ELIAS NEOCLEOUS & Co LLC

The GDPR and the effect on the Medical Profession

Introduction

The latest data protection reform is a legislative "bundle" introduced to update and modernize the existing data protection rules within the European Union. Included in the reform is General Data Protection Regulation ((EU) 2016/679")[1] which regulates the processing by individuals, companies or organizations of personal data relating to individuals in the EU (**"GDPR"** or **"the Regulation"**), replacing Directive 95/46 / EC. Since its implementation on 25 May 2018, there have been several regulatory actions taken against hospitals around Europe which have highlighted the significant impact these reforms have had on the medical profession.

Purpose of the GDPR

The GDPR aims primarily to enhance individual rights contained in Directive 95/46/EC and to improve business opportunities by facilitating the free flow of personal data in the digital single market, as well as aiming to introduce important obligations on how organizations and professionals handle personal data as controllers and processors. Controllers and processors have certain obligations under the GDPR.

Article 4 of the GDPR defines a Controller as the natural or legal person who determines the purpose and manner of processing.[2] The Processor is defined as a person who performs the processing of personal data on behalf of the controller.[3]

The GDPR is an integral part of any organisation that processes [4] and has access to personal, sensitive and confidential data of clients and employees including health-related data as to the physical or mental health of a natural person, which reveals information about the health status of the individual. As a result this legislation has a significant impact on the medical profession, as the treatment of patients necessarily involves the function of collecting, analysing, managing and storing the sensitive health information of patients. Such information is considered "special category" data for the purposes of the GDPR, for the processing of which special considerations apply.[5]

---

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council1, ie the new European Union (EU) General Data Protection Regulation (GCCA), regulates the processing by individuals, companies or organizations of personal data relating to individuals in the EU.

[2] Ibid 1, Article 4 (7) definitions and Law (Law 125(I)/2018) PART I (2)(1): 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

[3] Ibid 1, Article 4 (8) definitions and Law (Law 125(I)/2018) PART I (2)(1) 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

[4] Ibid 1, Article 4 (2) definitions and Law (Law 125(I)/2018) PART I (2)(1): 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

[5] Ibid 1, Article 9

Obligations Imposed by the GDPR

In general, the GDPR builds on existing principles and adds tighter obligations and restrictions on businesses.

The GDPR, inter alia, regulates the processing by individuals, companies or organizations of personal data relating to individuals in the EU, and requires those individuals, companies and organisations to ensure that the appropriate technical and organisational security measures are implemented to protect personal data.

Lawfulness of certain processing operations - When is it legal to process simple personal data?

According to Article 6 (1) of the Regulation, it is legitimate to process simple personal data of a data subject under any of the following circumstances; If the person's consent has been granted; for the performance of a contract to which the data subject is party; in order to take steps at the request of the data subject prior to entering into a contract; for the fulfilment of the legal obligations of the data controller; in order to safeguard the vital interest of the individual and/or other natural person; when it is necessary for the public interest; and/or for the exercise of public authority. Lastly, it is permissible when the processing is done pursuant to a legitimate interest of the data controller or a third party, except where it violates the fundamental rights or freedoms of the individual. [6]

In relation to "special categories data", such as health data, on the other hand, Article 9 (1) of the Regulation provides specific provisions for the processing of such data to be lawful**.** Indeed, Article 9 of the Regulation has fundamentally changed the way personal data may be handled, especially with regard to the medical profession since Article 9(2)(c) provides that data processing is allowed where it is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapacitated from giving consent. Therefore, where it is in the best interests of a patient, a medical practitioner should not refuse to provide the medical records of a patient "who is physically or legally incapacitated from giving his consent", to a member of the family of the patient or other person. According to the relevant regulation, any medical practitioner and/or doctor who refuses to provide such medical documents, could be in breach of their obligations as imposed under the GDPR. In such a case, a complaint may be filed at the office of the Commissioner for Data Protection who has a wide range of powers under the GDPR and Cyprus Law 125(1)/2018. [7]

Failure to comply with the GDPR - Administrative Fines And Offenses

The Commissioner has certain corrective powers under the GDPR[8], including the power to issue warnings and reprimands, to order compliance with the data subject's requests to exercise his or her rights pursuant to this GDPR as well as to order compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period.

[6] Ibid 1, Article 6 Lawfulness of processing

[7] Law providing for the Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement of such Data of 2018 (Law 125(I)/2018)

[8] Ibid 1, Article 58

In addition to corrective powers, according the Article 83 of the Regulation, administrative fines can be imposed by the Commissioner in respect of infringements of the GDPR by the controller or the processor for infringement of the GDPR provisions, including non-compliance with a corrective order issued by the Commissioner

Furthermore, Cyprus law[9] creates a number of criminal offences for the violation of certain articles of the Law and of the GDPR, punishable upon first conviction with imprisonment of 1 to 5 years and/ or a fine of 10,000 to EUR50,000 depending on the offence.

Enforcement of GDPR in Europe

The Dutch Data Protection Authority, called Autoriteit Persoonsgegevens (hereinafter referred to as the **"Dutch DPA"**), recently imposed its first GDPR fine of €460,000, on the Dutch Haga Hospital, for having an insufficient internal security of patient records which constitutes a breach of Article 32 of the Regulation.[10] In this scenario, prior to imposing the fine, the Dutch DPA initiated an investigation after it appeared that several employees from Haga Hospital had accessed the medical records of a patient, who was a Dutch celebrity, without her consent and authorization. During its investigation, the Dutch DPA checked whether the hospital's information security systems met the security requirements of Article 32 of the Regulation and, more specifically, certain health care sector security standards. Haga hospital is currently subject to monitoring to make sure that its security is improved. A penalty of €100,000 to as high as €300,000 per two weeks will be issued if security is not brought up to the standards demanded by GDPR, before the 2nd of October, 2019.

Pursuant to the GDPR, Haga hospital ought to have implemented appropriate technical and organisational measures to ensure a level of security appropriate to the risk, and had a duty to take steps to ensure that any person acting under their authority, and having access to personal data of the patients, does not process that data except on instructions from the Hospital.

Another case where a breach of the GDPR occurred and a fine was imposed to the hospital, is found in Portugal. The Portuguese Supervisory Authority, called Comissão Nacional de Protecção de Dados (hereinafter referred to as the "**CNPD**"), on the 17th of July, 2018, imposed a fine of €400.000, on a hospital for infringing the GDPR. According to a press report,[11] the CNPD carried out an investigation at the hospital, where it discovered that the hospital's staff had access to patient data through the use of fake profiles. The investigation found that the profile management system appeared to be deficient, since it was exposed that the hospital had only 296 doctors registered, whilst there were around 985 doctor profiles in the database. Also, the investigation found that regardless of a doctor's specialty, he/she had unrestricted access to all patient files.

On that basis, the CNDP concluded there was a clear violation of Article 5 (1)(c) of the Regulation in that an excessive number of users had access to the personal data of patient files. Furthermore, it was determined that in terms of Article 5 (1) (f) of the Regulation, the principle of integrity and confidentiality was breached. As a result of the investigation conducted by the CNPD, it was concluded that the hospital

[9] Law 125(I)/2018, Section 33

[10] By HIPAA Journal, Netherlands Hospital Hit with €460,000 GDPR Data Breach Fine, (on Jul 22, 2019), https://www.hipaajournal.com/netherlands-hospital-hit-with-e460000-gdpr-data-breach-fine/» accessed on 05/08/2019.

[11] By Anna Oberschelp de Meneses and Kristof Van Quathem, Portuguese hospital receives and contests 400,000 € fine for GDPR infringement (insideprivacy, on October 26, 2018) «https://www.insideprivacy.com/data-privacy/portuguese-hospital-receives-and-contests-400000-e-fine-for-gdpr-infringement/», accessed on 29/07/2019.

failed to put in place the appropriate technical and organizational measures required to comply with the GDPR, which intends to protect patient data.

The hospital sought to defend its actions on the basis that the information infrastructure used was the one provided by the Portuguese Ministry of Health for the public hospitals. However, it was decided by the CNPD, that the onus rested on the hospital to ensure that the appropriate technical measures were organised and put in place so as to ensure compliance with the GDPR.

Conclusion

By the introduction and implementation of the new GDPR, data subjects' rights are better safeguarded due to the further obligations placed upon organizations, and due to the fear of hefty fines. These organizations have the onus to familiarize themselves with their obligations and take all the necessary steps to implement the GDPR. Every company, organization, both in the public and private sector, which handles private data concerning individuals within the European Union, are obliged to comply fully with the GDPR and to re-examine and/or re-evaluate all the management procedures with regards to the handling of personal information. As highlighted in the cases referred to above, regulators around Europe are taking a very strict approach to implementing these obligations, especially when it comes to Hospitals and the processing of patient's personal health data.

Further, the provisions of Article 9(2) which provides a specific circumstance in which the processing of data is allowed, and indeed required, regardless of the Data Subject's consent, will have a profound impact on the medical profession in particular. Medical professionals regularly find themselves in the position of having a patient that is incapacitated and cannot give consent. Through this Article the GDPR seeks to address such situation by allowing the medical professional to disclose patient's data where the patient is incapacitated, and it is in the patient's vital interests to do so. Disclosure may become an obligation where it is requested by family members of an incapacitated patient, which if breached results in sanctions under the GDPR. Such approach may be problematic, both for the medical professional, and the regulatory authorities, as it is unclear at this stage how the regulators will approach the determination of the circumstances in which a medical professional (or any other) may or may not refuse a request. In the absence of any guidance from the authorities as to the parameters for making such decision, medical practitioners may be exposed to potential sanctions for professional decisions they make in the belief that it is in their patient's best interests, should others, or indeed the patient once they have recovered, take a different view.

Vasileiana Ioannidou