The General Data Protection Regulation (GDPR)

What is the GDPR?
The *General Data Protection Regulation* (GDPR) is a law of the European Union (EU) that enhances data privacy by imposing strict requirements on the use of personal data and by making data privacy laws more uniform across the European Economic Area (EEA).

In which countries does the GDPR apply?
The GDPR covers/applies to all EU member states and all countries in the EEA. These states include the following:

Austria	Finland	Latvia	Portugal
Belgium	France	Liechtenstein	Romania
Bulgaria	Germany	Lithuania	Slovakia
Croatia	Greece	Luxembourg	Slovenia
Cyprus	Hungary	Malta	Spain
Czech Republic	Iceland	Netherlands	Sweden
Denmark	Ireland	Norway	Estonia
Italy	Poland		

When/how is the GDPR apply?
The physical location of the subject determines the applicability of the regulation. **If the person is physically located within an EEA country at the time of the data collection, regardless of their country of citizenship, their personal data is covered by the GDPR.** Personal data of an individual who is physically located outside of the EEA at the time the data is collected is not covered by the GDPR, even if they are a citizen of a country that is a member of the EEA. However, if the personal data of this individual is subsequently processed (e.g., used, stored, or shared) after their return to the EEA, such data may be within scope of the GDPR.

How does this affect my research with human participants?
If your research involves any of the following, your project may be subject to the GDPR:

1. Recruitment through social media, such that some participants may be located in the EEA;
2. Use of a third-party "processor" (e.g., Qualtrics, Skype) to collect data from participants who may be located in the EEA;
3. Direct receipt of data from individuals (participants, collaborators, etc.) located in the EEA
4. Receiving data from third parties that have identified the data as being subject to the GDPR.

What does the GDPR consider "personal data"?
The GDPR defines *Personal Data* as any identifiable information about a natural person (i.e., an individual, not a company or other entity), also known as a "data subject". Examples include a person's name, email address, government-issued identification, other unique identifiers such as IP addresses or

cookies, and their personal characteristics, including photographs.

In addition, there are also "**Special Categories"** of personal data that merit a higher level of protection. This is due to their sensitive nature and consequent risk for greater privacy harm. These include information related to health, genetics, race or ethnic origin, biometrics, sex life or sexual orientation, political opinions, religious or philosophical beliefs, or union memberships. Although not considered a special category or personal data, criminal records are also subject to protection under the GDPR.

What research data fall within the scope of the GDPR?
Three kinds of data fall within the scope of the GDPR:

1. **Identifiable Data**
   Personal data collected from individuals who are, at the time of data collection, physically present in any of the EEA countries, is subject to GDPR. The GDPR can apply to data collected by a YSU employee or student, or data collected by a third party and sent to YSU researchers for analysis as part of a collaboration, from a data bank or repository, or pursuant to any other agreement or arrangement.

2. **Coded Data**
   Under the GDPR, **"pseudonymized data"** (coded data) is considered personal data even where one lacks access to the key-code/coding system/crosswalk required to link data to an individual data subject.

   Example: A non-YSU entity collects personal data from subjects who are located in the EEA, codes the data, secures the key, and sends only the coded data to YSU, such that YSU researchers have no means of accessing the identifiers. This data is still considered personal data in the hands of the YSU researchers, and is therefore subject to GDPR regulations.

   In this scenario, the non-YSU entity is considered the **"controller"** of the data, and harbors greater liability and responsibility for protecting the data, including the management of consent, options for withdrawing consent, coding the data appropriately, and conveying to YSU the conditions under which the data are to be used. YSU researchers, in most of these cases, would be considered a **"processor"** of the data under the GDPR. As a processor, a YSU researcher is be responsible for ensuring that they comply with the controller's terms for using and safeguarding the data.

   Note: Under the US regulations for human subjects' research, this type of coded data would not be considered to be human subject research and therefore would not require IRB review. Because the GDPR imposes significant new requirements for coded data, researchers are urged to consult the IRB office if their research is or may be subject to these regulations.

3. **Anonymized Data**
   The GDPR does not apply to data that have been anonymized. **In order for data to be considered completely anonymized, there can be no key code in existence anywhere that could re-identify the data**. Essentially, any record of identifiable information about participants must be destroyed, whether in a system or on paper.

Example: A survey conducted using Qualtrics or another third-party online survey tool where the researcher receives assurances that the data is not linked to any IP address or other identifiable information; or paper records where no information about the participant is collected or recorded.

What are the data processing requirements under the GDPR?

1. Under the GDPR a so-called **"lawful basis"** is needed. This justifies the processing of personal data, and establishes the circumstances under which it is lawful to collect, use, disclose, retain, destroy, or otherwise process personal data. For research involving human participants, informed consent is considered the lawful basis for collecting and processing personal data.

2. If the GDPR applies, **explicit informed consent** must be obtained from data subjects at the point of collection. The consent process must include a description of how a participant's personal data will be processed, and with whom it may be shared. This consent must describe any planned or expected use of the data. Please see the section of this document on specific consent documentation requirements.

3. If data is subject to the GDPR, data subjects must be able to exercise certain rights with respect to the data they provide. Data subjects have the right to access, amendment, erasure ("right to be forgotten"), restriction, and objection to processing. The "controller" of the data (which may or may not be the YSU researcher, as explained above) is responsible for responding to these requests from study participants.

    a. **If YSU is the controller:** In cases where a YSU researcher is directly collecting personal data from data subjects (i.e., when YSU is acting as the controller), consult with the YSU IRB if granting the participants the ability to withdraw data is not feasible for the study and can compromise analysis and outcomes. Otherwise ensure that the data is managed in a way that allows you to honor a request for withdrawal. The study consent form must include an explicit statement about withdrawal and contact information for the IRB.

    b. **If YSU is the processor:** In cases where a YSU researcher is the recipient of coded data from a third party and does not have the key or other mechanism to link data to individuals, contact information for the controller must be provided to participants.

4. The GDPR also requires researchers to implement appropriate technical and organizational security measures to ensure a level of data security that is appropriate to the risk of harm to the research participants.

5. In the event of a security breach, timely breach notification is required. If a breach occurs in the course of a study involving data that may be protected by the GDPR, the PI must inform the YSU IRB, YSU Information Security Services at security@ysu.edu, University Counsel and:

    a. either notify the appropriate EEA data protection authorities within 72 hours following the discovery of a personal data breach; or

b. without undue delay, notify the applicable controller of the data.

6. Contractual documentation is required when personal data is transferred from EEA countries to other jurisdictions that, in the eyes of the EEA, lack adequate data protection laws. The United States is one such jurisdiction. Documentation is required when:

    a. controllers provide GDPR-classified data to YSU researchers; or,

    b. YSU researchers use third parties to support their research (e.g. Qualtrics, Skype) where participants may be located in the EEA.

What can I do to make my project GDPR compliant?

1. **Collect the absolute minimum personal/demographic data needed.** Consider designing the study so that it can be done anonymously, or record no identifying information.
    a. Many online survey sites collect personal information, including IP addresses, by default. Since IP addresses are considered identifiable information, make sure that you need to collect this information for your study. If not, disable this feature. If other electronic systems are used, consult the IRB office for guidance.

2. **Use an active ("opt-in") informed consent.** Under the GDPR, consent must be freely given, specific, informed, unambiguous, and explicit. In your consent, include:

    a. a description of the data processing and how data will be transferred (electronically or via any other means) to non-EEA jurisdictions. ***NOTE:*** Following informed consent language, a button stating "click to proceed to the survey" or similar is considered active consent for these purposes. Silence, pre-ticked boxes, and inactivity do not meet the standard for active consent under the GDPR.

    b. details on how to withdraw consent and to whom participants may contact to exercise these rights

3. **Verify that contracts with any third-party website or software applications include language clarifying GDPR roles and responsibilities and specifying mechanisms to be used for global data transfers**. If you wish to use any other services or software solutions, a data processing agreement will need to be in place. If the third party does not have this agreement language, YSU can provide appropriate language.

4. For research where identifiable data will be collected, **include an executable plan to restrict processing or remove data in the event the participant requests to have their data removed**.

    a. ***NOTE:*** The informed consent document must notify the participant that their participation is voluntary and that they may leave the study at any point; however, the informed consent need not describe how the data erasure will take place if requested. It is sufficient if these procedures be in place and available internally.

5. **Utilize appropriate administrative and technical safeguards** to protect the personal data collected.

6. **In the event of a data breach or suspected loss of data, immediately notify the IRB** so that appropriate steps can be taken at the University level and proper, timely response and support may be provided. If the data breach involves information technology of any kind, such as computers, the PI must report the data breach to YSU Information Security Services at security@ysu.edu.

How is informed consent affected by the GDPR?

- Consent records, which must include the time and date of consent, must be maintained for each study participant. In the case of verbal, online, or other undocumented consent, the Principal Investigator is responsible for maintaining a consent log indicating each participant (either by name or study ID number), the date and time that they provided consent, and the method by which consent was given.

- Consent must be explicit, and be provided in clear, plain language. If a consent form or script serves multiple purposes (as in, a recruitment email that doubles as a consent form), the request for consent must be clearly distinguishable within the document or script.

- Participants must be given the right to withdraw consent at any time. Each subject must be informed of this right prior to giving consent. Withdrawing consent must be as easy as giving consent. If you believe that a participant withdrawal would jeopardize your research, consult the IRB.

- Consent must be an affirmative action. This means that opt-out procedures or pre-checked boxes indicating consent cannot be used.

- Consent must be freely given. Individuals in a position of authority cannot obtain consent, nor can consent be coerced. For example, faculty 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 any of the following special categories of information that will be gathered:
        - 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;
    - Data access and data security, including storage and transfer of data;
    - Information regarding automated processing of data for decision making about the individual, including profiling;
    - How long data will be stored (can be indefinite);
    - Whether and under what conditions data may be used for future research, whether or not related to the purpose of the current study.

Does recruiting participants or collecting data online fall under the GDPR?

It might, if you are seeking participants from the EEA countries. However, in cases where a survey is sent to potential participants without a geographical preference, where there is no mechanism by which the location of the participants will be identified, GDPR does not apply. Consult with the IRB office for clarification if you are seeking participants from the EEA countries, and are collecting identifiable personal information.

If there is a data breach, what needs to happen?

The GDPR has strict rules and timelines for the reporting of data breaches. If you identify that a data breach has occurred involving GDPR-covered research, immediately report the breach to the IRB and YSU Information Security Services at security@ysu.edu and include the following information:

1. Type of breach and timeline of events
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, in light of the breach
6. IRB Protocol number

If you are unsure if your research may be affected by the GDPR, contact the IRB or the Office of Research Services for assistance

Sources:
This handout was adapted for use with permission from Cornell University's IRB document, "The impact of the European Union (EU) General Data Protection Regulation (GDPR) on research data collected from human participants."