ORARC Tip Sheet:
GENERAL DATA PROTECTION REGULATION (GDPR)

Details:

The General Data Protection Regulation (GDPR) applies to all individuals and organizations with European Economic Area ("EEA")-based operations and certain non-EEA organizations that process personal data of individuals in the EEA. Of note, the EEA includes the 28 states[1] of the European Union and four additional countries: Iceland, Liechtenstein, Norway and Switzerland.

Definitions:

- "Personal data": 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, other unique identifier (such as an IP address), and/or personal characteristics, including photographs.
- "Pseudonymized data": Coded data; under GDPR considered 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.
- "Special categories" of personal data: Information about a 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.

How Does the GDPR Impact My Research?

If you are collecting or obtaining "personal data" from participants residing in the EEA, your project may be subject to the GDPR. Review the following information to learn how GDPR impacts certain research activities.

- **Secondary Use of Coded Data/Specimens**
  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/specimens to an individual. This is in stark contrast to US regulation protecting human subjects. For such research, investigators must comply with the applicable data protection obligations imposed by the GDPR. For secondary research, the pre-approved model contractual clause should be included in the data use agreement (DUA) with the data provider. Investigators should submit DUAs through the Agreements module at https://dua.harvard.edu/ for processing. Note that no data/specimens may be obtained from the EEA until the appropriate agreements have been secured.
- **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 Harvard 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 Harvard investigators. This is the case even where Harvard investigators have no

[1] EEA Countries include: Austria, Belgium. Bulgaria, Croatia, Cypress, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, United Kingdom.

access to the key-code/coding system/crosswalk required to link data to an individual data subject.

- **Prospective Data Collection**
  For research that involves collecting "personal data" from participants residing in the EEA, GDPR compliant consent documents must be implemented. Template consent documents with required GDPR language can be found in the ESTR Library.

Additional Information:

- The GDPR applies to all individuals within the EEA at the time of the research data collection. Citizenship or residency is not a factor as part of GDPR; the participant's *location within the EEA* is the pertinent criteria when considering GDPR applicability.
- Under the GDPR, waivers of consent and/or consent documentation for prospective studies is not allowed, even if the study is Exempt. That said, options for documentation of consent are much broader under GDPR and can be written or electronic. Electronic options include checking an "I consent" box or uploading a signed consent form. Regardless of the method, participant consent must be active and voluntary.
- The IRB-determined Data Security Level (DSL) may be elevated for GDPR studies, especially if the data are a "special category." Even if a study is Not Human Subjects Research or Exempt, the study may require a higher DSL level than a non-GDPR study due to the sensitive nature of the data, as defined by the GDPR. Investigators should be aware when designing their study that they may need to obtain DSL certification from IT prior to beginning their study.
- The IRB may determine that the study meets certain criteria requiring the Office of the Vice Provost for Research to review whether a Data Protection Impact Assessment (DPIA) is required for the study. In this case, the IRB Review Specialist will trigger the DPIA ancillary review in ESTR. This ancillary review must be completed before final IRB approval is be granted.

Case Examples:

- **Case 1:** A Harvard researcher conducts interviews with Syrian refugees now located in Germany. They will collect demographic data about the participants, as well as their experiences as a refugee and their political beliefs about the current conflict in Syria. Because participants are located in the EEA at the time of data collection, GDPR applies. Additionally, the data collected would be considered a "special category" because it will be about their political beliefs.
- **Case 2:** A Harvard researcher conducts interviews with former MDs from the United Kingdom (UK). The doctors have since left their positions in the UK and are now working at institutions in Canada and the US. The study is looking at clinic infrastructure in the UK, and wants to understand why the doctors have left their UK positions in favor of jobs elsewhere. Although the study is interested in the UK clinics' policies and problem areas, there is no personal data being collected in the UK. The doctors being interviewed are not within the EEA at the time of the interview and, therefore, GDPR does not apply.
- **Case 3:** A Harvard researcher conducts secondary analysis of a data set from Italy which includes information about caffeinated beverage consumption throughout the country. The Harvard researcher does not have access to identifiers, codes, or linkages, however, the original PI in Italy collected name, date of birth, and address as part of their study. Because the data would be considered "pseudonymized data" under GDPR, GDPR applies and the DUA must include a model contractual clause.
- **Case 4:** A Harvard researcher interviews health care leaders from Africa to study gender biases in institutional hiring practices. The interviews will be conducted over Skype and the participant could be anywhere in the world, including the EEA. In this case, GDPR may apply to participants in the study. The protocol will need to explicitly state that data may be collected within the EEA,

and ensure GDPR regulations are followed for anyone in the EEA. However, because these policies are not required for participants outside of the EEA, the consent or data storage procedures may be different within the protocol based on where the participant's data was collected from.

Resources at Harvard:

- The Harvard University GDPR Working Group has a website with some background and guidance on Harvard's response to the GDPR which is behind Harvard Key login. Check it frequently as information continues to be added. Additionally, visit the EU GDPR Portal.
- The Office for Human Research Protections (OHRP) has posted a "Compilation of European GDPR Guidances" which lists, by country, the data protection authorities of all EEA countries that fall under the GDPR. For each country, the compilation also provides the links to any general GDPR guidance, as well as specific guidance on the topics of Research, Legal Basis, Consent, and International Data Transfer.
- If you have any general questions about GDPR or wish to speak to someone regarding whether your research activities requires GDPR compliance, contact your department-assigned IRB Review Specialist.
- For assistance ensuring GDPR compliance (e.g., submission assistance; consent form editing, etc.), submit a service request to the Quality Improvement Program.

Additional ORARC Toolkit Materials:

- HRP-121 - SOP - HLC - GDPR
- HRP-325 - WORKSHEET - GDPR
- GDPR Notification for Participants