Frequently Asked Questions
European Union General Data Protection Regulation

Effective May 25, 2018, the European Union (EU) General Data Protection Regulation (GDPR) (EU 2016/679) replaces the 1995 Data Protection Directive (Directive 95/46/EC). The primary objective of this new regulation is to protect the fundamental rights and freedoms of data subjects and standardize requirements regarding covered data processing activities. Although the GDPR makes many important changes to EU data protection law, the GDPR is not a complete departure from existing principles. Many of the obligations outlined in the GDPR are not new for many organizations in the area of human subjects research. However, as noted below, the territorial reach of the new regulation has expanded and will impact U.S. organizations, including universities and academic medical centers.

The following Frequently Asked Questions (FAQs) provide an overview of the new regulation in the context of Human Subjects Research where the research involves the processing of *personal data* and *special categories of personal data* such as *sensitive data* or *data concerning health*. This document also briefly touches upon other key University activities that should be monitored for GDPR compliance.

1. **Does the GDPR apply to Human Subjects Research?**
   Yes. The GDPR applies to human subjects research (e.g., interventional trials, non-interventional trials, registry studies, student research, etc.) involving personal data as defined in the GDPR that is within the territorial scope of the regulation. The GDPR adopts a broad interpretation of research that includes publicly and privately funded research such as public health research, technological development and demonstration, fundamental research, and applied research. It also includes personal data processed for historical research and statistical purposes.

2. **What is the Territorial Scope of the GDPR?**
   The GDPR applies to organizations located within the EU *and* organizations outside of the EU *if they offer goods or services* to, or *monitor the behavior of,* EU data subjects and applies to all companies processing and holding the personal data of data subjects residing in the EU, 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 Directive 95/46/EC.

   Example 1: Sponsor in the EU/EEA
   If the sponsor is based in the EU/EEA then the GDPR applies to the data processing activities, even if the processing itself is not performed within the EU/EEA and even if there are no data subjects within the EU/EEA.

   Example 2: Sponsor not in the EU/EEA
   - If an organization has offices in the EU/EEA involved in some aspects of the clinical trial (e.g. a central data management organization and/or system managed from a EU/EEA-based establishment), then the sponsor may be considered as established in the EU/EEA and the GDPR may apply.

   - If the clinical trial data is intended to support a market authorization filing in the EU/EEA, then there is a data processing activity taking place in Europe for the purpose of the data submission. The GDPR may therefore apply.

   - If a full service CRO established in the EU/EEA, is being delegated the definition of the purpose of the clinical trial, and, as such, qualifies as a joint-controller, then the GDPR would apply even if the sponsor is not located in the EU/EEA.

Example 3: Data Subjects in the EU/EEA

- If the clinical trial includes data subjects within the EU/EEA, then the GDPR applies in its entirety. This applies irrespective of where the sponsor and CROs/vendors are located, where the data processing is performed or where the data submission is planned.

- If a sponsor not based in the EU/EEA is processing data from data subjects within the EU/EEA then they must nominate in writing a representative within the EU/EEA who fulfills their responsibilities with regards to GDPR. Note that this applies even if the data subjects are not EU/EEA citizens, if their information is collected while they are within the EU/EEA.

Example 4: Person Living or Traveling in the EU/EEA

- A person in the EU/EEA (even if not a citizen) is subject to the GDPR.

Example 5: Application to U.S. Organizations

- The GDPR applies to U.S. Organizations if under the circumstances below, and will apply in a broader range of circumstances than prior to the repeal of the Directive: (1) Established in the EU/EEA (e.g. branch or office) and acts as a data controller or data processor; (2) Offers goods or services to individuals in the EU/EEA; and (3) Monitors the behavior of individuals in the EU/EEA.

Example 6: Lead site for research activities taking place at EU/EEA sites

- A prime recipient of an NIH grant which flows through sub-awards to EU/EEA sites.

Example 7: Studies involving the use of technology in research that target enrollment in the EU/EEA

Example 8: Conducting clinical trials for organizations located in the EU/EEA with personal data being sent to and/or processed in the EU/EEA

Example 9: Research arrangements involving European governmental grants or contracts.

- Institutions may be direct awardees or sub-recipients from EU/EEA institutions of European governmental grants or contracts to perform research services.

- Terms of grant may require compliance with GDPR.

- Personal data flows to and from EU/EEA may require compliance with the GDPR if offering goods or services to data subjects.

Example 10: Use of an investigational product in a clinical trial. (This is an example of offering a good or service.) Using an app to monitor the behavior of research participants. (This is an example of monitoring the behavior.)

3. Which countries are Part of the European Union and European Economic Area

List of EU countries

1. Austria
2. Belgium
3. Bulgaria
4. Croatia
5. Cyprus
6. Czech Republic
7. Denmark
8. Estonia
9. Finland
10. France

11. Germany
12. Greece
13. Hungary
14. Ireland
15. Italy
16. Latvia
17. Lithuania
18. Luxembourg
19. Malta
20. The Netherlands
21. Poland
22. Portugal
23. Romania
24. Slovakia
25. Slovenia
26. Spain
27. Sweden
28. United Kingdom

List of EEA countries

All 28 EU countries above as well as Iceland, Liechtenstein, and Norway.

4. What are some of the key GDPR Definitions?

a. **What is the definition of Personal Data?**

The definition of *Personal Data* related to a *Data Subject* is essentially unchanged under GDPR. "Personal Data" means any information relating to an identified or identifiable natural person ("data subject"). A "*data subject*" is an identifiable person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

b. **What is the definition of Sensitive Personal Data?**

"*Sensitive Personal Data*" are special categories of personal data that are subject to additional protections. Under the GDPR, "*Sensitive Personal Data*" is defined as "personal data" revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; and the processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

c. **What is the Definition of Data Concerning Health**

"*Data Concerning Health*" is defined as personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

d. **What is the Definition of Pseudonymous Data and how is that different from Anonymous Data? *How is Data Subject to GDPR different than Data Subject to HIPAA?***

"*Pseudonymous Data*" refers to personal data that can be amended in such a way that no individuals can be identified from the data without a key that allows the data to be re-identified. A Coded data set is an example of pseudonymous data. The GDPR encourages organizations to consider pseudonymization as a security measure when appropriate.

"*Anonymous Data*" refers to data sets that can be amended in such a way that no individuals can be identified from the data (whether directly or indirectly) by any means or by any person. Data that is fully anonymized is outside the scope of the GDPR.

Personal Data under the GDPR is broader than what is covered under HIPAA as the GDPR applies to all sectors of the economy, not just healthcare.

e. **What is a definition of a Data Controller?**
A "*Data Controller*" is … "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. In clinical research, the Sponsor is always a controller". Other types of organizations may qualify as joint controllers such as a Contract Research Organization, Investigator, or joint collaborator on a research project.

f. **What is the definition of a Data Processor?**
A "*Data Processor*" is "… a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller". In clinical research, this corresponds to anyone appointed by the Sponsor to work with the clinical trial, including CROs (project management, monitoring, data management, statistics, medical coding, medical writing, etc.) and Vendors (eCRF/EDC and central labs, etc.).

g. **What is the definition of Processing?**
"*Processing*" is defined as "…any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as 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". An example is any operation that affects the data from a clinical trial during its entire life-cycle, from its collection by the sites as source data to its reporting, archival and destruction.

5. **What are some of the obligations of a Controller and Processor under the GDPR?**
Controllers must ensure that data protection principles and appropriate safeguards are addressed and implemented in the planning phase of processing activities and the implementation phase of any new product or service. As an entity that controls data on behalf of the Controller, a *Processor* must implement technical and organizational security measures to protect personal data. Examples of technical and organizational security measures include encryption, redundancy and backup at co-location facilities and security testing. There are also breach notification requirements.

6. **What is the Lawful Basis for Processing Personal Data under the GDPR?**
Under the GDPR, the processing of personal data must have a lawful basis. The lawful bases most likely to be relevant to a U.S. university are:
   - Data subject consent to the processing.
   - Processing necessary for the performance of a contract to which the data subject is a party.
   - Processing necessary to protect vital interests of the data subject or a natural person.
   - Processing necessary for the legitimate interests of the controller or a third party, except where such interests are overridden by the interest or fundamental rights and freedoms of the data subject.

   For a complete list, see GDPR, Article 6: https://gdpr-info.eu/art-6-gdpr/

7. **Are there Special Requirements for the Processing of Special Categories of Personal Data?**
Yes. The "processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for

the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation [is] prohibited" unless one of the following applies including:

- Explicit consent to the processing of the data.
- Processing necessary to protect the vital interests of the data subject where the data subject is incapable of giving consent.
- Processing necessary for reasons of public interest in the in the area of public health.
- Processing necessary for scientific or historical research purposes.

For a complete list, see GDPR, Article 9(2); https://gdpr-info.eu/art-9-gdpr/ .

8. What are the Requirements for the Transfer of Personal Data to the United States?

The GDPR requires a legal basis to transfer personal data from the EU/EEA to a country outside of the region such as the United States. A legal basis to transfer personal data from the EU/EEA includes, but is not limited to, the following:

- Obtaining the explicit consent of the data subject to the transfer of the personal data to the United States for processing
- Entering into model contract clauses approved by the European Commission between the EU/EEA entity transferring personal data from the EU/EEA to the US and the US organization (such as a university or sponsor) receiving the data.
- Data transfers necessary to protect the vital interest of the data subject.

Example: A research collaborator established in the EU/EEA transfers files of pseudonymised (coded) data to a US organization for research purposes. In this case, the organization needs a legal basis to transfer the personal data to the US and a legal basis to process the data in the US.

9. What are the Requirements for the Transfer of Personal Data from the United States to the EU/EEA?

If a US organization transfers personal data to the EU/EEA, the US organization does not require a legal basis to transfer the data. However, the sponsor established in the EU/EEA receiving the data requires a legal basis to process the personal data transferred from a US organization.

Example: US university may need to transfer clinical trial data of research subjects to the EU/EEA when the trial is sponsored by an EU/EEA-based entity or the EU/EEA-based entity serves as the lead site. In this case, the EU/EEA-based sponsor may require the US organization to obtain trial subjects' consent that meets the notice requirements of the GDPR and permits processing of their data in the EU/EEA.

Example: Clinical research sponsored by an EU/EEA-based company for which an EU/EEA-based university serves as a lead site or data coordinating center. In this case, a US university may need to transfer its employees' data to the EU/EEA if the US university is serving as a site for an EU/EEA organization. This may require the consent of the employees as they are considered data subjects under the GDPR.

10. What are the requirements of Consent under the GDPR?

Under the GDPR, consent means "any freely given, specific, information and unambiguous indication of the data subject's wishes by which he or she, by a statement or a clear affirmative action, signifies agreement to the processing of personal data relating to him or her." Depending on the nature of the processing, there also may be additional requirements. For example, when processing the personal data of children, the consent of the holder of parental responsibility may be required depending on the age and the type of processing.

11. What is an example of a GDPR compliant consent language?

Consent forms that include certain notice requirements and permits processing of the data subjects personal data in the EU/EEA *may be required* by sponsors established in the EU/EEA. The HRPP will work with the Investigator and the Yale IRB or external IRB of record for the study to ensure the appropriateness

of the language in the consent form and compliance with applicable regulatory requirements including GDPR.

12. **How will the Human Research Protection Program Assist Researchers with the Identification of Studies Subject to the GDPR?**
The HRPP currently includes questions in its IRB submission platform (IRES-IRB) and application that collects information regarding data use. See below for an example of the questions asked.

    - *What type of data will you collect, share, and/or store for this study?*

    - *Where will the study be conducted?*
      - ☐ *Yale University*
      - ☐ *Yale New Haven Health System*
      - ☐ *Other organization(s) outside of Yale University and Yale New Haven Health System*

      IF YNHH or Other Organizations options are chosen, a new field will appear to indicate the name of the organization.

    - *Will the study be conducted in the United States and/or another country?*
      - ☐ In the United State
      - ☐ Outside of the United States
      - ☐ Both inside and outside the United States

      Additional fields will open to indicate state and/or country.

    - *Will you send data related to this study FROM the United States TO another country?*
      - ☐ Yes
      - ☐ No

      If YES, a field will open to indicate country.

    - *Will you send data related to this study TO the United States FROM another country?*
      - ☐ Yes
      - ☐ No

      If YES, a field will open to indicate country.

    This information will help the HRPP identify whether the GDPR is applicable.

    The HRPP will also work with the Office of Sponsored Projects (OSP) for industry sponsored, industry authored clinical trials to determine whether a study is subject to a *Data Processing Agreement* and to confirm the location of the sponsor or CRO. If a study is not industry-sponsored, the HRPP will work with the Investigator and Yale IRB or external IRB of record to ensure compliance.

13. **What is a Data Processing Agreement?**
A Data Processing Agreement is an agreement entered into between the *Controller* and *Processor*.

14. **Are there Penalties for Noncompliance?**
Yes, there are penalties for noncompliance. "Under the GDPR, organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater). This is the maximum fine that can be imposed and in many cases, the fine may be lower; however, there is no doubt that noncompliance could have serious consequences.

15. **What are Other Key Areas with possible GDPR applicability?**

Other areas with possible GDPR applicability include, but are not limited to, the examples below. **See also FAQ 2 for examples related to research.** If you have questions regarding any of the areas below, please contact: Alyssa Greenwald (alyssa.greenwald@yale.edu) or Carolyn Marks (carolyn.marks@yale.edu).

Offering Good and Services	*Monitoring the Behavior of EU/EEA Residents*
Website directed to/targeted at people in the EU/EEA (e.g., translating the website into a EU/EEA members language, using EU/EEA member currency)	Online education programs that include EU/EEA participants states and use cookies to track student participation.
Study abroad Programs	Donor tracking of alumni and other donors in EU/EEA member states.
Recruiting that targets students in the EU/EEA	Telemedicine offered by a US-based physician to a patient in the EU/EEA.
Collaboration agreements with universities in EU/EEA member states to develop educational platforms and share data	
Patient referral arrangements between academic medical centers and EU/EEA health care providers. Occasional treatment to patients from the EU/EEA who travel to the US for treatment may not apply.	
Consulting arrangements in which US academic medical centers offers services to EU/EEA health care providers. Occasional informal consultation may not apply.	

16. What do I do if I have Questions regarding GDPR Compliance?

If you have questions regarding GDPR compliance, please contact:

- Office of General Counsel
  Attention: Alyssa Greenwald; Carolyn Marks
  iocc@yale.edu

- Human Research Protection Program
  Attention: Monika Lau; Linda Coleman
  HRPP@yale.edu

17. References

GDPR Regulation:
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Intersoft Consulting – Bookmarked version of GDPR Regulation:
https://gdpr-info.eu/

European Commission GDPR information and guidance:
https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en