





GDPR Compliance: Proposed Guidelines for Cloud-Based Health Organizations

Dimitra Georgiou^(✉)  and Costas Lambrinouidakis 

Systems Security Laboratory, Department of Digital Systems, School of Information and Communication Technologies, University of Piraeus, 150, Odyssea Androutsou Str., 18532 Piraeus, Greece

dimitrageorgiou@ssl-unipi.gr, clam@unipi.gr

Abstract. In this paper, we investigate the implications of the General Data Protection Regulation (GDPR) on the design of a Cloud-based Health System. Keeping secure healthcare information and protecting patients' privacy is a major responsibility of all healthcare providers. On May 25th 2018, when the GDPR has become mandatory within the European Union, this responsibility has been increased. Failure to comply with GDPR can result in huge fines. For this reason, it is of vital importance any health care organization to explore ways for achieving protection of the data subjects and ensuring GDPR compliance.

GDPR introduces the 'special category of personal data', that includes health data and is subject to special conditions regarding treatment and access by third parties. The focus of this research work is to provide guidelines for Cloud-based health Organizations in order to comply with GDPR and ensure patients' privacy and rights. In this paper, we demonstrate, in a practical way, how a Cloud provider may handle the difficulties of the legal framework by summarizing the legal text, identifying the GDPR requirements, highlighting the obligations that are specific for health data and providing guidelines for satisfying the GDPR requirements for a Cloud-based Health provider.

Keywords: GDPR · Cloud Computing · Data protection · Security · Privacy · Health data · SaaS

1 Introduction

Digitization plays an important role in today's life. New technologies are offering a variety of prospects to gather, use and share health data with efficiency, to empower patients in managing their diseases and to improve the quality, safety and efficiency of healthcare systems. Cloud computing is a new technology that has been spread in many ICT areas, significantly affecting the way in which personal data are processed and, subsequently, being protected. Over the past years, a lot of research has been conducted on security and privacy of Cloud environments and especially on Cloud-based Health systems. The GDPR [1] outlines rigorous new policies for collecting, processing and securing personal data and affects almost all industries but in the health care sector,

the new Regulation gives every patient enhanced control over the way his/her personal data are collected and processed. Today, complying with GDPR is a challenging and demanding task for organizations, highlighting the need for a process that could guide them in order to satisfy the requirements and build a GDPR compliant system.

The General Data Protection Regulation [1] was approved on April 2016 and came into force on May 2018, bringing along several challenges for citizens, institutions and other private and public organizations. GDPR has a direct impact on all 28 Member States of the EU and is the European Union's attempt to create an allied approach to online privacy. Unfortunately, even today, many Health-care businesses and Providers have not yet realized the huge fines that they are facing if they do not comply with GDPR, something which is also the case for those that provide their services through cloud infrastructures [2].

It is worthwhile to mention that the GDPR, applies to all companies that hold or process EU residents' data, including Cloud Computing users, Providers and their sub-contractors. GDPR creates a uniform data privacy law across all 28 EU member nations to be enforced wherever data processing and management practices affect EU citizens. In other words, unless one Organization deals with non-Europeans, it is subject to the regulation. For Cloud Providers, that act either as Processors or Data Controllers the new obligations are extensive and challenging. Since the compliance of companies with the regulation is obligatory, it is relevant to declare companies' level of preparation for the new GDPR requirements. This requirement must be met regardless of the means used to process the personal data and it also covers Cloud services used to process the personal data. Numerous industry sectors could have been chosen, but this research work focused on the health sector. The objective of this paper is to give a brief advice on what a cloud Health Organizations and Providers should consider and what further actions to take in order to comply with GDPR.

In terms of its structure, this paper is divided in five sections, starting with an introduction and continuing with Sect. 2 that presents the challenges in Personal Data Protection in the GDPR era. Section 3 describes analytically the GDPR requirements while Sect. 4 focuses on the key aspects of the GDPR for health. Section 5 proposes the basic countermeasures for satisfying the aforementioned requirements. Finally Sect. 6 concludes the paper.

2 Challenges Faced by Organizations During GDPR Compliance

The GDPR introduces a new set of rules for the processing and protection of personal data and the privacy of the users. In the Cloud Computing era, users enjoy several gains, but concurrently, they are facing increased risks regarding the protection of their personal data.

Although organizations should comply with GDPR by May 25, 2018, this is not yet the case. One of the main reasons for the slow compliance uptake is the complexity of GDPR and the various challenges that organizations have to overcome in order to achieve compliance. The GDPR indeed introduces strict rules and obligations and recognizes a small quantity of rights to individuals that must be expected by organizations.

Apart from the mandate for GDPR compliance—and the non-neglectable financial fines, organizations have an extra reason to adopt the underlying principles and the appropriate measures for data protection: growing people awareness of data breaches and their growing demand that companies protect their information. In other words, compliance is driven also by the market needs. Organizations subject to GDPR compliance claim difficulties in provisions' implementation, despite the money spent, although specific problems are encountered with regard to the new requirements GDPR introduces. This is due to various reasons, either technical or organizational. Challenges include:

- **GDPR requirements' interpretation:** Since the Regulation introduces principles rather than concrete rules, several organizations struggle to put them in practice into their technical and operational context.
- **Operational adaptation:** GDPR implementation requires significant planning and review about people, roles, systems, processes and transformation of business practices to privacy friendly processes. However, it is often hard to identify the flaws of business practices against GDPR requirements, in some cases even have a clear view on the precise practices themselves and to appropriately re-engineer processes for becoming privacy-aware by design.
- **Unified data view:** Organizations must have a clear view on data subjects' information structure, semantics, and storage patterns. Currently, data is typically scattered across different systems and databases, thus hardening control over them, as well as responding to access, rectification, erasure and portability requests. Further, they should maintain a comprehensive record of processing actions and the associated context and make it readily available to data subjects and regulators.
- **Security means enforcement:** The GDPR requires, explicitly or implicitly, the application of various security mechanisms for the protection of data. Organizations have to identify and “plug” suitable mechanisms to their operations, new and re-engineered processes, data records and customer and third parties' relations.
- **Customer relationship management:** The GDPR provides data subjects with control over their data, while granting various other rights that level up the requirements as regards management of customer relations, along with the means that should be maintained by organizations for their implementation.
- **Management of third parties:** In the complex service provision ecosystem, organizations should provide for privacy-aware data exchange and operations' outsourcing. This is hardened by the increasing use of Cloud and as-a-service technologies, where data and operations are entrusted to third parties, thus creating implications for both service providers and consumers.
- **Accountability:** The GDPR provides very little guidance as to what measures processors and controllers should adopt in order to meet their accountability obligations. Article 24 [1] introduces the concept of accountability, which requires controllers to perform all of their data processing operations in compliance with the GDPR and to be able to demonstrate such compliance, without providing any guidance on how to do that.
- **Lack of resources and capabilities:** In order for the above to be implemented, significant resources and know-how are required. While big companies may have money

to invest, this does not essentially apply for small organizations that typically operate with few employees and make heavy use of cloud resources.

In addition to the aforementioned challenges, organizations have to carefully consider the GDPR principles in relation to the processing of personal data.

2.1 Principles Relating to Processing of Personal Data in GDPR

One of the major GDPR achievements is the clear refinement of data processing principles in a way that they guarantee that any personal data processing is fair, lawful, limited to the purposes of processing. These principles are listed under Article 5 [1] and are presented in Fig. 1. Therefore, all exceptions to the processing principles must be provided by law in order to be acceptable.



Fig. 1. Principles of GDPR

Lawfulness, Fairness and Transparency

Personal data should be processed in such a way “*lawfully, fairly and in a transparent manner in relation to the data subject*” Article 5(1) (a) and Articles 37-40 [1]. These principles guarantee that data will be processed in accordance with the law, proportionally to the aim foreseen and with transparent means for the natural persons who should be informed of the collection of their personal data, usage and consultancy and the extent to which such operations go. Any processing must comply with the law which implies

not only data protection related law but also other legislations applying to the specific sector such as automotive services or energy providers. The principle of fairness brings a balance test that needs to be carried out for each processing activity, since the right to the protection of personal data must be balanced with other potentially conflicting rights. Such balance can be achieved through strict compliance with the general principles underpinning the processing of personal data, but also when ensuring the respect of data subjects' rights from the controller. Hence, processing can be lawful but still considered unfair with regard to the means foreseen. It is therefore essential that the processing entailed is always clear to the data subject and that the latter is aware of its rights under the GDPR.

Purpose Limitation

The collection of data should be limited to “*specified, explicit and legitimate purposes*” Article 5(1)(b) [1]. The purpose must be specific: a controller cannot collect data without knowing how and when these data will be used. When the purpose of data collection is determined then, the appropriate data will be collected and stored, only on condition that is necessary. Whether further processing is compatible with the original purposes of processing can be assessed by analyzing a number of factors, the nature of the data, the impact such further processing would have on the data subject, as well as the safeguards adopted by the controller in order to ensure that subject's rights are respected.

Data Minimization

Data minimization requests whether the same purpose can be achieved with a narrower collection of data and is one of the principles that is linked with data protection by design under the Regulation. The data gathered should be suitable and restricted to what is essential for the purpose foreseen. In reality, it can be more complicated to access since the added value of minimization depends on a multitude of criteria and the purposes of processing [3]. In some cases, such as police profiling, quality data is essential in order to ensure non-discrimination and acquiring more data ensures more accurate and fair results. For what concerns business purposes, collectors tend to acquire more data than what they actually need and this can be problematic.

Accuracy

In consequence, controllers should ensure accuracy at all stages of collecting and processing personal data, taking every step to guarantee that inaccurate data are deleted or rectified without delay. Thus, controllers should make sure that outdated data are eliminated or that data are correctly interpreted. The importance of this step varies according to the type of data collected and the sector to which these safeguards apply. The system should notify data subjects of their right to object or change personal data, as well as provide a communication channel where the user can inform about data dispute. Data should be analyzed for its quality and inaccurate or incomplete data should be erased either manually or automatically [4].

Storage Limitation

The data should only be stored for as long as necessary and the retention period should be decided at the moment of collection. However, in case of a new purpose that respects

the legal requirements of the GDPR, the data retained for a longer period should again be limited to what is necessary to accomplish the new cause. Traceability is once again essential for this principle. Being able to trace personal data to different locations is crucial when personal data has been backed up or distributed to different locations [4]. Attaching metadata makes it easier to identify the specific purpose and defined storage duration of personal data, allowing an (automatic) erasure procedure.

Integrity and Confidentiality

The processing of personal data should be as secure as possible, “*including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures*” [5]. For data protection by design purposes, it is important to limit unauthorized access, as well as implement systemic quality controls in order to ensure that an appropriate level of security is reached. Personal data contained in the system should be encrypted end-to-end, where the level of encryption depends on the risks of processing this personal data. Backups and distributed copies must also be taken into account. In order to ensure its integrity, personal data should be validated (e.g. using hashes), which also contributes to the accuracy of that data. Additionally, a suitable authentication mechanism should be implemented, taking into consideration the sensitivity of personal data. Lastly, access rights must be managed in order to prevent unauthorized access.

Accountability

The principle of accountability [6] in Article 5(2) [1] does not ensure that potential security problems will be avoided but guarantees the data subject that its rights will be lawfully respected. The significant fines under the new legislation illustrate the importance of ensuring that processing activities are well thought through, explained to the data subject and respectful of privacy principles. Accountability is an overarching principle that is reflected in several provisions of the Regulation. According to the GDPR, the controller is responsible for the processing and must be able to prove that processing operations are lawful. Additionally, he is responsible of mitigating the risks of violation of the rights of the data subject throughout the entire software development life cycle. Accountability is fulfilled through demonstration of legal compliance.

2.2 Other Security Aspects

In addition to the previous challenges, other security aspects are: the special categories of personal data, the anonymization/pseudonymization of data and the encryption that must be conducted by organizations.

Special Categories of Data

It is vital to bear in mind that not all data is of the same importance and that safeguards can vary with respect to the “sensitivity” of the data collected. The GDPR defines personal data broadly in order to increase the protection of the individuals. Hence, personal data is “any information relating to an identified or identifiable natural person”, i.e. the data subject, “*who can be identified, directly or indirectly, in particular by reference to*

an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person” Article 4 [1]. Furthermore, *“data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, [as well as] genetic data, biometric data [1], data concerning health or data concerning a natural’s person sex life or sexual orientation”* are considered *“sensitive”* Article 9 [1]. Controllers can only process this data if they respond to the requirements listed under Article 9(2) [1], otherwise the explicit consent of the data subject is required or an issue of public interest is raised for the need to process that data. Consideration of the risks is actually one of the most important changes of the new legislation which wishes to ensure that data controllers evaluate, through every operation, how a person’s rights are affected by the processing.

Pseudonymization

According to Article 4(5) of GDPR [1], pseudonymization is a method of processing personal data in a way that it can no longer be attributed to a specific data subject albeit the use of additional information, if that information is kept separately with appropriate technical and organizational measures.

Encryption

Encryption is mentioned several times in Articles 6, 32 and 34 by the GDPR [1] as an example of a privacy friendly measure, since it guarantees that data is protected and raises the trust of the data subject to the data controller. Strong and efficient encryption is necessary in order to guarantee integrity of data as well as a secure flow of information. As it was stated by the former Article 29 Working Party, *“encryption must remain standardized, strong and efficient, which would no longer be the case if providers were compelled to include backdoors or provide master keys”* [7, 8]. Personal data should be encrypted when stored (including creation of backups) and in transition.

3 Changes Introduced by the GDPR

During the process of conforming with GDPR requirements, cloud-based health organizations should carefully address the following points (Table 1).

3.1 Records of Processing Activities

The controller should keep records of all processing activities [8] including information on the name and contact details of the controller, the Data Protection Officer (DPO), when applicable, the processor if any, the purpose of processing, a description of the categories of persons involved and which data about them will be processed, the categories of recipients to whom the data will be disclosed, possible transfers in third countries or international organizations, planned time limits for erasure of the different categories of data, and where possible, a general description of the security measures adopted.

Table 1. EU-GDPR: Key Changes to the previous data protection framework

EU -GDPR: Key Changes to the previous data protection framework		
	Records of processing activities	3.1
	Territorial Scope	3.2
	Data Protection Impact Assessment	3.3
	Subjects' Rights	3.4
	Data Breach Notification	3.5
	Data Protection Officer	3.6
	Penalties	3.7
	Controllers and Processors	3.8
	Consent	3.9
	Data Protection by Design and by Default	3.10

3.2 Territorial Scope-Third Country Data Transfers

The GDPR also sets restrictions on how personal data is transferred outside EU. Data may only be transferred if certain criteria are met – for example, the third country or international organization offers “*an adequate*” level of data protection.

3.3 Data Protection Impact Assessment (DPIA)

Under the GDPR, companies should conduct formal Data Protection Impact Assessment regarding any processing that would result in “high risk” for individuals’ rights and

freedoms. The notion of high risk is not distinct in the GDPR, but there are three examples of high risk processing: (i) the large scale processing of sensitive personal data; (ii) automated decision taking; and (iii) systematic and large scale monitoring of publicly accessible areas.

3.4 Subjects' Rights

According to the provisions of the GDPR, citizens should regain control of their data. Therefore, companies in possession of personal data are obliged to inform the users of ways in which they use their data, provide them insight into their data, provide a copy of data or change incorrect data. Especially, the data subjects' right to data portability may challenge entities as they will have to provide datasets to their customers upon request. Other rights that are presented are: Right to information, Right to access, Right to rectification, Right to withdraw consent, Right to object, Right to object to automated processing, Right to be forgotten [1].

3.5 Data Breach Notification

Organizations must report data breaches to supervisory authorities and individuals affected by a breach within 72 h Article 33 [1] of the detection. According to Article 34, [1] a data subject should be also notified in cases where security breaches result in a risk to their rights and freedoms.

3.6 Data Protection Officer

The GDPR introduces the role and the duties of the Data Protection Officer in Articles 37–40 [1]. Specific tasks of the DPO and corresponding obligations of the employers are presented there. In addition, it is stated that the contact details of the Data Protection Officer should be made available to the public for ensuring continuous communication with data subjects. It is a responsibility of the controller and the processor to report to the supervisory authority the appointment of the Data Protection Officer.

3.7 Penalties

The GDPR significantly increases the fines that can be imposed for breaches of the data protection rules. At their highest, the fines can reach up to 4% of an organization's annual worldwide turnover or up to €20 million. The GDPR sets out a number of factors that would need to be taken into account by national Data Protection Authorities.

3.8 Controllers and Processors

The GDPR applies to both controllers (those who say how and why personal data is processed) and processors (those acting on the controllers' behalf). The obligations for processors – for example, being required to maintain records of personal data and processing activities – are new under the GDPR.

3.9 Consent

A person's consent for processing of their personal data is valid only if it is given in a voluntary, specific, conscious and unequivocal way, in a form of a statement, confirmation or other consent-expressing deed.

3.10 Data Protection by Design and by Default

These two principles place an obligation on organizations to ensure that all processing of personal data throughout the organization protects the privacy rights of individuals. Essentially, the principles require that an organization's practices and policies are privacy friendly. The GDPR requires the data controller to adopt internal policies and implement measures which comply with the principles of "data protection by design" and "data protection by default".

The GDPR suggests that data controllers should take the following measures:

- Minimize the processing of personal data
- Pseudonymize personal data as soon as possible
- Have complete transparency with regard to the functions and processing of personal data
- Enable the data subject to monitor data processing. The GDPR requires that in the design and creation of new products or services the data protection and privacy rights of individuals are considered throughout the design stage. Similarly, the principles of data protection by design and default should also be taken into consideration in the context of public tenders.

4 Key Aspects of the GDPR of Particular Relevance to Healthcare

After the analysis of GDPR key changes, we need to explore how these changes will influence the interaction of the user with the Cloud-based Health Provider. It is worthwhile to mention that our analysis provides a summary of the requirements that should be addressed by a cloud provider, in a private Cloud, acting as data Controller, categorized on the type of service.

4.1 Security

At this time that personal data protection is more than imperative, the question arises as to what the right way to process visitor data in health care units is (e.g. hospitalized patients or clinics, visitors to diagnostic laboratories, etc.) and which their rights, in accordance with European Regulation 679/2016 and current National legislation, are. Given that in this case "*specific categories of data*" are circulated, such as health data, genetic data and/or biometric data of the recipient of health services, the way in which the data is processed by the service provider is crucial. From their initial collection to their subsequent management and keeping in the medical file. According to the principle of integrity and confidentiality of data, the patient of a health care unit will expect the unit

to protect his personal data through appropriate organizational and technical protection measures. The above obligation of the health unit, in the capacity of “*data controller*”, arises from Article 32 [1] of the GDPR, regarding the confidentiality and the security of the processing of personal data. Appropriate organizational and technical measures concern the overall organization and operation of the unit on data protection issues, such as the existence of relevant procedures, the existence of confidentiality clauses and its training, the overall compliance of the health unit with GDPR etc. In this way, the chances of an “*unauthorized access or accidental disclosure*”, as well as of an “unauthorized or accidental alteration” of data, according to Article 5 [1], are minimized.

4.2 Request (Explicit) Consent

The GDPR strengthens citizen’s rights as regards the process of consent for the collection, use and sharing of their personal data. Article 9 [1] reflects that “consent” is the main legal base to process this type of data, which should be explicit and unambiguous, freely given, specific, informed and signified. It is clear that “explicit consent” for healthcare purposes will need the strongest forms of agreement, with explicit use(s) of data listed when getting such consent. Healthcare consent will also need to cover the case of many potential transfers of health data, including international data transfers and cloud storage. Users need to make a decision about whether to give consent to the collection of their personal information, they must have a button or a ticking box complemented with clear, specific and targeted information. Line (32) Article. 4 (11) Article. 22-2 (c) [1]. In addition, patients should be informed on how to withdraw consent prior to giving it Article 7 paragraph 3 [1].

4.3 Change in the Way Medical Results Are Obtained

The GDPR is particularly strict on the processing of sensitive personal data, i.e. health data, and points out that their processing is prohibited in the first place and that it is permitted only in exceptional cases, for reasons limited by law. This has practically changed the way health care providers operate. They are called upon to pay special attention on how they handle the communication of medical results to patients. For example, it is forbidden to provide medical results over the phone except in exceptional cases where this method of communication could not be avoided. In addition, the results of the examinations must be received by the patient in person and, in case he is unable to do so, by an authorized third party. If the patient chooses to receive his/her results via email, this should be done with encrypted email.

4.4 Strengthening of Data Subjects’ Rights

The GDPR strengthens subjects’ rights over their personal data. Although the rights of data subjects have been present in the former legal texts or case-law, GDPR’s accomplishment is to list them in clear terms within other data protection rights and obligations. In fact, GDPR’s focus on the data subjects aims to strengthen their protection by all means. Each patient, as a subject of personal data, has the right to be informed of his medical

record and also to receive copies of it and, accordingly, the health care provider, as the controller, is obliged to satisfy this right-Article 15 [1]. On the contrast, the right to deletion, as enshrined in the provisions of Article 17 [26] of the GDPR, does not apply to the processing of data in the field of health care, taking into account the provisions of (3) of Article 17 [1]. Data controllers will be more accountable for what they do with personal data and how they protect it.

4.5 GDPR Roles

Cloud participants, in GDPR terms, can be separated into two main roles: the data processors and the data controllers. Most of the times, cloud providers act as data processors on behalf of their customers/users who are the data controllers. The Data Controller is obliged to ensure that there are appropriate technical and security measures implemented within the organization.

4.6 Security and Privacy Policies

Cloud providers that collect/process such special categories should take further actions in order to satisfy GDPR requirements. To this extend, the types of sensitive data that are processed should be identified and analytically described in the security policy of the cloud, providing also the reasoning for their necessity. The Privacy Policy should be freely available to patients in short format with basic information and clear pointers on how to access the full Privacy Policy.

5 Basis Tasks that Health Organizations Should Do for the Compliance with GDPR

The satisfaction of the requirements has been always the most critical and also most challenging aspect to achieve compliance with the GDPR. Health Organizations, in particular, require the highest possible security due to the sensitivity of the processed.

Starting with the data processors and taking into account the previous analysis, we summarize the principles and provide tips that Health Organizations should take into account:

5.1 Identify Categories of Subjects and Personal Data

Taking into account the basic definitions of Article 4 [1] of the GDPR, as well as the provisions of Articles 6, 9 and 10 of the GDPR [1], they should identify and classify the categories of subjects (e.g. patients, medical and nursing staff, blood donors, participants in scientific research, clinical trials, etc.) and personal data, which health Organizations collect and maintain per processing activity (e.g. collection and registration of patient data upon arrival for outpatient clinics) - whether this processing is paperwork (or/and) electronic - and ultimately by filing system (e.g. medical patient data file). Data subjects are not only the beneficiaries of the services provided by law (patients, citizens) but also the employees within the institution, for which the institution collects and processes personal data.

5.2 Identification of Personal Data Sources and of Purpose of Processing

Health Organizations should identify each specific category of personal data - whether it is special categories of personal data according to Article 9 provision 1 and Article 10 of the GDPR [1] or whether it is simple personal data and specify precisely each data category, with its subcategories of personal data that are being processed.

Health Organizations should identify the sources of personal data. e.g. data collected directly from their subjects (patients, employees, etc.), as well as those collected by third parties (e.g. other nursing institutions, insurance companies, etc.). In the event that personal data is collected from other sources and not directly from the data subject, the information obligations of Article 14 [1] of the GDPR shall be applied.

Furthermore, the purpose of processing for which the personal data is collected should be clearly described.

5.3 Selection and Determination of the Legal Basis for Each Processing of Personal Data

Health Organization should identify for each category of personal data that is being processed, the legal basis for the processing according to Article 6, Articles 9 paragraphs 2 and Article 10 of the GDPR [1]. The consent of the subject is the necessary legal basis for the processing of personal data in the field of health service provision. The obligation to offer written information to the subjects in Articles 12, 13, 14 of the GDPR [1] must not be confused with obtaining consent for the processing of their personal data.

The most suitable legal bases for the processing of personal data concerning health (special categories) are:

- the provision of medical services according to Article 9 [1]
- the fulfillment of public interest in the sector of public health according to Article 9 [1]
- the need to fulfill archiving purposes in the public interest, for research or for statistical purposes in accordance with Article 89 [1]

5.4 Determining the Period Personal Data Are Maintained

For each category of personal data, Health Organizations should determine the period for which the data should be maintained, ensuring compliance with formal law provisions.

5.5 Special Actions for Compliance with the GDPR

Health Organizations should identify step-by-step, following the structure of the GDPR provisions, all the necessary actions to ensure compliance with the GDPR requirements and any other arrangements for the protection of the individual against the processing of personal data.

6 Conclusions

Organizations have to be prepared to comply with GDPR now in order to avoid risks and heavy consequences. In this paper, we have analyzed the security requirements for a GDPR compliant *Software as a Service* Health system and proposed specific measures that could be engaged in the process of GDPR compliance in cloud computing-based health environments. Understanding these implications has high practical relevance to Health providers as significant amounts of time, planning and money are typically needed to satisfy the requirements. The aim of our research is to assist the Cloud-based Health organizations to the hard road of GDPR compliance and to provide them with a compliance guide with a security perspective and, thus, to select the appropriate security measures for the protection of the data that they collect, process and store. Thus, this work is a necessary step to start dealing with required legal transformations. Future work comprises the development and test of proposed methods and features within real Health scenarios.

Acknowledgment. This research is co-financed by Greece and the European Union (European Social Fund-ESF) through the Operational Programme «Human Resources Development, Education and Lifelong Learning» in the context of the project “Reinforcement of Postdoctoral Researchers - 2nd Cycle” (MIS-5033021), implemented by the State Scholarships Foundation (IKY).

References

1. European Union: Regulation (EU) 2016/679 of the European Parliament and of the Council L 119. Official Journal of the European Union (2016)
2. GDPR: GDPR key changes (2017). <https://www.eugdpr.org/the-regulation.html>
3. Berendt, B.: ‘Better Data Protection by Design Through Multicriteria Decision Making: On False Trade-offs Between Privacy and Utility’, *Privacy Technologies and Policy*. Springer, Cham (2017)
4. ElShekeil, S.A., Laoyookhong, S.: *GDPR Privacy by Design: From Legal Requirements to Technical Solutions*. Department of Computer and Systems Sciences Stockholm University (2017)
5. Mohassel, R.R., Fung, A., Mohammadi, F., Raahemifar, K.: A survey on advanced metering infrastructure. *Int. J. Electr. Power Energy Syst.* **63**, 473–484 (2014). <https://doi.org/10.1016/j.ijepes.2014.06.025>
6. Newborough, M., Augoud, P.: Demand-side management opportunities for the UK domestic sector. *IET Proc. Gener. Trans. Distrib.* **146**(3), 283–293 (1999)
7. TACIT Project 2016: Threat Assessment framework for Critical Infrastructures proTection (2016). <https://www.tacit-project.eu>
8. WP29 Opinion 1/2009 on e-Privacy Directive, 10 February 2009