General Data Protection Requirements (GDPR) for European Union Data

The European Union's (EU) General Data Protection Regulation (GDPR) regulates the use, access, collection, and processing of all personal data from the European Union, regardless of the citizenship or residency status of the individual to whom the data pertains. Investigators conducting research with data from the EU should be familiar with their responsibilities.

Requirements for data collection and access

When the **personal data** (as defined below) of an EU subject is collected, used, or accessed, the researcher must present certain information to the subject. If **sensitive data** is being collected, used, or accessed, a full informed consent process must be used, with translation as appropriate. The researcher is required to collect only the minimum necessary information for the defined research purpose.

EU subjects must be informed of:

- The specific purpose for the use of the data
- The legal basis for using the data
- How long the data will be stored
- Who will view or use the data
- The data protection rights available (see below)
- Whether the data will be removed from the EU
- Where one could lodge a complaint about their data use or protection
- How to withdraw consent for use of the data once it has been given (and it must be "as easy" as the process for giving consent in the first place)
- Contact information for USC and the relevant Data Protection Officer

Rights of research subjects / Data Storage

The data of individuals from the EU must be stored in a way that enables the following rights:

- The right to access the data, free of charge, in an accessible format.
- The right to object to a particular use of that data.
- The right to correct the data in the event the individual feels that it is incorrect, incomplete, or inaccurate.
- The right to "be forgotten," or to erase all data relating back to that person in an irreversible fashion. Parents of children and children each individually hold this right, so either of those parties can require a child's data to be deleted.
- The right to move data; this means that the individual can ask you to transfer it to them, or to another party, in a commonly-used and machine-readable format.

The GDPR permits the retention of personal data for only as long as necessary to achieve the specific purpose for which it was collected. It must be deleted after that time. If there is a data breach which could pose any risk to participants, participants must be informed of the breach.

"Personal Data"

Project which uses personal data from the European Union must abide by the requirements of the GDPR. Personal data is "any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, constitute personal data."

For data to no longer considered "personal data" it must be rendered anonymous in such a way that the individual is not identifiable. The anonymization must be "irreversible." If a link or key exists between the data and subject identifiers (Pseudonymized data/coded data) the data is not anonymized and must be treated as personal data, regardless of whether the investigator has access to the key.

Examples of personal data:

- A name and surname
- A home address;
- An email address;
- Income;
- An identification card number;
- An Internet Protocol (IP) address;
- A cookie ID;
- Phone identifiers; or
- Data held by a hospital or doctor which could uniquely identify a person.

"Sensitive data"

Sensitive data is data concerning "one's health, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sexual orientation, biometric data, or data concerning a natural person's sex life." Explicit consent must be used for collection or use of sensitive data. Receipt of sensitive data from the EU must always be accompanied by the explicit consent of the individual, and for a specified purpose ("passive consent," or a Letter of Information, is not sufficient).

Data from minors

The GDPR defines a child (for the purposes of using or accessing personal data) as an individual under the age of 16. Parental consent is required for any personal data collected regarding a

child under the age of 16. Individual member states may utilize a different age of consent within their own jurisdiction.