sciendo

GDPR impact on the Romanian health clinics

Loredana COSTINA
Bucharest University of Economic Studies, Bucharest, Romania
loredana.costina@drept.ase.ro

Adrian COROBANĂ
Bucharest University of Economic Studies, Bucharest, Romania
corobanaadrian06@stud.ase.ro

Abstract. *The General Data Protection Regulation (GDPR) - Regulation (EU) 2016/679 came into effect on the 25 of May 2018 and changed the way both companies and consumers look at the importance of personal data. While the Regulation aimed to offer better protection of personal data, it also posed many challenges for the companies processing such data. A special category of personal data are the health data, considered sensitive data under the GDPR and subject to special conditions regarding the processing. Therefore, one of the main industries that was highly impacted by GDPR was the healthcare industry. The challenges that the industry faces, especially private small health clinics, are unique among the private companies. Starting from the legal provisions that the healthcare industry must comply to under GDPR, the article analysis the main mistakes that heal clinics make, the causes of such mistakes and the main challenges faced by health clinics, with the aim of offering possible solutions for a better application of the GDPR principles in the activity of health clinics for the benefit of both the healthcare industry and the patient.*

Keywords: General data protection regulation, Regulation (EU) 2016/679, personal health data, health clinics, patient rights.

Introduction

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) further referred to as GDPR, has come into effect on 25 of May 2018 and imposed not only new obligations for the companies processing personal data, but, due to the extensive information on the subject, a higher concern with the legality and importance of data processing among consumers, which further put a both welcomed (form the point of view of the necessity to comply with the regulation) and dreaded (from the point of view of the companies, that sometimes view the obligations under GDPR as one more impediment towards successfully doing business) pressure on companies to respect the regulation.

One special category of companies subject to implementing the GDPR are the private health clinics. The challenges for these companies arise mainly from the classification of health data as special data under GDPR, with unique restrictions on the processing of such data that are, in practice, in contradiction with the manner in which private health clinics have treated these data before GDPR, from the increasing use of new technologies in the healthcare industry and the collection of more and more health data, that need new solutions for the processing and safe storage of such large quantity of data, from the increasing demand of patients to have access to their personal data on any device, at any time, and to dispose of such data and at any time, including by erasure of such data, that sometimes comes into contradiction with the legal

DOI: 10.2478/picbe-2021-0084

provisions regarding storage of medical data, as well as from the limited time and training resources of healthcare providers that often see the obligations under GDPR as a time consuming activity that keeps them from doing what they do best – offering healthcare services. These and other challenges will be further analyzed in this paper.

The mistakes that health clinics make come mainly from the habits of processing data in a certain way before GDPR and the limited time the highly specialized medical personnel disposes of to learn and relearn a new way of doing business. These mistakes include mainly the reliance on consent as the main legal ground for processing health data, the unlimited access of all clinic's personnel to the health data of patients, even if some of the clinic's personnel is not medical personnel, the reliance on external IT support and the disclosure of health data to these third-party companies, the lack of proper information of patients and a lack of security measures regarding the storage of such data. These mistakes are further analyzed.

As health data are on of the most if not perhaps the most important data each and every one of us has about ourselves, and most of our health concerns are seen by small private clinics, their role in the protection of highly sensitive data of EU citizens is very important. Considering this, the paper analysis the legal provisions that the healthcare industry must comply to under GDPR, the mistakes health clinics make, the challenges they face in the GDPR implementation and tries to offer possible solutions, among which the acknowledgement of this particularly important role health clinics play in the protection of personal data might be the most important one.

The legal provisions that the healthcare industry must comply to under GDPR

One of the main mistakes health clinics make is relying on consent for the processing of personal health data of patients. This confusion most probably comes from the fact that, according to the Romanian Act no. 46/2003 Regarding the Patients' Rights and other European acts, the patient shall be informed before any medical procedure and such medical procedure shall be performed only with the informed consent of the patient.

Article 9 of GDPR regulates the processing of special categories of personal data, among which is included the data concerning health or data concerning a natural person's sex life or sexual orientation. The premises of article 9 of GDPR is that the processing of special categories of data is mainly forbidden, with the exceptions stated in the second part of article 9, paragraph 1 "*Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited*".

The situations in which the processing of health data is not prohibited are specifically described in article 9 paragraph 2 of GDPR. One of these is the situation in article 9, paragraph 2 (h) regards the possibility of health clinics to process such data: *"(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3*"

However, the processing of such data is conditioned by paragraph 3 of article 9 of GDPR, that states it is necessary that such data is processed by a professional subject to the obligation of professional secrecy: "*Personal data referred to in paragraph 1 may be processed for the*

purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies."

Therefore, from the analysis or article 9 GDPR arises the first rules health clinics must comply with: the health data must be treated as special data that poses great risk in case of unauthorized access to it and the health data must be processed only by professionals subject to the obligation of professional secrecy: mainly the doctors and nurses, the access of other clinics personnel being highly debatable, this being one of the provisions that are subject to many mistakes and difficulties in implementation.

Health clinics must comply with all the legal obligations that other type of data processors have, with the unique challenges arising from the unique patient – doctor relation and the legal provisions that regulate the patients' rights and the storage of medical data. In the specific case of Romania, the following provisions are to be taken into consideration and will be further analyzed in the chapter dedicated to the GDPR implementation challenges for health clinics: Act no. 46/2003 Regarding the Patients' Rights and Act no. 16/1996 Regarding the National Archives.

The obligations arising from article 5 of GDPR state that health clinics, similar to any other data controller has the obligations to respect the GDPR principles, among which Personal data shall be: "*processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'); collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation'); adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'); accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy'); kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation'); processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')*".

According to the provisions of article 6 of GDPR the health clinics shall correctly identify the legal ground upon which they process the data and must further comply with the obligation of informing the natural persons whose data are being processed.

One of the first obligations that arises from the GDPR is the obligation under article 30, of recording the processing activities. For this purpose, the clinics shall do, most of the for the first time, the mapping of all the personal data that the health clinics come into contact with: "*Organisations also need to map the processing of personal data which they perform and consider the various processing activities in order to determine the lawful basis on which they are relying for that processing. (…) An informed understanding of the organisation's processing activities underpins the preparation of appropriate privacy notices and the application of appropriate organisational and technical security measures*." (Duffy, 2018: 212).

This personal data includes, as it will be further analyzed in the section regarding the mistakes health clinics make, not only the health data, but also, an aspect highly overlooked, the data of the clinics personnel, hired of contracted, and the data of the natural persons representing the legal persons that are in a business relationship with the health clinic.

As regards the relationship with the third parties that have access to the personal data processed by the health clinics, the coming into force of GDPR was, for many clinics, the first time they were forced to look at this relationship and to acknowledge the very important transfer of personal data, both as regards the patients' health data and the data of their personnel and business partners. According to article 28 of GDPR, the health clinics shall conclude a written contract with the persons who process data on their behalf (the Processor). For health clinics, these persons are mainly the company that manages the software used to keep track of patients' data, and the medical personnel that is often not hired personnel, but a subcontracting party, private individual companies or small companies made up of two or three doctors, all operating under one medical brand.

All these data processing activities must be effectively communicated to the natural persons whose personal data are being processed. These persons include, mainly, the patient, but not only this category of natural persons, an aspect widely overlooked. According to article 13 of GDPR, paragraph 1, the clinics shall provide the data subject with all of the following information:

"*(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;*

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(e) the recipients or categories of recipients of the personal data, if any;

(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available".

According to article 13 of GDPR, paragraph 2, this further information should also be provided:

"*(g) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;*

(h) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

(i) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(j) the right to lodge a complaint with a supervisory authority;

(k) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

(l) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject".

Last but not least, the health clinics must implement robust security systems in order to protect especially the sensitive health data of patients. According to article 32, paragraph 1 of GDPR, *"taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:*

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing".

Considering that the health data is special data posing a high risk for the rights and freedoms of natural persons, as per article 9 of GDPR, it is safe to say that the best technical solutions available are to be considered.

As regards the obligation to appoint a Data Processing Officer (DPO), article 37 of GDPR states that health clinics "*shall designate a data protection officer in any case where:*

(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

(b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

(c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 or personal data relating to criminal convictions and offences referred to in Article 10".

The obligation to appoint a DPO is therefore subject to the analysis of the size and area of activity of the health clinic as an indicator of whether or not the processing is done on a large scale. It is out opinion that, in case of most small private health clinics the appointment of a DPO is not mandatory.

The main mistakes health clinics make

One of the main mistakes health clinics make is relying on consent for the processing of personal health data of patients. This confusion most probably comes from the fact that, according to the Romanian Act no. 46/2003 Regarding the Patients' Rights and other European acts, the patient shall be informed before any medical procedure and such medical procedure shall be performed only with the informed consent of the patient.

However, there in an important distinction between that consent and the consent regarding the processing of personal data. Health data must be processed not only for the medical intervention, but also in order to establish the right diagnosis and to decide on the course of action that is to be performed – on the recommended medical intervention. Only after such decision is made the patient can be informed and his or her consent can be taken for the

recommended medical procedure. Therefore, the processing of personal health data is necessary for each and every consultation and therefore the consent of the patient cannot be given freely without the consequence that no medical analysis can be made without the health data. In other words, as Duffy (2018: 212) puts it, some institutions might have challenges with this consent, especially if they rely on it for treatments. This is also the opinion of the Romanian "Association of Experts in Confidentiality and Data Protection", the initiator of a campaign named "*Eliminate the GDPR Consent in the Medical Field*" (Dumitrescu, 2018).

Another reason we consider the use of consent as a legal ground for processing of health data as a mistake is the fact that when the ground for processing is the consent, the patient shall have the right to withdraw such consent at any time, with the consequence erasing all data from the health clinic evidence. Such an erasure is in practice impossible, due to the fact that under Act no. 16/1996 Regarding the National Archives it mandatory that medical data are archived for a duration of 100 years.

Therefore, we consider that the legal ground for processing the health personal data is article 6, paragraph (1) (b) and (c) of the GDPR: the processing is necessary for the provision of the medical service and the processing is necessary for the health clinic to fulfill its legal obligations of storage of medical data and issuance of the medical report, with the data provided by Annex 43 of the Methodological Rules 2018 and Government Decision no. 140/2018, as long as the data is processed by the medical personnel according to article 9 para. (3) of GDPR.

Another common mistake regards the relationship with the persons who have access to patient data. One category of mistake regards the persons within the health clinic and the other regards the third parties who can and often have access to the patients' data.

Often health clinics fail to ensure that access to the patient data is given only to the medical personnel that is directly involved in the diagnosis and medical intervention on that specific patient and needs to know the data. Such was the case of Centro Hospitalar Barreiro Montijo, that has been fined 400,000 euros for violating the GDPR (Ferrándiz, Degli-Esposti, 2021; Schneider, 2020). Among the problems identified where the following:

"*Nine technical employees enjoyed the level of access reserved for the medical group, which resulted in the indiscriminate possibility of such employees consulting the clinical processes of all hospital users. Existence of access credentials which allowed any doctor, regardless of his/her specialty, to access at any time the data of the clients of a hospital. This was considered as violating the principle of "need to know" and the principle of "minimization of data." There were 985 users associated with the profile "doctor," but in the official hospital human resources charts there are only 296 doctors in that hospital. Maintenance of useless profiles for doctors who no longer provide services to the hospital. There were only 18 user accounts that were inactive and the last one was deactivated in November 2016*" (Monteiro, 2019).

This is not, however, an isolated case. In another case, the Dutch Haga Hospital was penalized with €460,000 by The Dutch Data Protection Authority for breaching GDPR regulations when employees accessed personal data of a local celebrity without authorization (Ioannidou, 2020; Iunker, 2019).

As regards the access to patients' health data, another mistake that we identified in our practice is the lack of the contract mandatory according to article 28 of GDPR with the processor, signed between the health clinic and the legal persons that are empowered to have access to such data. One of the most overlooked processor is the medical personnel that works with a collaboration (not employment) contract, as well as the IT company that provides medical

software for the storage of patients data and that, most often than not, has full access to all medical data.

As regards the relationship with the IT company that offers the medical software, a lack of technical security guarantees is common in the contracts signed between the health clinics and the IT companies. Part of the explanation is the fact that the content of the contract was drafted by the IT companies before the GDPR came into force and with the understandable interest of being beneficial for the IT company. Most health clinics did not negotiate such contracts, due to the lack of legal advice and the need to adopt an IT solution that is quick for the health provider to do what they do best: offer health services, without the added stress of contract negotiations.

Last but not least, concerned with difficulties of health data processing, most health clinics forget the fact that the personal data they handle are not only the personal data concerning the patients, but also the personal data concerning their employees and their partners. Therefore, more often than not, there are no measures being taken regarding the processing of this data or the information of these data subjects.

GDPR implementation challenges for health clinics

Most of the challenges of the health clinics arise from the classification of health data as special data under GDPR, with unique restrictions on the processing of such data that are, in practice, in contradiction with the manner in which private health clinics have treated these data before GDPR, as described in the previous section regarding the most common mistakes health clinics make.

One of the practical challenges is the implementation of different procedures regarding the informed consent of the patient for the medical procedure, and the information regarding the GDPR rights, two different things that were, before GDPR, given on a single piece of paper named: Informed Consent.

With the impossibility to legally use consent for the processing of health data, but with the necessity to still use the consent for the medical intervention, the medical personnel is often and understandably lost in the large number of documents that must be provided to the patient in a small amount of time. Also, the doctors and nurses must be concerned not only with the quality of the medical act, but also with the proper use of personal data and with the information of the patient on a highly specialized legal matter: legal ground for processing, the rights under GDPR, which adds, at least at the beginning of the implementation process, to adding a new source of stress to an already stressful job description, which leads to increased resistance to the implementation of GDPR in the health field.

Another big challenge comes with the increasing use of new technologies in the healthcare industry, starting with the software used for the storage of health data and continuing with the increased used of medical devices that store data in highly specialized language that is sometimes inaccessible to the medical personnel without the help of the IT personnel. However, as the IT personnel cannot have access to the health patient as regard article 9 paragraph (3) of GDPR, it is highly challenging to develop the systems that allow IT assistance without access to this sensitive data.

In close relation with the previous challenge, another challenge is the reliance of the medical personnel on the non-medical personnel for the administrative tasks regarding the relationship with the patient: from making the appointment for the consultation, at which point the non-medical personnel might come into contact with health data that the patient gives during the appointment conversation and to the printing of the medical report, when the non-medical

personnel will come into contact with the medical data. Therefore, IT systems and medical administrative tasks shall be changed.

A high challenge is also the increasing demand of patients to have access to their personal data on any device, at any time, and to dispose of such data and at any time, including by erasure of such data. This puts the pressure on the health clinics to develop apps and websites that allow secured access to such data and with further exposes them to data breaches.

Of high concern is the desire of the patients to have full control over their health data, including the right to erase the data from the evidence of the health clinic, a demand that may come in contradiction with the legal provisions regarding storage of medical data, as well as with the desire of the health clinic to keep such data for any future malpraxis accusation.

These challenges might explain the result of the study conducted by Lopes et al. (2020) regarding the General Data Protection Regulation in Health Clinics in Portugal, which shows that many clinics are still struggling to become GDPR compliant. It is also worth mentioning that the survey was sent to 190 clinics, however only 57 gave an effective reply, which corresponds to a response rate of only 30%.

Conclusions and possible solutions

The General Data Protection Regulation has come into effect on 25 of May 2018 and has imposed new obligations for the companies processing personal data. Among the most impacted companies are the health clinics, due to the fact that health clinics process health data considered to be sensitive data under GDPR, with unique restrictions on the processing of such data that are, in practice, in contradiction with the manner in which private health clinics have treated these data before GDPR.

We identified a few key mistakes that health clinics make, among which the most common and severe are the reliance on consent as the main legal ground for processing health data of patients, the unlimited access of the non-medical personnel to the health data of patients and the unlimited access of external IT support and the disclosure of health data to these third party companies, the lack of proper information of patients and a lack of security measures regarding the storage of such data.

We also identified a few of the challenges that health clinics face in the implementation of GDPR and the causes of these challenges: the necessity to benefit from the support of non-medical personnel, in the face of increasing data processing and new technologies, the increasing demand of patients to have access to health data and to have the possibility to erase such data to the limited time to dedicate for the study and learning of the legal requirement of GDPR by the medical personnel, a category of professionals already with high demands and responsibilities.

In conclusion, our practical experience working with health clinics showed us that the most important change that must occur for health clinics to implement the principles of GDPR in their activity is to understand the importance of health data for the patients, although for the medical personnel the health data are just usual pieces of information, absolutely necessary for the performance of their job. Also, the health clinics need to have a person who is responsible with the implementation of GDPR and everyday conduct of business in accordance with GDPR coming from within the clinic, and who understands both the medical practice and the requirements of GDPR. Also, it is mandatory that health clinics rely on IT systems that are very well integrated, easy to access, but also with a high degree of security. For this, the health clinics

shall work with IT companies that fully understand the requirements of GDPR and who accept a large responsibility for the implementation of such systems.

References

Duffy, S. (2018). General Data Protection Regulation and healthcare. Legalities, *Health Management,* 18(3), 212.

Dumitrescu, M. (2018). *Eliminați "Consimțământul GDPR" al pacientului pentru serviciile medicale*. Originally published on the official website of the Data Protection Officers Network (dpo-net.ro) on October 18th, 2018, at URL: https://dpo-net.ro/eliminati-consimtamantul-gdpr-al-pacientului-pentru-serviciile-medicale/, retrieved on October 21st, 2021.

Ferrándiz, E. M., & Degli-Esposti, S. (2021). After the GDPR: Cybersecurity is the Elephant in the Artificial Intelligence Room, *European Business Law Review*, 32(1), 1-24.

Ioannidou, V. (2019). *The GDPR and the effect on the Medical Profession*, Retrieved from https://www.neo.law/wp-content/uploads/2019/11/Data-protection-reforms-in-the-Medical-Profession.pdf.

Iunker, A.E. (2019). The New Data Protection Regulation claims under GDPR, *Journal of Information Systems & Operations Management*, 13(2), 100-115.

Lopes, I.M., Guarda, T., Oliveira, P. (2020). General Data Protection Regulation in Health Clinics, *Journal of Medical Systems*, 44 (2), 1-9.

Monteiro, A. (2019). *First GDPR fine in Portugal issued against hospital for three violations.* Retrieved from https://iapp.org/news/a/first-gdpr-fine-in-portugal-issued-against-hospital-for-three-violations/.

Schneider, T. (2020). *Cybersecurity Law, Standards and Regulations*, Rothstein Publishing.

General data protection regulation, Regulation (EU) 2016/679, available on the official website EUR-Lex, at URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj, retrieved on October 21st, 2021.

Legea nr. 16 din 2 aprilie 1996 privind Arhivele Nationale, available at URL: http://legislatie.just.ro/Public/DetaliiDocument/7937, retrieved on October 21st, 2021.