# General Data Protection Regulation and Research in the United States

Save to myBoK

By Shamsi Daneshvari Berry, PhD, MS, CPHI, and Jill Flanigan, MLS, MS, RHIT

The European Union (EU) protects the personal information of EU citizens through the General Data Protection Regulation (GDPR),[1] which went into effect on May 25, 2018 and replaced the Data Protection Directive.[2] The GDPR details some new rights of EU citizens and other European Economic Areas (EEA) such as Norway, Iceland, and Liechtenstein.[3]

Specifically, it impacts the right to:

- Know who is processing one's data, what data they are looking at, and why they are doing it
- Request an organization to inform one of the personal data it has in its system
- Request that personal data gets sent and exchanged between providers
- Have information deleted from specific systems
- Be asked before a company processes one's data
- Be informed of a data breach
- Have clear, straightforward language in privacy policies[4]

The key to these new rights is that they apply across the EU, regardless of where the data is stored or processed. The law also applies to non-EU companies—including those in the US—who collect or process the personal data of an individual residing in the EU when the data is collected or processed. This means even US companies and healthcare organizations can be covered by the law.

## GDPR and Personal Data

The regulation covers personal data that can be identified directly or indirectly through a "name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person," the regulation states.[5] This personal data can be used for research purposes but is subject to conditions unless it would "seriously impair" the research aims.[6] The purpose is to minimize the amount of personal data used in research. Although there are similar privacy efforts in the United States, there are some additional constraints that raise issues when it comes to international research involving the EU or EEA.

In addition, certain categories of personal data are considered especially sensitive and receive additional protection under Article 9 of the GDPR. Processing data described under Article 9 is prohibited unless a specific exception applies. The special categories include, "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 sole purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation… ."[7] In legal terminology, a natural person is one who is a human as opposed to a corporation.

Under the GDPR, there are three main differences from the previous directive that affect research. First, a person must consent in accessible language to have their personal data used.[8] They have the right to withdraw from the study as well as "be forgotten," which involves erasing their data from the system—not just eliminating it from processing.[9] Therefore, any study must receive consent from all participants unless the data set is anonymized. (Pseudonymized data, under Recital 26, is considered personal data.[10]) Thankfully for researchers there is a workaround that individuals can consent to "areas of research." Additionally, Recital 51 also allows for medical research that is in the public's interest.[1]11

Consent must be explicit for all categories of personal data that may be processed during a research study. Organizations engaged in research may be prepared to obtain clear consent for the use of health data, but if in the course of research data

on ethnicity, sexual orientation, or other protected categories is collected then researchers must ensure that they obtain explicit consent for the use of data in any of the special categories.[12]

The GDPR-covered person has the right to be forgotten, also known as the right to erasure. This may occur if consent is withdrawn, when the data is no longer needed, or other circumstances where the data is required to be erased to comply with other regulations or if there has been a violation of the data protection regulation.[13]

Second, data sharing outside the EU is allowed as long as the rights of the individual are not lessened in the country receiving the data.[14,15] In other words, if you are sharing EU medical data within the United States, the data must be HIPAA-compliant as well as GDPR-compliant.

Third, data must be portable.[16,17] This means that the individual must be able to get a copy of their data that is in a common machine-readable format. Article 20 of the GDPR describes the right of portability. The individual can request the data be provided directly to another entity that will control the data. The need to be able to provide the data copy will influence how the organization stores the data.[18]

## GDPR and the United States

If you are based in the US, the GDPR applies to you if you are using research subjects in the EU and EEA or are recruiting subjects in that region.[19] However, data is not just personal data because it involves a citizen of the EU or EEA. The data must be collected on them while they are located in the EU or EEA. Therefore, if an EU citizen travels to the US and requires healthcare, the GDPR does not apply.[20] It would only apply if the individual was recruited to use that healthcare system while still in the EU and EEA or if they were followed up with by a physician or researcher after returning to the EU.[21,22]

If the GDPR does apply to research, one important difference in comparison to HIPAA is the higher standard applied to de-identification. A data set is not considered de-identified if there is any reasonable way to directly or indirectly identify the individual or if a key code exists.[23]

## Notes


1. Official Journal of the European Union. “General Data Protection Regulation 2016/679/EU.” April 27, 2016. https://publications.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-en.
2. Ibid.
3. Broccolo, Bernadette M., Daniel F. Gottlieb, and Ashley Winton. “Does GDPR Regulate Clinical Care Delivery by US Health Care Providers?” *The National Law Review*. February 26, 2018. www.natlawreview.com/article/does-gdpr-regulate-clinical-care-delivery-us-health-care-providers.
4. Cornock, Marc. “General Data Protection Regulation (GDPR) and implications for research.” *Maturitas*. May 2018. www.maturitas.org/article/S0378-5122(18)30036-7/fulltext.
5. Rumbold, John Mark Michael and Barbara Pierscionek. “The Effect of the General Data Protection Regulation on Medical Research.” *Journal of Medical Internet Research*. February 24, 2017. www.ncbi.nlm.nih.gov/pmc/articles/PMC5346164/.
6. Official Journal of the European Union. “General Data Protection Regulation 2016/679/EU.”
7. Ibid.
8. Ibid.
9. Cornock, Marc. “General Data Protection Regulation (GDPR) and implications for research.”
10. Rumbold, John Mark Michael and Barbara Pierscionek. “The Effect of the General Data Protection Regulation on Medical Research.”
11. Official Journal of the European Union. “General Data Protection Regulation 2016/679/EU.”
12. Ibid.
13. Ibid.
14. Rumbold, John Mark Michael and Barbara Pierscionek. “The Effect of the General Data Protection Regulation on Medical Research.”
15. Cornock, Marc. “General Data Protection Regulation (GDPR) and implications for research.”
16. Official Journal of the European Union. “General Data Protection Regulation 2016/679/EU.”
17. Cornock, Marc. “General Data Protection Regulation (GDPR) and implications for research.”

18. Official Journal of the European Union. "General Data Protection Regulation 2016/679/EU."
19. Broccolo, Bernadette M., Daniel F. Gottlieb, and Ashley Winton. "Does GDPR Regulate Clinical Care Delivery by US Health Care Providers?"
20. Rumbold, John Mark Michael and Barbara Pierscionek. "The Effect of the General Data Protection Regulation on Medical Research."
21. Ibid.
22. Broccolo, Bernadette M. et al. "Does GDPR Regulate My Research Studies in the United States?" The National Law Review. February 5, 2018. www.natlawreview.com/article/does-gdpr-regulate-my-research-studies-united-states.
23. Ibid.

Shamsi Daneshvari Berry (srberry@umc.edu) is an assistant professor at the University of Mississippi Medical Center. Jill Flanigan (jflanigan@mxcc.edu) is an assistant professor and HIM coordinator at Middlesex Community College.

**Article citation**:
Berry, Shamsi Daneshvari and Jill Flanigan. "General Data Protection Regulation and Research in the United States." *Journal of AHIMA* 90, no. 1 (January 2019): 28-29.