Implementation of the General Data Protection Regulation: A Survey in Health Clinics

Isabel Maria Lopes
Instituto Politécnico de Bragança, Bragança, Portugal
UNIAG, Instituto Politécnico Bragança, Portugal
Centro ALGORITMI, Guimarães, Portugal
isalopes@ipb.pt

Pedro Oliveira
Instituto Politécnico de Bragança, Bragança, Portugal
pedrooli@ipb.pt

Abstract — **The new General Data Protection Regulation (GDPR) was approved on April 27 2016. The GDPR 2016/679 aims to ensure the coherence of natural persons' protection within the European Union (EU), comprising very important innovative rules that will be applied across the EU and will directly affect every Member State. Furthermore, it aims to overcome the existing fragmented regulations and to modernise the principles of privacy in the EU. This regulation will come into force in May 2018, bringing along several challenges for citizens, companies and other private and public organisations. The protection of personal data is a fundamental right. The GDPR considers a 'special category of personal data', which includes data regarding health, since this is sensitive data and is therefore subject to special conditions regarding treatment and access by third parties. This premise provides the focus of this research work, where the implementation of the GDPR in health clinics in Portugal is analysed. The results are discussed in light of the data collected in the survey and possible future works are identified.**

Keywords - regulation (EU) 2016/679; general data protection regulation; personal data; health clinics.

I. INTRODUCTION

Although this regulation was approved on April 27, its enforcement was set for the twentieth day after its publication in the Official Journal of the European Union. Therefore, it came into force on May 26 2016. The EU established a two-year transitional period for companies to implement the necessary changes until May 25 2018 in order to ensure the full compliance of their data treatment with the rules imposed by the GDPR.

The relevance of the GDPR is due to the major current challenge of ensuring control over data privacy in a time when the growing adoption of the Internet, social networks and digital business models create an equation which is hard to solve: on the one hand, people are enticed and share information about their personal life, more often than not without accounting for potential collateral effects; on the other hand, organisations collect increasingly more information on their clients, usually with the aim to provide more and better services or as a way to monetise the information [1].

Currently, there are 28 data protection acts based on the EU Data Protection Directive of 1995, that is, a regulation implemented over 20 years ago [2]. Technological evolution, and the increasingly common use of smartphones, wearable devices or the Internet of things brings along a pressing concern about our personal data and its protection and causes the regulatory entities to be more alert and implement new regulations.

Before the new GDPR, previous data protection legislation had become fragmented across the EU as different countries added to the basic principles enshrined in the original directive of 1995. Another reason why new legislation was needed is that the original directive of 1995 was formulated in what now appears to be a different technological era. Back then, just 1% of the world population was using the Internet, but today it is almost ubiquitous across the EU. Cloud computing and social media were not known then, nor were smartphones or tablets. Today, the vast majority of information is produced and consumed electronically, making it harder to protect [3].

The recent approval of the General Data Protection Regulation holds positive prospects for the future of data protection in Europe. The existence of a solid and uniform legal framework across Europe that has been updated to meet the needs of technology will not only allow for the potential of the Digital Market to be freed up, for the promotion of innovation, for the creation of employment and generation of wealth, but also for safeguarding the fundamental right of data processing protection for citizens or residents in Europe [4].

This regulation introduces significant changes in natural persons' protection with regards to personal data treatment, imposing new obligations to citizens, companies and other private and public organisations.

Since the transitional period is coming to an end for the full compliance of companies with the regulation, it is relevant to acknowledge companies' level of preparation for the new GDPR demands. Many industry sectors could have been chosen, but this research work focused on the health sector, through a survey conducted in health clinics in Portugal. The aim was to determine the point to which these companies are in compliance with the new personal data regulation.

The structure of the present work consists of an introduction, followed by a desk review on the general data protection regulation and its implementation. The following section focuses on the research methodology, identifying the target population and the structure of the survey. The results of the study are discussed in section 5, followed by the conclusions drawn from the study. Finally, the limitations of this research work are identified and possible future studies are proposed.

II. GENERAL DATA PROTECTION REGULATION

The enforcement of the GDPR on natural persons' protection regarding personal data treatment and movement, which repeals the Directive 95/46/CE of October 24 1995, poses innumerable

challenges to both public and private entities as well as to all the agents whose activities involve the treatment of personal data.

Although the full application of the new GDPR has been set for May 25 2018, date from which the directive 95/46/CE will be effectively repealed, its enforcement on May 25 2016 dictated the need for an adaptation to all the aspects changed or introduced by the regulation. Such adaptation of the present systems and models as well as of best practices regarding personal data treatment and protection by companies is now an imperative stemming from the regulation in order to safeguard its full applicability from May 25 2018.

However, before focusing directly on the new regulation, it is important to clarify exactly how the document defines 'personal data' since its protection is the focus of the act.

The GDPR defines personal data in a broad sense so as to include any information related to an individual which can lead to their identification, either directly, indirectly or by reference to an identifier. Identifiers include [5]:

- Names.
- Online identifiers such as social media accounts.
- Identification numbers (e.g., passport numbers).
- Data regarding location (e.g., physical addresses).
- Any data that can be linked to the physical, physiological, genetic, mental, economic, cultural or social identity of a person.

Companies collecting, transferring and processing data should be aware that personal data is contained in any email and also consider that third parties mentioned in emails also count as personal data and, as such, would be subject to the requirements of the GDPR [2].

The GDPR requirements apply to each member state of the European Union, aiming to create more consistent protection of consumer and personal data across EU nations. The GDPR mandates a baseline set of standards for companies that handle EU citizens' data to better safeguard the processing and movement of citizens' personal data.

The main innovations of the General Data Protection Regulation are [4]:

1. New rights for citizens: the right to be forgotten and the right to a user's data portability from one electronic system to another.

2. The creation of the post of Data Protection Officer (DPO).

3. Obligation to carry out Risk Analyses and Impact Assessments to determine compliance with the regulation.

4. Obligation of the Data Controller and Data Processor to document the processing operations.

5. New notifications to the Supervisory Authority: security breaches and prior authorisation for certain kinds of processing.

6. New obligations to inform the data subject by means of a system of icons that are harmonised across all the countries of the EU.

7. An increase in the size of sanctions.

8. Application of the concept 'One-stop-shop' so that data subjects can carry out procedures even though this affects authorities in other member states.

9. Establishment of obligations for new special categories of data.

10. New principles in the obligations over data: transparency and minimisation of data.

Among these points representing the main innovations imposed by the new legislation, we highlight point nine, in which the regulation recognises that health data integrates the 'special categories of data' considering that such data is sensitive and therefore subjected to special limitations regarding access and treatment by third parties.

Health data may reveal information on a citizen's health condition as well as genetic data such as personal data regarding hereditary or acquired genetic characteristics which may disclose unique information on the physiology or health condition of that person. The protection of such health data imposes particular duties and obligations to the companies operating in this sector.

As far as the security of personal data is concerned, the GDPR mandates the application of appropriate technical and organisational measures to ensure an adequate security level, among which:

- The pseudonymisation and encryption of personal data;
- The capacity to ensure the permanent confidentiality, integrity, availability and resilience of data treatment systems and services;
- The capacity to re-establish prompt availability and access to personal data in the event of a physical or technical hazard.

All organisations, including small to medium-sized companies and large enterprises, must be aware of all the GDPR requirements and be prepared to comply by May 2018. By beginning to implement data protection policies and solutions now, companies will be in a much better position to achieve GDPR compliance when it takes effect.

III. Implementation of the GDPR

The sooner organisations begin to prepare for the GDPR, the more they will minimise risks and reduce the likelihood of fines being imposed and the more able they will be to comply with the changes imposed.

Therefore, companies must determine what changes they need to make in order to comply with the new regulation and proceed to the implementation of such changes, which might even include the adoption of new security measures.

Organisations should get acquainted with the requirements under the GDPR. Following this, organisations should review all data processing activities currently undertaken and envisaged in order to identify any breaches in compliance with the GDPR and the associated risks. It is also important to review all contracts, privacy notices, consent forms and any other documentation

under which data processing occurs so as to ensure that these are in line with the GDPR.

The following figure (Fig.1) identifies the main stages towards the implementation of the GDPR as well as what to develop in each of them.

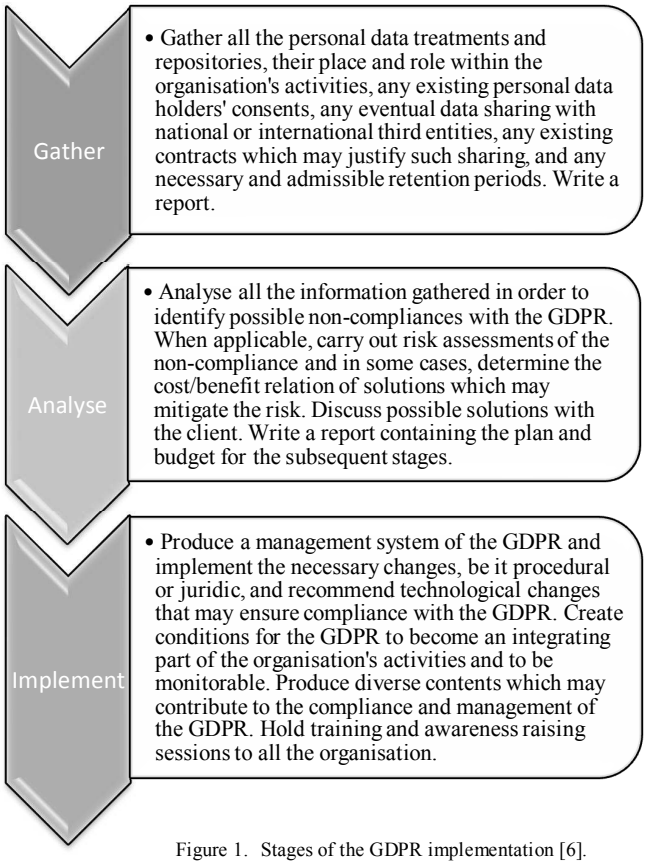

Figure 1. Stages of the GDPR implementation [6].

The implementation of the GDPR can be conducted in three different but complementary stages – Gather, Analyse and Implement. After the conclusion of theses stages, companies will have to ensure the continuity of their compliance with the GDPR, for which periodical compliance audits must be carried out.

This GDPR best practices guide puts forward a GDPR implementation methodology designed to [7]:

- Engage stakeholders to ensure timely and efficient organisational readiness for the GDPR.
- Implement effective procedures that embed GDPR-compliant operational behaviours.
- Establish assurance criteria that will sustain and evidence GDPR accountability.

The methodology consists of three phases (Prepare, Operate, Maintain), with each incorporating a number of supporting activities. The objective defined for each phase is attained once all of the activities for that phase have been successfully executed. The ultimate goal of the methodology is to sustain and evidence compliance with the GDPR Accountability Principle.

Table 2 below lists the phased activities which support the Accountability Life Cycle.

TABLE I. PHASED ACTIVITIES THAT SUPPORT THE ACCOUNTABILITY LIFE CYCLE

Phase	Activity
Prepare	Obtain the buy-in of key business stakeholders; Establish your GDPR readiness program team; Identify and assess relevant business functions; Identify and assess in-scope Third Party Processing activities; Establish a central Personal Data register; Distribute updated Data Protection policies and Privacy Notices; Educate internal Personal Data Handlers and external Data Processors.
Operate	Disseminate and maintain external Privacy Notices; Justify and record lawful Processing mechanisms; Process and record Data Subject rights requests; Validate and record Third Country data transfers; Report and manage Personal Data Breach incidents.
Maintain	Evidence understanding of Data Protection policies; Ensure the ongoing integrity and quality of the Personal Data Processing register; Trigger impact assessments for business change events; Verify compliance of Third Party Personal Data Processing activities; Demonstrate effectiveness of Personal Data handling practices.

Other opinion, referring four options that are possible to meet the GDPR vision of certification mechanisms, data protection seals and marks encouraging transparency and compliance with the Regulation, in line with Recital 100. The options demonstrate the range of possibilities that the GDPR supports. The options are [8]:

- Encouraging and supporting the GDPR certification regime;
- Accreditation of certification bodies;
- Certification by national data protection authorities;
- Co-existence of the above three.

These approaches provide a summary of the necessary phases or stages for the implementation of the GDPR. In the next section, information is given on the target population of this

research work so as to then present the results concerning the implementation of the GDPR in the health clinics surveyed.

IV. Research Methodology

The digital impact and transformation of recent years is visible in several sectors. The health sector is no exception and such transformation is an indisputable fact.

Digital revolution brings along inevitable concerns regarding users' data security, privacy and protection, especially as far as health and clinical information is concerned [9].

The choice of an appropriate data collection to characterise the implementation of the GDPR in medical clinics fell on the survey technique, since it enables a clear, direct and objective answer to the questions asked to the respondents. Also, the universe under study comprises thousands of clinics, among which 190 were surveyed, numbers which make the adoption of alternative research techniques not recommendable if not impossible.

The aim of the survey was to characterise the current state of health clinics with regards to the implementation of the GDPR, in other words, determine their level of knowledge and preparation regarding the issue of personal data protection and privacy.

A. Population

The survey was sent to 190 clinics, but only 57 gave an effective reply, which corresponds to a response rate of 30%. The sample subjects were selected randomly based on the kind of clinic and their location distributed throughout the 18 inland Portuguese districts as well as Madeira and the Azores.

Among the 190 contacts established, 35 replied via telephone and 22 via email after a first telephone contact.

In as many cases as possible, the respondent to the survey was the person in charge of the clinic's IT department. When there was no such person, the respondent was the person in charge of the clinic.

The study was conducted between October and December 2017.

B. Structure

The structure of the survey resulted from a desk review on personal data protection and the study of the legal framework Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27 – General Regulation on Data Protection.

The questions of the survey, of individual and confidential response, were organised in three groups.

The first group aimed to obtain a brief characterisation of the clinic as well as of the respondent. The two following groups contained questions concerning the GDPR applicability, preceded by the paramount core question: 'has the clinic implemented the measures imposed by the GDPR yet?'

After responding to this central question and when the answer was negative, respondents were asked whether they intended to implement such measures, since they were not in compliance with the regulation, and if so, whether the implementation process was already in motion. When the respondents did not intend to adopt any measure, they were asked about whether or not they were aware of the fines they may have to pay for the non-compliance with the regulation and why they did not intend to adopt such measures.

A positive answer to the central question would lead to the group of questions targeted at the companies which are already in compliance with the regulation or which are implementing the measures imposed. Some of the questions asked within this group were as follows: Are you aware of the GDPR? What impacts and challenges will clinics face in the compliance with the regulation? What stage of the implementation of the GDPR are you in? Have you identified or designated anyone for the post of Data Protection Officer? Has any training or awareness raising session been held about the new rules? Is the protection of personal data a priority in this clinic?

The survey was quite extensive. However, for this study, our focus lies uniquely on the implementation of the regulation, thus on the clinics which have implemented or are currently implementing the regulation.

V. Results

When asked whether they have started or concluded the process of implementation of the measures enshrined in the GDPR, 43 respondents (75%) answered no and 14 (25%) said that they have started or concluded the adoption of the measures (Fig.2).

Among the 14 clinics which gave a positive answer, only 4 (28%) consider that they are already in compliance with the demands of the regulation. The remaining 10 clinics (72%) are still implementing the measures.

This number seems residual when we observe that among the 57 clinics enquired only 7% have completed the implementation of the GDPR.

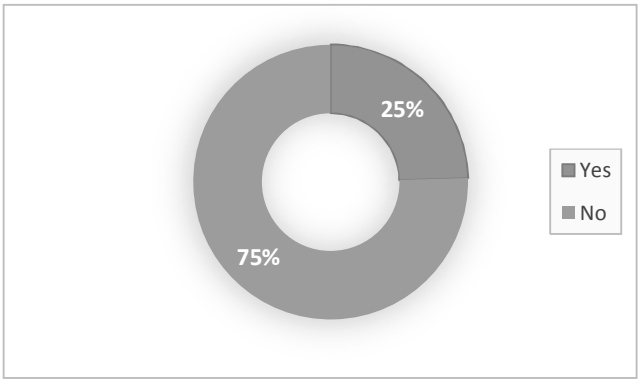

Figure 2. Clinics which are implementing the GDPR

For a better understanding of the results, we can group the clinics into three clusters (Fig.3):

- Cluster 1 – Clinics in compliance with the regulation;
- Cluster 2 – Clinics which are implementing the measures imposed by the regulation;

- Cluster 3 – Clinics which are not in compliance with the regulation.

Since this study focuses on the implementation of the GDPR, emphasis will be given to clusters 1 and 2 since cluster 3 comprises clinics which are not implementing the regulation.

The majority of the subjects surveyed are aware of the obligations and challenges posed by the new general data protection regulation, although this seems a contradiction since only 25% of the clinics have adopted or are adopting the measures imposed.

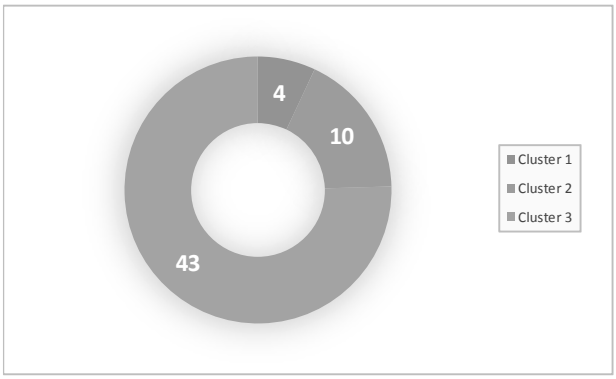

Figure 3. Clusters according to the GDPR transitional implementation

The implementation of the regulation requires a higher or lower level of demands depending on the size of the company as well as on whether they were already or not in compliance with the principles enshrined in the directive n. 95/46/CE.

In about 36% of the clinics surveyed, the respondents foresee that the adoption of the GDPR will entail a high or very high impact, 43% foresee a medium impact and 21% a low or very low impact as far as implementation time, effort and costs are concerned (Fig.4).

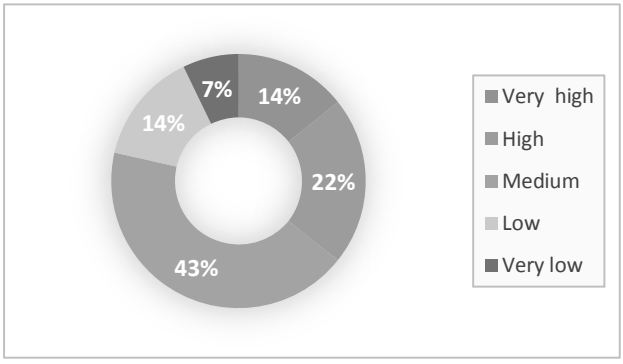

Figure 4. Impact of the GDPR implementation

When the clinics in cluster 2 were questioned about the implementation stage of the GDPR (gather, analyse and implement) they were in, half of the ten respondents stated to be in a stage which corresponds to gathering, 30% said they were in a stage of analysis, more specifically assessing the risk of not complying with the regulation, and 20% of the clinics are currently implementing measures identified in the previous stages and contained in the reports. The implementation will enable the creation of conditions to make the GDPR an integrating part of the organisation's activities as well as to make it monitorable (Fig. 5).

After the conclusion of these implementation stages, a compliance assessment must be conducted periodically since the data is not immutable and even the company business and activity may undergo changes which may make the measures initially implemented inadequate to the new circumstances.

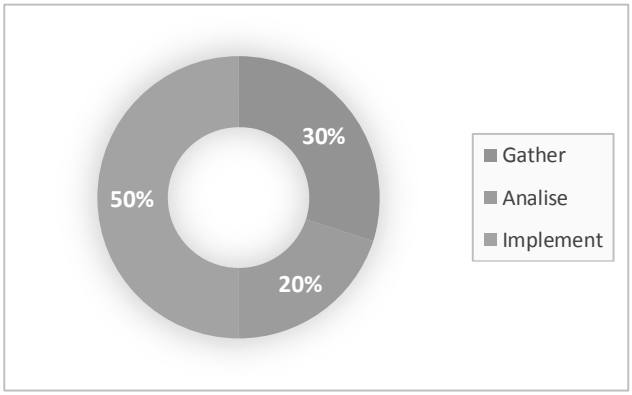

Figure 5. Stage of the GDPR implementation

When asked how they had implemented the new measures enshrined in the regulation, the respondents gave the same answer, namely that there was nobody in the company with enough knowledge to conduct the process. They stated to have hired the services of external companies for guidance in order to be able to meet the requirements imposed by the GDPR.

Also, we determined that among the four clinics which said to be in compliance with the regulation, only one has identified and designated the person who will be responsible for the data treatment, the Data Protection Officer.

Overall, the respondents showed to be sensitive to the importance of both board and workers' training. However, no training or awareness raising session has been held concerning the new rules to be adopted, but such sessions were said to take place soon. It is paramount to ensure that workers are aware of the GDPR implications and such sessions are the most appropriate way to communicate the new data protection rules to collaborators.

With regard to the acknowledgement of the sanctions and fines companies are subjected to, 28 respondents (65%) are not aware and 15 (35%) are aware of such sanctions and fines.

The GDPR reinforces the power of authorities and increases the fines. These sanctions are more burdensome and can reach the sum of 20 million euros or 4% of the overall turnover for the previous year.

Of the total number of clinics responding to the survey, most consider the stipulated two-year transitional period given to companies to adapt to the new GDPR insufficient, with results

distributed as follows: 10 (31.5%) consider that there is enough time, 29 (50.8%) consider this time insufficient, and the other 10 respondents (17,6%) had no formed opinion on the matter (Fig.6).

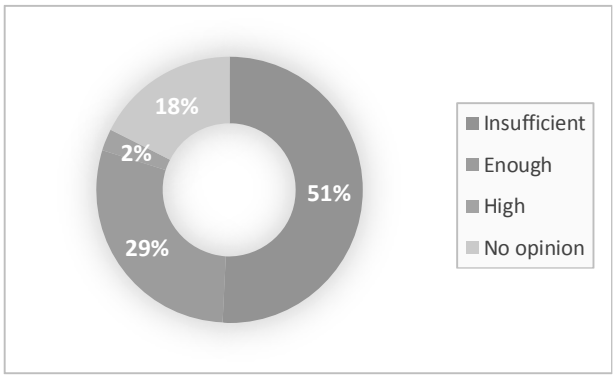

Figure 6. Transitional period for the GDPR implementation

The time taken to implement the GDPR will always depend on the complexity of the company's business activity, its organisational maturity, the volume and variety of the personal data used, the adequacy and flexibility of its information systems and on all its stakeholders' availability and willingness. It is not easy to establish the time it takes to ensure compliance with the regulation. Since many companies only take action on the deadlines, it is believed that most companies will be ready to comply within the set transitional period, especially considering the high applicable sanctions.

One of the grounds supporting the GDPR was the reinforcement of citizens' rights regarding the way companies and organisations collect and use their personal data. All the respondents to this survey agree with this principle and consider this regulation of high relevance and importance.

It is not enough for a company to claim that they comply with the regulation, they have to make proof that the personal data they use within the scope of their activity is being protected in accordance with the regulation.

VI. CONCLUSION

After years of wrangling, the GDPR is now a fact and compliance deadlines are looming. The time to start preparing is now. Organisations need to ensure that they are not caught out and face sanctions for non-compliance. With the right precautions in place, organisations should have little to fear. The time and effort required to achieve compliance will vary greatly from one organisation to another, but it is well worth the effort [3].

Since the GDPR is an EU law and not a directive, it is mandatory and has binding legal force. In Portugal, it will be regulated by the National Data Protection Commission (CNPD), which is the Portuguese data protection authority.

The implementation of the GDPR will imply challenges which will not be easily overcome. In many cases, it will imply a cultural change within the organisation. However, it may be an opportunity for many companies to finally document their processes and procedures, implement their values, consolidate their business ethics and display a convincing and motivating coherence to the market and to their clients, partners and collaborators.

The treatment of personal data must be a transparent process to subjects at all times from its collection to its deletion. The purpose of the data collection to which the subjects consent must be clear and no other data besides the strictly necessary must be collected.

The implementation of the regulation implies the definition of procedures, records and policies. Both people and technologies represent critical success factors to its implementation. Therefore, it might be relevant to carry out further research to determine to what extent this GDPR, although targeted at data protection, might not be as well a booster for the digital transformation of health clinics.

ACKNOWLEDGMENT

UNIAG, R&D unit funded by the FCT – Portuguese Foundation for the Development of Science and Technology, Ministry of Science, Technology and Higher Education. . Project n. º UID/GES/4752/2016.

This work has been supported by COMPETE: POCI-01-0145-FEDER-007043 and FCT – Fundação para a Ciência e Tecnologia within the Project Scope: UID/CEC/00319/2013.

REFERENCES

[1] Data Privacy da KPMG Portugal, O impacto do Regulamento Geral de Protecção de Dados em Portugal: Estudo, março 2017.

[2] L. Ryz, L. Grest, A new era in data protection, Computer Fraud & Security, v. 2016, nº 3, pp. 18-20, 2016.

[3] C. Tankard, What the GDPR means for business, Network Security, v. 2016, nº 6, pp. 5-8, 2016.

[4] E. Díaz, Díaz, The new European Union General Regulation on Data Protection and the legal consequences for inatitutions, Church, Communication and Culture, v. 1, pp. 206-239, 2016.

[5] European Parliament and Council, Regulation (EU) 2016/679 of the European Parliament and of the Counciel of 27 April 2016, Official Journal of the European Union, 2016.

[6] IIAAP (It Is All About People), Regulamento Geral de Proteção de Dados, 2017.

[7] MetaCompliance, GDPR Best Practices Implementation Guide - Transforming GDPR Requirements into Compliant Operational Behaviours, 2017.

[8] R. Rodrigues, D. Barnard-Wills, P. De Hert, V. Papakonstantinou, The future of privacy certification in Europe: an exploration of options under article 42 of the GDPR, International Review of Law, Computers & Technology, 30:3, pp. 248-270, 2016.

[9] SPMS – Serviços Partilhados do Ministério da Saúde, Privacidade da informação no setor da saúde, 2017.