Considerations regarding compliance with the Regulation (EU) 2016/679 (GDPR) in Human Resources Departments

Monica Florentina CALOPEREANU

The Bucharest University of Economic Studies, Bucharest, Romania
monica.calopereanu@gmail.com

PICBE | 548

Marian ȘUICĂ

Technical University of Civil Engineering of Bucharest, Bucharest, Romania
mariansuica@gmail.com

Alin Nicușor CALOPEREANU

The Bucharest University of Economic Studies, Bucharest, Romania
alin.calopereanu@gmail.com

Abstract. *Most companies and institutions, collect and process personal data about their employees, such as: name, phone number, email address, person's location information and activities at work, surveillance images from CCTV cameras, - all of these are personal data of individuals. And the list remains open. Consequently, all state or private institutions are affected by REGULATION no. 679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 ("GDPR"). In this paper we will present also, some of the past laws available in European Union prior to the approval of the REGULATION no. 679 of 27 April 2016. Those were also important for the life of the European citizens, but they have not been so well implemented and transposed into the legislation of all EU countries, which led in time to the appearance of the new REGULATION no. 679 of 27 April 2016. GDPR has a global impact as its rules are applicable to personal data that concern or describe the behavior of any natural person within the European Union even if the entities collecting and processing personal data are located outside the Union. Through this paper we aim to identify some of the main implications and risks deriving from the application of the GDPR at the level of the Human Resources Departments from the companies operating within the European Union.*

Keywords: GDPR, Human Resources, Data Protection, Compliance with Regulation (EU) 679/2016, Privacy.

Introduction

The right to the protection of personal data as well as the right to private life, are considered at European Union level, fundamental human rights. Unlike the European Union, in the United States of America, the right to the protection of personal data is considered a consumer right.

The interpretation and implementation of legislative regulations on the protection of personal data has become mandatory for all bodies (legal entities), in the European Union, or who offers goods and services on the territory of the European Union or to citizens of the European Union.

The Universal Declaration of Human Rights is the first international instrument that recognizes privacy / private life as the right of man. The right to private life and implicitly to

its protection (as well as personal data) is regulated for the first time in Art. 8 of the European Convention on Human Rights, respectively in Art. 7 of the Charter of Fundamental Rights of the European Union.

With the emergence of information technology in the 1960s, there has also been a need to adopt legal rules for the protection of personal data of individuals, with a series of resolutions of the Committee of Ministers of the Council of Europe on the protection of personal data, such as: Resolution 22 of 26 September 1973 on the protection of the Privacy of Individuals vis-a-vis electronic data banks in the public sector or Resolution 29 of 20 September 1974 on the protection of the privacy of individuals vis-a-vis electronic data banks in the public sector (Rădulescu et al., 2018).

Convention no. 108 for the protection of individuals with regard to the automatic processing of personal data was signed at the Council of Europe level on 28 January 1981 and represents one of the first legal instruments adopted at international level in the field of personal data protection (Rădulescu et al., 2018). Romania ratified this act by Law 682/2001, and by Law 55/2005 ratified the Additional Protocol to the Convention for the Protection of Individuals with regard to automatic processing of personal data, concerning control authorities and cross-border data flow (Rădulescu et al., 2018).

Literature review

On 24 October 1995, DIRECTIVE 95/46 / EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data was adopted.

The main reasons that led to the adoption of the documents are:

- creating an ever closer union among the peoples of Europe;
- promoting closer ties between member states;
- removing the barriers that divide Europe;
- data processing systems are in the service of man and must respect fundamental rights and freedoms, in particular the right to privacy;
- enhancing scientific and technical cooperation;
- the level of protection of the rights and freedoms of the person with regard to the processing of such data must be equivalent in all member states;
- member states will no longer be able to impede the free movement of personal data on grounds of protection of the rights and freedoms of the individual, in particular the right to privacy.

On April 27, 2016, was adopted Directive (EU) 2016 on the protection of individuals with regard to the processing of personal data by the competent authorities for the purposes of the prevention, detection, investigation or prosecution of criminal offenses or the enforcement of penalties and on the free movement of such data and repealing Council Framework Decision 2008/977 / JHA. The reason for the adoption of the Directive is that rapid technological developments and globalization have created new challenges for the protection of personal data in the context of the unprecedented increase in the volume of data processed (Rădulescu et al., 2018).

In the Official Journal of the European Union, series L 119/1, was published Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals 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).

Reasons for adoption of Regulation (EU) 2016/679

The principles relating to the protection of individuals with regard to the processing of their personal data should respect their fundamental rights and freedoms, regardless of the nationality or place of residence of natural persons.

PICBE | 550

The Regulation seeks to contribute to an area of freedom, security and justice, to economic and social progress, to the consolidation and convergence of economies within the internal market and to the welfare of individuals;

Defense of the right to intimate, family and private life in the processing of personal data.

According to "Article 4: Definitions": "personal data" means any information relating to an identified or identifiable natural person ("the data subject"). Meaning, *"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;"* (European Parliament, 2016).

"Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." (European Parliament, 2016).

At Article 6 - Paragraph 1 clearly states that *"Processing shall be lawful only if and to the extent that at least one of the following applies"* (European Parliament, 2016):

Consent - the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

Contract - processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

Legal obligation - processing is necessary for compliance with a legal obligation to which the controller is subject;

Vital interests - processing is necessary in order to protect the vital interests of the data subject or of another natural person;

Public interest - 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 controller;

Legitimate interests - processing is necessary for the purposes of the legitimate interests pursued by the controller 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 rights of individuals

In GDPR there are set forth rights of individuals, as regards the processing of personal data.

Right of access to processed personal data: the right to obtain a confirmation that your personal data are processed or not, and, if so, access to the type of personal data and the conditions of its processing by making a request to that effect to the operator;

Right to request the rectification or deletion of personal data: the possibility to request, by submitting a request to that effect to the operator, to rectify personal data that is inaccurate, supplementing personal data if they are incomplete or deleting personal data in situations where:

- personal data is no longer required for its original purpose (and there is no new legal purpose for processing);
- the legal basis for the processing is the consent of the data subject and the data subject withdraws his / her consent and there is no other legal basis for the processing;
- the data subject exercises his right to object and the operator has no reason to continue the processing that prevails;
- personal data has been processed unlawfully;
- deletion is required to comply with EU or Romanian law;
- personal data has been collected in connection with the provision of information society services provided to children (where applicable), for which consent is governed by special rules.

Right to request Restriction of Processing: You have the right to obtain restriction of processing in situations where:

- consider inaccurate personal data to be processed for a period that allows the operator to verify the accuracy of personal data;
- processing is illegal, but it is not desirable to delete personal data, requiring only restriction of their use;
- where the operator no longer requires personal data to process them for the purposes mentioned above, but data are required for the establishment, exercise or defense of a right in court;
- the data subject opposed to the processing for the period of time in which it is checked to see that the legitimate grounds of the operator prevail over the rights of the data subject.

The right to withdraw your consent for processing, when processing is based on consent, without affecting the lawfulness of the processing carried out until the consent is withdrawn;

The right to object to the processing of personal data; on grounds relating to the particular situation where the processing is based on a legitimate interest and at any time on the processing of personal data for direct marketing purposes, including the creation of profiles;

The right not to be the subject of a decision based solely on automated processing, including the creation of profiles, which produces legal effects concerning the data subject or similarly affects them to a significant extent;

The right to data portability, that is, the right to receive personal data that has been provided to the operator in a structured, commonly used and readable form, and the right to transmit such data to another operator, where the processing is based on consent or execution of a contract and is carried out by automatic means;

The right to lodge a complaint with the National Supervisory Authority for Personal Data Processing and the right to appeal to the competent courts.

Principles of the processing of personal data

The principles of the processing of personal data are provided in Art. 5: "Principles related to the processing of personal data":

Legality, equity and transparency - an essential principle associated with fundamental human rights. Personal data must be processed "*legally, fairly and transparently to the data subject*" (European Parliament, 2016).

Goal limitations - Personal data must be collected for well-defined, explicit and legitimate purposes, and subsequent processing must not deviate from these purposes.

Data minimization - By this principle operators are advised that any collection of personal data must be thoroughly analyzed before data is actually obtained, which must be most relevant and strictly limited to what is absolutely necessary for the purposes of which are processed.

The accuracy of the information - operators must take all measures to ensure the validity of the data and the inaccurate ones must be updated quickly or deleted.

Storage limitation - The data should be kept as long as necessary for the assumed processing.

Integrity and confidentiality - The processing of personal data must be done in its own safe conditions, including "*protection against unauthorized or unlawful processing and against loss, destruction or accidental damage by taking appropriate technical or organizational measures.*" (European Parliament, 2016). Whoever does not respect this principle is directly exposed to security breaches and confidentiality, being a safe candidate for extremely severe penalties.

In GDPR (Article 5, paragraph 2), the principle of responsibility is clearly stated: "*The operator must be responsible for compliance with paragraph 1 and be able to demonstrate that compliance ("responsibility").*" (European Parliament, 2016).

In other words, the most important provision of the Regulation is the principle of responsibility. GDPR asks you not only to follow the principles - for example, by documenting your decisions about a processing activity, but also to demonstrate this responsibility at any time.

Concluding, the rules established in accordance with the stated principles are contained in Recital 39 of the GDPR:

- Any processing of personal data must be legal and fair;
- The principle of transparency requires that any information and communication relating to the processing of such personal data must be easily accessible and easily understandable and that simple and clear language is used;
- Individuals should be informed of the risks, rules, guarantees and rights in the processing of personal data and how to exercise their processing rights;
- The specific purposes of processing personal data must be explicit and legitimate and determined at the time of collection of the data;
- Personal data must be appropriate, relevant and limited to what is necessary for the purposes for which it is processed;
- Personal data should only be processed if the purpose of the processing cannot reasonably be met by other means;
- The operator must set deadlines for the deletion or periodic review;

- Personal data must be processed in a way that adequately ensures security and confidentiality, including to prevent unauthorized access to or use of unauthorized personal data and equipment used for processing.

A considerable amount of personal data is processed within human resources departments. The new European regulation opens up plenty of opportunities for employees, which can cause trouble for employers. Employees may be pretentious about the protection of their personal data, may generate security breaches, complain to the National Data Protection Authority because they are well aware of the employer's vulnerabilities. Unlike accounting, HR and IT employees who, by the assumption that they are well paid, they are trustworthy, personal data protection issues can be generated by any employee regardless of his or her position in the organization (Savescu, 2018).

Many of the work relationships involve the processing of personal data, sometimes even sensitive data, or data of a special nature. Thus, from the moment of employment, the employer processes information about the future employee (such as those contained in his CV), which is becoming more and more numerous, depending on of the employment relationship (information on the family situation, the state of health , income levels, professional assessments, etc.) (Alexe, Ploesteanu, Sandru, & (coordonatori), 2017).

Recital 4 of the preamble to the Regulation states that the right to privacy, as well as the right to the protection of personal data, are not absolute rights, but must be assessed in relation to the social function performed and balanced with other essential rights, in accordance with the principle of proportionality, such as the protection of the reputation and rights of the employer, the protection of employees' rights and freedoms, or the prevention of disclosure of confidential information.

The rules on security of processing entail an obligation on the operator to implement appropriate technical and organizational measures to prevent unauthorized intervention on the processing operations. Data security is not only achieved by implementing hardware and software, but also by organizational rules such as:

- Accessibility of information on data security rules, confidentiality rules;
- Clearly designate responsibilities for data processing;
- Implementing physical protection measures, including those relating to computer equipment;
- Regular training of personnel with access to personal data.

Protection of personal data in the human resource activity

According to GDPR, in the human resource activity, processing of personal data includes any personal data processing operation. Among the most common examples of data processing include: keeping work contracts in the company's physical or electronic archive, recording video using CCTV, geolocation, monitoring the use of the Internet, email or activity on a computer, including the use of social networks.

All this processing is a sensitive issue not only from the perspective of GDPR, but also from the perspective of the European Convention on Human Rights, which states that the employee has the right to privacy and private life even in the workplace, regardless of the understanding between him and the employer.

Confidentiality clause for employees

From the point of view of ensuring personal data protection measures, we feel that it is necessary for the employer to include a confidentiality clause in the CIM (individual employment contracts) of the persons who have the tasks of processing these data (usually for the staff of the human resource departments and payroll, marketing, customer relationships, but also in the case of other employees who access / process personal data).

It is advisable to update the job descriptions of the employees who have access to and process personal data, in order to clearly specify the specific tasks in terms of personal data processing so that each employee to know what is authorized and what is not authorized to do with the personal data which he manages.

These aspects should also be provided in the operational / working procedures that employees apply in their work so that they should know what operations they are responsible for and how to do them, but also how to avoid and signal unauthorized access to personal data.

Retention of personal data

According to the provisions of Annex no. 6 of Law 16/1996 of the National Archives, published in the Official Gazette no. 71 of April 9, 1996, in the list after which the documents on the national interests can be given in the research, citizens' rights and freedoms have the following terms:

- Clearly designate responsibilities for data processing;
 - medical documents, 100 years after their creation;
 - civil status registers, 100 years after their creation;
 - personal files, 75 years after their creation;
 - documents about a person's private life, 40 years after his death;
 - the documents related to national security and integrity, 100 years after their creation;
 - criminal business documents, 90 years after their creation;
 - foreign policy documents, 50 years after their creation;
 - documents of commercial companies with private capital, 50 years after their creation;
 - tax documents, 50 years after the creation;
 - Notary and judicial documents, 90 years after their creation;
- In conclusion, the term for archiving personal files is 75 years after their creation.

The basis of the processing of personal data in accordance with the Regulation (EU) 679/2016

As regards the processing of personal data in accordance with Regulation (EU) 679/2016, we have the following processing bases:

Execution of the contract

When employee data is required for the effective execution of the employment contract, the company will be able to process those personal data and only those data using that basis (Ruxandra Pîrlan, 2017).

Compliance with legal obligations

If there are legal obligations (i.e. resulting from a law or order of a public authority) that the company has as an employer, such as: the transmission of employees' data for the purpose of labor protection or social security, the transmission to the tax authorities,

processing purposes related to occupational medicine, assessment of the employee's work capacity, the company has a legal basis for processing the data necessary to fulfill these obligations. Any other personal data collected in addition could be considered excessive, attracting the risk of fines (Ruxandra Pîrlan, 2017).

Consent

The processing of employee personal data on the basis of consent has become blamed over the last few years, just before the adoption of GDPR, through the various official documents published at EU level. The main argument is that the employee is in a relationship of subordination, of economic dependence on the employer, which calls into question his ability to manifest his will freely. Employees may feel compelled to consent to the processing of their data required by the employer, for fear or unwillingness to suffer adverse consequences at the workplace. For this reason, an employee's consent to the processing of his data, for example in the context of monitoring, could be considered invalid (Ruxandra Pîrlan, 2017).

Legitimate interest

The legitimate interest of the employer may be used as a basis for the processing of data, if it does not interfere with the private life of the employee. However, before implementing measures based on legitimate interest, society must carry out a proportionality test to assess the extent to which its aims prevail over the employee's private life or whether there are other ways to collect the necessary information, without interfering with the privacy of its employees (Ruxandra Pîrlan, 2017).

Monitoring employee activity

Employee monitoring cannot be done on the basis of their consent. Instead, it can be done on the basis of the legitimate interest of the employer if it does not cause an unacceptable interference in the employee's private life. In all cases, the employer must provide detailed information on how to conduct the monitoring, even before it starts.

Monitoring of documents and personal communications

Non-discriminatory monitoring of email, social networks, location information, personal preferences etc. should be avoided by minimizing the collection of personal data stored in personal devices only to those required only for risk areas identified by the company and related to the company's activity.

As a general rule, personal documents and communications should not be monitored, nor do some sensitive areas (e.g. recreation areas, religious sites, sanitary groups, use of the webcam to record the activity of the employee working at home, geolocation should not monitor continuously if the machine is available to the 24/24 employee, but only during working hours). It is advisable to use the probing check at certain time intervals in the work program instead of checking by continuous recording (Ruxandra Pîrlan, 2017).

Employee's right to oppose

Any monitoring, regardless of the basis and manner of deployment, must be completely transparent to the employee. Also, the employee has the right to oppose such processing if the monitoring is based on legitimate interest. In this case, the employer will have to demonstrate that his / her legitimate interest overrides the employee's right to privacy (Ruxandra Pîrlan, 2017).

Processing of personal data in the context of recruitment

Personal data collected in the context of recruitment should, as a rule, be deleted as soon as the recruitment process has been completed and it is clear that the persons concerned will not be employed, unless a reasonably established storage period has been specified for the data subject.

However, the employer could justify a legitimate interest in retaining such data until subsequent recruitment processes, but the opportunity of this interest must be assessed in real terms. The potential employee should be extensively informed about this, including the length of time that his data are stored, which must be reasonable and with the right to oppose the processing.

Transferring employee's personal data to other states

GDPR considers that companies belonging to a group may have a legitimate interest in transmitting personal data of employees within the group of companies for internal administrative purposes. This transfer can be done without prior authorization when personal data are transferred within the EU.

When data is transferred to a non-EU country, the rules remain unchanged. Thus, on the basis of the Binding Corporate Rules (BCR) expressly mentioned in the GDPR, this transfer may be made to a third State that has not been assessed and approved by the Commission as providing an adequate level of protection. Other compliant ways of transferring employee data to third countries are: standard protection clauses adopted by the Commission, codes of conduct accompanied by binding and enforceable commitments or certification mechanisms accompanied by binding and enforceable commitments.

Keep records and supervise authority

Companies with over 250 employees will be required to keep records of personal data processing activities in writing / electronically. The same obligation will be imposed on companies with less than 250 employees if the processing they perform is likely *"to create a risk to the rights and freedoms of the data subject, in particular in respect of criminal convictions and offenses."* (European Parliament, 2016).

Verification of compliance with GDPR provisions will be performed by the National Authority for Personal Data Processing Supervision (ANSPDCP). At the time of authority control, the company will be solely responsible for demonstrating that it complies with the legal provisions, and to do so, will need to document all processing activities and implement policies and procedures for processing personal data. The maximum fines to be applied in case of irregularities are EUR 20 million or 4% of the total turnover of the company.

Data Protection Officer (DPO)

One of the novelties of the GDPR has been the appointment of a Data Protection Officer (DPO) whose primary role is to coordinate and supervise the implementation of GDPR compliance conditions, as well as a link between the organization and the authority responsible for data protection.

By virtue of the nature of its functions and powers, a DPO has a central, strategic role in an organization:

- *"is properly and timely involved in all aspects of the protection of personal data"* (European Parliament, 2016).

- *"The operator and the person empowered by the operator shall ensure that the Data Protection Officer receives no instructions as to the performance of those tasks."* (European Parliament, 2016). A DPO may not be dismissed or sanctioned by the operator for the performance of his duties.

- the data protection officer responds directly to the highest level of management of the operator or the person empowered by the operator.

- he has an obligation to respect secrecy and confidentiality in the performance of his duties

Methodology [Cambria Heading, 14, bold, capitalise first word, justified]

The specificity of the qualitative methodologies consists in the analysis of the approved official documents and documents regarding the evolution and development of the personal data protection field (analysis of the national and European regulations in this matter), respectively comparative analyzes between the existing regulations at national and international level.

The purpose of the qualitative analysis is to precisely define and delineate the field of research, to support specific aspects of the analyzed field, namely, the field of personal data protection, and to contribute to the foundation of the research in this field.

The research carried out is based on specialized papers of the specialists in the field and on the information gathered from the legislative acts issued by the Romanian authorities and other documents issued within the framework of the legislative process within the European Union.

Results and discussions

It is important to note that, regardless of the processing for which employers choose, the right to the data processing must be correctly identified and the employee's rights in relation to the processing must be respected.

GDPR raises the obligation to protect personal data for all private or public bodies in the European Union. Claims that certain categories of activity do not apply to them, are likely to affect the rights and freedoms of the data subjects and subject the organization to major risks.

Conclusion

As a conclusion to this article, after reviewing the Regulation (EU) 679/2016 and other important books that deal with this area, among the measures that we consider necessary for alignment with GDPR provisions in the field of Human Resources, are:

- designation of a Data Protection Officer (DPO) - Responsible for personal data protection - where necessary. Please note that all public institutions in the EU have the obligation to appoint a DPO. This may be a person appointed from among employees, or an outsourced service.

- elaboration, revision / updating of strict procedures and policies at the level of the institution in the field of personal data protection;

- identification of the risks presented by the new types of activities developed at the level of the institution in order to know the processing carried out, in order to ensure the rights and freedoms of the data subjects, respectively the elaboration of the impact assessment on the data protection;

- making the declaration of the obligation to maintain confidentiality regarding personal data and signing it by all employees;

- introduction of data protection clauses / specifications into employment contracts.

These clauses must achieve the following:

- It should be specified which categories of data are collected from the employee, the purpose and legal basis of the processing. Consent is not, as a rule, the legal basis for the processing of personal data in the relationship between the employer and the employee. Execution of the contract and legal obligations usually provide the legal basis for collecting data from the employee.

- If data is exported outside the European Union (it is a common practice in multinational groups), it is necessary to specify the legitimate interest in doing so and it is mandatory to provide information on the destination and types of data processing exported, legal and security guarantees provided in that territory.

- In employment contracts, it is necessary to specify which are the subsequent recipients of the data collected by the employers, which is the purpose of such processing.

- If data is collected about employees from third parties, these should be specified. If the collection is done after employment, the employee must be informed within 30 days of collection.

- It is mandatory for the contract to clearly indicate the retention period of the data, or the criteria taken into account, to determine when the data should be deleted.

- The person concerned (the employee) must be informed of his / her rights. It is desirable and advisable to use clear, straightforward language, without technical terms or legal jargon in drafting clauses.

- Annual training / when needed for employees, respectively training of new employees, in view of the entry into force of GDPR;

The subject of personal data protection is extremely wide, the absence of explicit rules of application being the engine of endless discussions in the interpretation of some articles of the Regulation.

In essence, in the application of the Regulation, we can identify our own personal data protection system, designed by each responsible person and according to that domain. This can be seen as a threat to the institution as well as an opportunity to build a system of protection for the organization, a pretext for reorganizing it.

References

Alexe, I., Ploesteanu, N.-D., Sandru, D.-M., & (coordonatori). (2017). Marius Eftimie, Adina Rus – Protecția datelor cu caracter personal în relațiile de muncă. In *Protectia datelor cu caracter personal* (p. 280). Bucuresti, Romania: Editura Universitara. Retrieved from https://www.editurauniversitara.ro/media/pdf/598450449ddc9Protectia_datelor_cu_caracter_personal.pdf

European Parliament. (2016). 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 Da. *Official Journal of the European Union*, 59, 1–88. Retrieved from <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

- Rădulescu, D. M., Radu, D. I., Radu, M. E., Ramona Liliac, O. D., Iacob, N. M., Iorga, B. G., ... Barbu, L. (2018). *Implementarea Și Impactul Regulamentului Ue Privind Protecția Datelor Cu Caracter Personal (Gdpr) În România • Studii • Legislație • Jurisprudență*. Bucuresti, Romania: Editura Dio. Retrieved from <http://www.edituradio.ro/magazin/implementarea-si-impactul-regulamentului-ue-privind-protectia-datelor-cu-caracter-personal-gdpr-in-romania-studii-legislatie-jurisprudenta>
- Ruxandra Pîrlan, A. bpv G. Ștefănică. (2017). GDPR: Protecția datelor în relația angajat – angajator. Retrieved from <http://hrmanageronline.ro/gdpr-protectia-datelor-in-relatia-angajat-angajator/>
- Savescu, A. (Savescu&Asociatii). (2018). Noutățile Din Codul Muncii 2018 - Top 13 Cele Mai Controversate Modificari Ale Legii. Retrieved from <https://legislatiamuncii.manager.ro/a/25365/noutatile-din-codul-muncii-2018-top-13-cele-mai-controversate-modificari-ale-legii.html>