University of Rochester
September 2018

What You Should Know About GDPR

What is the GDPR?

The European Union's General Data Protection Regulation ("GDPR)", effective May 25, 2018, is a far-reaching regulation applicable to organizations with European Economic Area ("EEA") based operations and certain non-EEA organizations that process personal data of individuals in the EEA. The EEA includes the 28 states of the European Union and three additional countries: Iceland, Liechtenstein and Norway. The GDPR aims to protect individuals' fundamental rights to data protection and the free flow of personal data.

What is considered "Personal Data"?

For purposes of the GDPR, personal data refer to any information that relates to an identified or identifiable natural person (*i.e.*, an individual, not a company or other legal entity), otherwise known as a "data subject". Examples of personal data include a person's name, e-mail address, government issued identifier, or other unique identifier such as an IP address or cookie number, and personal characteristics, including photographs.

There is a subset of personal data, referred to in the GDPR as "special categories" of personal data, which merit a higher level of protection due to their sensitive nature and associated risk for greater privacy harm. Special categories of personal data include several items that are often collected as part of a research study, including information about a data subject's health; genetics; race or ethnic origin; biometrics for identification purposes; sex life or sexual orientation; political opinions, religious or philosophical beliefs; or trade union membership.

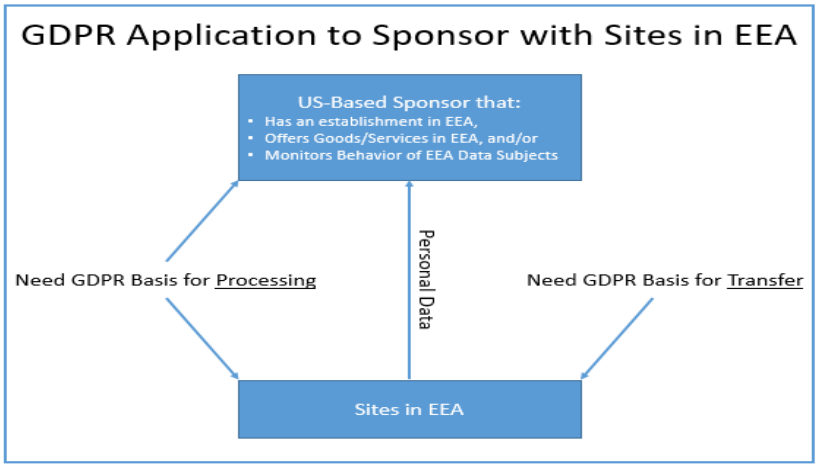
What is the Territorial Scope of the GDPR?

The GDPR applies to organizations located within the EEA and organizations outside of the EEA if they offer goods or services to, or monitor the behavior of, EEA data subjects and applies to all companies processing and holding the personal data of data subjects residing in the EEA, regardless of the company's location and whether the person is a citizen. The GDPR is therefore a significant change because the territorial scope of the regulation is more expansive than prior EEA privacy regulations.

How does the GDPR affect research?

The GDPR may be applicable to a broad range of research activities. For example, the GDPR may apply when

- A UR Investigator collects or receives personal data of subjects in the EEA, e.g. as part of a clinical trial, through participation in a repository, database or research consortium, or by receiving a research study data set
- UR acts as a **core data facility or lead site** for a multi-national research study with EEA-based sites,
- UR acts as a **sponsor** of research occurring in EEA member states, or
- UR conducts research in which it **transmits U.S. participant data to the EEA**, e.g. to sponsors, servers, or data core facilities in the EEA.



GDPR covers the personal data of research staff as well as data subjects. Therefore, researchers may receive notices from EEA sponsors or collaborators, disclosing that data such as the researcher's email address is "processed" in the EEA.

What if the study does not involve the collection of personal data from individuals?

In short, GDPR would not apply. Research studies may not involve the receipt of personal data because the data received may not relate to an identified or identifiable natural person. For example, studies that do not collect information that is linked to a subject's identity, such as anonymous surveys in which the identities of survey subjects cannot be traced, would not involve the receipt of personal data.

What if I am only receiving coded data?

The GDPR considers key-coded data to be "personal data" and still subject to GDPR. Key-coded data is referred to as "pseudonymized data" under the GDPR. This is in contrast to the position under many US research and privacy laws, such as the Common Rule and HIPAA; pseudonymized data are regarded as identifiable personal data and therefore remain subject to the GDPR's protections, even when in the hands of a person who lacks the key needed to link the data to the data subject's identity.

Is it possible to de-identify data so that GDPR does not apply?

The GDPR does not apply to data that have been "anonymized." However, for data to be anonymized, the GDPR requires that there be no key to re-identify the data. For example, if UR serves as the sponsor of a research study with a site located in the EEA and receives only key-coded information from the EEA site, the key-coded data from the EEA site remain "personal data" in the hands of UR. This is the case even if UR has no access to the key needed to re-identify the coded data. Unlike in HIPAA, there is no "safe harbor" under the GDPR to which data can be rendered de-identified by removing a specific list of identifiers. Rather, anonymization is judged on a facts and circumstances basis taking into account all the means

reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. Given this definition, anonymization is an extremely high standard that is difficult to meet in practice.

I have heard that subjects have additional rights under the GDPR. Is that true?

Yes, and honoring those rights may require a change in UR processes and workflows. The GDPR creates a range of rights that are available to research subjects under certain situations, and a right to claim compensation through EEA courts for violation of their rights and misuse of their personal data. This potentially subjects UR to litigation in the EEA. Some of the rights under the GDPR include the **right to access, rectification of data and an accounting** of how their data was shared. These rights are broader than in HIPAA. Research subjects also have the right to **withdraw consent** to further processing of their personal data and to request that their data be "erased" (this is known as the "**right to be forgotten**"). If these rights are exercised, one can no longer retain the personal data for the purpose of research, including in pseudonymized (key-coded) form. However, one may retain the data if necessary for legal compliance (*i.e.*, for adverse event reporting). Also, the researcher could continue to process the data for research purposes if the data have been fully anonymized through removal of all identifiers associated with the data, including destruction of the key linking the subject's data to his or her identity (*Please see previous note on "anonymized" data*).

What Information Security controls must be implemented to protect personal data covered under GDPR and what are the requirements for breach notification?

The controls required to honor the subjects' rights detailed above are largely system dependent. Standard University security controls for Legally Restricted data will adequately protect the data at rest and in transit, but it is up to the researcher to implement the controls and ensure that systems are configured appropriately to allow e.g. identification, extraction and deletion of a particular user's data. The controls required for Legally Restricted data can be found here.

The breach notification requirements under GDPR are more stringent than in the US, making quick response critical. Notification must be made to the appropriate supervisory authority within 72 hours of discovery of the breach, with updates thereafter. Data subjects must be notified without "undue delay".

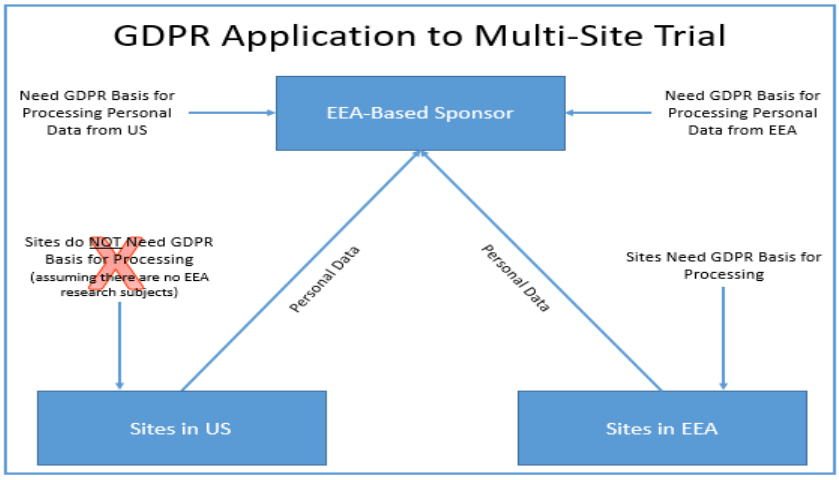
What is a "Controller" and what is a "Processor", and what are their responsibilities?

A "Data Controller" is a person or entity that determines the purposes and means of the processing of personal data. In research involving several parties, the lead site likely will be the Controller. Some situations (e.g. certain collaborative studies) will have joint controllers who each are liable to the data subject.

A "Data Processor" is a person or entity that processes personal data on behalf of the controller. This includes central labs, core labs, and participating sites that collect, organize/analyze, or store data, or perform other activities that fall within GDPR's definition of "processing".

Controllers have more responsibilities than processors, such as providing notices to data subjects, responding to the exercise of subject rights, notifying supervisory authorities and data subjects of breaches, and maintaining records of processing. Controllers are required to enter controller-processor contracts that bind their processors to comply with GDPR. Joint controllers typically will apportion responsibilities amongst themselves via a contract, but each remains individually liable to the data subject.

Controllers need to ensure that there is a "lawful basis" for processing personal data, and that this lawful basis is communicated to data subjects. In addition, if personal data is being transferred from the EEA to another country such as the U.S. which is deemed to lack "adequate protection" for personal data, then there needs to be a lawful basis for transfer. One lawful basis for transfer is the use of "model contract clauses" that bind the parties to comply with GDPR. Data subject consent can be the lawful basis for processing and/or transfer, but GDPR requirements for consent are potentially problematic in the research setting.



In the above multi-site trial example, contracts among the parties will be necessary as well:

Example: US sponsor of multi-site study engages US core lab to process data from both US and EEA participating sites:

-US sponsor needs to enter controller-processor agreement with US core lab

-US sponsor needs to enter model contract clauses with EEA participating sites or obtain explicit consent of research subjects to the transfer of their data to a country without adequate protection.

What should I do to achieve GDPR compliance?

- **Identification of affected studies.** We have established a collection point for examples of studies that may be affected by GDPR. Further, situation-specific guidance will be issued after review of these examples. If you have a pending or proposed study that potentially falls within the scope explained above, or if you have received any requests or notices pertaining to GDPR, please provide particulars via email to Research-GDPR@rochester.edu.

  Please include:

  - Data being collected from EEA residents, by whom, and in what form (identified, coded, fully de-identified)
  - Role of UR with respect to that data, i.e. what does UR do with the data?
    - See definitions of Controller and Processor, but please provide specific facts
  - Involvement of EEA sponsor or participating site(s)
  - RSRB # if applicable

- **Seek support.** If you receive notices, requests or other documentation (including consents or amendments to existing contracts) that mention GDPR or European privacy rules, in addition to apprising RSRB and ORPA in accordance with usual processes, please contact Kathleen Tranelli (kathleen_tranelli@urmc.rochester.edu) or Mark Wright (mark.wright@rochester.edu) and indicate GDPR in the subject line. Studies will need to be evaluated on a case by case basis. We do not want UR to assume obligations it does not need to, or is unable to, honor.

Example of a problematic request: EEA sponsor asks UR as participating site to send Notices to US research subjects specifying not only that data will be transferred to the EEA for processing, but that US subjects may complain to their local data protection authority if their privacy rights are violated and may claim compensation through the courts.