The European Union (EU) General Data Protection Regulation (GDPR)

What is the GDPR?
The General Data Protection Regulation (GDPR) is a European law that established protections for privacy and security of personal data about individuals in European Union (EU) and the European Economic Area (EEA)-based operations and certain non-EEA organizations that process personal data of individuals in the EEA. It applies to the collection and use of personal information:

- Through activities within the borders of EU/EEA countries
- That is related to offering goods and services to EU/EEA residents, or
- That involves monitoring the behavior or EU/EEA residents.

The Effective Data for the GDPR is May 25, 2018. The UTHSA Office of Legal Affairs has interpreted the regulation to be applicable when ***targeting*** an individual in the EU/EEA.

What countries 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	UK	Norway	Iceland
Lichtenstein				

Why does this affect me in the United States?
Personal data collected in, or transferred from, any of the above countries is subject to the GDPR. Failure to follow these regulations if they apply 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 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.

GDPR and Coded Data
Of significance to the research community, GDPR considers *pseudonymized data* (e.g., coded data) to be *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 regulation protecting human subjects.

GDPR and Anonymized Data

The GDPR does not 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 UTHSA 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 UTHSA investigators. This is the case even where UTHSA 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?

- It establishes the circumstances under which it is lawful to collect, use, disclose, destroy, or otherwise process *personal data.*
- It establishes certain rights of individuals in the EEA, including rights to access, amendment, and erasure (right to be forgotten).
- 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.
- 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 are the key differences between GDPR and HIPAA?

The key difference between GDPR and HIPAA is the focus. GDPR focuses on protecting EU citizens' PII. Therefore, any organization that handles an EU patient's information can be subject to GDPR regulations. In contrast, HIPAA is focused on organizations – covered entities and business associates – that handle protected health information (PHI) within the United States. In addition to this fundamental difference, GDPR has a much broader scope of coverage than HIPAA. Despite similarities between GDPR's data concerning health and HIPAA's PHI, GDPR also addresses "sensitive personal data" such as racial or ethnic origin and religion. HIPAA, in contrast, is limited to PHI alone.

What activities are subject to the GDPR?

- 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).
- Activities involving the transfer of personal data collected under the GDPR from an EEA country to a non-EEA country.

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 asthe researcher. When using third-party sites, you as the researcher are responsible for ensuring the third-party site being used is operating in a GDPR-compliance way. This can be done by vetting (to the extent possible) the privacy and security policies of the site you are using.

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 **and you are "targeting" individuals in the EU for their participation or are monitoring their behavior in the EEA as part of the study**. Contact IRB@uthscsa.edu if you have a specific question related to an ongoing or upcoming project.

What activities are NOT subject to the GDPR?

Activities involving collection of identifiable personal data from individuals within the EEA who **are not specifically being *targeted*** either by offering goods or services to them or by monitoring their behavior are not subject to the GDPR**.**

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

Probably not, as long as individuals in the EU/EEA **are not specifically being targeted.** The GDPR does not apply to occasional instances of internet use. Rather, regulators look for other clues to determine whether the organization set out to target people in the EU/EEA. An internet survey or recruitment site provided solely in English and Spanish would not necessarily target the EU/EEA. However, a website translated in German would be an example that targets an EU/EEA population and would be subject to the GDPR.

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?

No, provided that the sharing of *personal data* is not related to a specific offer directed at individuals in the EU/EEA or to a monitoring of their behavior in the Union.

My study is currently approved. Do I need to do anything further to be in compliance 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 activities and specifically targeting individuals in the EU/EEA or you are utilizing a company located within the EU/EEA, contact the IRB through the IRB@uthscsa.edu mailbox to ensure you are in compliance:

- Recruitment through social media site(s)
- Use of a third-party internet site (Qualtrics, Skye, etc.) or app to collect data
- Direct receipt of data from individuals (participants, research collaborators, etc.) in a country affected by GDPR
- Submission of a modification may be required to bring your project into compliance.

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

- Collect only the absolute minimum personal/demographic data needed to complete the study. If a study can be completed using only de-identified data that is strongly encouraged. 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.
- 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.
- To the extent possible, verify any third-party website or app being used for data collection is GDPR-compliant.
- Ensure that the consent form is compliant with GDPR requirements (see question below on this issue)
- For activities in which identifiable data is collected, include an executable plan 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.
- In the event of a data breach, notify the IRB and the Compliance office immediately so that appropriate steps can be taken at the University level.

How is the consent documentation and process affected by GDPR?

- 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.
- 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.
- 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.
- Consent must be an affirmative action. This means that opt-out procedures or pre-checked boxes indicating consent are not permitted.
- 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.
- 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.
- 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:
    - Racial or ethnic origin;
    - Political opinions;
    - Religious or philosophical beliefs;
    - Trade union membership;
    - Processing of genetic data;
    - Biometric data for the purposes of unique identification;
    - Health data; and/or
    - Sex life or sexual orientation information;
- The right to withdraw from the research and the mechanism for withdrawal;
- 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 is *right to erasure*?
Under the GDPR individuals have the right to request that their previously provided data be erased. 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 Human Research Protection Office through IRB@uthscsa.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 Institutional Compliance and Privacy Office (210-567-2014). The following information should be communicated:

- Type of breach
- Nature, sensitivity, and volume of personal data
- Severity of consequences for individuals
- Number and characteristics of affected individuals
- Ease of identification of individuals
- Protocol number

You must also report the breach to IRB and through the Prompt Reporting in REDCap within 7 calendar days.