JOURNAL OF INFORMATION SYSTEMS ENGINEERING & MANAGEMENT

Journal of Information Systems Engineering & Management, 2018, 3(4), 30
ISSN: 2468-4376

lectito

GDPR Compliance in SMEs: There is much to be done

Maria da Conceição Freitas [1]*, Miguel Mira da Silva [1]

[1] *Instituto Superior Técnico, Universidade de Lisboa,* Lisboa, PORTUGAL

***Corresponding Author:** conceicao.freitas@tecnico.ulisboa.pt

Citation: Freitas, M. C. and Mira da Silva, M. (2018). GDPR Compliance in SMEs: There is much to be done. *Journal of Information Systems Engineering & Management*, 3(4), 30. https://doi.org/10.20897/jisem/3941

Published: November 10, 2018

ABSTRACT

The obligatory adaptation of Organizations to the General Data Protection Regulation (EU) 2016/679 (GDPR), will imply a set of legal, technological and functional changes, with a direct impact on the daily life of Organizations as a result of their increased responsibility with data protection subjects that has been reinforced by the new legislation. On the other hand, the transfer of responsibilities from the national authorities to the Organizations obliges them to prove, at all times, full compliance with the legislation. Organizations are subject to heavy fines when a non-compliance is detected. This new reality is a challenge for any Organization, and in particular for small and medium-sized enterprises (SMEs), which have fewer human and financial resources to carry out the necessary measures to comply with legislation. In order to know how SMEs are preparing themselves, we have conducted face-to-face interviews with ten industrial SMEs. The main conclusion is that, given these companies' lack of awareness of their obligations and duties in relation to Personal Data Protection, it is urgent to define a methodology to be able to comply with GDPR.

Keywords: GDPR, personal data protection, SME, general data protection regulation (EU) 2016/679

INTRODUCTION

The obligatory adaptation of Organizations to the GDPR (Regulation, 2016) will imply a set of legal, technological and functional changes, as well as the need to train managers and staff in general on this matter.

We must consider that, in general, Organizations have the technical and human resources needed to fulfil their objectives and find it difficult to understand and identify the means and costs required to comply with the referred Regulation and the major alterations in personal data processing and protection it will imply.

Thus, first and foremost, we must raise managing officials´ awareness on this issue. In fact, this regulation replaces Directive 95/46/CE (Directive, 1995), transposed to Portuguese law by Law no. 67/98 (Law on Personal Data Protection) (Law, 1998) still in force, which requires that Organizations communicate Personal Data processing (there are some exemptions) to the National Committee on Data Protection (Comissão Nacional de Proteção de Dados - CNPD) before collecting, storing and processing data. Currently, in those cases in which Personal Data processing involves sensitive data, only upon authorization by the CNPD is it possible for the Organization to collect, store and process those data (Law, 1998).

Replacing a "Directive" by a "Regulation" makes it applicable in all EU member states without the need of approval as national legislation and allows for harmonization of rules within the European Union (Stupka et al., 2017).

The new Regulation eliminates the need for Organizations to communicate processing of personal data to CNPD, and makes them responsible for the security, availability, confidentiality and integrity of the Personal Data

they may collect, store and process, in compliance with the new Regulation, as well as the responsibility to prove that compliance.

The most noteworthy aspects of the new Regulation are the reinforcing of rights of data subjects, the high fines Organizations may be charged in case of non-compliance and the fact that national authorities are given auditing and supervisory responsibilities. At the same time, national authorities are overwhelmed with the procedural handling of thousands of personal data processing which, if involving sensitive data, requires that the national authority issues a positive opinion before data may be collected, stored and processed.

The Regulation lays down a set of principles to process personal data: legality, loyalty and transparency, specified objective, limitation of data to be collected, accuracy, limitation of storage time, integrity, confidentiality and the principle of accountability [de Hert et al., 2016]. Additionally, it requires Organizations to communicate to the national authority, within 72 hours, whenever there is a breach of security if it implies a high risk to rights and freedom of data subjects and the data controller is not able to take measures to prevent that risk from occurring (Heimes, 2016).

This transfer of responsibility to Organizations raises the issue of how small and medium enterprises (SMEs) are preparing themselves for this and the least expensive means to meet those requirements, especially in the case of very small organizations with limited budgets, since compliance with the new Regulation may prove too expensive for small Organizations (Layton et al., 2017).

To better understand the situation (the compliance with the Regulation), we conducted face-to-face interviews in ten industrial SMEs based on a questionnaire.

When approaching these companies, we started by emphasizing the most important aspects of this new Regulation, assessing the measures that have already been implemented or are ongoing in order to adjust to this new scenario so as to better understand what still needs to be implemented. Based on our analysis of the replies, we will describe how ready SMEs are in view of the new legislation. We have concluded that most companies are not aware of their current and future obligations and duties in regards to Personal Data Protection.

GENERAL DATA PROTECTION REGULATION (GDPR)

The Regulation is the most important change in terms of data privacy of the last 20 years (Wróbel et al., 2017).

Since this Regulation is applied to all Organizations, we asked respondents if SMEs were ready or had ongoing activities so as to comply with the new Regulation until May 28, 2018, considering that they represent 99.9% of business in Portugal (Pordata, 2015).

The new Regulation is not applied the same way in all Organizations. Each Organization will implement organizational and/or technological procedures depending on its complexity and risk factors. Organizations must implement organizational and technical measures to foster good practices which are, from a global perspective, a privacy protection and management program, which poses a challenge to SMEs.

Personal Data means "any information relating to an identified or identifiable natural person ('data subject'); 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" (art. 4.1) EU 2016/679. Thus, all Organizations, regardless of their size, must ensure and evidence compliance in regards to the personal data of their employers, clients and suppliers (Regulation, 2016).

Organizations may only store and process personal data "collected for specified, explicit and legitimate purposes" (art. 5.1-b) if: (1) authorized by the data subject; (2) within the scope of a contract agreement; (3) fulfilling a legal obligation; (4) in the interest of the data subject or other natural person; (5) in the exercise of official authority (art. 6.1). Moreover, personal data may be "adequate, relevant and limited to what is necessary in relation for the purposes for which they are processed ('data minimisation')" (art. 5.1-c) (Regulation, 2016).

Organizations that collect, access, store or process personal data are now obliged to inform data subjects about what data they collect and what are their objectives in processing those data in an understandable and transparent way, using clear and simple language (Tesfay et al., 2018).

The Regulation reinforces the rights of Data Subjects, namely the right to information and access to personal data, their correction or deletion, limiting their processing, data portability, as well as opposing automatic decision including profile definition, thus forcing Organizations to adopt organizational and/or technical procedures so as to comply with the rights of the data subjects. Organizations must protect the rights of those who have given them their personal data, i.e., Organizations must comply with the Regulation and evidence that compliance (art. 5.2) (Regulation, 2016).

In some cases, prior consent of data subjects is now compulsory for the Organization to be able to collect, store and process personal data and, at any moment, data subjects may withdraw their consent (Safari, 2016).

Consent must be concise, understandable, easily accessible and written clearly and accurately (Chowdhury et al., 2017).

Information Governance in an Organization describes how information is managed and all the procedures involved. The following should be known about the data: their source, how they are processed, reliability in terms of integrity and accuracy, and traceability (Wróbel et al., 2017).

Reducing the risk of fines will depend on the Organization's ability to evidence a fast, adequate, accurate and robust response to any threat concerning security, confidentiality, integrity and availability of personal data (Mansfield-Devine, 2016).

RESEARCH METHODOLOGY

Interviews are commonly used to collect information that would not be available in the literature and through observation. An interview is defined as a process of social interaction between two people, in which one, the interviewer, aims to obtain information from the other, the interviewee (Haguette, 1992).

The design of an interview is crucial to obtain the interviewee's trust, as the interviewer's job is to create an environment that leads to the interviewee's replies being reliable and valid (Selltiz, 1974).

Interviews may be of three types, depending on the questions asked: non-structured, semi-structured and structured. In a non-structured interview, the questions arise spontaneously during the natural interaction, i.e., as in informal conversation. The semi-structured interview is based on a script of questions and, depending on the answers, the script provides secondary questions which may or may not be asked. In a structured interview, the questions asked to all interviewees are the same and they are asked in a pre-defined order. In terms of the replies, an interview may include open text answers or establish a set of possible answers for each question, among which the interviewee must choose the one that he or she considers most suitable.

A qualitative structured interview is a survey but with a set of previously defined questions, whose response is open. Opting for this research methodology allows interviewees to express their points of view and experience. In a face-to-face interview, there is synchrony in terms of space and time, allowing the interviewer to collect more information, including non-verbal communication, body communication, and tone, and the interviewee may supply or request more detailed information and change points of view and share concerns.

The questions in a qualitative structured interview should be open, unbiased (you should avoid using words that may influence the replies) and clear (Turner III et al., 2010); they are more adjusted to collecting facts and information; the information provided by interviewees may not be what is expected and may not easily be quantifiable (King, 1994).

Interviews have some disadvantages, the main ones being the fact that the interviewee may be influenced by the interviewer, the costs of travelling, the time needed to conduct and transcribe the interviews; however, it allows the interviewee to require more details on questions and for the interviewer to clarify replies (Opdenakker, 2006).

QUESTIONNAIRE

Since the Regulation is rather complex and long, we selected some questions (**Table 1**) that allowed assessing whether SMEs were in compliance or conducting activities to adjust to the most critical issues of the new Regulation.

Upon analysis of the GDPR, we selected critical themes for SMEs regardless of their business sector, which would be easily understood by the interviewees. The main themes are those in **Table 1**.

RESULTS

Ten SMEs were analyzed, three in the district of Lisbon, four in the district of Aveiro, and three in the district of Leiria, considering the competitiveness rate of those regions.

The competitiveness rate assesses the potential of each region in terms of competitiveness (human resources and physical infrastructures), as well as the degree of efficiency in their strategy (measured considering educational, professional, corporate and productive profiles) and efficiency in producing wealth, and the ability evidenced by business in competing at international level (INE, 2017). The competitiveness rate divides Portuguese regions into five major groups; the cities of Lisboa and Aveiro are included in the first group, the group with the highest score, and Leiria is in the second group. The companies in these districts are, in principle, those better equipped to adjust to the changes imposed by the GDPR.

The questionnaire was applied to senior officials of SMEs who, either in view of their position or responsibility, might influence collection, storage and processing of personal data within the Organization.

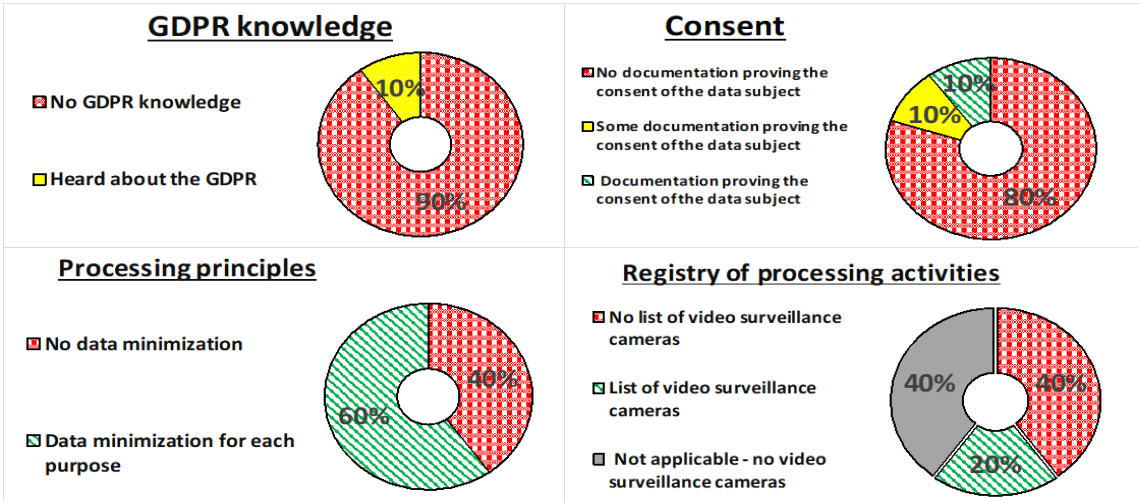

Figure 1. Knowledge, consent, processing principles and registry of processing activity

The interviews were recorded for transcription, after which they were destroyed; anonymity of interviewees and companies was also ensured.

In the present exploratory study, we opted for small and medium-sized companies because they are a significant part of Portuguese business and represent an important percentage of employment in the country. One senior official of each of these SMEs was interviewed face-to-face (Freitas et al., 2018).

The summary of replies to interviews conducted in September, October and November 2017 is presented in **Table 2.**

The interview proved to be the adequate methodology, allowing some interviewees to obtain further information on each question.

ANALYSIS OF RESULTS

We will analyze the replies on each of the themes referred to in **Table 1**.

Knowledge, Consent, Processing Principles and Registry of Processing Activity

According to the charts below **Figure 1**, most interviewees were neither aware of the new General Data Protection Regulation nor of their duties and obligations as a company in terms of consent, processing principles and registry of processing activities.

Labour Law and Security

The most companies are unaware of their obligations regarding aspects of labour law as well as of their duties to implement security mechanisms on the personal data they store and process.

Rights of Data Subjects

All companies replied they were unaware of the rights of data subjects, which is why they have not implemented procedures to ensure those rights.

Data Protection Officer

All companies replied they had less than 250 employees and that they have not appointed a Data Protection Officer.

Contracts

All companies that contract third parties were unaware of the need to have those contracts compliant with the GDPR if the third parties must collect, store, access or process personal data to supply their services.

Transfer of Personal Data to Third Countries or International Organizations

No company transfers data to countries outside the European Union/ European Economic Area.

Table 1. Questions grouped in terms of GRDP articles

Question	Theme
1. What department do you work for and what is your position? 2. What are your responsibilities regarding "Personal Data Protection" in your Organization?	Context
3. Do you know that the General Data Protection Regulation (GDPR) will come into full force on 25 May 2018?	Knowledge
4. In your point of view, does the organization have formal written consent of all personal data subjects in a clear and simple way? 5. Considering that the new regulation reinforces the concept of consent and introduces new conditions to obtain that consent, has your organization checked how and in what circumstances the consent of personal data subjects was obtained?	Consent (art. 6, 7 and 13)
6. In your point of view, are the personal data collected those strictly necessary for the objectives they are collected?	Processing principles (art. 5)
7. Does your Organization have an updated list of all surveillance cameras in your facilities? 8. Does your Organization have an updated list of all phone numbers whose calls are recorded?	Registry of processing activity (art. 30)
9. In your point of view, does your Organization monitor the use of telephone/e-mail/Internet? 10. Does your Organization make documentation available to its employees on the rules regarding use of the company's means of communication for private purposes?	Labor law (art. 88)
11. Does documentation supporting procedural protocol regarding requests by data subjects (for access, correction, opposition to processing and profile definition, deletion, data portability) aiming to enforce their rights establish maximum response time? 12. Is there registry of reporting process to third parties on data correction, deletion or processing limitation requested by data subjects?	Rights of data subjects (art. 15, 16, 17, 19, 20, 21 and 22)
13. Does your Organization have more than 250 employees? If yes, are you the appointed Data Protection Officer?	Data Protection Officer (art. 37, 38 and 39)
14. In your point of view, does your Organization have the tools to ensure the security and confidentiality of the personal data under your responsibility?	Data processing security (art. 32)
15. If your organization signs contracts with third parties for personal data processing, has your organization checked compliance of those contracts to the new regulation?	Contracts (art. 28)
16. If your organization transfers data to countries outside the European Union/European Economic Area, does your organization confirm whether it is legally authorized to transfer data to countries outside the European Union/European Economic Area?	Transfer of personal data to third countries (art. 44, 45, 46)
17. Are those in your organization with access to personal data informed of their obligations and the obligations of the organization?	Training (art. 25, 28 and 47)
18. Since the new regulation requires that your organization conducts training to those who, either permanently or regularly, have access to personal data, do you know the training plan already in place or to take place?	
19. Does your organization regularly assess compliance to regulations and laws on Personal Data Protection?	Accountability of data controller (24)
20. Does your organization have a written notification procedure in case of breach of security?	Notification of personal data breach to the superisory authority (art. 33)

Training

All companies replied that those employees with access to personal data are not informed of their duties and obligations and of the company's duties and obligation; only one company mentioned having a training plan on this matter.

Accountability of Data Controller

All companies are unaware of the accountability of the data controller. None of the companies regularly or from time to time assesses compliance with the regulations and laws on Personal Data Protection.

Notification of Personal Data Breach to the Supervisory Authority

All companies replied they were unaware of this obligation.

CONCLUSION

SMEs do not know Law no 67/98 and the new Regulation 2016/679. There is urgent need of a plan for implementing organizational and/or technological procedures to ensure compliance with new requirements of Personal Data Protection. This task should be carried out in collaboration with industry, sales or services Associations.

Table 2. Summary of Replies

Theme/Question number	Percentage of replies (%)				Analysis of replies
	No	*Partially*	*Yes*	*NA*	
Awareness (3)	90	10			Most respondents do not know the Regulation
Consent (4 and 5)	80	10	10		Most organizations do not have consent of data subjects
	100				
Principles of data processing (6)	40		60		Most respondents affirm that the collected personal data are those strictly required
Registry of data processing activities (7 and 8)	40		20	40	Most organizations which have video surveillance cameras do not have a list of those cameras. No organization records calls.
				100	
Labor law (9 and 10)	70		30		30% manage the company's means of communication but do not provide information on rules regarding the use of the company's means of communication for private purposes
	100				
Rights of data subjects (11 and 12)	100				No company has implemented procedure to ensure the rights of Data subjects
	100				
Data protection officer 13	100				No company has appointed a Data Protection Officer
Data processing security (14)	90		10		Most does not have a registry of security measures to ensure the security and confidentiality of personal data
Contracts (15)	100				No company has analyzed compliance of contracts with third parties regarding personal data processing under the GDPR
Transfer of personal data to third countries or international organizations (16)				100	No company transfers data to countries outside the European Union/ European Economic Area
Training (17 and 18)	100				In most companies there is no staff trained on personal data nor is there planned training on this matter
	100				
Accountability of data controller (19)	100				All companies are unaware of the accountability of the data controller
Notification of personal data breach to the supervisory authority (20)	100				No company has implemented a procedure for notification of personal data breach to the supervisory authority

All organizations must comply with the new Regulation, not only to avoid heavy fines but also to supply services to compliant companies as that guarantees their sustainability and survival in an increasingly global world, which implies that we must find solutions that will allow SMEs to comply with the new Regulation.

Since SMEs in the processing sector do not know Law 67/98 nor the new Regulation 2016/679, there is urgent need to design a method that will allow them to become compliant with Law 67/98 and then implement organizational and/or technological procedures so that they become compliant with Regulation 2016/679.

Considering that the human resources staff is not in sufficient number to comply with the obligations this Regulation imposes and that, in some cases, there are huge budget limitations, it is crucial to find efficient and effective solutions.

REFERENCES

Chowdhury, M. J. M., Colman, A., Han, J. and Kabir, M. A. (2018). A Policy Framework for Subject-Driven Data Sharing. *In Proceedings of the 51st Hawaii International Conference on System Sciences*. https://doi.org/10.24251/HICSS.2018.594

de Hert, P. and Papakonstantinou, V. (2016). The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Computer Law & Security Review*, 32(2), 179-194. https://doi.org/10.1016/j.clsr.2016.02.006

Directive, E. U. (1995). 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 of the EC*, 23(6).

Freitas, M. C. and Mira da Silva, M. (2018). GDPR in SMEs. *In IEEE Information Systems and Technologies (CISTI), 2018 13th Iberian Conference on (pp. 1-5).*

Haguette, T. M. F. (1992). Metodologias qualitativas na sociologia. RJ. Vozes.

Heimes, R. (2016). Global InfoSec and Breach Standards. *IEEE Security & Privacy*, 14(5), 68-72. https://doi.org/10.1109/MSP.2016.90

INE. (2017). Índice Sintético de Desenvolvimento Regional 2015. *Destaque Informação à Comunicação Social, Instituto Nacional de Estatística, Portugal, 2017*.

King, N. (1994). *The qualitative research interview*. Sage Publications, Inc.

Layton, R. and Baranes, E. (2017). GDPR: Short Run Outputs vs. Long Term Welfare. Mapping the EU's General Data Protection Regulation to Best Practices for Online Privacy.

Law no. 67/98. (1998). Available at: https://www.dre.pt

Mansfield-Devine, S. (2016). Data protection: prepare now or risk disaster. *Computer Fraud & Security*, 2016(12), 5-12. https://doi.org/10.1016/S1361-3723(16)30098-7

Opdenakker, R. (2006). Advantages and disadvantages of four interview techniques in qualitative research. *In Forum Qualitative Sozialforschung/Forum: Qualitative Social Research*, 7(4).

Pordata, I. N. E. (2015). Average dimension of households.

Regulation, G. D. P. (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. *Official Journal of the European Union (OJ)*, 59, 1-88.

Safari, B. A. (2016). Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard for Personal Data Protection. *Seton Hall L. Rev.*, 47, 809.

Selltiz, C. (1974). Métodos de pesquisa nas relações sociais. EPU.

Stupka, V., Horák, M. and Husák, M. (2017). Protection of personal data in security alert sharing platforms. *In ACM Proceedings of the 12th International Conference on Availability, Reliability and Security (p. 65)*. https://doi.org/10.1145/3098954.3105822

Tesfay, W., Hofman, P., Toru, N., Kiyomoto, S. and Serna, J. (2018). PrivacyGuide: Towards an Implementation of the EU GDPR on Internet Privacy Policy Evaluation. *In ACM Proceedings of the 4th ACM on International Workshop on Security and Privacy Analytics (pp. 15-21)*. https://doi.org/10.1145/3180445.3180447

Turner III, D. W. (2010). Qualitative interview design: A practical guide for novice investigators. *The qualitative report*, 15(3), 754.

Wróbel, A., Komnata, K. and Rudek, K. (2017). IBM data governance solutions. *In IEEE Behavioral, Economic, Socio-cultural Computing (BESC), 2017 International Conference on* (pp. 1-3).

