Journal of Medical Systems (2020) 44: 53
https://doi.org/10.1007/s10916-020-1521-0

SYSTEMS-LEVEL QUALITY IMPROVEMENT

General Data Protection Regulation in Health Clinics

Isabel Maria Lopes [1,2,3] · Teresa Guarda [1,4,5] · Pedro Oliveira [3]

Received: 1 July 2019 / Accepted: 2 January 2020 / Published online: 10 January 2020

Abstract

The focus on personal data has merited the EU concerns and attention, resulting in the legislative change regarding privacy and the protection of personal data. The General Data Protection Regulation (GDPR) aims to reform existing measures on the protection of personal data of European Union citizens, with a strong impact on the rights and freedoms of individuals in establishing rules for the processing of personal data. The GDPR considers a special category of personal data, the health data, being these considered as sensitive data and subject to special conditions regarding treatment and access by third parties. This work presents the evolution of the applicability of the Regulation (EU) 2016/679 six months after its application in Portuguese health clinics. The results of the present study are discussed in the light of future literature and work are identified.

Keywords General data protection regulation · Regulation (EU) 2016/679 · Personal data · Health data · Health clinics

Introduction

Our digital society is changing rapidly, with emerging new technologies such as artificial intelligence and machine learning, robotics, and the internet of things. These changes trigger new questions relating to privacy and data protection [1].

The EU established a two-year transitional period for companies to implement the necessary changes until May 252,018 in order to ensure the full compliance of their data treatment with the rules imposed by the GDPR.

The GDPR comes at a time when businesses are increasingly data driven. The volume of personal information that they are collecting and keeping is forever increasing with the information becoming, in many cases, a key business asset. Also, some data is considered to be more 'sensitive' than other, namely data regarding health, children, among others.

Businesses that understand their data protection obligations and seek to meet them in an intelligent way will be best placed to unlock the benefits of the personal data that they hold. Getting data protection right is not just a matter of legal compliance. It also makes sound business sense. So, whether evolutionary or revolutionary, the GDPR requires a step change for businesses in their management and delivery of personal data and privacy. Planning is required, priorities need to be set and resources allocated, but no responsible business can afford to turn a blind eye to the GDPR's many requirements [2].

Since we are over the deadline imposed to companies for implementing the regulation, it is relevant to assess the companies' level of preparation to comply with the GDPR demands by comparing the present results with those of studies conducted before the end of the deadline. 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

This article is part of the Topical Collection on *Systems-Level Quality Improvement*

✉ Isabel Maria Lopes
isalopes@ipb.pt

Teresa Guarda
tguarda@gmail.com

Pedro Oliveira
pedrooli@ipb.pt

[1] Centre ALGORITMI, Guimarães, Portugal

[2] UNIAG (Applied Management Research Unit), Valença, Portugal

[3] School of Technology and Management, Polytechnic Institute of Bragança, Bragança, Portugal

[4] Universidad Estatal Peninsula de Santa Elena – UPSE, La Libertad, Ecuador

[5] Universidad de las Fuerzas Armadas – ESPE, Sangolquí, Ecuador

focuses on the research methodology, identifying the target population and the structure of the survey. The results of the study are discussed in section 4, followed by the conclusions drawn from the study. Finally, the limitations of this research work are identified and possible future studies are proposed.

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 241,995, 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 252,018, date from which the directive 95/46/CE will be effectively repealed, its enforcement on May 252,016 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 252,018. In Fig. 1, we can see all the stages which the GDPR has undergone.

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.

What is personal data [4]?

- The GDPR applies to the processing of personal data that is:
  - wholly or partly by automated means; or
  - the processing other than by automated means of personal data which forms part of, or is intended to form part of, a filing system.
- Personal data only includes information relating to natural persons who:
  - can be identified or who are identifiable, directly from the information in question; or
  - who can be indirectly identified from that information in combination with other information.
- Personal data may also include special categories of personal data or criminal conviction and offences data. These are considered to be more sensitive and you may only process them in more limited circumstances.
- Pseudonymised data can help reduce privacy risks by making it more difficult to identify individuals, but it is still personal data.
- If personal data can be truly anonymised then the anonymised data is not subject to the GDPR. It is important to understand what personal data is in order to understand if the data has been anonymised.
- Information about a deceased person does not constitute personal data and therefore is not subject to the GDPR.
- Information about companies or public authorities is not personal data.
- However, information about individuals acting as sole traders, employees, partners and company directors where they are individually identifiable and the information relates to them as an individual may constitute personal data.

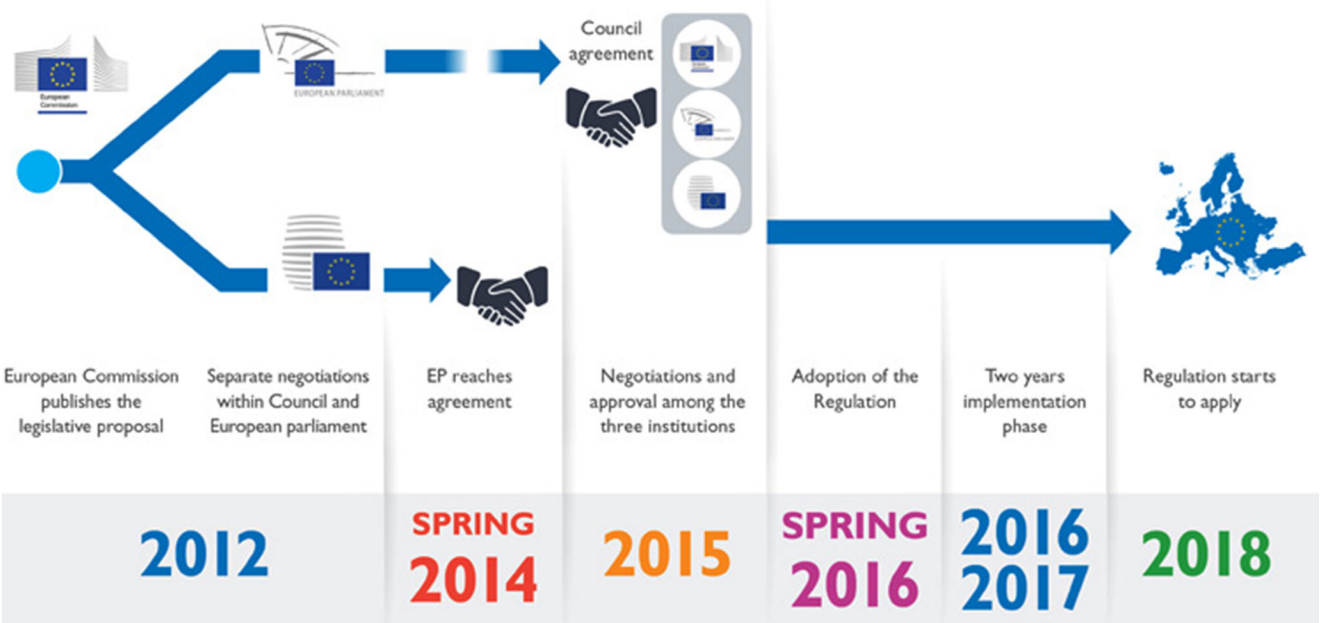

Fig. 1 Stages of the GDPR [3]

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 [6].

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 Regulation is based on a lot of familiar legal practice from the existing legislation, and many articles have the same content. However, a number of new initiatives are introduced.

Among the new initiatives, the following are to be highlighted [7]:

- Partial harmonisation of rules as well as interpretation of rules and case-law across the European countries.
- Removal of the obligation to notify the supervisory authority when it comes to processing of personal data.
- Some degree of one-stop-shop where the main establishment of the company interacts with only one European supervisory authority.
- New rights for data subjects.
- New obligations for controllers and processors.
- More cooperation between the European supervisory authorities.
- Introduction of significant penalties including administrative fines for failing to comply with the Regulation.

According to another author [8], the main innovations of the General Data Protection Regulation are:

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.

The GDPR implementation program covers four distinct dimensions which are critical to the GDPR compliance: Technology, Data, Process and People (see Fig. 2).

Organizations must work on these four dimensions, each of which having its own specificities, starting the process by 'preparing', followed by 'protecting' and finally by 'maintaining', so that the GDPR adoption can be a reality and organizations can be in compliance with the regulation.

Among these points representing the main innovations imposed by the new legislation, we highlight point nine of GDPR, 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.

All organisations, including small to medium-sized companies and large enterprises, must be aware of all the GDPR requirements and be prepared to comply.

Research methodology

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

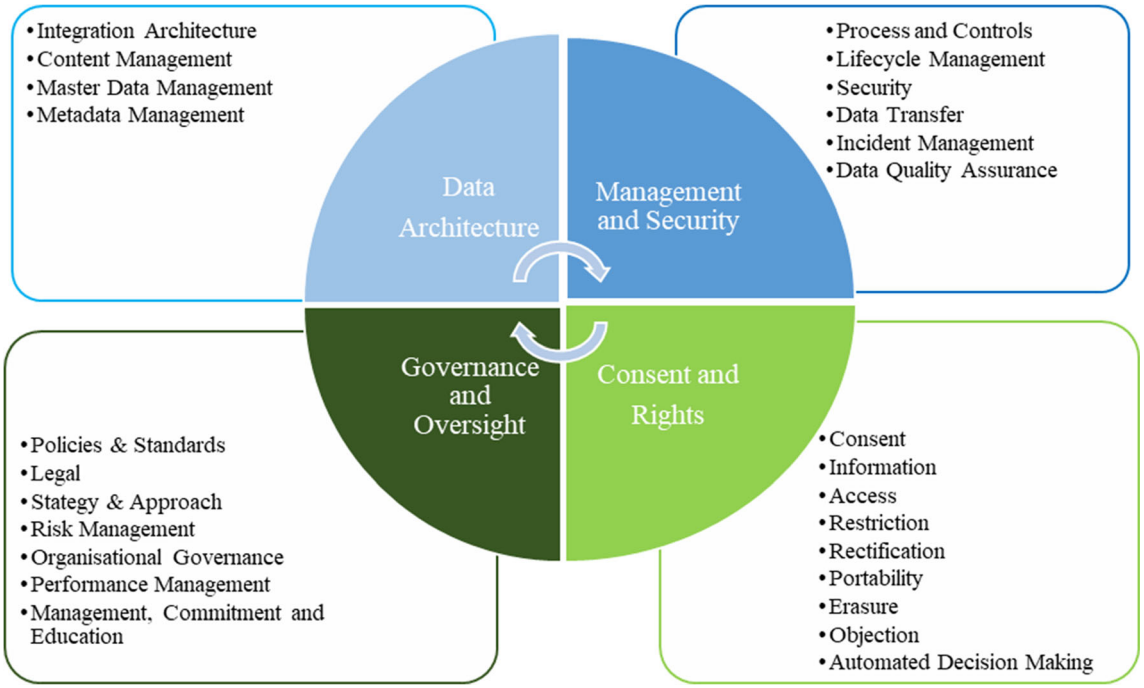

Fig. 2 The four dimensions of the GDPR framework [9]

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 regard 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, as well as their evolution since the conduction of the last survey.

Population

The first 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 Information Technology department. When there was no such person, the respondent was the person in charge of the clinic.

In order to compare the two surveys, one conducted before and another after the enforcement of the GDPR, the same clinics were contacted. The first study was conducted between October and December 2017. The second study was carried out between October and November 2018.

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, this study focuses particularly on the analysis of the core questions so as to assess the evolution between two different time windows.

Results

The first group of questions concerned the characterisation of the clinics as well as that of the respondent to the survey. Since such data is confidential, Table 1 shows the characterisation of the clinics involved in the study according to their type. The second survey targeted the same clinics involved in the first study. All the 57 clinics responded, with the slight change being that in three of them, the person who answered the survey was not the same since they were not available.

For the question about whether or not the companies had started or completed the process of implementation of the measures imposed by the GDPR, the results were as follows: in the first study (2017), 43 (75%) answered no and 14 (25%) answered yes; in the second study (2018), 39 (69%) replied no and 18 (31%) said that they had already started or completed the adoption of such measures (Fig. 3).

In the first study, only 4 (28%) of the 14 clinics which gave a positive answer consider to be in compliance with the legislation. The remaining 10 clinics (72%) are still implementing the measures. In the second study, there was a small evolution since from the 18 clinics in the implementation stage, 7 (39%) consider that the process is completed, and the remaining 11 (61%) still have some measures to implement.

These numbers seem residual when we observe that from the 57 clinics surveyed, only 7% (2017) and 12% (2018) actually have implemented the GDPR. Over one year, which was the lapse of time between the two studies, the evolution observed was of 5%, which corresponds to 3 clinics more to have completed the process. Such improvement seems insufficient when taking into account that the second study was

Table 1 Clinics surveyed

Type of clinic	Clinics surveyed
Nursing	12
Dental	16
Ophthalmology	4
Medical and Diagnostics	15
Orthopaedics	3
Physiotherapy	7

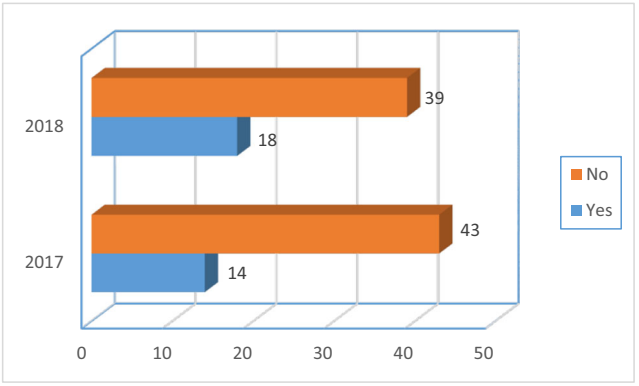

Fig. 3 Clinics which are implementing the GDPR

conducted almost 6 months after the enforcement of the GDPR.

For a better understanding of the results, we can group the clinics into three clusters (Fig. 4):

- 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 as 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% and 31% of the clinics have adopted or are adopting the measures imposed.

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.

When the clinics in cluster 2 were questioned about the implementation stage of the GDPR they were in (gather,

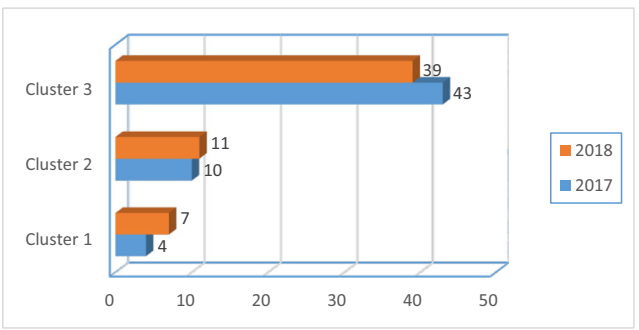

Fig. 4 Clusters according to the GDPR transitional implementation

analyse or implement), the answers in 2017 were 30%, 20% and 50%, respectively; and in 2018, the answers were 9%, 27% and 64%, respectively (Fig. 5).

The results show that from 2017 to 2018, the number of clinics implementing the measures imposed by the regulation increased significantly in the implementation stage. We can also highlight that there is only one clinic still in the gathering stage in 2018.

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. 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.

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 (2017) and seven clinics (2018) 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 (DPO).

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.

The results obtained with regard to the acknowledgement of the sanctions and fines companies are subjected to are presented in Fig. 6.

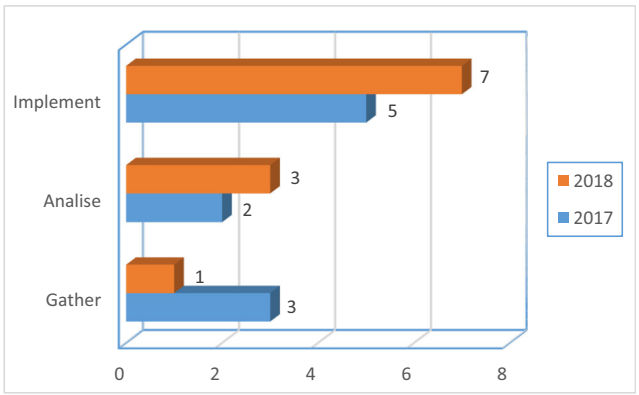

Fig. 5 Stage of the GDPR implementation

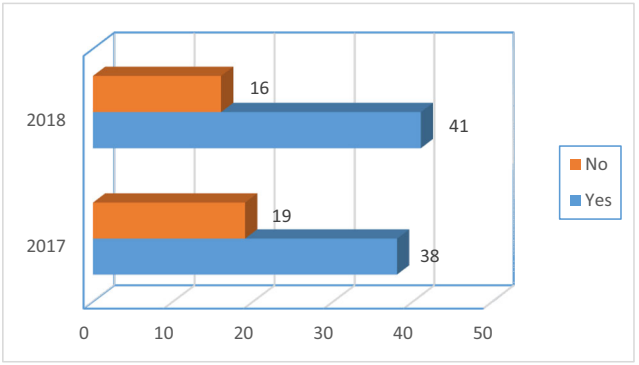

Fig. 6 Acknowledgement of the sanctions

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.

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. We could say that companies only take action at the last minute. However, this study shows that even after the deadline for the implementation of the measures imposed by the regulation, only 12% actually do have such measures implemented.

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.

With regard to the four dimensions presented in Fig. 2, their taking into account increases the patients' trust towards the health clinic.

The dimension – Technology, responsible for data Architecture, is crucial in order to monitor activities in an automatized way, managing and protecting contents and data. Thus, compliance with the GDPR implies the implementation of data protection technology.

In the dimension – Data, where Management and Security are conducted, and bearing in mind that most data treatment activities are based on the use of information systems and automatized means, it is necessary to assess the systems used, the levels of access and the security measures implemented.

In the dimension – Process, responsible for the Consent of Rights, the processes are honed so as to respond to the data holders' rights and manage data processing.

The conjunction of these actions to enhance the implementation of GDPR in the Health clinics can be summarized in six essential points:

1. Review periodically - Data protection is not a destination, it's a journey! So, re-view on a regular basic and correct your course accordingly
2. Raise Awareness - Conduct staff training and awareness sessions. Most breaches occur due to staff ignorance so make them aware and mitigate the risk.
3. Review policies & related documents - Review existing policies and create new ones where needed. These policies allow you to formulate processes and procedures for staff to follow
4. Make a plan - Based on the audit and risk assessment, determine a roadmap to achieve compliance. While it's important to address high risk areas, don't ignore the low hanging fruit. Small, easy wins can get the project off to a positive start!
5. Identify & Assess privacy related risks - Assess the risks associated with how are processing the data. Compile a risk register.
6. Conduct an audit - Know your Data-how you got it; who can access it, where it's stored; how long you keep it etc. Create a list of recommendations to address areas of concern.

Transitional and capacity building options encompass the promotion of activities aimed at disseminating knowledge and building the capacity by institutions to meet the challenges of GDPR compliance.

For institutionalization de GDPR in the field of action, the institutionalization process can occur essentially according to two formats: in a naturalist way or based on agents' action [10]. The first format matches a situation in which the phenomenon is gradually institutionalized in a natural way, which normally represents a slow and long process. The second format, based on agents' action, introduces a catalyzing element – the agent – which enables the acceleration of the institutionalization process. Contrarily to what happens in the naturalist way, in the institutionalization based on agents' action, the normative frameworks are designed, created and modified rationally, through conscientious and deliberate processes, the same happening with cultural-cognitive elements which, in this case, also tend to be conscientiously conceived and spread by certain agents.

The strategy based on agents is a way to enhance the institutionalization of the GDPR. The main agents who may play an active part in this process are the organizations' headships, the workers in charge of implementing the GDPR and the Government which proposes and passes the draft law ensuring the national execution of the GDPR.

Another author [11] has proposed a methodology that consists of a 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 sustaining and evidencing compliance with the GDPR Accountability Principle.

This methodology forwards a GDPR implementation designed to engage stakeholders to ensure timely and efficient organisational readiness for GDPR, implement effective procedures that embed GDPR-compliant operational behaviours, and establish assurance criterion that will sustain and evidence GDPR accountability (Fig. 7).

The first phase "Prepare" considers the activities necessary to ensure GDPR readiness for your organisation. It is very important that you engage key business at the outset to inform and educate them. If done effectively, you will obtain their buy-in and support, a fundamental success factor for achieving your GDPR readiness goals. Following on from this you will need to appoint your GDPR program team, identify and assess relevant Personal Data Processing activities, prioritise a

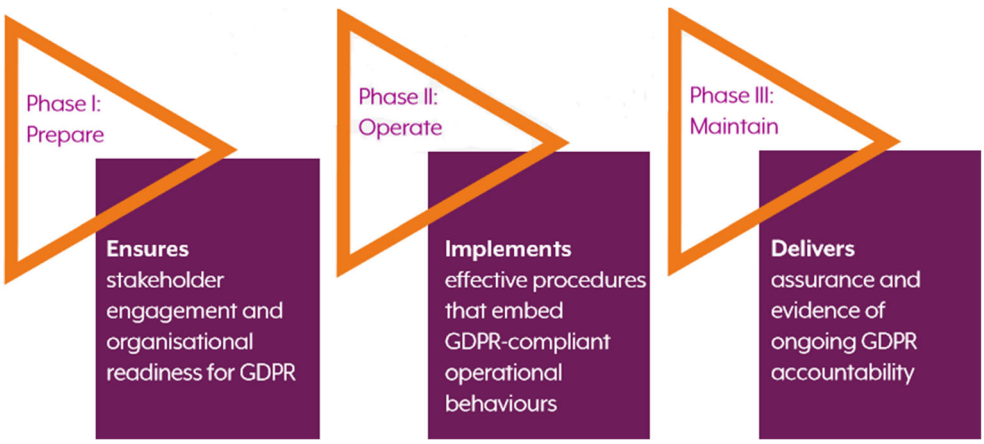

Fig. 7 Methodology forward GDPR implementation (basede on [11])

set of remediation actions, establish a centralised Personal Data register, educate Personal Data Handlers and Data Processors and update your Data Protection policies and Privacy Notices.

The phase "Operate" of the life cycle addresses the need to define and embed procedures that enable staff who handle Personal Data to carry out their duties in an efficient and compliant manner. The GDPR requires not just that your Personal Data Handlers perform their duties in alignment with GDPR obligations, but that there is also a record maintained of their decisions and actions in relation to carrying out those duties.

This final phase "Maintain" of the life cycle incorporates a series of recurring activities that address the need to evidence accountability with GDPR on an ongoing basis. As mentioned earlier, the European Data Protection Supervisor has stated that accountability involves assessing your organisation's implementation of GDPR and demonstrating, to external stakeholders and Data Protection Authorities, the quality of that implementation. The ability to demonstrate the quality of your GDPR implementation requires forward planning regarding the areas that need to be assessed and the performance metrics that will be used to measure and evidence effectiveness.

Conclusion

The implementation of GDPR can be a challenge for Health Clinics. Most of the information which was previously shared in paper is currently shared digitally, thus posing new digital challenges and threats concerning security and privacy, namely regarding personal data protection in a society increasingly digital [12].

There are currently 28 laws of data protection based on the 1995 EU Data Protection Directive, which was implemented over 20 years ago and is gradually being replaced by the new GDPR [3]. Considering the advances witnessed in information and communication technologies over the last two decades, such laws can only be totally inadequate to the necessary protection of both individuals and companies' data.

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 [12–14].

The implementation of the regulation implies the definition of procedures, records and policies. Both people and technologies represent critical success factors to its implementation.

A considerable effort is being made by companies to be in compliance with the GDPR. However, it is a long path and the instructions regarding the four dimensions (Technology, Data, Process and People) must be properly implemented and, above all, maintained bearing in mind that periodic improvements are necessary. This process is never completely closed and reviews must be conducted whenever necessary.

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.

Compliance with ethical standards

Ethical approval This article does not contain any studies with human participants or animal performed by any of the authors.

Informed consent Informed consent was obtained from all individual participants included in the study.

References

1. Hijmans, H., and Raab, C. D., Ethical dimensions of the GDPR (July 30, 2018). In: Cole, M., Boehm, F. (Eds), *Commentary on the General Data Protection Regulation*. Cheltenham: Edward Elgar, 2018.
2. Allen & Overy: Preparing for the General Data Protection Regulation 2018.
3. Goubau, T.: How GDPR Will Change Personal Data Control and Personal Data Control an Affect Everyone in Construction. https://www.aproplan.com/blog/construction-news/gdpr-changes-personal-data-control-construction, last Accessed 2018/07/20.
4. ICO – Commissioner's Office, Guide to The General Data Protection regulation, 2018.
5. European Parliament and Council, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, Official Journal of the European Union, 2016.
6. Ryz, L., and Grest, L., A new era in data protection. *Comput. Fraud Secur.* 2016(3):18–20, 2016.
7. Guideline General Data Protection Regulation – Implementation in Danish Companies. In: Henning Montensen (eds.), The Danish ICT and Electronics Federation, DI Digital 2016.
8. Díaz, E., The new European Union General Regulation on Data Protection and the legal consequences for institutions. Church, Communication and Culture 1:206–239, 2016.
9. Ian West, The big scan thing! – How the EU General Data Protection Regulation (GDPR) will affect your business! https://www.slideshare.net/CraigShipley1/digital-enterprise-festival-birmingham-130417-ian-west-cognizant-vp-data-management-the-implications-of-the-eu-global-data-protection-regulation-on-every-business-and-their-digital-service-providers, last Accessed 2018/12/01.
10. Scott, W. R., *Institutions and Organizations: Ideas and Interests*. 3rd edition. Thousand Oaks: Sage, 2008.
11. MetaCompliance, GDPR Best Practices Implementation Guide, Transforming GDPR Requirements into Compliant Operational Behaviours. https://www.infosecurityeurope.com/__novadocuments/355669?v=636289786574700000, last Accessed 2019/06/28.

12. SPMS – Serviços Partilhados do Ministério da Saúde, Privacidade da informação no setor da saúde, 2017.
13. Martins, J., Gonçalves, R., Branco, F., Pereira, J., Peixoto, C., Rocha, T. How Ill Is online health care? an overview on the iberia peninsula health care institutions websites accessibility levels. New Advances In Information Systems And Technologies, 445:391–400. Springer, 2016.
14. Martins, J., Gonçalves, R., Oliveira, T., Cota, M., and Branco, F., Understanding the determinants of social network sites adoption at firm level: A mixed methodology approach. *Electron. Commer. Res. Appl.* 18:10–26, 2016.

Further reading

15. Lopes, I. M., Oliveira, P. Implementation of the General Data Protection Regulation: A Survey in Health Clinics, 13ª Iberian Conference on Information Systems and Technologies, Vol. 2018-June, pp. 1–6, 2018.