The European Union (EU) General Data Protection Regulation (GDPR) Frequently Asked Questions

What is the GDPR and what countries have adopted it?

The General Data Protection Regulation (GDPR) is a European law that went into effect on May 25, 2018 and establishes protections for privacy and security of "personal data" about individuals in European Economic Area (EEA)-based operations and certain non-EEA organizations that process personal data of individuals in the EEA.

The following countries making up the EEA are adopting GDPR:

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	United Kingdom	Also Norway, Iceland, Lichtenstein	

Why does this affect me in the United States?

GDPR applies to any organization that operates within the EU and processes personal information. The GDPR also applies to any organization outside of the EU that processes the personal information of an individual who is physically located in the EU, which either (i) offers goods or services to such individual, or (ii) monitors the behavior of such individual. The GDPR does not cover individuals by virtue of their citizenship, but their physical presence in an EU country. For example, personal information of an EU citizen collected at a U.S. location is not covered by the GDPR unless the controller or processor continue to monitor the EU citizen upon their return to the EU.

Failure to follow the GDPR when applicable puts the University at risk of noncompliance, monetary fines, and reputational harm. Fines associated with noncompliance under the GDPR can be up to 20 million Euros or 4% of the University's prior financial year worldwide annual revenue.

What is the difference between a "controller" and a "processor"?

A controller is an entity or person that "determines the purposes and means of processing of personal data" (e.g., as a sponsor, lead investigator, or primary research site). A processor is an entity or person that "processes personal data on behalf of the controller" (e.g., as a subcontractor, data coordinating center, or another study site). A processor may not by itself be subject to the GDPR except and until it has been engaged to provide data processing services to a controller. The controller will impose certain obligations related to data use and security on the processor through a written agreement. In addition, special rules apply to transfers of personal information out of the EU.

What is personal data?

Under the GDPR, "**personal data**" refers 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, email address, government-issued identification, or other unique identifier such as an IP address or cookie number, and personal characteristics, including photographs.

The GDPR highlights some "special categories" of personal data, which merit a higher level of protection due to their sensitive nature and consequent risk for greater privacy harm. This includes 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. Although criminal convictions and records are not considered "special categories" of personal data, this information is subject to amplified protections under the GDPR.

Although there are similarities between HIPAA and the GDPR, the GDPR is broader and covers information not covered by HIPAA. For additional information, see Appendix I, "HIPAA vs. GDPR."

- ***GDPR and Pseudonymized/Coded Data***

  Of significance to the research community, GDPR considers "pseudonymized data" (e.g., coded data) to be identifiable "personal data" even where one lacks access to the key-code/coding system/crosswalk required to link data to an individual data subject. This is in stark contrast to US regulations protecting human subjects.

- ***GDPR and Anonymized Data***

  The GDPR <u>does not</u> apply to data that have been anonymized. Under the GDPR, however, in order for data to be anonymized, there can be no key-code in existence to re-identify the data. For example, if TU serves as the sponsor of a research study with a site located in the EEA and receives only coded data from the EEA site, such data from the EEA site remain "personal data" in the hands of TU investigators. This is the case even where TU investigators have no access to the key-code/coding system/crosswalk required to link data to an individual data subject.

How does the GDPR relate to research in general?

GDPR permits processing of special categories of personal information for scientific or historical research purposes. Under this mechanism, use must be limited such that it is proportionate to the aim pursued, respects the essence of the fundamental right to data protection, and provides for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. This implies that where the research purposes can be fulfilled by further processing which does not require the identification of data subjects then the research shall be fulfilled in a manner that does not permit such identification. Specifically:

1. It establishes the circumstances under which it is lawful to collect, use, disclose, destroy, or otherwise process "personal data."
2. It establishes certain rights of individuals in the EEA, including rights to access, amendment, and erasure (right to be forgotten).

3. It requires researchers to implement appropriate technical and organizational security measures to ensure a level of data security that is appropriate to the risk of the data.
4. It requires notification to data protection authorities and affected individuals within 72 hours following the discovery of a personal data breach, which is a security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

What activities ARE subject to the GDPR?

1. Activities involving identifiable information if personal data is being collected from one or more research participants ***physically located*** in the EEA at the time of data collection (even if the participant is NOT an EEA resident).
2. Activities involving the transfer of personal data collected under the GDPR from an EEA country to a non-EEA country.

What are examples of activities that are NOT subject to the GDPR?

Activities involving collection of identifiable personal data from individuals who are ***physically located within the United States*** at the time of data collection (even if the participant is an EEA citizen).

What steps can I take to help ensure my project will be GDPR compliant?

1. Collect only the absolute minimum personal/demographic data needed to complete the study. It is strongly encouraged that if a study can be completed using only de-identified data (never collecting or recording identifiable information), that does so. NOTE: Many online survey sites collect personal information including IP addresses, by default. Ensure you set up your study to receive only the information you are seeking.
2. Use an active ("opt-in") informed consent. Under the GDPR, consent must be freely given, specific, informed, unambiguous, and explicit. A description of the data processing and transfer activities to be performed, if applicable, must be included in the informed consent document. Following an informed consent description, a "Click next to proceed to the survey" button or equivalent is sufficient for "active" consent for online data collection. Silence, pre-ticked boxes, and inactivity do not constitute "active" consent.
3. To the extent possible, verify any third-party website or app being used for data collection is GDPR-compliant.
4. Ensure that the consent form is compliance with GDPR requirements (see question below on this issue)
5. For activities in which identifiable data is collected, include an executable plan (pre-approved by the Chief Information Security Officer (CISO) to remove data in the event a participant requests to have their data removed. NOTE: The informed consent document requires that the participant be notified that their participation is voluntary and that they may leave the study at any point; the informed consent document does not require the researcher to document HOW the data erasure will take place if requested.
6. In the event of a data breach, notify the General Counsel and CISO (as described below) immediately so that appropriate steps can be taken at the University level. You will also need to contact the Research Compliance Coordinator (RCC) and submit a completed "TU IRB Adverse Events-Problems Form".

My study is currently approved. Do I need to do anything further to comply with the GDPR?

If you are collecting or will collect "personal data" from human subjects in the EEA for your research, your project may be subject to the GDPR. If your research involves any of the following, contact the Research Compliance Coordinator at carmen-schaar-walden@utulsa.edu and the CISO at jonathan-kimmitt@utulsa.edu to ensure you are in compliance:

1. Recruitment through social media site(s)
2. Use of a third party internet site (Qualtrics, SurveyMonkey, etc.) or app to collect data
3. Direct receipt of data from individuals (participants, research collaborators, etc.) in a country affected by GDPR

*****NOTE: submission of a modification may be required to bring your project into compliance.

How is the consent documentation and process affected by GDPR?

Data can be used in scientific research with the freely given, specific, informed, unambiguous, express written consent of the individual data subject. The consent documentation must include a "well-described purpose" for the scientific research and must be clearly distinguishable from other matters. Unfortunately, although the GDPR does recognize that it is often not possible to fully identify the purpose of data processing for research purposes at the time the data is collected, the consent cannot be broadly drafted. Guidance suggests that while the initial consent may be broad in nature, the data subjects would then be given the opportunity to consent to each individual use of the collected data as the new purpose becomes clear.

A controller must provide the data subject with a notice of the controller's privacy practices. This notice must be: (i) concise, transparent, intelligible, and easily accessible; (ii) written in clear and plain language, particularly if addressed to a child; and (iii) free of charge. Generally, the notice must answer the who/what/why/where/when/how questions related to data collection and use:

1. What information is being collected/processed?
2. Who is collecting/processing it (including contact information)?
3. How is it collected/processed?
4. Why is it being collected/processed, including the lawful basis?
5. How will it be used?
6. How will it be stored and for how long?
7. Who will it be shared with (including third-parties)?
8. What will be the effect of this on the individuals concerned?
9. Is the intended use likely to cause individuals to object or complain?
10. Will it be transferred to a third country and, if so, what is the lawful basis for such transfer?
11. The data subjects must also be informed of their rights to request access, rectification, erasure or restriction of processing, to object to processing, and the right to data portability.

1. In the context of consented research, such notice can be built into the informed consent form. With respect to the consent process at TU: Consent records, including *time* and *date* of consent, must be maintained for each subject. In the case of verbal, online, or any other type of undocumented consent, the Principal Investigator is responsible for maintaining a consent log indicating each subject (either by name or study ID number) and the date and time that they provided consent.

2. Consent must be explicit. If the consent form or consent script serves multiple purposes (e.g., a consent form that is also the recruitment email), then the request for consent must be clearly distinguishable within the document.
3. Each subject has a right to withdraw consent, at any time. Each subject must be informed of this right prior to giving consent. Withdrawal of consent must be as easy as giving consent.
4. Consent must be an affirmative action. This means that opt-out procedures or pre-checked boxes indicating consent are not permitted.
5. Consent information must be provided in clear and plain language in an intelligible and easily accessible format. Consent forms using excessive jargon or that do not have separate sections with section headings will be returned for revision.
6. Consent must be freely given. Individuals in a position of authority cannot obtain consent, nor can consent be coerced. This means that faculty members or teachers cannot obtain consent from their own students.
7. **Consent forms must contain the following information:**

- ✓ The identity of the Principal Investigator;
- ✓ The purpose of data collection;
- ✓ The types of data collected, including listing of special categories:
  - o Racial or ethnic origin;
  - o Political opinions;
  - o Religious or philosophical beliefs;
  - o Trade union membership;
  - o Processing of genetic data;
  - o Biometric data for the purposes of unique identification;
  - o Health data; and/or
  - o Sex life or sexual orientation information;
- ✓ The right to withdraw from the research and the mechanism for withdrawal (this may mean keeping the link or master list indefinitely);
- ✓ Who will have access to the data;
- ✓ Information regarding automated processing of data for decision making about the individual, including profiling;
- ✓ Information regarding data security, including storage and transfer of data;
- ✓ How long data will be stored (this can be indefinite);
- ✓ Whether and under what conditions data may be used for future research, either related or unrelated to the purpose of the current study.

What if consent is withdrawn?

Upon the withdrawal of consent at any time, the controller should delete or anonymize the personal data straight away and its use of the data for the research study should stop. However, if the data needs to be retained after consent is withdrawn; the informed consent form must specify as such and indicate at the outset that, even if consent is withdrawn, the entity will retain the data for another identified lawful basis. However, this does not mean that the controller can swap from consent to another lawful basis. When data is processed for multiple purposes, the controller must be clear at the outset about which purpose applies to each element of data and which lawful basis is being relied upon.

My study involves data collection from EEA participants, but the data being collected is not private identifiable information. Is my project still subject to the GDPR?

No, as long as the collected data cannot be used to directly or indirectly identify participants.

*****It is important to remember that some third-party data collection sites might collect personal data covered by the GDPR; even if this information is not passed on to you, the researcher. When using third-party sites, you are responsible for ensuring the third-party site used is operating in a GDPR-compliant way. This can be done by vetting with the CISO (to the extent possible) the privacy and security policies of the site you are using.

I will be traveling to a country covered by the GDPR and will be sending data to the United States while on the trip. Is this affected by the GDPR?

Yes, if you are sending any "personal data" as defined by GDPR. Any personal data you send when physically located in an EEA country falls under the GDPR, even if you are a U.S. citizen. Any data falling under the GDPR requires the data subject to provide consent to allow the data transfer to occur there. **If consent is not obtained, the data cannot be transferred.**

My research project involves recruiting participants and/or collecting data through internet sites. Does this fall under the GDPR?

It might. Since online surveys can be completed from any location with internet access, a participant may be engaging in your research project from an EEA location without your knowledge. One way to assist with this determination would be to add a question at the beginning of your survey to determine if the individual is participating from an EEA location. You could use this information either to ensure compliance with GDPR or to remove those individuals from the participant pool prior to collecting any identifiable data thereby ensuring your activity does not fall under the GDPR.

I am contacting study participants in the EEA directly to obtain information for my research. Does this fall under the GDPR?

Yes, if the participants are providing you "personal data" as defined by the GDPR. Contact the Research Compliance Coordinator at carmen-schaar-walden@utulsa.edu and CISO jonathan-kimmitt@utulsa.edu, if you have a specific question related to an ongoing or upcoming project.

What is "right to erasure"?

Under the GDPR, individuals have the right to request that their previously provided data be erased. Given this right of erasure, investigators may need to keep the link or master list indefinitely. If an individual covered by the GDPR contacts you at any point after data collection asking for their data to be erased, please contact the Research Compliance Coordinator at carmen-schaar-walden@utulsa.edu.

If there is a data breach for research subjects to GDPR, what needs to happen?

The GDPR has strict rules and timelines regarding report of data breaches. As such, any data breach occurring on a project involving GDPR-covered research must be reported within 24 hours upon identification of the breach to the General Counsel at (918) 631-2525 and the Chief Information Security Officer at (918) 631-2743. Potential breaches can also be reported to TU Incident Response at incident-response@utulsa.edu. The following information should be communicated, to the extent known:

1. Type of breach
2. Nature, sensitivity, and volume of personal data
3. Severity of consequences for individuals

4. Number and characteristics of affected individuals
5. Ease of identification of individuals
6. TU IRB Protocol number and title

As more information or guidance becomes available or when/if the GDPR is revised to address the research community, notification will be sent out to the TU research community.

***For EU GDPR informed consent requirements see:**

TU IRB ICF and GDPR Instructions

https://www.hhs.gov/ohrp/sachrp-committee/recommendations/attachment-b-implementation-of-the-european-unions-general-data-protection-regulation-and-its-impact-on-human-subjects-research/index.html

Appendix I: HIPAA v. GDPR

GEOGRAPHIC SCOPE

HIPAA	GDPR
Limited to organizations that meet the definition of a "Covered Entity" or a "Business Associate" HIPAA does not address extraterritoriality	The GDPR also applies to any organization outside of the EU that processes the personal information of an individual who is physically located in the EU which either (i) offers goods or services to such individual, or (ii) monitors the behavior of such individual

ROLES IN DATA COLLECTION AND USE

HIPAA	GDPR
"Covered Entity" – health plans, health care clearinghouses, and health care providers who electronically transmit health information for certain transactions "Business Associate" - performs or assists in performing, for or on behalf of a covered entity, a function or activity regulated by HIPAA	"Controller" - 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 "Processor" - a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

COVERED DATA

HIPAA	GDPR
"PHI" – individually identifiable health information created or received by a health care provider, health plan, or health care clearinghouse	"Personal Data" - any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This would include data on the PI or research team members. "Special Category Data" - race; ethnic origin; politics (including opinions); religion; trade union membership; genetics; biometrics (where used for ID purposes); health; sex life; or sexual orientation. "Data concerning health" - 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

DE-IDENTIFIED DATA

HIPAA	GDPR
"De-Identified Data" - Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information 18 identifiers must be removed Once properly de-identified then no longer considered PHI and subject to HIPAA	"Anonymized Data" - data rendered irreversibly anonymous in such a way that the data subject is not or no longer identifiable "Pseudonymization" - the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information.

Appendix I: HIPAA v. GDPR

PERMITTED PROCESSING AND USE		
HIPAA	**GDPR**	
Consent	Permitted pursuant to an individual's authorization, which must include a number of required elements.	Permitted if the data subject has freely given consent to the processing of his or her personal data for one or more specific purposes
Medical Treatment	"Treatment" exception is part of the standard "TPO Exception" (treatment, payment, operations)	Permitted when necessary for the purposes of medical diagnosis, the provision treatment or management of health systems.
Legally Required	Permitted when disclosure is required by law	Permitted to comply with a legal obligation
General	PHI may be used or disclosed for the administration of the entity holding the data or to fulfill its obligations under a contract	Permitted when processing is necessary for the purposes of the legitimate interests pursued by the controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject
Research	PHI may be disclosed for research purposes – limited data set with data use agreement, consent, IRB waiver	Permitted for scientific and historical research purposes or statistical purposes – must have safeguards in place