be responsible for, and be able to demonstrate compliance with the law in relation to any processing. As pointed out above, the processing of employees' personal data is allowed, and workers have to accept a certain limitation of their right to privacy. The balance between the interests shall be construed through the principles stated by the Article 5 of the Regulation 2016/679.

Firstly, the personal data shall be processed lawfully, fairly and in a transparent manner in relation to the employee. The employer shall take appropriate measures to provide any information relating to processing to the employee in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the employee, the information may be provided orally, provided that the identity of the employee is proven by other means. The information can be provided in a sole document, such as company's policy on data protection, but references to the data protection processing could

be made in the internal regulations, specific policies, collective agreements or even in the individual employment agreement. Some employers opted to draft a separate document which addresses the issues pointed out in the Article 13 of the Regulation:

(1) the identity and the contact details of the employer and, where applicable, of the controller's representative;

(2) the contact details of the data protection officer;

(3) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(4) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the employer or by a third party;

(5) the recipients or categories of recipients of the personal data;

(6) the fact that the employer intends to transfer personal data to a third country,

(7) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(8) the existence of the right to request from the employer access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

(9) where the processing is based on consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
(10) the right to lodge a complaint with a supervisory authority;

(11) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

(12) the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

The contents of the information cover an important number of aspects, ensuring undoubtedly, the transparency of the process. However, this transparency may be affected if the document, although following the legal structure and contents, is drafted in technical terms, unappropriated for the employees' comprehension. Consequently, the employer shall conciliate the transparency of processing and the accessibility of the form.

Secondly, the employer shall comply with the principle of purpose limitation, therefore data must be collected for a specified, explicit and legitimate purpose and not further processed in a manner that is incompatible with those purposes. Where the employer intends to further process the personal data for a purpose other than that for which the personal data were collected, the it shall provide the employee prior to that further processing with information on that other purpose and with any relevant further information.

Data minimisation is the third principle stated by the Article 5 of the Regulation. The employer shall ensure that the processed data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. For example, the employer may need to know if applicants have their residence near the employer's premises, but it would be against de data minimisation principle to ask further information about the housing.

Employee personal data shall be accurate and, where necessary, kept up to date. The employer shall take necessary steps to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. Even if the

employee is the one who provides the personal data (social status, children, address), the employer shall state an obligation for the employee to inform about any change in his or her personal data that are processed by the employer.

The principle of storage limitation imposes to the employer to keep the personal date in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. As a general rule, data should be kept no longer that the duration of the employer agreement, with the exception of the data that are relevant for payroll, for which the law establishes a 50 years storage duration (Ministry of Public Finance, Order no. 2.634/5 November 2015 regarding the accounting and financial documents, published in the Official Gazette no. 910/ 9 December 2015). Therefore, when establishing the duration of the storage, the employer shall take into account an intrinsic criterion related to the purpose of the processing, but also extrinsic criteria, deriving from law and regulations (Bourgeois, 2017).

The data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. This principle, called „integrity and confidentiality" obliges the employer to implement technical or organisational measures at the workplace to guarantee that the employees' persona data are secure, including *inter alia* as appropriate: pseudonymisation and encryption of personal data; the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Moreover, where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of employees, the employer shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A data protection impact assessment is a concept introduced by the Regulation 2016/679 and it is designed to describe the processing, assess the necessity and proportionality of a processing and to help manage the risks to the rights and freedoms of natural persons resulting from such processing (WP29, 2017). Article 29 Data Protection Working Party considers that a company monitoring its employees' activities, including the monitoring of the employees' work station or internet activity falls under the following criteria which characterized a processing "likely to result in high risk": systematic monitoring and data concerning vulnerable data subjects. In this case, the employer should perform a Data Protection Impact Assessment (DPIA) prior to the processing and the assessment shall be reviewed and updated where necessary.

Rapid technological developments and globalisation have brought new challenges for the protection of employees' personal data. Effective protection of employees' personal data requires setting out in detail of the obligations of the employers and the Regulation 2016/679 extends the legal ground set by the Directive 95/46/EC, in the view to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union. Thus, all European employers are bound by the same level of obligations, whatever their nationality. The implementation of the legal provisions will entail a deeper interpretation of the Regulation, the provision of which requires further clarification in order to ensure a unitary application through the European Union.

References

1. Article 29 Data Protection Working Party, *Opinion 08/2001 on the processing of personal data in the employment context*, WP48, Url: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf, 13 September 2001.
2. Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, 4 April 2017.
3. Article 29 Data Protection Working Party, *Opinion 02/2017 on data processing at work*, WP249, url: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169, 8 June 2017 (a).
4. Beaugrand, Th., Marcellin, S., Staub, S., Castets-Renard, C, Blum, P., Rasle, B., Brogli, M. & Younes-Fellous, V., (2017. *Protection des données personnelles*, Paris: Editions Legislatives.
5. Bourgeois, M., 2017. *Droit de la donnée. Principes théoriques et approche pratique*, Paris: LexisNexis.
6. European Court of Human Rights, Case of Radu v. The Republic of Moldova (Application no. 50073/07), Judgment of 15 April 2014.
7. European Court of Human Rights, Grand Chamber Case of Bărbulescu v. Romania (Application no. 61496/08) Judgment of 5 September 2017.