Decision Support Systems and Education
J. Mantas et al. (Eds.)

doi:10.3233/978-1-61499-921-8-155

GDPR and Health Personal Data; Tricks and Traps of Compliance

Andrej OREL[a,1] and Igor BERNIK[b]
[a] *Marand d.o.o. Ljubljana, Slovenia*
[b] *University of Maribor, Faculty of Criminal Sciences and Security, Ljubljana, Slovenia*

Abstract. The GDPR fixes general rules applying to any kind of personal data processing as well as specific rules applying to the processing of special categories of personal data such as health data taking place in the context of scientific research or clinical software development. A short overview of new rules about how to consider where scientific and professional projects include the processing of personal health data, genetic data or biometric data and other kinds of sensitive information whose use is strictly regulated by the GDPR is provided. Some key facts to researchers and developers to adapt their practices and ensure compliance to the EU laws are included.

Keywords. GDPR, privacy, EU, e-health, research, development

1. Introduction

After a long and intense reform, the European Union (EU) adopted the new Regulation (EU) 2016/679 [1] 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. It is the General Data Protection Regulation (GDPR). With the GDPR, the EU reaffirms its attachment to the protection of fundamental rights and freedoms of individuals, notably those related to the protection of individuals' privacy including the specific fundamental right to personal data protection enshrined within the Charter of the Fundamental Rights of the EU

The GDPR performs several updates [2] and introduces new individual rights and procedures of importance, which affect scientific research activities. The GDPR applies to the data controllers and processors acting in the public and private sectors for profitable and not-profitable purposes. It differentiates between two kinds of personal data by strictly regulating the processing of special categories of data (the so-called 'sensitive personal data' such as health data, genetic data and biometric data) because of their potential risks regarding the rights and freedoms of the data subject. It considers scientific research activities as a specific context of personal data processing where the equilibrium between individual freedom [3] and the freedom of research triggers particular challenges and ethical issues.

[1] Corresponding Author, Andrej Orel, Marand d.o.o., Koprska ulica 100, SI-1000 Ljubljana, Slovenia; E-mail: andrej.orel@marand.si.

2. Methods

The GDPR maintains the approach of the previous Directive by fixing general principles, which are to be observed in any context of personal data processing, including in research and development, and for archiving purposes in the public interest, and regardless of the kind of personal data, including to the processing of data qualified as sensitive personal data. Nevertheless, the GDPR adds three new general principles of importance.

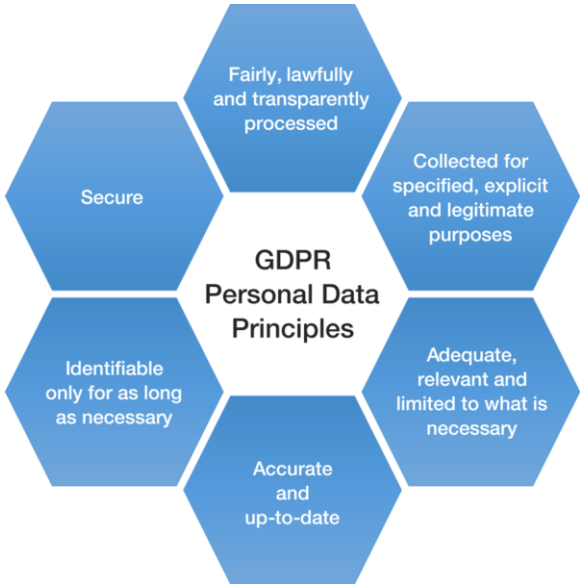

Figure 1. The GDPR principles.

The first new general principle, states that personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject; collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; 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; 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.

The next principle is about respect of the data integrity and of their confidentiality. This principle imposes that the data be processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. This principle will find application not only through the enforcement of health professional rules and research ethics guidelines, such as those ensuring scientific and research integrity, but also through technical measures, such as the use of coding techniques (e.g. pseudonymisation, cryptography or anonymisation technics), the use of protected servers against external threats, closed-controlled system of data processing etc.

The third new principle states that, the controller shall be responsible for, and be able to demonstrate compliance with the general principles of data processing. This necessitates, in particular, that the controller or its representatives in the EU, and the processors organize and maintain clear and secured records of any data processing activities performed in order to be able to demonstrate compliance with the GDPR. In research, such records can constitute archives to be retained for a certain period according to applicable law.

3. Results and discussion

Understanding the legal terminology is paramount for ensuring its proper dissemination and application. In the field of research, lawyers met difficulties in understanding and circumventing notions, which are very scientifically based and depend on the evolution of technologies and contexts. With the GDPR, we can salute the work that has been done by the EU legislator to design several definitions of direct utility in the context of scientific research and that represent the new common benchmark for the Member States. In particular, the GDPR introduces some new definitions of certain special categories of personal data whose processing is forbidden, by principle, but exceptionally admitted for research or archiving purposes in the public interest. Those are:

Figure 2. The GDPR data issues concerning health.

- "***Data concerning health***" means 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. There are further details about what shall be considered as personal health data under the GDPR, and we can

see that this notion is inclusively defined as '*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 status of the data subject*. This includes information about the natural person important for research such as a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived 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.'

- "***Genetic data***" [4] means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question. In addition to this, it is specified that genetic data can consist of '*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.*
- "***Biometric data***" [5] means personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

Regarding the condition of the data, the GDPR also adopts some definitions [6].

- "***Pseudonymisation***" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
- "***Anonymous data***" are defined as information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.

One of the most important issues, which is extremely important in e-health, is provided by the GDPR [1].

- "***Consent***" of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. This notion is specified regarding the unambiguous feature of the consent, which does not rise doubt about the scope of the activities agreed by the data subjects. The form of consent must be a statement or a clear affirmative action.

4. Conclusion

For the conclusion here are some rules regarding the reuse of personal data for research purposes. It is a daily practice in scientific research that personal data are used for a purpose that is different from the initial collection (also called 'secondary use' or 'further processing') and processed otherwise. Allowing this kind of processing is crucial as the access to personal data that can be reused for different objectives constitutes an essential activity for scientific and translational research.

As a general principle stated under Article 5 of the GDPR, the processing of personal data for purposes other than those for which the personal data were initially collected should only be allowed where the new purpose of the processing is compatible with the purposes for which the personal data were initially collected. This is a good news for health registries, cohorts and research bio-banking maintaining personal sensitive data available for future scientific or statistical reuses. However, this presumed compatibility is not fully automatic and must answer to several requirements such as the respect of data minimisation principle. Indeed, according to GDPR provisions, this further processing 'is to be carried out when the controller has assessed the feasibility to fulfil those purposes by processing data which do not permit or no longer permit the identification of data subjects (e.g. pseudonymisation of the data), and provided that appropriate safeguards exist (e.g. secured and separated storage of the identifiers (codes) and respect of the relevant ethical standards in the field).

Consent has always been a central ethical element for participating in research projects involving human beings. New research practices triggered debates in Europe about the risk that the GDPR require systematic consent before each and every data processing and around the necessity to allow the practice of broad consent intended to maximise the use of personal data, including sensitive data for several different and unknown research purposes.

Acknowledgement

I would like to thank the company Marand d.o.o., the producer of the ThinkEhr© platform, the finest building stone for health information systems in the OpenEhr© world, for generously supporting me at my studying the e-health security and privacy issues.

References

[1] Regulation (EU) 2016/679 of the EU Parliament and of the Council of 27 April 2016 (General Data Protection Regulation (GDPR)) *Official Journal of the EU*, 2016; L119/1-L119-88
[2] Directive 2011/24/EU of the EU Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare. *Official. Journal of the EU*, 2011; L88/45-L88/65
[3] Regulation (EU) 536/2014 of the EU Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use. *Official Journal of the EU*, 2014, L158/1-L158/68
[4] H.E. Check, Privacy protections: the genome hacker, *Nature* **497** (2013), 172–174.
[5] S.P. Murphy, *Healthcare Information Security and Privacy*, McGraw-Hill, New York, 2015.
[6] G.W. Van Blarkom, J.J. Borking, J.G.E. Olk, *Handbook of Privacy and Privacy-Enhancing Technologies - The Case of Intelligent Software Agents,* College bescherming persoonsgegevens*,* The Hague, 2003.