JOURNAL OF CLINICAL RESEARCH BEST PRACTICES

Vol. 15, No. 3, March 2019 "Happy Trials to You"

The European Union General Data Protection Regulation (GDPR)

The Most Important Change in Global Data Privacy Regulation in 20 Years

By Rupal V. Vora

Introduction

Effective as of May 25, 2018, the European Union (EU)'s General Data Protection Regulation (GDPR) replaced Directive 95/46/EC (General Data Protection Regulation), commonly referred to as the "Old Directive."

The GDPR applies to "natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data." The Regulation states that its objective is to "protect fundamental rights and freedoms of natural persons and, in particular, their right to the protection of personal data."

The GDPR applies directly to countries in the European Union, which include: Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the United Kingdom (UK). As of the date of this publication, the UK is scheduled to leave the EU on March 29, 2019. After "Brexit," the UK will likely have its own data protection regulation, which is currently anticipated to be similar to the EU's GDPR.

As a regulation under EU law, the GDPR applies directly across all European Economic Area (EEA) member states. The EEA includes the above-mentioned EU countries, as well as Iceland, Liechtenstein and Norway. Although Switzerland is not a member of either the EU or the EEA, it is part of the single market, which means the GDPR applies there, as well.[1]

Why Does the GDPR Matter in the U.S.?

GDPR Article 3 addresses the territorial scope of the Regulation. It states that the GDPR applies to all EEA entities and EEA personal data. GDPR Article 4 defines "personal data" as any information relating to an identified or identifiable natural person ("data subject").[2] The GDPR applies to any entity, *regardless of location*, that processes the personal data of data subjects who are in the EEA. In other words, if a clinical study includes data collected from any person in the EEA (even if they are just passing through) or processed in the EEA, that data is covered by the GDPR.

The GDPR applies to processing activities that fall under one of two scenarios. In the first scenario, an entity offers goods or services to data subjects in the EU, irrespective of any payment by the data subject. An example would be Amazon selling goods to people in the EEA. In the second scenario, the processing activities are related to the monitoring of behavior of people in the EEA. An example would be Facebook collecting data on the activities of their European users. GDPR Article 3, Recital 1 states that the GDPR applies to the processing of personal data of EEA data subjects, regardless of whether the entity processing it is located within the EEA.

Based on these scenarios, the GDPR has the potential to apply to all agreements with a European sponsor, a European contracting entity, or where European data is involved.

Although it is too early to know how vigorously the GDPR will be enforced, the penalties are significant. Maximum penalties are €20 million (approximately US$26 million, as of this writing) or 4% of the entity's worldwide annual revenue in the prior financial year.

Major Differences between HIPAA and the GDPR

The major U.S. data privacy regulation is the Health Insurance Portability and Accountability Act of 1996, as amended (HIPAA). There are significant differences between HIPAA and the GDPR. First and foremost, the set of data to which the GDPR applies is much broader than that covered by HIPAA. The GDPR applies to all "personal data" across all sectors of the economy. This definition is much broader than HIPAA, which addresses only personal identifiers and patient health information. Second, HIPAA concepts like de-identified data, limited data set, and protected health information (PHI) do not cleanly map to GDPR concepts. U.S. entities should include both HIPAA and GDPR requirements in contracts involving personal information, to ensure compliance with both regulations.

Key GDPR Terms

Interpreting the GDPR requires a basic understanding of several key terms defined in GDPR Article 4. As addressed previously, the GDPR applies to all "personal data," which includes any information relating to a "data subject." Data "processing" means any operation or set of operations performed on personal data. Examples of processing include collection, recording, storage, consultation, transmission and use of data. The GDPR applies to pseudonymized data, which is personal data that can no longer be attributed to a specific data subject without the use of additional information. In contrast, the GDPR does not apply to anonymized or anonymous data, per GDPR Recital 26. Anonymized data is information that does not relate to an identified or identifiable natural person.

A GDPR "controller" determines the purposes and means of processing personal data. In contrast, a "processor" simply processes personal data on behalf of the controller. In some cases, both parties to a contract could be determining the purpose and means of processing the personal data. In such situations, the parties would be "joint-controllers," and each would have to comply with the obligations of a controller.

Under the previous Directive 95/46/EC, which was repealed under the new GDPR, the European Commission established "standard contractual clauses" to address the transfer of personal data to processors in "third countries" (countries outside the EEA). Until the European Commission updates these clauses per the new GDPR, the standard contractual clauses seem to apply.

Responsibilities and Obligations under the GDPR

GDPR Article 5 outlines the controller's obligations, which are more significant than the obligations of processors. Controllers must ensure the personal data is (a) processed lawfully; (b) collected for specified, explicit and legitimate purposes; (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; (d) accurate and kept up to date, with every reasonable step being taken to ensure that personal data that are inaccurate are erased or rectified without delay; (e) kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; and (f) processed in a manner that ensures appropriate security of the personal data.

Controllers must engage processors that provide sufficient guarantees to implement appropriate technical and organizational measures. A controller is obligated to engage in a

contract that is binding on the processor and addresses the following items: sets out the subject-matter and duration of the processing, describes the nature and purpose of the processing, describes the type of personal data, lists the categories of data subjects, and outlines the obligations and rights of the controller.

GDPR Article 28 outlines the responsibilities of processors who act on behalf of the controller: A processor shall not engage another processor (also referred to as a "subprocessor") without the controller's prior specific or general written authorization. The written contract between a controller and a processor shall state that the processor has the following duties:

> (a) processes the personal data only on documented instructions from the controller, including transfers of personal data to a third country, (b) ensures that persons authorized to process the personal data have committed themselves to confidentiality, (c) takes all measures to ensure security of processing, addressed in GDPR Article 32, (d) ensures engagement of subprocessors follows stipulations of GDPR Article 28, including written authorization from controller and a binding contract on subprocessor, (e) taking into account the nature of the processing, assisting the controller by appropriate technical and organizational measures, insofar as this is possible, (f) assists the controller in ensuring compliance with its obligations under GDPR, taking into account the nature of processing and the information available to the processor, (g) at discretion of the controller, the processor shall delete or return all personal data after the end of the provision of services relating to processing, and deletes existing copies unless EU or Member State law requires storage, and (h) makes available to the controller all information necessary to demonstrate compliance with GDPR obligations and allow for audits.

As the requirements above demonstrate, the processor's primary responsibility is to assist the controller in meeting its requirements under the GDPR. In addition, the processor must maintain a record of all categories of processing activities carried out on the controller's behalf. The processor must also immediately inform the controller if, in the processor's opinion, an instruction infringes the GDPR or other EU or member state data protection provision.[3]

Data Use for Scientific or Research Purposes

GDPR introductory notes seem to indicate that the regulation's primary objective is to protect data from large data controllers, such as social media firms that collect and store personal data for commercial and professional use. A natural question is, therefore, how does the GDPR apply to academic use and scientific research? GDPR Article 89 addresses the "Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes." The GDPR states that the processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. Further processing for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes should be considered to be compatible lawful processing operations under the GDPR.

The GDPR provides this additional guidance regarding future use of scientific or research data: "In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, *inter alia*: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the

reasonable expectations of data subjects based on their relationship with the controller as to their further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations."[3]

GDPR Article 89 addresses processing with purposes rooted in the public interest, scientific research, historical research, or statistics. Article 89 broadly outlines safeguards that should be in place when processing data for research purposes, including pseudonymization of data or anonymizing data when the purpose can be achieved using those means. The research exception in the GDPR seems to account for data processing in the public interest, scientific research, historical research, or statistical purposes.[4]

GDPR Article 89 appears to apply to the subsequent use of data collected in the two commercial scenarios above, rather than to data collected initially for scientific purposes, e.g., in a clinical study. In other words, GDPR seems to be intended to cover commercial, rather than scientific, purposes, which is a good sign for clinical research, especially when conducted by academic and nonprofit institutions.[5]

Conclusion

Clarification of the above issues, as well as many others, requires guidance from the European Commission or testing in enforcement and subsequent litigation. In the meantime, the best option is to comply with the letter of the GDPR to the extent practical and, where specifics are lacking, comply with its spirit.

References

1. https://eugdpr.org/
2. https://www.enterpriseready.io/gdpr/how-to-read-gdpr/
3. GDPR Full Text: 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)
4. https://iapp.org/news/a/how-gdpr-changes-the-rules-for-research/
5. https://www.mwe.com/en/thought-leadership/publications/2018/02/does-gdpr-regulate-research-studies-united-states

Author

Rupal V. Vora, J.D. is a Senior Contracts Associate at Duke Clinical Research Institute, Duke University. Contact her at rupal.vora@duke.edu.

