HUMAN RESOURCES AND PERSONAL DATA PROTECTION: AN INDISSOLUBLE RELATIONSHIP

Georgiana Florentina TATARU
Faculty of Law, „Alexandru Ioan Cuza" University of Iași
Iași, Romania
florinatataru@gmail.com

Ștefan Răzvan TATARU
Faculty of Law, „Alexandru Ioan Cuza" University of Iași
Iași, Romania
razvantataru@gmail.com

Abstract: *Starting from the application file, payroll information, medical file and getting to employees' internet behaviour or the images taken through the surveillance camera, these personal data are processed by employers all around the world. As the essence of the human resources is dealing with various types of information on the individuals working within an organization, it is of great importance to have a clear outline on how this data is to be processed. The EU's General Data Protection Regulation (GDPR) provides a comprehensive framework that helps smoothing the unfolding of the indissoluble relationship between HR activities and data protection methods.*
Keywords: *human resources; data protection; GDPR; employee data; HR data;*

INTRODUCTION

Human resources (HR) is an umbrella term that has evolved throughout the years and has gone beyond the "hire-and-fire" meaning. It now encompasses a variety of functions such as recruitment, training, employee satisfaction, employment law compliance etc. Starting from their role in the organization, we can generally say that human resources represent a *sine qua non* condition in the production process, a factor that can directly influence the level of performance of the organization. By managing the most important asset - people - the HR department in any company is a vital part that ensures the smooth running of the business, the engagement of the workforce and the lack of detrimental lawsuits regarding labour matters. Without the effective presence of people who know what, when and how to do it, it would be impossible for organizations to achieve their goals.

Moreover, the organizations face a multitude of challenges, ranging from a constantly changing workforce to ever-present government regulations and an unexpected shift of approach caused by the coronavirus pandemic that forced employers to re-think the way they manage the human resources.

The concept of human resources designates - in a utilitarian and economic way - the people who work within an organization. Thus, we consider that the processing of personal data is the essence of human resources activities, all of which involve information on individuals.

The emergence of new regulations in the field of personal data protection (Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, further mentioned as GDPR) determined organizations, through their HR departments, to pay more attention to the way they process the data of candidates, employees and former employees. HR departments act as the custodians of significant volumes of often sensitive or confidential personal data within any organization, and must therefore take center stage as this demanding law bites (Mintern T. & Rayner S., 2018).

Every individual has a set of personal data that they can either share or hide, but when it comes to working, there is an obligation to provide this kind of data. Everything starting from the resumes sent by applicants to employment contracts contains personal data. By the nature of their work, HR departments collect and process an immense amount of personal data not only from their employees, but also from job applicants and former employees. The information they possess includes sensitive data such as health information, medical records, etc. Hence, it is of utmost importance that HR professionals are aware of the requirements of the new data protection regulation and process personal data accordingly.

THE PROCESSING OF PERSONAL DATA IN HR ACTIVITIES

In labour relations as well as in HR activities, the parties involved are the employer and the natural person who has the quality of candidate, employee or former employee. According to the GDPR, the latter has the quality of Data Subject and the employer is the Controller of personal data, this being the one who, according to art.4 para.(7), *"alone or jointly with others, determines the purposes and means of the processing of personal data"*. Personal data are defined in art.4 para.(1) of the regulation as *"any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"*.

The processing of personal data represents, according to art.4 para.(2), *"any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction"*.

The types of data, the purposes of the processing and the legal basis must be analysed according to three stages present in the HR activities: a) recruitment; b) hiring and performance of the contract; and c) subsequent to the termination of employment.

1. Recruitment

According to Edwin B. Flippo, recruitment is *"a process of searching for prospective employees and stimulating and encouraging them to apply for jobs in an organisation"*. Essentially, it is the process of finding the most qualified candidate for a

job opening, in a timely and cost-effective manner. The company may then select those applicants with qualifications that are closely related to job descriptions.

Frequently, recruitment begins when a manager initiates an employee requisition (a document that specifies job title, department, the date the employee is needed for work, and other details). With this information, managers can refer to the appropriate job description to determine the qualifications the recruited person needs. The next step in the recruitment process is to determine whether qualified employees are available within the organization (the internal source) or if it is necessary to look to external sources, such as colleges, universities, and other platforms (Mondy, R. & Martocchio J. J., 2016).

When done internally, the access to personal data comes in handy. Human resource databases are a valuable recruitment device that allows organizations to determine whether current employees possess the qualifications for filling open positions (Mondy, R. & Martocchio J. J., 2016).

Candidates are the data subjects because they can be identified through the personal data they give to companies when they apply for a job. As aforementioned, their resumes may include their names, addresses, or phone numbers. The question that naturally arises is which are the mandatory elements of a resume or what personal data one must provide when applying for a job. This varies from country to country, but generally the main elements remain the same: personal information (name, address and contact information), employment history, and education. In some countries, during the application process, there is a requirement to disclose any military service.

Some companies prefer to use standardized application forms rather than to receive resumes from applicants. The reason can be to avoid receiving unnecessary information or intentional omission of information that it is disadvantageous for the applicant.

Although, in a standardized job application form, potentially discriminatory questions inquiring about factors such as gender, race, age, convictions, national origin, citizenship, birthplace, dependents, disabilities, religion, colour, and marital status should be avoided (Mondy, R. & Martocchio J. J., 2016).

For example, the UK government prohibits recruiters from asking the applicants about their marital status or whether they have children or plan to have children. Moreover, questions about health or disability are allowed only *a)* if there are necessary requirements of the job that cannot be met with reasonable adjustments, *b)* for finding out if someone needs help to take part in a selection test or interview or *c)* in the case of a 'positive action' taken to recruit a disabled person.

There is a great debate on whether to add a photo to a resume or not. In countries such as Ireland, United Kingdom and United States of America, strict anti-discrimination and labour laws do not allow the use of photos in resumes. Therefore companies, out of precaution, prefer not to see candidate photos accompanying job applications.

We consider that photography is not a mandatory element in the recruitment stage, except for those jobs for which the appearance and physical condition of the employee are particularly relevant (*e.g.* news anchors, TV hosts, models, and so on). In other cases, the processing of the candidate's image is unjustified and may be considered, as the case may be, abusive or discriminatory.

Additionally, specifying your age is a two-edged sword. It can be problematic for the job applicant that could be subjected to ageism (being discriminated against for being

too old or too young for a certain job) or, on the other hand, it can be beneficial in the context of the organization's diversity and inclusion practices.

According to art.10 of the GDPR, the employer must not process personal data relating to criminal offenses or convictions of the candidate, unless this is a condition of employment provided by national or European law. For example, in Romania, the processing of criminal records is legal only for employment as a legal advisor (Law no.514 of November 28, 2003 on the organization and exercise of the profession of legal advisor), manager (Law no.22/1969 on hiring managers, establishment of guarantees and liability in connection with the management of the assets of economic operators, authorities or public institutions), security guard (Law no.333 of 8 July 2003 on the protection of objectives, property, values and protection of persons), or civil servant (GD no.611 of 4 June 2008 for the approval of the norms regarding the organization and career development of civil servants).

Diversity and the free access to the labour market

Given the ever-growing globalization and free movement of people across the European Union, diversity and inclusion have become major focus points for businesses. Migration - voluntary or forced - increased the demand of jobs. While the forced migrants came looking for refuge and safety as well as for means of subsistence, the skilled workers with higher education were urged by "pull-factors" such as higher living standards, better education institutions and better paid jobs (Tataru, G.F., 2019).

Diversity in the workplace has become important because it is historically unprecedented. Diversity goes beyond demographic characteristics like age, race or gender and can be defined as understanding, accepting, and valuing differences between people of different races, ethnicities, genders, ages, religions, disabilities and sexual orientations, as well as differences in personalities, skill sets, and education.

Moreover, employers may process sensitive data such as ethnicity, age, sexual orientation, spiritual beliefs, or disability as part of their equal opportunities monitoring programmes.

During the recruitment phase, the employer processes various types of personal data, such as: identity data (name, surname), contact details (home address, email address, telephone number), data on physical characteristics and / or physiological (gender, age, image, voice), data on education (educational background, studies, specializations, certifications), data on professional experience (previous jobs, seniority), other data that were included by the candidate in the resume and / or the documentation sent for the application on the job (letter of recommendation / letter of intent).

The processing of the aforementioned data aims at going through the process of recruitment and employment of human resources within the controller's organization and will be carried out based on art.6 lit.b) GDPR, "*processing is necessary [...] in order to take steps at the request of the data subject prior to entering into a contract*" (conclusion of an employment contract).

Last but not least, at the stage of the interviews, the candidate may disclose new personal data that have not been previously mentioned in the documents sent for selection. The controller must provide for safeguards for this new information, even though it is transmitted orally and it is not stored.

If the employer has outsourced the recruitment and selection of staff, he must ensure that the authorized person (the company providing the recruitment services) has guarantees regarding compliance with personal data protection regulations. If the employer uses outsourced recruitment services from another non-EU state, the employer must ensure that there are adequacy decisions that guarantee an adequate level of protection of personal data (according to Article 45 GDPR).

A particular situation, specific to the recruitment stage, is represented by the processing of personal data of candidates who have not been selected for employment, data that further remains with the controller. The latter has the obligation either to delete the data of the candidates who have not been selected or to obtain their consent for the storage of the data in order to contact the persons concerned in the event of a vacancy.

2. Employment and the performance of the employment contract

In carrying out labour relations, the employer - as the controller, processes a large and varied volume of personal data belonging to employees. In addition to the data collected in the previous stage, that of recruitment and employment, during the execution of the individual employment contract, the employer may process the following information: unique identifiers (national identification number, identity card`s number and series), work card series, banking data (bank account), amount of salary, position and job, periods of leave, health data (information obtained from compulsory medical examinations, information resulting from sick leave), image (processed through internal supervisory systems), trade union membership, religious beliefs (depending on which the employer grants the employee some days off) and other data. Depending on the object of activity of the organization and the position held by the employee, different categories of personal data will be processed.

Most of the processing of personal data carried out during labour relations is based on either the provisions of art.6 lit.b) of the GDPR, the processing being necessary for the performance of a contract to which the data subject is party (*e.g.* payment of the salary in the bank account); either on the provisions of art.6 lit.c) of the GDPR - the processing being necessary for compliance with a legal obligation to which the controller is subject (*e.g.* payment of social health insurance contributions). There are also situations in which the processing of personal data is necessary for the purpose of legitimate interests pursued by the controller (art.6 para.1, f)), such as processing the image of employees through the installed video surveillance system, in order to ensure security and protection of property and persons.

In carrying out labour relations, the employer processes personal data for multiple purposes, such as: a) the purpose of fulfilling obligations and exercising specific rights in the field of employment, social security and social protection, in the context of concluding, performing and terminating the employment contract; b) the purpose of fulfilling the fiscal obligations - taxes, duties and contributions - of the employer or, as the case may be, of the employee; c) purposes related to preventive medicine or occupational medicine, the assessment of the employee's work capacity or compliance with occupational safety and health legislation; d) the purpose of the payment of salaries and other benefits offered by the employer.

According to the provisions of art.13 para.(1) of the GDPR, for the processing of personal data analysed above, the employer has the obligation to inform the employee

about: (a) the identity and contact details of the controller; (b) the contact details of the Data Protection Officer; (c) the purposes for which the personal data are processed and the legal basis for the processing; (d) where the processing is carried out pursuant to Article 6 (1) (f), the legitimate interests pursued by the controller [...]; (e) the recipients or categories of recipients of personal data; (f) where applicable, the intention of the controller to transfer personal data to a third country or an international organisation [...]. In addition to this information, when the personal data are obtained, the controller shall provide the data subject with the following additional information necessary to ensure fair and transparent processing: (a) the period for which the personal data will be stored [...]; (b) information on the data subject's rights (in the case of analysis - the employee) and how they can be exercised; (c) the existence of an automated decision-making process including profiling.

Data processing that exceeds labour relations

If the employer intends to process personal data belonging to employees for purposes other than those determined by the performance of the employment contract or the legal obligations incumbent on him, he will have to obtain the consent of the employees concerned by the processing. For example, in order to create an anniversary calendar with photos of the employees, the employer will have to obtain the consent of the employees for the processing of their image, prior to the processing and in compliance with the conditions imposed by art.7 GDPR.

We believe that the principles of transparency and accountability, both provided for in the GDPR Regulation (Iftimiei A., 2018), should apply bidirectionally in labour relations - the employer and the employee should show both transparency in the processing of personal data, and responsibility in the way in which it protects and ensures the confidentiality of personal data. Thus, the employer must create the general framework for the protection of all personal data processed by the organization and in turn, the employee must maintain the confidentiality of the data which he comes into contact with in the performance of his duties.

A relevant example of non-compliance with the GDPR's fundamental principles and the sanctioning of the employer for his interference with the privacy of employees is the case of the monitoring of several hundred employees of the H&M Service Center in Nuremberg by the company's management team (European Data Protection Board, 2020). The multinational company H&M was fined 35.3 million EUR by the Hamburg Personal Data Supervisory Authority for the illegal processing of personal data belonging to employees. In the present case, H&M processed a large amount of sensitive data regarding its own employees (health data consisting in medical leaves and diagnostics, information on employee`s holidays, information on religious beliefs and family matters) without complying with the provisions imposed by the GDPR. Some of this data was recorded, digitally stored and analysed by approximately 50 managers throughout the company. Data collection was carried out with a high level of detail and over longer periods of time, documenting aspects of the employee's private life. In addition to the in-depth assessment of individual work performance, the data collected were also used for profiling the employees and were subsequently used in taking measures and decisions on employment relationships (employment/dismissal/promotion) (European Data Protection Board, 2020).

3. After the termination of employment

Obviously, with the termination of employment, the processing of personal data of employees is reduced to the minimum necessary, generally limited to the storage of existing data in the personnel file. The employer, on his own account or at the request of the former employee, may delete personal data from the personnel file, except for the data for which the employer has a legal obligation to keep (*e.g.*, in Romania, the payroll must be kept for 50 years to guarantee the possibility of proper calculation and recalculation of pensions).

One aspect worth mentioning is the fact that employers must instruct employees on how to process personal data in the performance of work activities, but also on the obligation of confidentiality they have regarding data and information to which they have or have had access in the execution of the employment contract. Thus, the obligation of confidentiality incubates the employee both during the period of employment and for a period of time determined after their termination / after he no longer has the quality of employee.

THE RIGHTS OF DATA SUBJECTS

The GDPR establishes minimum data protection obligations and standards for Controllers in the context of personal data processing operations and, at the same time, establishes rights for the data subject. Thus, according to Chapter III of the GDPR, the data subject has the following rights: the right to be informed, the right to access data, the right to rectify data, the right to restrict processing, the right to object, the right to data portability and the right to be forgotten, the right to withdraw consent, the right to file a complaint or grievance (Tataru Ș.R. & Nica I.T., 2020).

In the case of the labour relations analysed in this study, the rights conferred by the GDPR to the persons subject to the processing of personal data may be exercised by candidates from the recruitment and selection stage, by employees (during the employment contract) and by former employees.

The right to be informed consists in the correlative obligation of the Controller to disclose to the data subject information on: the identity and contact details of the Controller, personal data to be collected and processed or, if they are already held by the Controller, the source of the data, the purposes and means in which they are processed, the period for which they will be stored and others.

The right of access to data, regulated by art. 15 of the GDPR, provides the right of the data subject to obtain confirmation from the Controller that he or she processes personal data concerning him or her and, in the event of an affirmative answer, access to that data.
The right to rectify data is the right of the data subject to request the Controller and to obtain from him, without undue delay, the rectification of inaccurate personal data concerning him. In order to meet the needs of employees, the employer should carry out regular campaigns to update their personal data.

According to art. 18 of the GDPR, the data subject shall have the right to obtain from the controller the restriction of the processing of its personal data. Where processing has been restricted, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of

legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

The right of opposition consists in the data subject's right to object at any time to the processing of data, the Controller having the obligation to cease the processing of data, unless he demonstrates the existence of legitimate and compelling reasons justifying the processing.

Art.20 of the GDPR provides the right to data portability and the conditions under which the data subject may exercise this right. Thus, the data subject has the right to receive the data he has provided to the controller, in a structured, commonly used and automatically readable format, and has the right to transmit those data to another controller, without obstacles from the controller.

According to art.17 of the GDPR, the right to be forgotten or the right to delete data establishes the possibility for the data subject to request the deletion of data. The controller has the obligation to delete personal data, without undue delay, if they are no longer necessary to fulfil the purposes for which they were collected or if the data subject has withdrawn his consent to their processing (Șerban A., 2017). The deletion of the data will also be performed in the situation where the data subject opposes the processing, the data have been processed illegally or the controller has a legal obligation to delete the data in question.

If the processing of data by the controller is based on the consent of the data subject - of the employee - the latter has the right to withdraw his consent at any time. Once the consent has been withdrawn, the controller must ensure that the data is deleted, unless there is another legal basis for the processing. For example, if the employer uses the image of employees to promote campaigns or events (based on their consent and in accordance with the provisions of Article 7 of the GDPR), if those employees withdraw their consent, the employer will no longer be able to use their image in set purpose and will have to delete those data.

According to the provisions of art. 77 of the GDPR, any data subject has the right to lodge a complaint with a supervisory authority, in particular in the Member State in which he or she has his or her habitual residence, place of employment or alleged infringement, if he or she considers that the processing of personal data concerning it violates the legislation in the field of personal data protection (Ungureanu C.T., 2019; Șerban A., 2018, p. 163). Before addressing the supervisory authority, the data subject whose rights have been infringed has the possibility to address directly to the controller, this being in some cases a more efficient method of remedying the non-compliant way in which the data are processed (Tataru Ș.R. & Nica I.T., 2020).

CONCLUSIONS

The General Data Protection Regulation has led to significant changes in the way organizations process the personal data of employees, customers, consumers and other categories of data subjects. Human resources activities need to be redesigned to comply with data protection regulations.

In labour relations, regulations in the field of personal data protection contribute to the legal mechanism of protection of the employee against abuses that could be committed by the employer. Thus, the employer has the obligation to maintain the confidentiality of

any personal information about the employee, regardless of whether it was provided directly by the employee or acquired by the employer during the performance of the employment contract, except for the processing of data for which the employee gave his consent or was previously and explicitly informed about.

The impact of the new data protection regulations has been strongly felt in human resources activities but, in the current context, the effect produced by GDPR reminds operators that people, human resources, like data, are not an easy "commodity" to exploit, but involve responsibility, transparency and respect for human rights.

References

1. European Data Protection Board (2020). *Hamburg Commissioner Fines H&M 35.3 Million Euro for Data Protection Violations in Service Centre.* Retrieved from: https://edpb.europa.eu/news/national-news/2020/hamburg-commissioner-fines-hm-353-million-euro-data-protection-violations_en
2. Iftimiei A. (2018). Protecția datelor cu caracter personal. Aspecte de drept european. în *Analele Științifice ale Universității "Alexandru Ioan Cuza" din Iași, Științe juridice*, tomul LXIV, nr. 1/2018.
3. Mintern, T. & Rayner, S. (2018). *Society for Human Resource Management*, Bird & Bird. Retrieved from: https://www.shrm.org/resourcesandtools/legal-and-compliance/employment-law/pages/global-gdpr-hr.aspx
4. Mondy, R.W. & Martocchio J. J. (2016). *Human Resource Management.* (Fourteenth Edition). Pearson Education. Harlow, United Kingdom.
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, 4.05.2016.
6. Șerban A. (2017). Reglementarea dreptului de a fi uitat. în *Analele Științifice ale Universității "Alexandru Ioan Cuza" Iași, Științe Juridice*, nr. 2/2017.
7. Șerban, A. (2018). Soluționarea litigiilor privind datele cu caracter personal. în *Analele Științifice ale Universității „Alexandru Ioan Cuza" Iași, Științe Juridice*, Tomul LXIV, Supliment 2018.
8. Tataru, G.F. (2019). Migration – an Overview on Terminology, Causes and Effects. *Logos Universality Mentality Education Novelty: Law*, 7(2), 10-29. doi:10.18662/lumenlaw/24
9. Tataru, Ș.R. & Nica I.T. (2020). Privacy & Data Protection in Sport Industry. *Sport and Society - Interdisciplinary Journal of Physical Education and Sports*, Volume 20, Issue 1. DOI: 10.36836/2020/1/12.
10. Ungureanu, C. T., (2017). Protecția datelor cu caracter personal în contractele internaționale. în *Analele Științifice ale Universității "Alexandru Ioan Cuza" Iași, Științe juridice*, Tomul LXIII, nr. 2/2017.
11. Ungureanu, C. T. (2019). Legal Remedies for Personal Data Protection in European Union. *Logos Universality Mentality Education Novelty: Law*, 6(2), 26-47. https://doi.org/10.18662/lumenlaw/10.