General Data Protection Regulation (GDPR) FAQs

What is the European Union (EU) General Data Protection Regulation (GDPR)?

The GDPR, which became effective May 25, 2018, is an EU regulation that relates to personal data that is collected in the European Economic Area (EEA), which includes 28 EU states as well as Norway, Iceland, Liechtenstein, and Switzerland. It describes requirements for entities that collect, use and store personal data in the EEA (including study sponsors located in the EEA who will obtain personal data about study subjects located in the United States). It also requires that EEA entities inform subjects of their privacy rights and remedies related to their personal data. If the entity processes personal data collected from individuals in the EEA, the GDPR may apply even if that entity is not in the EEA. See the next FAQ for information about current stance of the United States (U.S.) on the GDPR's applicability to U.S. government agencies.

Does GDPR apply to NIH?

The GDPR is not a U.S. law. The U.S. Government is not subject to GDPR, e.g., it does not automatically apply, because the U.S. is not part of the EEA. Further, Institutes and Centers do not have the legal authority to agree to follow GDPR and bind NIH to its terms.

There is an absence of an official recognition by the EEA that U.S. laws ensure an adequate level of protection (an "adequacy decision") under the EEA standards. NIH is unable to use standard, GDPR-approved data protection clauses as they conflict with U.S. law and policy of federal agencies.

Due to uncertainties in the scope and interpretation of the GDPR requirements, the Department of State is advising U.S. government agencies not to sign, or agree to, contractual language that implies that the U.S. government complies with or will comply with the GDPR.

What should NIH investigators do when a sponsor makes requests of the investigator related to the GDPR (e.g. the sponsor requests that the NIH study consent form used for enrollment of subjects be modified to include information about the GDPR, that NIH provide GDPR-related forms to subjects, or the sponsor requests that the NIH investigator be a point of contact to answer subject questions about the GDPR)?

Any NIH investigator who is asked to provide GDPR language to participants on behalf of the sponsor should contact Heather Bridge (heather.bridge@nih.gov), who will facilitate next steps with the Office of the General Counsel (OGC). For example, current practice within the NIH Intramural Research Program is to provide a separate GDPR information sheet for participants rather than insert GDPR language into research consents. Information sheets must be reviewed and approved by OHSRP, working with OGC, and approved by the IRB before being provided to subjects. Further, NIH investigators should not promise to or answer questions about the EU GDPR on behalf of the Sponsor. Instead, NIH investigators should refer the subject to the

Sponsor's point of contact or webpage that explains the rights of "data subjects," which will be included in the above-referenced information sheet.

What is meant by "personal data" under the GDPR?

Personal data under GDPR is more broadly defined than under the Common Rule and is explained in the European Union's webpage "What is personal data?"

What are "special categories of personal data" under the GDPR?

There are additional requirements for processing "special categories" of personal data. Special categories of personal data comprise the following (and include data often collected for research purposes):

- Racial or ethnic origin
- Data concerning health
- Data concerning a natural person's sex life or sexual orientation
- Genetic data
- Biometric data used for the purpose of uniquely identifying an individual
- Political opinions, religious or philosophical beliefs, or trade union membership.

What does "data processing" mean? [1]

Processing covers a wide range of operations performed on personal data, including by manual or automated means. It includes the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data.

What do the regulations mean by data "controller" vs. "processor"?

A **controller** alone or jointly determines the purposes and means of processing personal data (e.g. acts as a collaborator on a research project) while a **processor** processes personal data on behalf of the controller (e.g. a fee-for-service lab for a research projects). Both are regulated under the GDPR, but controllers have more responsibilities.

[1] Data "processing" as defined on the European Commission (EC) website, *EU data protection rules*

When does GDPR apply?

Examples of when the GDPR may apply to non-governmental entities (i.e., not to NIH) include the following if the organization/entity:

- Monitors the behavior of individuals in the EEA
  - Conducting research with participants located in the EEA could involve activities that fall into this category (e.g. a US-based sponsor serves as a lead site for a multi-site protocol with sites in the EEA)
- Offers goods or services to individuals in the EEA (irrespective of whether connected to payment) and could include examples related to research such as the following:
  - Clinical Trial Agreement between a US based sponsor and an EEA study site
  - US based sponsor provides investigational product (IP) to EEA study sites
- Is established in the EEA and acts as a data controller or processor

References:

European Commission (EC). EU data protection rules. (website)

NIH OSP. GDPR: Crossing the Data Sharing Bridge, One Regulation at a Time (2019)

PRIM&R. EU General Data Protection Regulations: What US Research Institutions Need to Know (2018) [At the bottom, enter information and click "Launch"]

SACHRP. Attachment B-European Union's General Data Protection Regulations (2018)