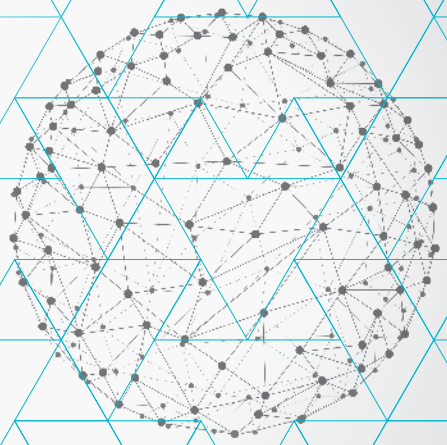
ADDI
Alzheimer's Disease
Data Initiative

Q&A:
Impact of General Data Protection Regulation (GDPR) On Research Projects Involving the European Economic Area (EEA)[1]



These questions and answers are designed to assist researchers in understanding some of the legal considerations under the GDPR that arise when initiating a research project with an EEA institution or involving data obtained from an EEA institution. This brief Q&A is not comprehensive of all legal considerations; each researcher should consult with his or her own legal counsel before entering into any data sharing arrangement.

UPDATED DECEMBER 2020

What is the GDPR?

The GDPR is a law that has, since it came into effect on May 25, 2018, created new obligations for organizations that collect, use, and store personal data obtained from data subjects in the EEA. The GDPR was enacted to strengthen and harmonize privacy rights across the EEA, superseding the prior EU Data Protection Directive (1995). The directive provided general principles, which were adapted in different manifestations across the EEA Member States. The GDPR can affect scientific research conducted by academic medical centers, other research organizations, and industry in the U.S. and other countries when personal data used in the research originate in the EEA.

[1] The European Economic Area ("EEA") includes the 27 member states of the European Union and three additional countries: Iceland, Liechtenstein and Norway. As of the date of this guide, the United Kingdom is expected to continue to apply the GDPR even following the United Kingdom's recent departure from he European Union, commonly referred to as "Brexit."

Will the GDPR apply to my research activity?

The GDPR applies to entities that process personal data, including when the processing is performed for research studies. The GDPR can apply extraterritorially to researchers located outside of the EEA in certain contexts when such researchers gather personal data pertaining to EEA data subjects in connection with offering goods or services to data subjects located in the EEA or when monitoring the behavior of data subjects who are located in the EEA. The GDPR generally would not apply directly to a researcher located outside of the EEA who receives data from an EEA researcher or institution for secondary research; however, the GDPR requires that such international data transfers be conducted under a framework that may extend GDPR-level protections to the data (discussed below).

Does the GDPR apply to U.S. citizens who are in the EEA or to EEA citizens who are in the U.S.?

The GDPR is agnostic to citizenship. Thus, the GDPR applies to the processing of personal data of data subjects who are located in the EEA, regardless of their citizenship. In contrast, and notwithstanding some limited exceptions, the GDPR generally does not apply to the processing of personal data collected from EEA citizens who are located in the U.S.—whether visitors or permanent residents.

Will the data in my study be considered "personal data" subject to the GDPR?

For purposes of the GDPR, the term "personal data" refers to any information that relates to an identified or identifiable natural person, which the GDPR refers to as a "data subject." Personal data may include data that could be attributed to a data subject through the use of additional data, even if those data come from a third-party. "Pseudonymized" or "key-coded" data are typically considered to be "personal data," even when used by a person who lacks access to a key needed to re-identify such data.

Does the GDPR treat sensitive personal data, like medical records, differently?

There is a subset of personal data, referred to in the GDPR as "special categories" of personal data, which are afforded a higher level of protection under the regulation. (See below for more information on processing special categories of personal data.) These categories include several types of data that are often collected as part of a research study, including information about a data subject's health, genetics, race or ethnic origin, biometrics for identification purposes, sex life or sexual orientation, political opinions, religious or philosophical beliefs or trade union membership.

What if the data I receive are aggregate or summary level data?

Aggregate and summary level data generally do not pertain to an identified or identifiable natural person, and thus they would not constitute "personal data" subject to GDPR.

If the data I receive are key-coded, does the GDPR apply?

The GDPR considers "pseudonymized data," such as key-coded data, to be "personal data" subject to all regulatory protections of the GDPR. In this respect, the GDPR diverges from the position under many U.S. research and privacy laws such as the Common Rule and HIPAA.

How can personal data be removed from the GDPR's requirements?

The GDPR does not apply to data that have been "anonymized." Unlike HIPAA, the GDPR affords no "safe harbor" pursuant to which data can be rendered de-identified by removing a specific list of identifiers. Rather, the GDPR judges anonymization on a facts-and-circumstances basis, taking into account all the means reasonably likely to be used, either by the controller or by another person, to identify the natural person directly or indirectly. Given this definition, anonymization is a high standard that can be difficult to meet in practice, but some third-party entities (e.g., UK Medical Research Council, UK Anonymisation Network) have published their own anonymization recommendations.

Will my institution or I be considered a "controller" or a "processor"?

The obligations and responsibilities imposed on organizations by the GDPR vary depending on an organization's roles in the processing of personal data, with the GDPR imposing more requirements on "controllers" than on "processors." Whether an entity is a controller or processor is a facts-and-circumstances test that depends on the entity's freedom with respect to the data. A "controller" is an entity that alone, or in conjunction with others, is responsible for rendering key decisions about the means and purposes of processing personal data. A "processor" refers to an entity that performs data processing on a controller's behalf, such as a fee-for-service vendor.

What do data subjects need to be told about my research?

The GDPR requires that controllers provide to data subjects notices describing various details of data processing, including the identity of the controller and the purposes of, and lawful bases for, processing. In the research context, the elements of the GDPR notice are generally incorporated into an informed consent form. When a controller does not collect data directly from the data subject, as in secondary research, notice may not be required when it would prove impossible or would involve a disproportionate effort.

What bases allow me to process personal data?

In all cases, even when notice is not required to be given to the data subject, a controller must have a lawful basis to process personal data to which the GDPR applies. The GDPR's bases for processing personal data include consent of the data subject, necessity for compliance with a legal obligation, necessity for a task carried out in the public interest, and necessity for legitimate interest of the controller. When the controller processes "special categories" of personal data (which is often the case for research activities), an additional basis must be identified for processing the personal data. Some potentially applicable bases for research include explicit consent, necessity for reasons of public interest

in the area of public health, and necessity for scientific research purposes in accordance with EU or EEA member state law.[2] One evolving point of regulatory interpretation of which researchers should be aware is that some data protection authorities take the position that consent should not be the basis for processing personal data in connection with an interventional medicinal clinical trial.

What bases allow research processing of data that were originally gathered for a non-research purpose?

When data originally collected for another purpose, such as clinical care, are processed for research purposes, the research subject often will not have consented to the specific processing involved in the study. Some regulatory guidance disfavors the use of broad consent to future data processing under the GDPR, notwithstanding that GDPR Recital 33 states that, "[i]t is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research. . . ." The Article 29 Working Party's guidance on consent took a narrower view with respect to the application of this recital, noting that "Recital 33 does not disapply the obligations with regard to the requirement of specific consent." Likewise, the European Data Protection Supervisor recently reaffirmed the Working Party position, noting:

> Specific consent normally required under GDPR may therefore become less appropriate in the case of collected and inferred data and especially in the case of special categories of data on which much scientific research relies. Recital 33 does not however take precedence over the conditions for consent set out in Articles 4(11), 6(1)(a), 7 and 9(2)(a) of GDPR, and it requires the controller to carefully evaluate the rights of the data subject, the sensitivity of the data, the nature and purpose of the research and the relevant ethical standards. Therefore, when research purposes cannot be fully specified, a controller would be expected to do more to ensure the essence of the data subject rights to valid consent are served, including through as much transparency as possible and other safeguards.[3]

Therefore, researchers typically rely on other lawful bases to process data in secondary research, including compatibility, legitimate interests, scientific research and public interest in the area of public health.

Does the GDPR require study subjects who were consented prior to the GDPR's May 25, 2018 effective date to be re-consented?

No, provided that the historic consent is consistent with the GDPR's requirements.[4]

---

[2] The GDPR expressly permits Member States to enact additional conditions and limitations with regard to the processing of genetic data, biometric data, or data concerning health. *See* GDPR art. 9(4).

[3] EDPS, *A Preliminary Opinion On Data Protection And Scientific Research* at 19 (Jan. 6, 2020), https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf.

[4] *See* GDPR, Recital 171 ("Where processing is based on consent pursuant to Directive 95/46/EC, it is not necessary for the data subject to give his or her consent again if the manner in which the consent has been given is in line with the conditions of this Regulation, so as to allow the controller to continue such processing after the date of application of this Regulation.").

What does the GDPR require for personal data to be transferred from the EEA to countries, such as the U.S., that have not been found by the European Commission to have "adequate" data protection legislation?

The GDPR generally prohibits the transfer of personal data from the EEA to a country or international organization outside the EEA (known as a "third country") unless the European Commission has found the recipient country to have adequate data protection legislation (referred to as an "adequacy decision") or unless the transferor puts in place a legal basis for the data transfer.[5] The U.S. has not been granted an "adequacy decision."

The GDPR permits the transfer of personal data to countries lacking an adequacy decision based on certain legal bases, which include but are not limited to the following: (i) obtaining the consent of the data subject to the transfer after warning the data subject of the risk of the transfer, (ii) entering standard contractual clauses ("SCCs") published by the European Commission with the party transferring the data,[6] (iii) where the transfer is necessary for important reasons of public interest, and (iv) where the transfer is necessary for the protection of the "vital interests" of the data subject (typically restricted to "life and death" situations).

In summer 2020, the Court of Justice of the European Union ("CJEU") invalidated the EU-U.S. Privacy Shield, which previously had served as a basis for certain for-profit U.S. companies to receive transfers of data from the EEA.[7] The CJEU decision also requires that data exporters perform independent assessment of the recipient country's data protection standards when SCCs are used in order to ensure that the transfer under the SCCs in fact affords a level of data protection equivalent to the EEA.[8] The European Data Protection Board issued guidance on November 10, 2020 comprising a "roadmap of steps" as to how data exporters should be accountable with respect to evaluating data exports from the EEA.[9] The guidance emphasizes the need to assess whether the planned transfer mechanism (such as the SCCs) is effective in light of all the circumstances of the transfer. The decision notes that data exporters might need to put in place supplementary measures to offer additional protection

[5] A list of countries for which the European Commission has granted an "adequacy decision" can be found here: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

[6] The standard contractual clauses can be found here: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.adequacy-decisions_en.

[7] *See Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems,* Case C-311/18.

[8] *See* id. (finding that the GDPR "must be interpreted as meaning that the appropriate safeguards, enforceable rights and effective legal remedies required by those provisions must ensure that data subjects whose personal data are transferred to a third country pursuant to standard data protection clauses are afforded a level of protection essentially equivalent to that guaranteed within the European Union by that regulation, read in the light of the Charter of Fundamental Rights of the European Union. To that end, the assessment of the level of protection afforded in the context of such a transfer must, in particular, take into consideration both the contractual clauses agreed between the controller or processor established in the European Union and the recipient of the transfer established in the third country concerned and, as regards any access by the public authorities of that third country to the personal data transferred, the relevant aspects of the legal system of that third country, in particular those set out, in a non-exhaustive manner, in Article 45(2) of that regulation.").

[9] *See* Recommendation 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (adopted Nov. 10, 2020) https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransf erstools_en.pdf.

to data. The EDPB provides as one example of such supplementary measures pseudonymizing data before transferring the data to a third country for analysis and ensuring that the additional information needed to link the pseudonymized data to the individual data subject's identity remain in the EEA or a third country that has obtained an adequacy decision.

In response to the CJEU decision, the European Commission released in November 2020 new draft SCCs, which were open to public comment until December 10, 2020.[10]

What other requirements and obligations apply to research organizations that process personal data under the GDPR?

Controllers have a variety of obligations, including providing notice of processing to data subjects and vindicating data subjects' rights (access, rectification, data portability, erasure, restriction of processing, objection, etc.).

[10] *See* https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries.