The relationship between human resources activities and the general data protection regulation

Vanesa Madalina VARGAS

Bucharest University of Economic Studies, Bucharest, Romania

vanesa.vargas@fabiz.ase.ro

Sonia BUDZ

Bucharest University of Economic Studies, Bucharest, Romania

sonia.budz@yahoo.com

Bogdan Cristian ONETE

Bucharest University of Economic Studies, Bucharest, Romania

bogdan.onete@com.ase.ro

Abstract. *The goal of GDPR is to harmonize consumer rights in the European Union regardless of where they are or where they come from. This has an impact on the processing of personal data within organizations - especially in human resources departments. GDPR has major consequences in the HR field as the employer processes employee data (and potential employees) on a large scale. At the formal level, the Human Resources Director must ensure that the new concepts introduced by the Regulation are correctly reflected in the internal documents governing the duties and responsibilities of the employees. The biggest challenge in this regard is defining the role of the data protection officer at the organization level. The methodological section of this article includes a narrative analysis based on an interview with a data protection officer, head of compliance guide to GDPR. The purpose of this study reflects the impact of the Personal Data Regulations on the Human Resources activities. It is useful for organizations and subjects to know what particular attention should be paid regarding GDPR to the recruitment process, the access methods of the equipment available to the employee, the data protection solutions in the systems and the employee monitoring system.*

Keywords: Data protection, privacy policy, consumer rights, human resources activities, consent, data sharing.

Introduction

The European Parliament voted on the General Data Protection Regulation (GDPR) in May 2016. The GDPR came into force and replaced the Data Protection Directive 95/46/ EC in May 2018. It improved data subjects' privacy protection and facilitated organizations and companies' work through its clarified rules, more concretized requirements and even direct instructions on the implementation. All companies handling EU residents' personal data or monitoring data subjects' behavior within the EU, regardless of where they are based, are governed by the GDPR (European Union Agency for Fundamental Rights & Council of Europe, 2014). This indicates that non-EU and international companies will have to comply with both their national legislation and the GDPR.

Rapid technological development due to the convergence of calculation power progress, increased storage capacity (Subic et al., 2010) and advanced network technology makes it possible for companies to collect, process and interlink data in an expanded way (Dima & Maassen, 2018). They increasingly tend to use these data for various purposes, such as personalized services and marketing (Tahal & Formánek, 2020). As a result of technological development,

DOI: 10.2478/picbe-2021-0050

© 2021 V. M. Vargas, S. Budz, B. C. Onete, published by Sciendo.

This work is licensed under the Creative Commons Attribution 4.0 License.

along with globalization, new and increased challenges for personal data protection have emerged (Reding, 2010).

Irrespective of the subject matter of a company (whether or not involving the processing of personal data), if it has a single employee, that company is considered to be an operator within the meaning of the General Data Protection Regulation (GDPR) employee (Thüsing & Traut, 2013). We had an interview with the data protection officer of one of the biggest tech organization in the world, which requested to remain unknown in the current article. The officer explained the steps they took before the GDPR begin its effects, how they changed their human resources documents, policies, but also ways of recruitment. The Director of Human Resources must ensure that any action taken with regard to employee data is in line with the requirements of the Regulation. This applies to all processes managed by the human resources team, from the recruitment process, to the conclusion and implementation of the employment contract and to its termination.

Literature review

The success of the TCP/IP protocol was more than a simple technical innovation. As quoted by the Internet founders themselves, “the Internet is at once a world-wide broadcasting capability, a mechanism for information dissemination, and a medium for collaboration and interaction between individuals and their computers without regard for geographic location”. This amazing development permitted organizations all over the world to store and exchange data from any location (Miron et al., 2009). The digital interactions between humans and machines and between machines and machines gave birth to a new data type. This metadata is very sensitive because it can provide individuals behavior (Chivu et al., 2015). The national authorities do not have enough money, time and competence in order to process every interaction. The self-regulatory instruments are not enough especially when the purpose of the organization is not the most positive. The new GDPR improves these shortcomings and makes data controllers accountable for their practices (European Commission, 2012). Additionally, it encourages organizations to use certification procedures.

As Conroy notes, globalization of trade turned the brand into a strategic asset and its wider exposure made the brand very sensitive to all events that could have detrimental effects (Bejtkovský & Copca., 2020). Thus, certification offered multinationals a business strategy to “avoid the risk of brand damage ... an insurance against malfeasance” (Conroy, 2007). The outsourcing of manufacturing facilities in countries that do not always guarantee social, health and environmental protections, created demand to cover the legal risks created by the absence of reliable regulation. It has been argued that certification offered a suitable response to the legal uncertainty created by the globalization of trade and authorities’ incapacity to enact binding transnational regulations. Cafaggi (2014) and Havinga (2012) rather see, in the rise of certification, one of the outcomes of the growing intertwinement between public and private regulators in the transnational processes of regulation.

To Bartley, certification could be a compromise in the balance of power between multinationals, authorities and civil society representatives (Bartley, 2015). Multinationals would adopt certification to protect their brand image (Milićević et al., 2020). The authorities would consider this procedure to be soft monitoring preventing new administrative burdens and, for NGOs, a “shift in firm’s acceptable behavior” (Vogel, 2008).

The General Data Protection Regulation (GDPR) adopted on 24 May 2016 by the European Union and became applicable from 25 May 2018. Most of the theoreticians said that this regulation will be a game changer for the whole business environment and for all organizations providing

services or good for Europeans (Mantelero, 2013; Bird & Bird, 2017). All of a sudden, many start-ups emerged with offers in order to help the companies adapt to the new legal framework. Corporations were eager to invest in different trainings and courses, especially for the human resources department in order to align with the new regulations. It has been highly debated by scholars and legal practitioners, if the GDPR should be seen as a regulatory revolution or not (European Commission, 2002). It is certain that this regulation has a precedent and is not a very innovative or new legal framework (Council of Europe, 1950). The Data Protection Directive (DPD) was adopted in 1995 (European Commission, 1995). This means the new documents will just add some additional changes and the ones who already were complying with the former DPD, should adapt their operations and practices to the new legislation. Still, the list of data subject rights contained in the DPD is less expensive than its GDPR equivalent.

Methodology

The selected methodology for the paper is a qualitative research technique, which involves “conducting intensive individual interviews with a small number of respondents to explore their perspectives on a particular idea, program or situation” (Boyce & Neale, 2006) and is very modern. The format of the interview is a structured one, because there will be only one respondent, the personal data officer of a company. Since the interviewer can control the quality of the result the training before taking it becomes crucial. The questions were organized in details and rehearsing the interview was a way to practice it. Still, open answers were expected and the continuity of the discussion was an unknown. The research will introduce a process that includes the three main steps: information retrieval, comparing the data gathered from the interview with the general information found on the internet about the subject and presenting the analysis in a narrative method.

One complex aspect of this analysis will be information retrieval and data preparation. The correct extraction and preparation of the data from the personal data officer will have a major impact on the success of the study. The information retrieval process should be able to gather the latest news items released by the company and all the major changes they did after the GDPR took effect. The real challenge is to find out even practices that are not very popular among organizations and what it takes in order to keep the security of a company intangible. After the information retrieval process, the data needs to be classified, the most important paragraphs of the interview must be selected compared to other companies’ practices.

Results and discussions

According to GDPR, the right of access to personal data has been extended and gives the employee the right to be informed about:

- how long the employer wants to keep the data;
- if the data will be used for automated decision making;
- if the employer intends to transfer the data to overseas and, if so, what guarantees will be provided in this context (European Commission, 2016b).

In addition, the employer must inform the employee of the right to rectification and the right to file a complaint with a supervisory authority as well as the right to delete personal data, the so-called “right to be forgotten” (European Commission, 2016b). In practice, employers need to be clear about the purpose for which employee personal data is used and clearly motivate why they need to process these data.

In the recruitment area, we have the situation where the company makes a recruitment announcement and asks the candidates to send resumes, so they request personal data. Whether the recruitment announcement is posted on a job site or directly by sending an electronic newsletter to the internal database, the company still has to provide information on how the data will be processed (or used) how long it will be stored and if the data it has passed to the company will be transferred to third parties. Also, recruiters have a new obligation, namely to provide more information about how a candidate can access the data you have about him. One of the key changes is that anyone who collects data is then responsible for how data is processed even if they were transferred to third parties.

Asked which are the types of personal data the company processes about their employees, the respondent replied it depends a lot on the country the employee is located in. Still, the main types of personal data the company processes are as follows:

- Personal Information such as name, address, telephone numbers, email addresses (for work and home), date of birth, marital status, family status, dependents, emergency contact details;
- Identification Information such as photographs, government identifiers (where the company is required to collect this), passport, driving license, organization employee IDs, ID badges, IP address and MAC address;
- Compensation and Benefits Related Information such as bank details, salary, grading, commissions, bonuses, equity awards, tax codes, disability or sickness payments and benefit entitlements, elections and beneficiaries;
- Hiring related information such as background checks, CV, education, former employment and career history, academic qualification certificates, medical certificates, medical and occupational health questionnaires, references, offer letters and employment contracts;
- Job Related Information such as employment status, entitlement to work, work or residency permits and visas, job code, job title/grade, job change, training and development plans and records, professional affiliations, ex-patriate postings and resignation or redundancy details;
- Leave of Absence Information such as vacation requests and details of sickness, medical leave, paternity or maternity leave, adoption or parental leave, special leave, military leave and education leave;
- Performance and Management Related Information such as performance evaluations or reviews, disciplinary actions and grievances. Expenses and Travel Related Information including credit cards, expense management information, driving license and passport information;
- IT and Communications Related Information such as log in credentials, remote access and usage records and information about work related communications through the use of email, skype or telephone, internet, intranet and helpdesk services;
- Social Media Platform Related Information such as posts, comments or other content including photographs and videos posted on any public forum or internal site, social network, blog or other such outlet;
- Asset and Asset Use Related Information such as the allocation and usage of company cars, laptops, mobile phones, printers and credit cards;
- Access and Security Control Related Information such as CCTV, access and security controls to the extent this is necessary and permitted by law; security clearance applications required to support services provided to public sector customers;
- Health & Safety such as occupational health assessments and details of work accidents;
- Surveys such as responses you give to surveys on matters such as pro bono or volunteer service and diversity;

- Compliance Data such as records of compliance allegations, investigations and reports.

In limited circumstances the employee may provide with information related to the family members, e.g. emergency contacts, birth or marriage certificates and in connection with benefits.

The right to be informed about the personal data (European Commission, 2016b) is one of the big changes the GDPR provides, so the companies all around the world must specifically let their employees know exactly with what purpose they collect their data and how will they use it. “Every candidate needs to know the type of data collected, the purpose of collecting them, the type of access to the personal data they will send (ie who sees them and who processes them), how they are processed (where they are stored, what the processing time is, what happens after the recruitment process), as well as all the rights that he or she is entitled to.” Information on the processing of candidates' personal data can be made either with the recruitment announcement or with a separate policy eventually published on the employer's website in a dedicated section. “We process your personal data to comply with law and for legitimate business purposes and seek to collect the minimum amount of data required to do so.”

The main purposes of the company in the personal data collection are “Employment Management to establish and perform the employment contract, meet our legal obligations to you as your employer, maintain or terminate the employment relationship and enable you to perform your job.” This includes: recruitment, hiring, redeployment, re-location and termination; administration of payroll and payroll taxes, compensation, other awards and benefits including medical insurance, retirement plans, stock plans; absence, time and attendance management; performance, talent management, training and development; occupational health and safety; and disciplinary and grievance management. But also “Business Management to ensure the company can operate our business effectively and provide products and services to our customers.” and “Security to ensure your personal safety and the protection and security of HPE premises, assets, IT and communications systems, the HPE brand, intellectual property and the data of HPE and our customers from physical and cyber-related threats” (HPE Legal Department, 2018)

One of the big questions after the GDPR appeared, but also one of the reasons why these regulations were needed on the market is how the companies share their data to other parties. The personal data officer of the interviewed company gave us a neutral answer, rather a standard one: “we share or disclose your personal data within the group of companies where necessary for the purposes outlined above but also to a specific group outside the company group. We tried to ask further about this specific group, but all we got is:

- Government authorities and/or law enforcement officials to: respond to duly authorized information requests of police and governmental authorities; comply with law, regulation, subpoena, or court order; enforce/protect the rights and properties of company or its subsidiaries; or protect the rights or personal safety of company, our employees, and third parties on or using company property when allowed and in each case in accordance with applicable law;
- Company customers or business partners (e.g. resellers, distributors, OEMs) if needed to interact with them, provide product, services or support, quality control or billing;
- Company suppliers or business partners who provide services to support our business or provide services or benefits to our employees. All company suppliers and partners are required to enter into contracts with company that include privacy and security terms to ensure the appropriate use and protection of our employees' personal data. In some cases, the supplier may provide a service to you personally (e.g. health insurance) and will be responsible for the collection and

use of your personal data in compliance with law and their own privacy policy (European Commission, 2016a);

- To other companies and their professional advisors in the event we consider or decide to sell, buy, merge, reorganize or outsource all or part of the business, we may need to disclose certain information about you to these companies to facilitate or effect the transaction. We seek appropriate contractual protections from the prospective buyers or sellers in these situations and may also seek your consent where required by local law.

Conclusion

The objective of this study was to identify the upcoming GDPR requirements' practical implications for personal data intensive companies' organizational and technical privacy protection measures, as well as business strategy and policy development. Understanding these implications has high practical relevance to such companies, as substantial amounts of time, strategic planning, employee training and financial and human resources are typically needed to implement the requirements.

Consent is a critical pillar of the new legislation, and GDPR affirms that companies can only use personal data for the explicit purpose for which they were given (Spiekermann, 2012). For human resources teams, this means that employees must explicitly engage in allowing the employer to use their personal data and must be fully aware of how these data will be used.

GDPR also sets out strict mandates for reporting theft or loss of personal data. For the most companies, this is an issue for customer data, but speaking about HR department, the employee data is highly personal in nature. Thus, the regulation clearly states that data should be processed in a manner that ensures adequate security measures. That is, including protection against unauthorized access or unlawful processing, destruction or integrity damage. So, if the companies know they are not doing well in the online security area, companies need to consider additional measures to protect this information. If a cyber-attack leads to the loss of this information and the privacy of the employees is jeopardized, companies will have to notify the authorities within a maximum of 72 hours. Obviously, it's ideal for everyone in the company to avoid security breaches by paying more attention to the mail or spam messages they receive, the pages they enter, and the disclosure of passwords (things that employees should be alert anyway). This is because a breach of security, whether accidentally or unlawfully, leads to the unauthorized loss, destruction, disclosure or modification of personal data processed and stored by the company and unauthorized access to them. This is why the company where we interviewed the officer for personal data sends from time-to-time test e-mails in order to check how the employees react to this kind of phishing mails.

HR teams will explicitly require employee consent to collect and store this personal data. At the same time, companies can use their employees' personal information only for the purpose for which they have been requested and for which they have received the consent of their subordinates. If they want to use the data for something else, they will need to ask employees again. In other words, organizations will have to have a process of total transparency regarding the relationship with employees on their personal data processing area. This means the HR department must be in continuous dialogue with his employees.

References

- Bartley, T. et al. (2015). Looking behind the label: global industries and the conscientious consumer. Indiana University Press.
- Bejtkovský, J., & Copca, N. (2020). The Employer Branding Creation and HR Marketing in Selected Healthcare Service Providers, *Management & Marketing. Challenges for the Knowledge Society*, 15(1), 95-108. doi: <https://doi.org/10.2478/mmcks-2020-0006>.
- Bird & Bird. Guide to the General Data Protection Regulation; 2017. Available from: <https://www.twobirds.com/~media/pdfs/gdpr-pdfs/bird-bird-guide-to-the-general-data-protection-regulation.pdf?la=en>. [Accessed 5 October 2018].
- Boyce, C. & Neale, P. (2006). "Conducting in-depth Interviews: A Guide for Designing and Conducting In-Depth Interviews", Pathfinder International Tool Series.
- Cafaggi, F. (2014). A comparative analysis of transnational private regulation: legitimacy, quality, effectiveness and enforcement, *Private Transnational Regulatory Regimes – Constitutional Foundations and Governance Design*. Hague Institute for the Internationalization of Law.
- Chivu, L., Ciutacu, C., & Georgescu, L. (2015). Household income in Romania. A challenge to economic and social cohesion. *Procedia Economics and Finance*, 22, 398-4.
- Conroy, M.E. (2007). The value of Coca Cola brand has been evaluated at \$ 136 billion in 2002. For companies having the highest market value, the value of their brand represents more than 50% of their own value. *Branded! How the certification revolution is transforming global corporations*. New society publish. chap 1, 9.
- Dima, A.M., Maassen, M.A. (2018). From waterfall to agile software: Development models in the IT sector, 2006 to 2018. impacts on company management. *Journal of International Studies*, 11 (2), pp. 315-326.
- Havinga, T. (2012). Conceptualizing Regulatory arrangements: Complex Networks of Actors and Regulatory Roles Nijmegen Sociology of Law Working Papers Series 2012/01.
- Council of Europe. European Convention for the Protection of Human Rights and Fundamental Freedoms. Strasbourg: European Court of Human Rights; 1950.
- HPE Legal Department, Employee Privacy Policy, 4.05.2018, Confidential document.
- European Commission. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal L* 281, 23/11/1995, 0031–0050; 1995.
- European Commission. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (directive on privacy and electronic communications). *Official Journal L* 201, 31/07/ 2002, 0037-0047; 2002.
- European Commission. Proposal for a regulation 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 (General Data Protection Regulation). COM (2012) 11 final; 2012.
- European Commission. Commission implementing decision of 12.7.2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield. C (2016) 4176 final; 2016a.
- European Commission. 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 the Directive 95/46/EC (General Data Protection Regulation). Official Journal L119, 04/05/2016; 2016b.
- European Union Agency for Fundamental Rights & Council of Europe. Handbook on European data protection law. Luxembourg: Publications Office of the European Union; 2014.
- Mantelero, A. (2013). The EU proposal for a general data protection regulation and the roots of the 'right to be forgotten'. *Comput Law Secur Rev* 2013, 29(3), 229-235.
- Milićević, S., Petrović, J., & Đorđević, N. (2020). ICT as a factor of destination competitiveness: The case of the republics of former Yugoslavia, *Management & Marketing. Challenges for the Knowledge Society*, 15(3), 381-392. doi: <https://doi.org/10.2478/mmcks-2020-0022>.
- Miron, D., Dima, A. M., & Vasilache, S. (2009). Indexes of regional economic growth in post-accession Romania. *Romanian Journal of Economic Forecasting*, 11(3), 138-152.
- Reding, V. (2010). The upcoming data protection reform for the European Union. *Int Data Privacy Law* 2010, 1(1), 3-5.
- Spiekermann, S. (2012). The challenges of privacy by design. *Commun ACM* 2012, 55(7), 38-40.
- Subic, J., Vasiljevic, Z., & Andrei, J. (2010). The impact of FDI on the European economic development in the context of diversification of capital flows. *Proceedings of the 14th International Business Information Management Association, Business Transformation through Innovation and Knowledge Management: An Academic Perspective*, Istanbul, Turkey, 23-24.
- Tahal, R., & Formánek, T. (2020). Reflection of GDPR by the Czech Population, *Management & Marketing. Challenges for the Knowledge Society*, 15(1), 78-94, doi: <https://doi.org/10.2478/mmcks-2020-0005>.
- Thüsing, G, Traut, J. (2013). The reform of European data protection law: harmonisation at last? *Intereconomics* 2013, 48(5), 271-6.
- Vogel, D. (2008). *Private Global Business Regulation*. Haas School of Business, Department of Political Science, University of California. Berkeley, 262.