

December 13, 2018

To: IRB Directors, Research Administrators, Researchers, and Research Staff

Subject: General Data Protection Regulation Notice and Consent Requirements

Purpose

This memo provides information on the European Union’s [General Data Protection Regulation](#) notice and consent requirements in informed consent forms.

Background

The General Data Protection Regulation (“GDPR”) is a European privacy law in effect as of May 25, 2018. GDPR protects the personal data of individuals located in the European Economic Area (EEA), which includes the European Union, the United Kingdom, Iceland, Liechtenstein and Norway. When organizations, including the University of California (UC), offer goods or services to people in the EEA or monitor the behavior of individuals in the EEA, any Processing of Personal Data must meet the requirements of GDPR. This includes UC’s research activities that involve the collection or analysis of Personal Data from individuals living in the EEA.

Under GDPR, “Personal Data” refers to any information that can identify, or be used to identify individuals located in the EEA, otherwise known as a Data Subject. The law affords Data Subjects certain rights relating to the processing of their Personal Data. “Processing” broadly refers to any use of Personal Data, and includes accessing, storing, combining and even deleting Personal Data. Further, Data Subjects have even greater rights under GDPR with respect to how more sensitive data, such as racial, ethnic, or health-related data, is processed.

Among other requirements, GDPR requires that Data Subjects, including research subjects, be informed about the Processing of their Personal Data. This obligation to inform can be met by providing the proper information in a notice of privacy made available to Data Subjects. Other uses of Personal Data in the research context, specifically the use of more sensitive data, the transfer of Personal Data to the United States, as well as the use of Personal Data to make decisions or predictions that could significantly affect a Data Subject (such as using Personal Data to enroll a Data Subject in a placebo arm of a study), require consent from the Data Subject. The specific requirements of notice and consent under GDPR are described in the following sections.

Guidance

GDPR applies when Personal Data of research subjects located in the EEA¹ is collected or used by the research team or UC. Therefore, when GDPR applies, research subjects must be informed about the use of their Personal Data, and, where required by the GDPR, consent to the use of their Personal Data.

What is Personal Data?

“Personal Data” is defined as “any information that relates to an identified or identifiable natural person².” Different pieces of information, which, when collected or used together that can lead to the identification of a particular person, constitute Personal Data. The following types of Personal Data are some *examples* of Personal Data:

- A name and surname;
- A home address;
- An e-mail address of an individual;
- An identification card number;
- An Internet Protocol (IP) address;
- A browser or Internet cookie ID;
- Phone identifiers; or
- Demographic, behavioral or health-related information that could identify a person.

Personal Data is more broadly defined under GDPR than the types of data protected by any one U.S. federal or state privacy law, such as under the Health Insurance Portability and Accountability Act (HIPAA) or the Family Educational Rights and Privacy Act (FERPA).

“Pseudonymized Data,” or coded data, is Personal Data that 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 security measures to ensure that the Personal Data used in the research cannot be attributed to an identified or identifiable individual. GDPR considers Pseudonymized Data to be Personal Data even where one lacks access to the key-code required to link data to an individual data subject. This varies from U.S. privacy laws. For example, HIPAA provides a list of 18 data identifiers that, when removed, would render the data “anonymous.” However, under GDPR even if a data set removes all 18 identifiers that would render data de-identified under HIPAA, the data may still be subject to GDPR if it relates to individuals in the EEA.

Though Pseudonymized Data is still subject to GDPR, pseudonymization is one way UC can safeguard Personal Data. In fact, GDPR requires that organization consider pseudonymization as a security measure when appropriate.

¹ GDPR applies to individuals who are located in the European Economic Area, not “citizens” of the EEA. Therefore, it will apply where a UC researcher is conducting a study in the EEA that involves Personal Data, or where the UC researcher receives Personal Data from individuals in the EEA. Generally, GDPR will not apply when a UC researcher conducts research on Personal Data from an EEA citizen where the Personal Data is collected outside of the EEA (i.e., the research is conducted outside of the EEA).

² [Article 4\(1\)](#).

Data about individuals is not subject to GDPR only when it is anonymized. Anonymization is a high standard under GDPR: all direct and indirect identifiers of an individual must be removed, and UC must implement safeguards that ensure that the data can never be re-identified. For data to be truly anonymized under GDPR, the anonymization must be irreversible.

When GDPR Applies: Notice and Consent Requirements

GDPR requires that where Personal Data of a Data Subject in the EEA is collected, used, or accessed for research purposes, the researcher must provide the Data Subject specific information in a notice of privacy and, under certain circumstances, must also obtain the explicit consent of the Data Subject for certain Processing activities.

Notice Requirements

When Personal Data of an individual in the EEA is collected, used, or accessed for research purposes, GDPR requires that individuals be informed of the following information:

- The specific types of Personal Data collected and processed;
- The reasons, or purposes, for using the individual's Personal Data (i.e., using the Personal Data in order to conduct the research study);
- The expected duration for retaining Personal Data;
- The types of entities or individuals who will have access to or receive the Personal Data;
- A description of the individual's rights under GDPR (which should also include language that informs the Data Subject that their Personal Data will be protected under GDPR and how withdrawal of their consent to participate in the study will affect UC's subsequent use of their Personal Data);
- Notice that his or her Personal Data will be available in the United States (or other countries outside the EEA), and a description of how UC will protect the personal data;
- If Personal Data is being used to make decisions about the person or to create a profile, relevant information (this is discussed in more detail below); and
- Contact information for UC and the local privacy officer.

This information must be provided to Data Subjects located in the EEA in any research study that involves collecting or using their Personal Data.

If the Personal Data of an individual located in the EEA is used in research, where the Personal Data is provided to UC by a third party, individuals also must be informed of:

- The source of the data; and
- A description of the categories of personal data.

Consent Requirements

In addition to giving research subjects notice of the information required above, GDPR also requires that Data Subjects provide consent to certain Processing activities. GDPR stipulates that consent must be freely given, specific, informed and an unambiguous indication that the Data Subject has consented to the particular Processing of Personal Data.

Consent is required where:

1. Special Categories of Data, discussed below, are collected and processed;
2. Personal Data will be transferred to the United States, or even accessed in the United States; or
3. Personal Data is used to assign a research subject to receive, or not receive, a certain treatment in a study;

Each scenario requiring consent is discussed in more detail below.

1. Special Categories of Personal Data

Certain types of Personal Data require additional protection under GDPR. Generally, when research involves Special Categories of Personal Data, the individual must explicitly consent to the use of this data for a given purpose. GDPR explicitly identifies the types of Personal Data that constitute Special Categories of Personal Data, which are:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric data for the purpose of uniquely identifying a natural person;
- Health-related data; and
- Sex life or sexual orientation.

If any Special Categories of Personal Data of an individual in the EEA is collected, used, or accessed for research purposes, the researcher must obtain explicit consent for the use of that sensitive data from the Data Subject. This can be accomplished by ensuring that the Data Subject is informed of the use of the specific Special Category of data, the purpose of the use (i.e., to conduct the research study, which is summarized for the Data Subject), and requiring that the Data Subject consent to participation in the research study.

2. Personal Data Transfers to the United States

When UC researchers collect Personal Data from individuals in the EEA and intend to access the data in the United States, or transfer the data to the United States, generally, the researcher must obtain the explicit consent of the Data Subject. Thus, in most, if not all scenarios in which a researcher is collecting Personal Data, consent to transfer the data to the U.S. will be required. In addition to obtaining consent of the individual, GDPR requires that the Data Subject also be informed that the United States does not protect Personal Data in the same manner as Personal Data may be protected in the EEA.

Note that if a UC researcher is not collecting the Personal Data, but is instead receiving or using Personal Data collected or obtained from a researcher or institution in the EEA, [standard contractual clauses](#) approved by the European Commission should be included in any underlying agreements between UC and the EEA researcher or institution providing the Personal Data. Thus, though individuals do not need to consent to the transfer, they must still be informed by UC that their Personal Data is protected through one set of standard

contractual clauses, and they have the right to obtain a copy of the clauses used to protect their Personal Data. This can be accomplished, for example, by referring the Data Subject to a publicly-available Statement of Privacy related to UC's research uses of data that includes such language.

3. Personal Data to Assign Subjects to Different Treatments

GDPR gives Data Subjects the right not to be subject to a decision based solely on the automated processing of their Personal Data, where there is a legal or similarly significant effect on the person. A decision is based solely on automated processing when there is no meaningful human involvement in the decision. A decision that affects the healthcare a person receives can be considered one that has a significant effect on an individual. For example, assigning clinical trial subjects to receive an intervention or placebo based solely upon each subject's diagnostic data, where the assignment is done without any meaningful input from a physician or the research team, could be regulated by GDPR.

However, GDPR does allow solely automated processing that could significantly affect a Data Subject where the Data Subject explicitly consents to the activity. Thus, where the research involves assignment to various treatments based upon Personal Data alone, the researcher must obtain the explicit consent of the Data Subject. Where the decision will use special categories of Personal Data, the Data Subject must also explicitly consent to the uses of such data for this purpose.

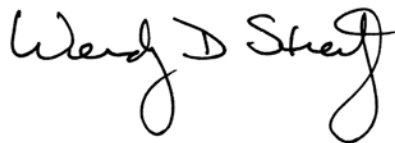
Finally, the Data Subject must also be informed of how the decision is made (i.e., the logic involved), the potential consequences of the decision, the right to obtain human involvement in the decision, and to challenge the decision, if the research allows.

Resources

- [RPAC web resources with graphic and glossary about GDPR](#)
- [Link to UC Systemwide Information Security Policies and Standards that contains information on how UC protects data](#)

Contact

Agnes Balla
Agnes.Balla@ucop.edu
(510) 987-9987



Wendy D. Streit
Executive Director
Research Policy Analysis & Coordination