GDPR GUIDELINES FOR HUMAN SUBJECTS RESEARCH STUDIES

November 9, 2019

The EU General Data Protection Regulation (**GDPR**) is a European prvacy and data protection law that went into effect May 25, 2018. **These Guidelines address the application of the GDPR to human subjects research involving clinical or medical studies**. The GDPR is a very complex law and is further complicated by the fact that individual countries located in the European Economic Area[1] (**EEA**) may have additional laws and regulations that could impact the treatment of research data. As a result, these Guidelines provide only a summary of the most important GDPR concepts. The University's Office of the General Counsel (**OGC**) is charged with interpretation of the GDPR and should be contacted with any questions not answered by these Guidelines.

What does the GDPR require for human subjects research studies?

For human subjects research studies that involve enrollment of individuals (**Research Subjects**) located in the EEA (**EEA Research Subjects**), the GDPR requires certain information to be provided to the Subjects *in addition to* the information required by the U.S. Common Rule (45 CFR 46, Subpart A) in an informed consent form (a **Common Rule Consent Form**).

Specifically, the following GDPR information must be provided to EEA Research Subjects:

- A privacy notice describing how the EEA Research Subjects' Personal Data (as defined below) will be used, shared, and handled, as well as the rights afforded to them under the GDPR (the **GDPR Privacy Notice**); and
- A GDPR consent form that EEA Research Subjects must sign to provide consent to the use of their Personal Data in the research study (the **GDPR Consent**).

A template document that includes both the GDPR Privacy Notice and GDPR Consent language may be found here, in the "General Data Protection Regulation" section: https://research.columbia.edu/human-research-policy-guide. The GDPR Privacy Notice and GDPR Consent language may be added to a Common Rule Consent Form. In that way, the EEA Research Subject will need to sign only one document to provide both the informed consent required by U.S. federal law and the GDPR Consent, and to receive the GDPR Privacy Notice.

Human subjects research studies conducted in the United States by Columbia researchers may also be required to comply with the GDPR if the research involves collecting or processing Personal Data from non-EEA subjects while they are located in the EEA.

What if the human subjects research study has a Sponsor (other than Columbia) located in the EEA, but the study does not involve enrollment of EEA Research Subjects?

[1] The European Economic Area consists of the following countries: Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and (for the present) the UK.

The GDPR will likely apply to the Sponsor located in the EEA because the Sponsor has an establishment in the EEA. Whether the Sponsor is a "controller" under the GDPR for the purposes of the study will depend on the nature of the project and the degree of involvement the Sponsor has with the collection, processing, and use of Personal Data. Where the Sponsor in the EEA is a controller, the Sponsor will likely be required to provide Research Subjects with a GDPR Notice and obtain any required GDPR Consents. In this case, the Sponsor may request Columbia to assist with delivering GPDR Notices and obtaining GDPR Consents (even if the Research Subjects are not located in the EEA).

However, if the Sponsor is not receiving Personal Data (if the data is anonymized under the GDPR, as discussed below) or if the Sponsor is not involved in data collection or designing the research protocol, then the study may not be subject to the GDPR, especially if the study does not involve EEA Research Subjects.

Please contact the OGC for further guidance if you are working on a study that has a Sponsor located in the EEA. It is important that you contact the OGC at the outset of the study, as the GDPR analysis may affect the nature and structure of the proposed research and/or collaboration.

What if the human subjects research study data is collected by Columbia from EEA Research Subjects who are participating in a research study while temporarily located in the U.S.?

In this instance (and where the Sponsor is not located in the EEA), the GDPR likely will not apply to the study, unless the Columbia researcher continues to monitor the EEA Research Subjects or provides after-care to them after they return to the EEA.

What is Personal Data under the GDPR in research studies?

Personal Data broadly means any information relating to an identified or identifiable natural person. An identifiable natural person is "one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person."

The following categories of Personal Data are considered to be "sensitive data" under the GDPR (**Sensitive Personal Data**):

- Health information, genetic data or biometric data;
- Information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; and
- Information about a person's sex life or sexual orientation.

The GDPR does not apply to Personal Data that has been anonymized. The GDPR has strict requirements for the anonymization of Personal Data. Whether Personal Data is anonymized is judged on a facts and circumstances test and there is no "safe harbor" as there is under U.S. law,

so data that has been deemed to have been "de-identified" under HIPAA and the Common Rule may not meet the GDPR's standards for "anonymized" data.

Key-coded research data is considered to be "Pseudonymized Data" and therefore Personal Data under the GDPR because the data can be attributed to a person by the use of additional information such as a key code. If the researcher maintains the key (or a third party maintains the key for the researcher), such data will generally not be treated as anonymized Personal Data under the GDPR. Full anonymization of Personal Data requires not only the removal of all identifiers from the data set, but also the destruction of any key codes.

If questions remain regarding whether Personal Data in a study may be considered to be "anonymized," please consult with the OGC.

Must a researcher also obtain an EEA Research Subject's GDPR Consent to process Personal Data for human subjects research purposes?

Yes. In most cases, Columbia will need to obtain an EEA Research Subject's GDPR Consent in addition to providing the GDPR Notice.

The processing[2] of an EEA Research Subject's Personal Data must have a lawful basis under the GDPR. One example of a lawful basis is the EEA Research Subject's consent. Consent must be freely given, specific, informed and unambiguous and must be given by a clear affirmative action such as a signature or checking a box on the GDPR Consent form. The use of Sensitive Personal Data requires "explicit consent," unless an exception has been met.

In lieu of obtaining explicit consent from EEA Research Subjects, the GDPR permits Columbia to conduct a scientific research study, even if it involves Sensitive Personal Data, when (a) the processing of the data is necessary for the study; (b) the study is based on European Union (EU) or EEA Member State law, such as the EU's Clinical Trials Directive; (c) the personal data is appropriately safeguarded through technical and organizational controls, and (d) certain other criteria are met.[3] In some cases, pseudonymization may be considered to be an appropriate safeguard. However, it is important to note that the ability to rely on the research exception varies between EEA Member States.[4]

---

[2] "Processing" means any action that is taken on Personal Data, including the collection, use, storage, analysis manipulation, and sharing of Personal Data with other parties.

[3] These additional criteria are: the processing of personal data must be proportionate to the aim of the activity; the processing of Personal Data must respect a research subject's right to the protection of their Personal Data; and the processing of Personal Data must include measures to safeguard the research subject's fundamental rights and interests. *See* GDPR, Article 9(2)(j).

[4] For example, the UK Medical Research Council has issued guidance, which states that "scientific research purposes in accordance with safeguards" (under Article 9(2)(j)) should be the primary lawful basis for processing rather than GDPR Consent. *See* GDPR: Consent in Research and Confidentiality, *available at:* https://mrc.ukri.org/documents/pdf/gdpr-guidance-note-3-consent-in-research-and-confidentiality. GDPR does not, however, affect legal requirements for consent to obtain samples from individuals (for example, when required under the UK Human Tissue Act) or for meeting the requirements of patient confidentiality. Notices need to set out the lawful basis relied upon for each instance of processing (for example, tissue sample gathering, sharing with third parties, and use for research purposes).

From a compliance point of view, the least risky approach is for the researcher to obtain GDPR Consent from the EEA Research Subject rather than relying upon this research exception.

To explore whether the foregoing exception to the GDPR Consent requirement applies to your study, please consult with the OGC.

Can a researcher obtain consent from an EEA Research Subject to use his/her Personal Data for future research?

In the U.S., obtaining authorization for a broad use of data and its use in future research is permitted by both HIPAA and the Common Rule. The GDPR recognizes that it is not always possible to fully identify the purpose of processing Personal Data for scientific research and states that Research Subjects should nonetheless be allowed to give their consent to general areas of scientific research when doing so is consistent with ethical standards.[5] On the other hand, the GDPR suggests that a researcher should re-contact and obtain additional consent for each subsequent step in the project instead of obtaining consent for future research activities at the outset of the project, but this is generally not feasible and may be confusing to the Research Subjects.

There are certain measures that Columbia may take when obtaining EEA Research Subjects' consent for future research activities, such as providing Research Subjects with options to consent to only certain categories of future research or providing notices on an ongoing basis regarding future research activities as they unfold. Note that use of Personal Data for purposes other than research purposes, such as sharing with charities, commercial partners, or other institutions, will likely go beyond the scope of the original consent. It is important to describe in as much detail as possible any anticipated use cases in the GDPR Notice and/or GDPR Consent. The purposes underlying those use cases must be clear so that an individual understands what he or she is giving permission for and how to object. These measures may reduce the risk of noncompliance under the GDPR with respect to obtaining consent for future research activities.

If your study will involve the use of Personal Data for future research purposes, please consult with the OGC.

Can an EEA Research Subject withdraw a GDPR Consent?

Yes. An EEA Research Subject who has given GDPR Consent has the right to withdraw his/her consent.

Upon an EEA Research Subject's withdrawal of his/her GDPR Consent, the researcher generally can no longer retain the Subject's Personal Data for the purpose of research, including data in key-coded form, and must destroy or anonymize the data. The exception to this rule is that the

[5] *See* GDPR, Recital 33.The Article 29 Working Party in their *Guidelines on Consent under Regulation (2016/679)* states that applying the flexible approach of Recital 33 "will be subject to a stricter interpretation and requires a high degree of scrutiny." According to the Guidelines, scientific research projects can only include personal data on the basis of consent if they have a "*well-described purpose*," and Recital 33 cannot be used as a way to navigate around the key principle of specifying purposes for which consent of the data subject is asked.

researcher may retain the Personal Data if it is necessary for adverse event reporting, for legal or regulatory compliance reasons, or for maintaining the integrity of the study.

Note that if the EEA Research Subject's Personal Data were anonymized in accordance with GDPR requirements *before* his/her withdrawal of GDPR Consent, the researcher may continue to use the anonymized data for research activities.

If an EEA Research Subject withdraws from participation in a study and/or withdraws his/her GDPR Consent, please consult with the OGC.

May an EEA Research Subject's Personal Data be transferred to the United States?

In some cases, Columbia will need to transfer an EEA Research Subject's Personal Data from the EEA to Columbia's research site in the U.S. The GDPR requires appropriate safeguards for the transfer of an EEA Research Subject's Personal Data to the U.S.

For example, the GDPR provides the option of obtaining the EEA Research Subject's consent to the transfer of his/her Personal Data to the U.S. Sample consent language is included in the template GDPR Notice and Consent document that may be found here, in the "General Data Protection Regulation" section: https://research.columbia.edu/human-research-policy-guide.

The Personal Data to be transferred may not have been collected by the Columbia researcher; for instance, Columbia may be receiving Personal Data that was collected by an entity in the EEA for research or non-research purposes (*e.g.*, school, legal or medical records). If the Personal Data being transferred is obtained from such an entity, Columbia may enter into a Data Protection Agreement with the entity in the EEA that was responsible for collecting Personal Data. The Data Protection Agreement is required to include certain terms for safeguarding the Personal Data, such as "Standard Contractual Clauses" published by the European Commission.

Transfer of Personal Data to Columbia in the U.S. is permitted if such Data are properly anonymized in compliance with the GDPR.

Please consult with the OGC to determine whether entering into a Data Protection Agreement would be appropriate for your research study and to obtain a template agreement.

***

Please note that these Guidelines do not include procedures for the implementation of all of the GDPR's various requirements, such as the obligation to respond to EEA Research Subjects' requests to access, amend, or delete their Personal Data, and the additional requirements for Sensitive Personal Data.

If you have questions regarding the GDPR or any implementation issues, please contact the OGC.