ISSN 2704-8012

European Journal of Privacy Law & Technologies



Special issue (2020)

G. Giappichelli Editore

European Journal of Privacy Law & Technologies

Directed by Lucilla Gatt

Special issue (2020)

Edited by Massimo Foglia

G. Giappichelli Editore

European Journal of Privacy Law & Technologies
On line journal
Italian R.O.C. n. 25223

G. GIAPPICHELLI EDITORE - TORINO
VIA PO, 21 - TEL. 011-81.53.111 - FAX 011-81.25.100
http://www.giappichelli.it



The Journal is one of the results of the European project TAtoDPR (Training Activities to Implement the Data Protection Reform) that has received funding from the European Union's within the REC (Rights, Equality and Citizenship) Programme, under Grant Agreement No. 769191.

The contents of this Journal represent the views of the author only and are his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

Published Online by G. Giappichelli in September 2020
www.ejplt.tatodpr.eu

PATIENTS AND PRIVACY: GDPR COMPLIANCE FOR HEALTHCARE ORGANIZATIONS

Massimo Foglia, University of Bergamo

Abstract:

After the entry into force of the GDPR, the change in the regulatory framework also affected the health profession, since the entire set of rules on data processing, including data concerning health, was amended. This paper argues that the purpose of the personal data protection legislation is not the mere defence of the personal data, but the protection of the most inner dimension and dignity of the natural person. It is from this point of view that any provision with respect to the protection of personal data, including data concerning health, should be read.

Keywords: privacy, patient, healthcare organization.

Summary: 1. Introduction. – 2. Processing of personal data concerning health. – 3. Conclusion.

1. Introduction

After the entry into force of the GDPR, the change in the regulatory framework also affected the health profession, since the entire set of rules on data processing, including data concerning health, was amended [1]. I have divided my presentation in three parts. In the first part I am going to focus on the definition of personal data concerning health within the Italian regulatory framework after the entry into force of the GDPR. In the second part I am going to point out some features of data processing based on the data subject's consent. Finally, I

[1] See also S. SELLETTI-A. SCALIA, *L'impatto della nuova normativa "privacy" sugli studi clinici,* in *Rass. dir. farm. e salute*, 2018, 1009-1014; A. E. MATARAZZO, *Nuovo regolamento UE in materia trattamento dati personali dei lavoratori ed i rapporti con il codice della privacy*, in *Stato civ. it.*, 2016, 66-69.

am going to focus on the role of the Data Protection Officer (DPO) in healthcare organizations.

2. Processing of personal data concerning health

The Italian legislation on personal data protection is based on the Legislative Decree No. 196 of 30 June 2003, which is the so-called "Privacy Code". The Privacy Code was then amended by the Legislative Decree No. 101 of 10 August 2018 in order to comply with the GDPR provisions [2].

It should be noted that no specific definition of "personal data concerning health" existed before the entry into force of the GDPR. A broad definition was laid down in the Italian Privacy Code, which provided for a general category of "sensitive data" [3] including those defined as "data revealing state of health" [4].

On the contrary, the GDPR does not define "sensitive data" (as the Italian legislator did in the past) as it was replaced with "special categories of personal data" according to art. 9 GDPR, which should be subject to specific measures so as to prevent significant violation of the rights and fundamental freedoms of natural persons.

In particular, art. 4 of the GDPR defines "data concerning health" [5] as «personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status».

Furthermore, the Recital No. 35 specifies «Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health

---

[2] See V. CUFFARO-R. D'ORAZIO-V. RICCIUTO, *I dati personali nel diritto europeo* (Torino 2019); E. TOSI, *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy* (Milano 2019); V. CUFFARO, *Il diritto europeo sul trattamento dei dati personali*, in *Contr. e impr.*, 2018, 1098 ss.; ID., *Quel che resta di un codice: il D.Lgs. 10 agosto 2018, n. 101 detta le disposizioni di adeguamento del codice della privacy al regolamento sulla protezione dei dati*, in *Corr. giur.*, 2018, 1181 ff.

[3] On the concept of "sensitive data" see F. PIRAINO, *Il contrasto sulla nozione di dato sensibile, sui presupposti e sulle modalità del trattamento*, in *Nuova giur. civ. comm*., 2017, 1232-1240.

[4] See S. CORSO, *Sul trattamento dei dati relativi alla salute in ambito sanitario: l'intervento del Garante per la protezione dei dati personali,* in *Resp. medica*, 2019, 225 ff.; P. GUARDA, *I dati sanitari*, in *I dati personali nel diritto europeo* (Torino 2019) 591 ff.; A. PALMA ORTIGOSA-S. LORENZO CABRERA, *Data in the Healthcare sector* (2019) 2 *European Journal of Privacy Law and Technologies*, 16 ff.

[5] See T. MULDER, *The Protection of Data Concerning Health in Europe* (2019) *European Data Protection Law Review*, 209 ff.

status of the data subject. This includes information […] deriving from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test».

It is worth mentioning that "Data concerning health" are distinguished from "genetic data" [6] and "biometric data" [7] by the GDPR. Genetic data can be considered a specification of health data.

According to Recital no 34: Genetic data should be defined as personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained.

On the other hand, pursuant to Recital no 14 and no 51: biometric data means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

Now, as a general rule, the processing of special categories of personal data, including data concerning health, is prohibited according to art. 9 GDPR, with a few exceptions, as I will mention.

The point is that several doubts have arisen on the interpretation of this set of new rules on the processing of data concerning health. Hence, the Italian Data Protection Authority has intervened to provide some guidelines on the application of such rules in the healthcare field with the General Application Order No. 55 of 7 March 2019 [8].

Thus, the Italian Authority has clarified the processing of data concerning health is prohibited with the exception of:

a) reasons of substantial public interest, on the basis of Union or Member State law;

---

[6] On genetic data see L. CALIFANO, *Il trattamento dei dati genetici: finalità di ricerca, esigenze di sicurezza e diritto alla protezione dei dati personali*, in *Cultura giuridica e diritto vivente*, 2017, 13 ff.; R. PACIA, *Campione biologico e consenso informato nella ricerca genetica: il possibile ruolo delle biobanche,* in *Jus civile*, 2014, 40 ff.

[7] On biometric data see F. FONTANAROSA, *Dati biometrici e tutela della "privacy" tra divergenze giuridiche ed esigenze di unificazione*, in *Ann. dir. comp.,* 2019, 807-844.

[8] M. PANEBIANCO, *Il trattamento dei dati nel Sistema Sanitario Nazionale italiano alla luce del Provvedimento del Garante del 7 marzo 2019*, in *Cib. dir.*, 2019, 241-269.

b) reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices (for example health emergencies due to earthquakes or food safety);

c) 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 undertaken by (or under the responsibility of) a health professional subject to professional secrecy or by other person also subject to an obligation of secrecy».

In particular, with regards to the case at let. g) par. 2 art. 9, legal scholars have pointed out that its wording may be too vague and extensive, given that the concept of substantial public interest is deferred to Member States. This might cause abuses and incoherent interpretations, in contrast with the idea of jurisdictions' harmonisation [9].

Furthermore, in relation to the exception at let. h) of the same paragraph, case that can be defined as "health-related purposes" (*finalità di cura*), the Italian Authority observes that - and this is probably the crucial point in the General Application Order - that now, differently from the past, it is no longer compulsory that the physician, subject to professional secrecy, asks for the patient's consent for the processing of data related to the medical treatment, irrespective of the fact that the physician is affiliated to a medical institution.

On the other hand, the Italian Authority made it very clear that processing of personal date not strictly related to the medical treatment requires the data subject's consent. For instance:

a. data processing related to the use of medical App;

b. data processing designed to increase customer's loyalty;

c. data processing in health field undertaken by private entities for promotional or commercial purposes;

d. processing undertaken by health professionals for commercial or voting purposes;

e. processing undertaken through the Electronic Health Record.

In order to add information to the Electronic Health Record, existing provision in the field of health require the data subject's consent (cf. art. 75 Italian Privacy Code) [10]. Nevertheless, in the light of the new regulatory framework,

---

[9] M. Granieri, *Il trattamento di categorie particolari di dati personali nel Reg. UE 2016/679*, in *Nuove leggi civ.*, 2017, 165-190; A. Busacca, *Le "categorie particolari di dati" ex art. 9 GDPR. Divieti, eccezioni e limiti alle attività di trattamento*, in *Ordine Internazionale e Diritti Umani*, 2018, 19.

[10] On Electronic Health Record see V. Peigné, *Il fascicolo sanitario elettronico, verso una*

the Italian Authority suggested a possible amendment removing the consent requirement for processing personal health information through the Electronic Health Record. On the other hand, such a solution is considered as dangerous and risky for the security of health information processed beyond the data subject's control.

As far as online medical report is concerned, the Italian Authority made it clear that the current legislation requires the data subject's consent in respect of the delivery of the medical report.

Among the data subject's rights laid down in the GDPR it is useful to mention the right of access which allows the data subject to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data (art. 15 GDPR).

Furthermore, a strong emphasis was placed on the right to erasure (also called 'right to be forgotten')[11]. According to art. 17, par. 1, GDPR, the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay. This rule sets out a substantial right of informational self-determination. Hence, the right to erasure has to be guaranteed not only whereas the personal data have been unlawfully processed, but also in the case of lawful and fair processing.

At the same time, according to Art. 12 GDPR, any communication relating to processing to the data subject should be made in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child[12].

"trasparenza sanitaria" della persona, in *Riv. it. med. leg.*, 2011, 1519-1547; P. GUARDA-R. DUCATO, *Profili giuridici dei "Personal Health Records": l'autogestione dei dati sanitari da parte del paziente tra "privacy" e tutela della salute,* in *Riv. crit. dir. priv.,* 2014, 389-419; E. STEFANINI, *Telemedicina, "mHealth" e diritto*, in *Rass. dir. farm*., 2016, 1023-1032.

[11] On the right to be forgotten V. CUFFARO, *Una decisione assennata sul diritto all'oblio*, in *Corr. giur.,* 2019, 1195-1197; R. SENIGAGLIA, *Reg. UE 2016/679 e diritto all'oblio nella comunicazione telematica. Identità, informazione e trasparenza nell'ordine della dignità personale*, in *Nuove leg. civ. comm*., 2017, 1023 ff.; A. THIENE, *Segretezza e riappropriazione di informazioni di carattere personale: riserbo e oblio nel nuovo regolamento europeo*, in *Nuove leg. civ. comm.*, 2017, 442; S. BONAVITA, R. PARDOLESI, *GDPR e diritto alla cancellazione (oblio)*, in *Danno e resp.*, 2018, 269-281; F. SCIA, *Riservatezza e oblio: diritti dei minori e servizi della società dell'informazione* (2019) 2 *European Journal of Privacy Law and Technologies*, 16 ff.

[12] I. A. CAGGIANO, *"Privacy" e minori nell'era digitale. Il consenso al trattamento dei dati dei minori all'indomani del Regolamento UE 2016/679, tra diritto e tecno-regolazione*, in *Familia*, 2018, 3-23; A. ASTONE, *I dati personali dei minori in rete. Dall'internet delle persone e all'internet delle cose* (Milano 2019); R. SENIGAGLIA, *Autodeterminazione e minore età. Itinerari di diritto minorile* (Pisa 2019).

One of the most important novelties introduced by the GDPR concerns the role of the Data Protection Officer (DPO) [13].

As is known, the DPO performs a supervisory role in keeping the control over the compliance with regulations on privacy.

As a general rule, either public or private medical institutions must appoint a DPO [14]. With respect to public institution given that the processing is carried out by a public authority or body (art. 37, par. 1, let. a), whilst as far as private institutions are concerned as 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 GDPR (art. 37, par. 1, let. c).

On the other hand, physicians practicing their professional activity outside a medical institution are not obliged to designate a DPO pursuant to Recital 91 GDPR according to which: "The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer. In such cases, a data protection impact assessment should not be mandatory".

With particular reference to the so-called E-Health, it is worth mentioning the function of the Data protection impact assessment [15]. According to Article 35 GDPR, «Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the pro-

---

[13] M.C. GAETA, *Hard law and soft law on data protection: what a DPO should know to better perform his or her tasks* (2019) 2 *European Journal of Privacy Law and Technologies*, 61 ff.; S. ANGELETTI, *Data Protection Officer: una nuova professione nelle amministrazioni pubbliche?*, in *RU Risorse umane nella pubblica amministrazione*, 2019, 32-43; S. LINGUANTI, *La figura del DPO/RPD nel regolamento UE 2016/679 in tema di privacy*, in *Disc. comm.*, 2018, 59-62; F. LORÈ, *Il ruolo del Responsabile della protezione dei dati personali nella pubblica amministrazione alla luce del Regolamento generale sulla protezione dei dati personali UE 2016/679*, in *Amministrativamente*, 2018, 22; A. TORTORA, *Il nuovo regolamento europeo per la protezione dei dati (GDPR) e la figura del "Data Protection Officer" (DPO): incidenza sulla attività della pubblica amministrazione,* in *Amministrativamente*, 2018, 19; M. RECIO, *Practitioner's Corner Data Protection Officer: The Key Figure to Ensure Data Protection and Accountability* (2017) *European Data Protection Law Review,* 114-118.

[14] G. PEDRAZZI, *Il ruolo del responsabile della protezione dei dati (dpo) nel settore sanitario*, in *Riv. it. med. leg.,* 2019, 179 ff.

[15] See F. CIRILLO, *The Impact of e-Health on Privacy and Fundamental Rights: From Confidentiality to Data Protection Regulation* (2019) 2 *European Journal of Privacy Law and Technologies*, 95 ff.; V. HORDERN, *The final GDPR text and what it will mean for health data* (2016) *eHealth Law & Policy*, 3-5; L. WILLIATTE-PELLITTERI, *New Technologies, Telemedicine, eHealth, Data...What Are You Talking About? The Lawyer's Point of View*, A. ANDRÉ (eds.), *Digital Medicine, Springer, Cham* (Berlin 2019), 93; N. CORTEZ, *The Evolving Law and Ethics of Digital Health*, H. RIVAS-K. WAC (eds.), *Digital Health Scaling Healthcare to the World, Springer* (Berlin 2018), 249.

cessing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data […]»

On this issue, it might be useful to report a recent decision of the Portuguese Authority (*Comissão Nacional de Protecção de Dados*), which imposed a penalty of four hundred thousand euros on a hospital with CNPD 984/2018 resolution (9932/2018 procedure).

The case was about the failure to define the criteria for access to the healthcare information system called SONHO, a patient management system launched by the Portuguese Ministry of Health.

Basically, the same access to patient data was assigned to physicians as well as technical-administrative staff. This is a clear infringement of the principle of "data minimisation", according to which processing of personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which personal data are processed.

The controller and the processor have the duty to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including the ability to ensure the ongoing confidentiality, integrity and availability of personal data. Therefore, such a violation should have been detected by the DPO.

3. Conclusion

I have tried to point out some of the many fulfilments required to health professionals and especially to health institutions in the perspective of the GDPR compliance.

As I said, the Italian Data Protection Authority argues that patient's consent is no longer necessary for data processing in the case of health-related purposes.

However, it should be borne in mind that the contractual party's consent (on which the health assistance contract is based) does not amount to data subject's consent to data processing [16]. They have different content and purposes.

[16] See G. RESTA-V. ZENO-ZENCOVICH, *Volontà e consenso nella fruizione dei servizi di rete*, in *Riv. trim. dir. proc. civ*., 2018, 411 ff.; V. CUFFARO, *Il consenso dell'interessato*, in V. CUFFARO - V. RICCIUTO (a cura di), *La disciplina del trattamento dei dati personali* (Torino 1997), 221; S. PATTI, *Il consenso dell'interessato al trattamento dei dati personali*, in *Riv. dir. civ*., 1999, 455 ff.; P. MANES, *Il consenso al trattamento dei dati personali* (Padova 2001) 81 ff.; L. GATT-R. MONTANARI-I.A. CAGGIANO, *Consenso al trattamento dei dati personali e analisi giuridico comportamentale. Spunti di una riflessione sull'effettività della tutela dei dati personali*, in *Pol. dir*., 2017, 363 ff.; I.A. CAGGIANO, *Il consenso al trattamento dei dati personali nel nuovo Regolamen-*

Furthermore, it should be pointed out that data concerning health are a peculiar category of data, as they disclose part of the story of the patient's life; they reveal fragments of their identity.

Hence, the purpose of the personal data protection legislation is not the mere defence of the personal data, but the protection of the most inner dimension and dignity of the natural person. It is from this point of view that any provision with respect to the protection of personal data, including data concerning health, should be read.

to europeo. Analisi giuridica e studi comportamentali, in *Osserv. dir. civ. e comm*., 2018, 69 ff.; S. THOBANI, *I requisiti del consenso al trattamento dei dati personali* (Santarcangelo di Romagna 2016); ID., *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento di massa dei dati personali* (Milano 2018), 118 ff.; G. BUTTARELLI, *Banche dati e tutela della riservatezza. La privacy nella società dell'informazione* (Milano 1997) 285; F. CAGGIA, *Il consenso al trattamento dei dati personali nel diritto europeo*, in *Riv. dir. comm.*, 2019, 405-432.