General Data Protection Regulation – A Primer for Researchers

What is it? The General Data Protection Regulation ("GDPR") is a standard data protection law that applies across the 28 member nations of the European Union as well as Iceland, Lichtenstein, and Norway (the EU and these 3 nations collectively make up the European Economic Area or "EEA" – references to the EU includes all nations of the EEA). The GDPR imposes strict rules on *controlling* and *processing personal information* of any individual *residing in the EU*.

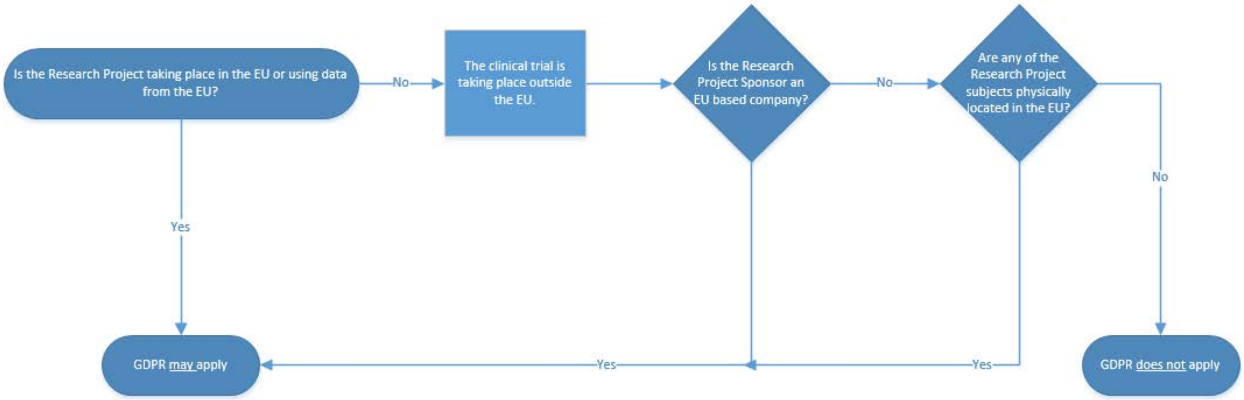
Residing in the EU: If an individual is physically present in the EU they are covered by the GDPR.
Controlling Personal Information: A controller is anyone that determines the purposes and means of processing personal data (e.g., as a sponsor, lead investigator, primary research site, etc.).
Processing Personal Information: A processor is anyone that processes personal data on behalf of a controller (e.g., as a subcontractor, data coordinating center, secondary study site, etc.).
Personal Information: includes any information relating to an identified or identifiable natural person.

Is the University of Utah a Controller or a Processor? This depends on various factors. UofU will analyze on a case-by-case basis.

If the UofU is a *controller*, the UofU is primarily responsible for GDPR compliance. This means the UofU will make an initial decision on the lawful basis for collecting and processing *personal information* (e.g., individual consent, or do the scientific research or public health exceptions under the GDPR apply). If the UofU is a controller, the UofU is responsible for drafting documents for individual research subjects (e.g., consents) and agreements for any subcontractors or processors to ensure their GDPR compliance.

If the UofU is a *processor*, this means the research project sponsor is a controller and will pass on certain GDPR compliance obligations to the UofU through a written agreement. This may include GDPR-required model clauses, data security standards, and drafts of documents we must provide to research subjects (e.g., consents and privacy policies).

Does the GDPR Apply to My Research Project?


Is the Research Project taking place in the EU or using data from the EU?
No
The clinical trial is taking place outside the EU.
Is the Research Project Sponsor an EU based company?
No
Are any of the Research Project subjects physically located in the EU?
No
Yes
GDPR may apply
Yes
Yes
GDPR does not apply

Researcher Agreement

If your research study involves the collection of personal data of individuals physically located in the EU, whether directly or indirectly or through in-person or electronic methods, you agree to:

1. Contact the University of Utah Center for Clinical and Translational Science (CCTS) Biomedical Informatics Core (BMIC) to receive support for GDPR compliant data capture (REDCap). To request REDCap support go to: ProTrackS . This link will register your project and connect you with the BMIC.

2. Contact the University of Utah Information Security Office at 801-587-2510 to assess whether your research environment is secure under the GDPR.

3. Retain personal information for only as long as necessary, and design a study that will allow you to delete personal information at the conclusion of the research study. GDPR requires personal information be deleted at the conclusion of the research study (unlike American law, which allows retention of research data beyond the conclusion of the study). Design a study that considers data protection at an early stage, for example, by collecting only de-identified or pseudonymized data at the outset.

4. Collect only the minimum personal information necessary for the study. For example, if you are using an online survey site that collects IP addresses, change the default settings not to include that information unless required for the study.

5. Limit the use of personal information to the consent provided by each research subject. GDPR does not allow you to use the data for any other purpose.

6. Maintain complete and accurate records of processing activities on personal information (e.g., details of other recipients, all transfers within or outside the U.S., record retention period, details of security measures).

7. Develop or identify a method to communicate with data subjects.

8. Use an opt-in informed consent, when applicable, that includes a description of the data processing and transfer activities to be performed. Under the GDPR, consent must be freely given, specific, informed, unambiguous, and explicit.

9. Provide a notice of privacy practices where applicable. The notice can be included in consent documents. The University of Utah has prepared a notice of privacy practices that will be suitable in most cases: GDPR Privacy Notice.

10. Ensure that collaborators, vendors, third parties, and tools used are GDPR compliant.

11. Work with OSP, TVC, and OGC as appropriate to review GDPR-related contractual language.

12. In the event of a data breach, notify the Information Security Officer at 801-652-0003 or the Office of General Counsel immediately at 801-585-7002.

Key Resources and Contact Information:

OGC: Scott Smith, Dennis Owens, Christopher Stout, and Brian Watts, all at 801-585-7002, can assist with contract review of GDPR language and other GDPR-related legal issues.

TVC: Miriam Allen, Contracts Manager: 801-581-7792 (office), miriam.allen@tvc.utah.edu; Eric Paulsen, Manager, Grants & Contracts: 801-581-7792 (office), epaulsen@tvc.utah.edu.

OSP: Brent Brown, Director & Assistant VP: 801-581-6903 (office), brent.brown@osp.utah.edu; Trevor Gordon, Manager, Grants & Contracts: 801-585-6945 (office), trevor.gordon@osp.utah.edu.

ISO: Corey Roach, Chief Information Security Officer: 801-213-3397 (office), corey.roach@utah.edu; Trevor Long, Associate Director Information Security: 801-587-2510 (office), trevor.long@utah.edu.

IRB: Ann Johnson, IRB Director: 801-581-3655 (office), Ann.Johnson@hsc.utah.edu; Sarah Mumford, IRB Associate Director: 801-581-3655 (office), sarah.mumford@hsc.utah.edu.

Privacy: Jamie Ross, UUH Privacy Officer: 801-213-3235 (office); jamie.ross@hsc.utah.edu.