IRB Guidance for Research Subject to EU General Data Protection Regulations (GDPR)**

Updated: 03/12/26

What is the GDPR?

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.

Human Research involving "personal data" about individuals located in (but not necessarily citizens of) the following European Union member states, Norway, Iceland, Liechtenstein, and Switzerland are subject to EU General Data Protection Regulations.

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

* UK update: https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/transition-period-faqs/

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.

Special categories of personal data

The GDPR highlights some "special categories" of personal data which merit a higher level of protection due to their sensitive nature and 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.

GDPR and Coded Data

Importantly, the GDPR considers “pseudonymized data” (e.g., coded data) to be “personal data” even where one lacks access to the key-code/crosswalk required to link data to an individual data subject. *This is inconsistent with U.S. regulations protecting human subjects and, therefore, important for researchers to understand.*

GDPR and Anonymized Data

The GDPR *does not apply* to data that have been anonymized. Under the GDPR, in order for data to be anonymized, there can be **no key-code in existence to re-identify the data**. For example, if UMass Boston 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." This holds true even when UMass Boston researchers have no access to the key-code/crosswalk required to link data to an individual data subject.

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. Of note, the participant **does not need to be an EEA resident**.

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

Activities involving collection of identifiable personal data from individuals who are ***physically located within the U.S.*** at the time of data collection -- *even if the participant is an EEA citizen* -- are not subject to the GDPR.

How do I ensure that my study complies with the GDPR?

- Collect only the absolute minimum personal/demographic data needed to complete the study. If your study can be completed using only de-identified data, then we strongly advise you to take this approach.

- Many online survey sites collect personal information, including IP addresses, by default. Ensure that you set up your study to receive **only** the information you are seeking. To the extent possible, verify that any third-party website or app being used for data collection is GDPR-compliant.

- 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.

- Ensure that your consent form is in compliance with GDPR requirements (see below).

- For activities in which identifiable data is collected, you must have an executable plan to remove data in the event a participant requests to have his/her data removed.

How are the consent documentation and process affected by GDPR?

The good news is that many of the consent requirements under the GDPR are consistent with those that you already implement as part of standard consent processes and documentation. Below are the GDPR requirements:

1. 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 consent was provided.

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.

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 are not permitted.

5. Consent information must be provided in clear and plain language in an intelligible and easily accessible format.

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: 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.

Other Considerations:

- For all prospective Human Research subject to EU GDPR, contact institutional legal counsel or the institution's Data Protection Officer to ensure that the following elements of the research are consistent with institutional policies and interpretations of EU GDPR:
    - Any applicable study design elements related to data security measures.
    - Any applicable procedures related to the rights to access, rectification, and erasure of data.
    - Procedures related to broad/unspecified future use consent for the storage, maintenance, and secondary research use of identifiable private information or identifiable biospecimens.

- Where FDA or DHHS regulations apply in addition to EU GDPR regulations, ensure that procedures related to withdrawal from the research, as well as procedures for managing data and biospecimens associated with the research remain consistent with Appendices A-1 and A-2 above.

- In the event of a data breach, notify the University of Massachusetts IRB immediately so that appropriate steps can be taken.

We thank the **Brown University IRB for sharing this resource with us.