IRB Standard Operating Procedure
**Compliance with the European Union's General Data Protection Regulation (GDPR)**

**INTRODUCTION**

The GDPR is a broad-scale regulation designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way organizations across the region approach data privacy.

EU countries are: 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 and the UK. The EEA includes EU countries and also Iceland, Liechtenstein and Norway. (When the UK exits the EU, the UK Government has indicated it will implement an equivalent or alternative legal mechanisms which are expected to be based on the GDPR.)

**SCOPE**

The GDPR applies to European Union (EU) and non-EU European Economic Area (EEA) nationals, regardless of where they are residing, and non-EU/EEA nationals residing in EU and EEA countries.

The GDPR applies to **US-based organizations** if that organization offers goods or services to individuals in the EEA, is established in the EEA and acts as a data controller or processor, and/or monitors the behavior of individuals in the EEA.

College of Charleston human participant researchers must comply with the provisions of the GDPR when they

- recruit participants using social media,
- target participants who are nationals of EEA countries,
- conduct research in countries covered by the GDPR, and/or
- conduct research involving College of Charleston students who are nationals of EEA countries.

**DEFINITIONS**

Anonymized Data is data in which there are no *identifiable pers*ons, i.e., all personal identifies have been removed.

An ***identifiable person*** is one 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 person. Parental consent will be required to process the personal data of children under the age of 16 for online services; member states may legislate for a lower age of consent but this will not be below the age of 13.

***Legal Basis*** is a GDPR-specific term that is a justification for the collection and processing of personal data. The Legal Basis options that would affect College human participant research are:

- **Consent -** the individual has given clear consent for you to process their personal data for a specific purpose.

- **Legitimate interests -** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests, e.g. research for which a waiver of consent can be justified.

***Personal data*** is any information relating to an ***identifiable person*.**

***Special categories of personal data*** are defined in the GDPR as potentially sensitive data and include racial or ethnic origin, data concerning health, data concerning a natural person's sex life or sexual orientation, genetic data, biometric data used for the purpose of uniquely identifying an individual, and political opinions, religious or philosophical beliefs, or trade union membership. Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its storage and use.

***Pseudonymised data*** is coded data. It is considered to be *personal data* subject to the protections of the GDPR. This is in contrast to the Common Rule, which generally does not protect such information as "identifiable private information" provided that certain steps are taken to prevent the investigator from obtaining the means to link the code to the subject's identity.

A ***Privacy Notice*** is another GDPR-specific term that refers to the notification required for the collection and transfer of the data of ***identifiable persons***. .

For IRB Purposes, the Consent Form serves as the Privacy Notice. The College of Charleston IRB Consent form templates now include the language necessary to satisfy the requirements for a Privacy Notice.

**IRB PROCEDURES RELATED TO GDPR REQUIREMENTS**

The following Information must be included in the IRB application:

- Methods and Procedures Section - proposed uses and storage of the data, including any expected future use. Use of identifiable data beyond the original uses stated in the consent form will require re-consent of the participants.
- Privacy and Confidentiality Section –
    - The period for which the data will be stored, or the criteria used to determine that period
    - Statement that data will be delete or anonymized immediately if a participant withdraws their consent.

Note: Because of the emphasis on full informed consent, research involving deception will be much more difficult to justify for participants covered by the GDPR.

IRB Templates have been updated to include the necessary language to meet the GDPR requirements. This information is:

- The period for which the data will be stored.
- Any projected future use of the data.
- The fact that consent may be withdrawn and data will be deleted.

**Resources**

GDPR Portal - https://www.eugdpr.org/

UK International Commissioner's Office - https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

IRB Approval: Pending