

University of Kentucky (UK) General Data Protection Regulation (GDPR) Guidance

The General Data Protection Regulation (GDPR) is a regulation affecting the way data is processed in the European Economic Area (EEA)*. This regulation increases the rights afforded to research participants and reshapes the way organizations handle and process personal data from individuals located in the EEA.

What is different about this rule?

The GDPR replaces the outdated European Union Data Protection Directive and increases the scope of the data to be regulated among persons located in the European Union. Rather than only applying to work completed by an entity in the EEA, the GDPR extends its reach to researchers located in the United States collecting data on participants present in the EEA (for example – conducting international research or research involving internationally located individuals).

When is a research study subject to the GDPR?

To determine whether a study is subject to the GDPR, the type of study population must first be considered. If a study involves using, collecting, or processing data in person, or online, from anyone located in one of the countries of the EEA, the study is subject to the GDPR. The broad nature of this regulation extends beyond mere citizenship. For example, data from a U.S. citizen studying abroad in one of the EEA countries would be regulated by the GDPR .

A second consideration is whether the data to be collected/analyzed is personal and/or sensitive. Any research utilizing personal data from research participants located in the EEA must adhere to the requirements of the GDPR. The scope of personal data under the GDPR is broader than Protected Health Information (PHI) in the U.S. Items listed as personal information under the GDPR include:

- Name
- Home Address
- Email Address
- Income
- Identification Card Number
- IP Address
- Cookie ID (for electronic research)
- Phone Identifiers
- Data held by a hospital or doctor which could uniquely identify a person
- A combination of information that could lead to the identification of a subject may also be considered personal information under the GDPR.

De-Identified Data

De-identified data is not regulated by the GDPR. Data is considered de-identified if there are no reasonable means through which someone who has access to the de-identified data can re-identify a research participant.

GDPR Requirements for Consent

The GDPR affects the consent requirements that must be considered when conducting research involving persons located in the EEA. If your study is subject to the GDPR, make sure your consent includes the GDPR required conditions of consent listed below. Under the GDPR, consent must be:

- Clear and Distinguishable via some Affirmative Action (signed consent form)
- Freely Given (voluntary)
- Specific (describes what information is collected and shared and for what purpose)
- Informed (proper consent process)
- Unambiguous (explicit in description)
- As easy to withdraw as it is to give. If consent is obtained via checking a box, the method of withdrawing consent must also be as easy as checking a box.

The GDPR contains a few other participant rights such as a right of access, a right to be “forgotten,” and a right of “erasure.” The right to be forgotten and the right to erasure mean that once data are no longer needed for their original processing purpose, or the research subject has withdrawn his or her consent, a subject has the right to refuse/withdraw from further data sharing.

GDPR Requirements for Privacy Notice

The GDPR requires a privacy notice in addition to the informed consent form. A copy of the privacy notice should be given to the participant during the informed consent process. A GDPR privacy notice informs individuals what data are collected, where and how it was collected, and for what purpose it was collected. See the privacy notice template for further guidance.

The right of access to data contains several requirements that a researcher must meet to successfully carry out research involving members of the European Union. Included in this right of access is information about the:

- categories of personal data processed
- recipients or categories of recipients
- planned duration of storage of information
- right (and instructions on how-to) file a complaint regarding the collection of data
- safeguards that will be in place for data protection and confidentiality

Sensitive Data Protections

If personal data is also “sensitive,” it requires additional protection. Data that is considered “sensitive” may only be obtained/accessed after active and explicit consent is obtained from the individual to whom it refers. Additionally, this information may only be obtained for a specified purpose, of which the subject is fully aware (no deception research).

Sensitive data includes data concerning a subject’s:

- health
- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- sexual orientation and/or data concerning an individual’s sex life
- biometric data

Waiving Informed Consent

The GDPR does not include provisions for a waiver of informed consent.

Research Involving Children

The GDPR defines a child (for the purposes of personal data use) as an individual under the age of 16. For any personal data collected from this class of individuals, the “holder of parental responsibility” must explicitly consent to use of that child’s data.

If you have questions regarding a study and GDPR compliance, please contact the Office of Research Integrity at (859) 257-9428 before initiating your study.

*European Economic Area (EEA) includes the following countries: Iceland, Liechtenstein, Norway, and the countries of the European Union (Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and the United Kingdom.

J:\Master Outreach Documents\Survival Handbook\D - Guidance-Policy-Educational\D147-General_Data_Protection_Regulation_Guidance.docx