Implementation of GDPR: Learning with a Local Administration Case Study

Fernando Martins(✉), Luís Amaral, and Pedro Ribeiro

Information Systems Department/ALGORITMI Research Centre, School of Engineering, University of Minho, Guimarães, Portugal
fernandorui@outlook.com, {amaral,pmgar}@dsi.uminho.pt

Abstract. The General Data Protection Regulation has come into force in the European Union in May 2018 in order to meet current challenges related to personal data protection and to help harmonise the data protection across the EU. Although the GDPR was expected to benefit companies, being private or public, by offering consistency in data protection activities and liabilities across the EU countries and by enabling more integrated EU wide data protection policies, it poses new challenges to companies. However, if we take a step back and think that this regulation has been in transit for more than 2 years, and that only after the implementation of this regulation has begun the real concern is: are companies ready to make this leap?

Keywords: GDPR · Data · Data protection · Data claims · Data rights

1 Introduction

The General Data Protection Regulation (GDPR) has come into force in the European Union (EU) in May 2018 in order to meet current challenges related to personal data protection and to help harmonise the data protection across the EU.

Although the GDPR was expected to benefit companies, being private or public, by offering consistency in data protection activities and liabilities across the EU countries and by enabling more integrated EU wide data protection policies, it poses new challenges to companies [1].

The projects of implementing the GDPR have emerged with high frequency, offering new opportunities and challenges to the companies [2], being private or public. This situation led these companies to seek support from consulting firms in order to increase the likelihood of success and achieve compliance in the shortest time possible.

However, the greatest distinction between a public company and a private company is related to a lack of legal definition and public procurement that the former is obliged to follow [3], and therefore more time necessary for the implementation of these kind of efforts.

Throughout this document, it will be described the whole process followed by a local administration company in Portugal.

H. Santos et al. (Eds.): SmartCity 360 2019, LNICST 323, pp. 205–216, 2020.
https://doi.org/10.1007/978-3-030-51005-3_19

2 What Is GDPR?

The GDPR. was initiated, in 2012, by the European parliamentarian Viviane Reding, then the vice-president of the European Commission.

According to Viviane Reding, the main concern that led to this regulation was "the concern about the big companies, like the American GAFA—the French coinage for Google, Amazon, Facebook, and Apple" and the way they just ignored the old law [4].

A driving force behind all the arguments was the various scandals created around countless data losses, either voluntarily or involuntarily. For example, the Facebook Cambridge Analytica scandal, if it had happened after the May 26th of 2018, it would have cost billions of euros to Facebook, among others [5].

The GDPR aims to take the high ground in order protect all European citizens in the defence of their personal and sensitive data.

This is driven by philosophical thinking, and stance, as far as data protection is concerned [6]. Its core is based on the concept of privacy as a fundamental human right and seeks to extend to the whole EU [7].

This new regulation is intended to cover the personal data of all EU residents, this takes place regardless of where the data can be stored or processed.

The European Parliament and the Council of the European Union, using their legislative powers conferred under European Union law, deliberated on the subject of Data Protection, culminating, as such, in the EU General Data Protection Regulation (GDPR) of the European Parliament and of the Council of 27 April 2016) [7], which has been in force in the EU since 25 May of this year. This regulation should be considered in the practices of organisations, as it "is binding in its entirety and directly applicable in all Member States" [7].

In certain matters under the GDPR, the European legislator allows Member States to be able to specify some internal rules in certain matters within the GDPR. However, although Council of Ministers approved Law 120/XIII [8] to specify these internal rules, it has not yet been approved, so that "until there is national legislation implementing the GDPR repealing Law 67/98 on matters covered by the regulation, Law 67/98 remains in force in everything that does not contradict the GDPR.

According to Article 4 of the Regulation, personal data is information that can, directly or indirectly, identify an individual, in particular by reference to an identifier, such as a name, an identification number, location data, identifiers by electronic means (i.e. e-mail) or a more specific element of the physical, physiological, genetic, mental, economic, cultural or social identity of that individual " [7]. This is a more comprehensive regulation than its North American counterpart [6].

GDPR is often confused as one that deals only with technology, however, the GDPR protects personal data regardless of the technology used for processing that data.

The GDPR is technology neutral and considers both automated and manual processing, provided the data is organised in accordance with pre-defined criteria. It also doesn't matter how the data is stored – being in an IT system, through video surveillance, or on paper [9]. In all cases, personal data is subject to the protection requirements set out in the GDPR.

2.1 Territorial Adaptation

Despite the European regulation, there is some flexibility to adapt to the national reality of each member country of the European Union, however, until a national law to adapt this regulation comes into reality, this document comes into force on the 25th of May of 2018 [10].

This means that there is a unified and directly applicable data protection law for the European Union which replaces almost all of the existing Member States' provisions and which is applied by businesses, individuals, courts and authorities without transposition into national law [10].

Thanks to its broader territorial scope and the definition of personal data, it is a fact that the application of this regulation has a significant impact on organisations, whether private or public, and on the perceived fragility of all this information by its owner.

Regarding data processing carried out by competent authorities for the detection, prevention, investigation and prosecution of criminal offenses and for the execution of criminal sanctions, the Portuguese law 67/98 remains applicable in its entirety [11].

Thus, taking as its starting point the GDPR [7] and the Portuguese law 67/98 [11], as it remains in use at the time, this is considered as the relevant legal, statutory, regulatory and contractual requirements regarding data protection and retention periods dispersed by various normative acts.

The Portuguese law 67/98 [11] is applied to all forms of personal data processing whether resulting from the context of the business activities or the monitoring of individual activities.

Another fact that is quite relevant is the fact that the national laws that are more restrictive or impose requirements not addressed by this policy overlap with it [12].

2.2 Opportunity or Threat?

The GDPR was "the most contested law in the E.U.'s history, the product of years of intense negotiation and thousands of proposed amendments" [4].

The need to require affirmative consent, which must be freely given, specific, informed, and unambiguous [1] can be seen as an opportunity because it obtains a biddable authorization of all the treatment carried out.

It is then a determining factor the ability of each company to make the use of GDPR and turning that factor into an opportunity.

Regaining control of the data, stored and managed by the enterprises, will bring a whole host of benefits beyond compliance, demolishing the data silos and obtaining a more systemic view of all the data and processes that obtain the same data.

The need to change the way that the management of information is made will produce more accurate and useful insights [13] and a greater clarity across enterprise data.

The biggest threat, and more noteworthy, lies in the time that Portugal took to implement European legislation in which it only saw its final version adopted on June 12, 2019, which entered into force in all the member states of the European Union for more than a year [14].

3 Case Study

All companies have different scopes. Some exist in business contexts related to industry or commerce activities, others are public entities and there is still room for those that do not have any profit objective.

Despite this distinction in their scope they all have internal structures, which represent their mission, vision and strategy that serve as a foundation for all the objectives of these same companies.

Teatro Circo de Braga, EM, S.A., (see Fig. 1), is a company located in Braga, Portugal, that operates in the cultural sector, functioning in one of the most beautiful buildings of Portugal.

Fig. 1. Teatro Circo de Braga, EM, S.A.

This company is heir to a long tradition, but its ambition leads them to make future every present day through its dynamic image and continuity, looking continuously for a program that captivates and brings new audiences to its beautiful theatre room.

Nowadays, customizing the offer is always supported by a huge data processing regarding the data of its customers and possible clients.

3.1 Theatro Circo de Braga EM, S.A

In the past three years the TCB has been very involved in a process of external validation of the company, causing restrictions in the regular development of its activity and with repercussions in the programmatic and management options.

The year 2017 would mark the beginning of a new cycle through the visa awarded by the Court of Auditors to the contract programme. Thus, TCB could finally establish long-term commitments, including one to initiate the process that could lead to the compliance with GDPR, leading to several substantive changes to the day-to-day operation and processes of TCB [15].

As a local administration company, it is still imperative to mention that, in addition to the internal dynamics and TCB's willingness to reinvent itself and define new objectives every year, there are still other responsibilities resulting from the commitments made to the city's strategy are being proposed by the Municipality of Braga.

3.2 Motivation

TCB is committed to conducting its business in accordance with the European Union data protection legislation and the national data protection legislation and being in line with the highest standard of ethical conduct.

This policy establishes the principles that employees and third parties must follow in relation to collection, use, retention, transfer, disclosure and destruction of data of natural persons regarding the processing of personal data and the free movement of such data.

Personal data is subject to legislation and regulations that impose restrictions on how organisations can handle such data. An organisation that treats personal data and makes decisions about its use is designated as "controller". While being the "controller"[1], the TCB is responsible for ensuring compliance with the personal data protection requirements defined by this policy.

The top management is committed to the continuous and effective implementation of this policy and expects employees and third parties to share the same principle and the violation of this policy may result in disciplinary proceedings.

One of the great difficulties identified is the absence of standard documents and processes. By default, there was no documented process that identifies the necessary steps or a matrix of responsibilities in order to support the cycle of a said process or to sustain the decision-making process or improvements.

The absence of these processes creates a gap and therefore an opportunity of improvement in terms of management that, considering the challenge created by the implementation of the GDPR, can justify the need to create all processes, and its documentation, in order to identify the owners of the process and all the data treated and the classification of the same data according to the sensitivity that they have before this same regulation [13].

3.3 Protection of Data from Conception to Default

It is recognized that the main step towards a correct implementation of the GDPR is the involvement of all employees, the dissemination of information and the application of the various processes that are created or improved in order to dramatically improve legal certainty and coherence in the area of data protection law [10].

According to the regulation, it is recommended, and even imperative in several situations, that the organisations should have one or more Data Protection Officer (DPO) [6] in order to ensure the application of the principles of personal data protection in the institution.

[1] See Article 4.º, paragraph 7 of the General Data Protection Regulation.

The DPO should keep a register of all personal data processing operations in their institution [16]. Providing advice and making recommendations on rights and obligations.

This new actor is of extreme importance, for example if there are conflicts between this policy and the national legislation, the Data Protection Officer (DPO) should be consulted.

In order to increase the success rate of the implementation, the privacy value for TCB must be determined. Since the personal data of the stakeholders play a relevant role for the organisation, all the data must be treated in a way that guarantees a high level of privacy and a control by each data subject.

Therefore, all the key objectives of the privacy program must be understood in order to guarantee an adequate level of risk to the rights and freedoms of singular persons; to achieve a high level of privacy; full control by the data subject; compliance of European and national privacy rules; raising the awareness of stakeholders and continuing this process with a perspective of continuous improvement through process monitoring and metrics, and therefore, privacy by design.

3.4 The Need of Documented Processes

As stated earlier, the presence of a process that defines and helps to determine a special need in the data processing is of high importance, so a default process, as illustrated in Fig. 2, has been created in order serve as a basis for all TCB internal processes and which will ensure unprecedented control over the continuity and continuous improvement that the GDPR requires.

This way, and in order to achieve the previous objectives regarding the compliance of GDPR, TCB has developed and followed a strategic model consisting of eight steps that can be seen on Table 1:

The GDPR compliance project requires numerous changes of functions in terms of human resources, work processes and documentary.

Table 1. Strategic model of the implementation of the General Data Protection Regulation.

#	Step
1	Definition of the context of the organisation and governance
2	Classification, transfer mechanisms and inventory of personal data
3	Awareness of all the internal and external stakeholders
4	Evaluation and treatment of information security risks in the organisation (internal stakeholders) and in the relationship with third parties (external stakeholders)
5	Operational life cycle
6	Management of personal data incidents
7	Performance monitoring and effectiveness of the implementation of the Regulation
8	Conformity

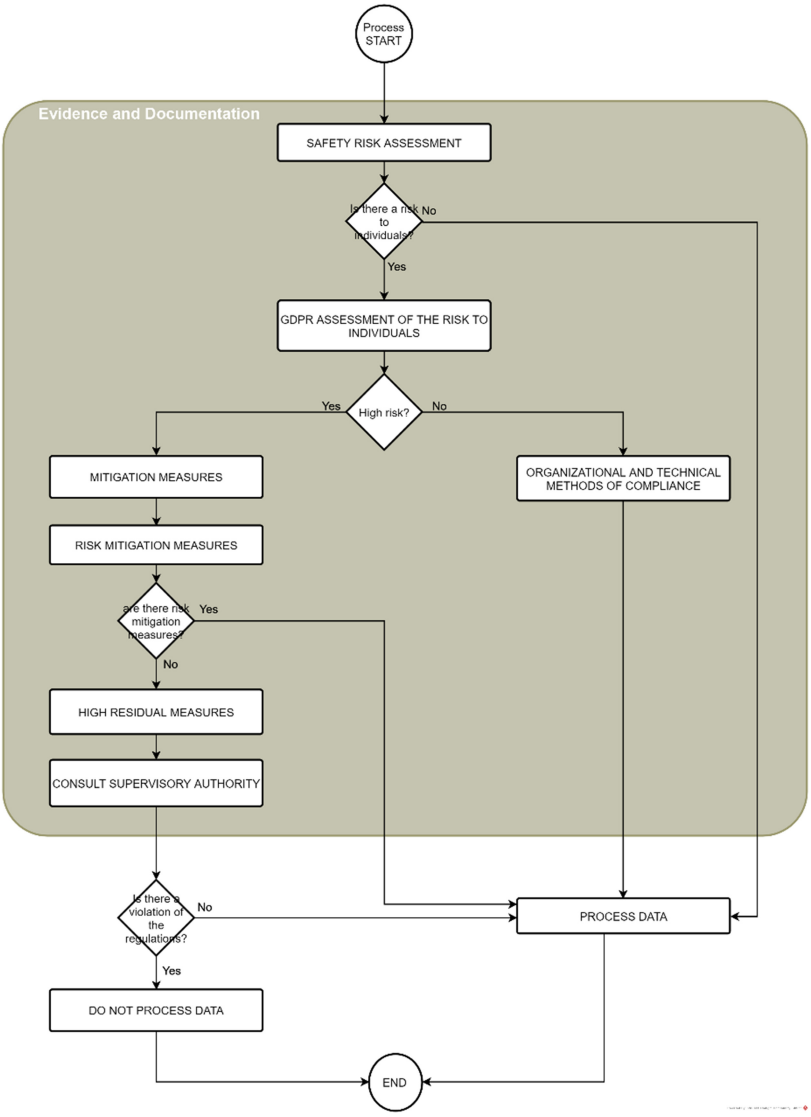

Fig. 2. Data privacy by design

4 GDPR – The Effort of Compliance

The GDPR compliance project, already completed in the TCB, required numerous changes of functions in terms of human resources, work processes and documentary.

This effort was expected to take two months of dedicated work (8 weeks), however, and as a result of an initial misidentification of the commitment of the employees, the project was extended by two weeks.

One of the main steps in the implementation of the GDPR is the commitment of the top management and the creation of a motivated team [17].

In order to demonstrate the commitment to data protection, TCB has adopted the role of Data Protection Officer (DPO)[2] [7].

It is recognized that the main step towards a correct implementation of the GDPR is the involvement of all employees, the dissemination of information and the application of the various processes created.

Therefore, all employees responsible for the processing of personal data and subcontractors are aware of and apply this policy.

All new programs, systems and processes as well as their revision and expansion are subject to a change management and approval process in the Privacy Group [7].

For each program, system and process it is necessary to carry out data protection impact assessment (DPIA)[3] [7] - in cooperation with and approved by the DPO.

The following scenarios, seen in Table 2, always require full DPIA and not just an assessment of their need:

Table 2. Scenarios needing DPIA

#	Scenarios needing DPIA
#1	New technologies whose treatments are likely to pose a high risk to the rights and freedoms of natural persons in accordance with the risk perception methodology in force
#2	Systematic and comprehensive assessment of personal aspects related to natural persons, based on automated processing, including profiling
#3	Large-scale processing of special data categories
#4	Systematic control of large-scale publicly accessible areas

As part of this process, external stakeholders who may be affected by the project (such as customers, suppliers, regulators, unions, workers' commission, lawyers or other parties who may provide a unique perspective on the privacy risks they see as which need mitigation) should be heard.

Risks that cannot be mitigated in a timely manner or that cannot be mitigated should be disclosed to regulators and stakeholders if applicable.

To ensure an adequate level of compliance by TCB to the Data Treatment Policy, the DPO must perform annually an audit of the processing of personal data on a regular basis where it should be conducted for the specific purpose of evaluating actions taken based on an external event such as a complaint, violation, inquiry or exercise of a right.

A deliverable of this kind of implementation is the adoption of the principles stated in the Table 3.

[2] See articles 37.º, 38.º and 38.º of the General Data Protection Regulation.

[3] See article 35.º of the General Data Protection Regulation.

Table 3. Adopted principles of the GDPR

#	Principle
1	personal data is processed lawfully, fairly and transparently in relation to the data subject[a] [8]
1	personal data is collected for specific, explicit and legitimate purposes and cannot be further processed in a way that is incompatible with those purposes[b] [8]
3	personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed[c] [8]
4	personal data is accurate and up-to-date where necessary, and all appropriate measures must be taken to ensure that inaccurate data for the purpose of processing are erased or rectified without delay[d] [8]
5	personal data is stored in a way that allows data holders to be identified only for the period necessary for the purposes for which they are processed[e] [8]
6	personal data is processed in a way that ensures their safety, including protection against unauthorized or unlawful processing and loss, destruction or accidental damage by adopting appropriate technical or organisational measures[f] [8]
7	Presence of the capacity to demonstrate compliance with the six principles previously announced.

[a]See article 5º. (1) (a) of the General Data Protection Regulation.
[b]See article 5º. (1) (b) of the General Data Protection Regulation.
[c]See article 5º. (1) (c) of the General Data Protection Regulation.
[d]See article 5º. (1) (d) of the General Data Protection Regulation.
[e]See article 5º. (1) (e) of the General Data Protection Regulation.
[f]See article 5º. (1) (f) of the General Data Protection Regulation.

All the efforts made in controlling the information can not only be performed within the walls of the TCB, for example the web pages.

TCB also trails the following process in order to investigate, allegedly, improper practices performed by employees in relation to violations of established corporate rules that may result in violation or affect the rights and freedoms of natural persons, that process can be seen in the Table 4.

Upon completion of the GDPR compliance project, TCB shall initiate a process for reviewing and improving the Privacy Management System (PMS) achieved.

However, the effort made it possible to reach a risk mitigation index of around 84%, and only 15 risks remain and are expected to be solved during the first year after the closure of this project.

Table 4. Response Process to the Claim

Processes	Description
Policy	This process is tailored to the different types of allegations that may be concerned about the conduct of the employee. Other policies and procedures such as the rules of procedure and the code of conduct should be observed in addition to this process and conduct research in full respect of existing legislation
Risk	Not all alleged violations of the rules imposed constitute an adverse risk to the rights and freedoms of natural persons. The organisation's risk methodology should be followed to assess whether the risk requires treatment or whether it is likely to be classified as residual, and there is no need to take mitigation actions
Researchers	The choice of who will lead the research, one should choose someone who is independent, objective and not superior to the alleged collaborator
Plan of action	The action plan consists of the response to the claim
Evidence	These can be in the format of videos, mail exchange, interviewing witnesses among others. A signed statement from the person who reported the alleged misconduct or practice should be collected and kept as evidence. All evidence must be assigned an identification number, cataloguing and description
Report	Create a summary of the research highlighting the evidence gathered and the actions to be taken. Include evidence of support, applicable laws, regulations and internal policies that are relevant to the case, and which highlight the actions required to be taken. This report should be classified as confidential and restricted access
Corrective action	This phase may include training actions for the employee, trigger a disciplinary process, the creation of new policies or the review of existing policies. Once the correct action or actions are determined, immediate action must be taken in the implementation of the solution
Monitoring	After the implementation of the action or corrective actions, the parties involved should be monitored to evaluate the effectiveness and impact of the measures taken

5 Conclusions

It is notorious that this data protection regulation fundamentally challenges businesses that trade in personal data, however, which company does not currently handle personal data? Being this data from customers to suppliers or even employees?

Regaining control of the data, stored and managed is the main objective, and should not be a threat but rather an opportunity.

Invoking responsibility for themselves, the companies, as TCB has done, is a show of determination, responsibility and commitment to all individuals within the European community and theirs mostly unknown rights.

The fact that Portugal took too much time to implement European legislation in which it only saw its final version adopted on June 12, 2019, although it did not have a general consensus in the final document for approval, can be a demonstration that cultural factors represent an impediment in the understanding of personal rights and in the information that each one has, especially when there is a grey area between what is physical information and digital information.

Looking more closely to the case study, and upon completion of the GDPR compliance project, TCB is not looking at this regulation as a threat or a constraint, but rather looking at the broader compliance picture to find a way to focus all the efforts and make them more efficient. Turning the compliance effort, a regular business process that is in constant review and development.

This is a fine example of the opportunity and gains that the implementation of the regulation offers.

Acknowledgements. This work has been supported by national funds through FCT – Fundação para a Ciência e Tecnologia within the Project Scope: UID/CEC/00319/2019.

References

1. Tikkinen-Piri, C., Rohunen, A., Markkula, J.: EU General Data Protection Regulation: changes and implications for personal data collecting companies. Comput. Law Secur. Rev. **34**(1), 134–153 (2018)
2. Tankard, C.: What the GDPR means for businesses. Netw. Secur. **2016**(6), 5–8 (2016)
3. Martins, Fernando, Ribeiro, Pedro, Duarte, Francisco: Improving project management practice through the development of a business case: a local administration case study. In: Rocha, Álvaro, Adeli, Hojjat, Reis, Luís Paulo, Costanzo, Sandra (eds.) WorldCIST'18 2018. AISC, vol. 745, pp. 433–448. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-77703-0_43
4. Powles, J.: The G.D.P.R., Europe's New Privacy Law, and the Future of the Global Data Economy. The New Yorker (2018). https://www.newyorker.com/tech/annals-of-technology/the-gdpr-europes-new-privacy-law-and-the-future-of-the-global-data-economy. Accessed 28 June 2019
5. Houser, K., Voss, W.G.: GDPR: the end of Google and Facebook or a New Paradigm in data privacy? SSRN Electron. J. **25**, 1 (2018)
6. Goddard, M.: The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. Int. J. Mark. Res. **59**(6), 703–705 (2017)
7. The European Parliament and the Council of the European Union: 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)
8. Assembleia da República: PROPOSTA DE LEI N.o 120/XIII (3.a). Debate Parlam. da Assem. da República, pp. 30–48 (2018)
9. European Commission: What is personal data?—European Commission (2019). https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en. Accessed 25 June 2019
10. Albrecht, J.P.: How the GDPR Will Change the World (2016)

11. Assembleia da República: Lei n.º 67/98 de 26 de Outubro - Lei da Protecção de Dados Pessoais (1998)
12. APOGEP: National Competence Baseline - NCB 4.0. ssociação Portuguesa de Gestão de Projetos (2017)
13. Garber, J.: GDPR – compliance nightmare or business opportunity? Comput. Fraud Secur. **2018**(6), 14–15 (2018)
14. R. do J. de Notícias: Aprovada versão final de execução do RGPD. Jornal de Notícias. https://www.jn.pt/nacional/interior/aprovada-versao-final-de-execucao-do-rgpd-11003399.html. Accessed 28 June 2019
15. Theatro Circo de Braga, "Relatório e Contas 2017," Braga, 2018
16. European Commission: The PM2 Project Management Methodology (Guide 3.0), The PM2 Gu. European Commission, DIGIT (2018)
17. Demchenko, Y., Turkmen, F., De Laat, C.: Bootstrapping GDPR: technical infrastructure requirements and architectures to implement GDPR, December 2018