THE UNIVERSITY OF ARIZONA Research & Partnerships

European Union General Data Protection Regulation Requirements

Background

The General Data Protection Regulation (GDPR) effective March 25, 2018, is a broad-scale regulation designed to harmonize data privacy laws across the Europe Union (EU), to protect and empower all EU citizens' data privacy, and to reshape the way organizations across the region approach data privacy. Investigators should be aware that research involving "personal data" about individuals located in the EU and European Economic Area (EEA) must comply with the GDPR.

EU countries are: Austria, Bulgaria, Croatia, Republic of Cyrus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, and Sweden. The EEA includes EU countries as well as Iceland, Liechtenstein, and Norway.

Note: The UK government has exited from the EU. The UK will implement an equivalent or alternative legal mechanism which are expected to be based on the GDPR.

Quick Facts

- GDPR establishes protections for privacy and security of "personal data" as described below.
- GDPR only applies to personal data and coded data (i.e., pseudonymized data).
- GDPR data requires the use of an additional GDPR consent addendum.
- There must be an executable plan to remove data in the event a participant requests to have their data removed.

Scope

The GDPR applies to the processing of "personal data" by a controller or processor who is not physically established in the EU/EEA when the processing is related to (a) the monitoring of behavior of research subjects who are in the EU/EEA, or (b) offering goods or services to research subjects in the EU/EEA.

The United States (US)-based use and processing of "personal data" that has been collected in the EU/EEA, for clinical or other research purposes is subject to the GDPR. The GDPR also applies to "personal data" collected for clinical or other research purposes from research subjects who have relocated to reside in the EU/EEA.

Identifiable data collected from an EU/EEA citizen at a location in the US will be subject to US law and not GDPR, unless the data was solicited from an individual while in the EU/EEA, or the organization continues to monitor the EU/EEA citizen after the citizen returns to the EU/EEA.

University of Arizona human subjects researchers must comply with the provisions of the GDPR when their research involves:

- data collection from persons physically located in the EU/EAA (**note**, this includes a US citizen who is in the EU/EAA at the time of data collection);
- data obtained from an entity in the EU/EAA, such as an industry-sponsor located in the EU/EAA, about individuals located anywhere in the world;
- data collection from accounts or websites of persons or entities in the EU/EEA; or
- "personal data" collection from collaborating researchers/parties in the EU/EEA.

Definitions (specifically as they relate to GDPR Requirements)

- *Anonymized Data* means data in which there are no identifiable persons (i.e., all personal identifiers have been removed).

- *Biometric Data* means personal data resulting from specific technical processing relating to the physical, physiological, or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images of fingerprint data.

- *Data Concerning Health* means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about their health status.

- *Genetic Data* means personal data relating to the inherited or acquired genetic characteristics of a natural person which gives unique information about the physiological or the health of the natural person and which result from an analysis of a biological sample from the natural person in question.

- *Identifiable Person* means 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.

    - Note: 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 by this will not be below the age of 13. Human Subjects Protection Program (HSPP) procedures surrounding parental permission still apply. Please refer to HSPP Guidance, *Research Involving Children* for more information.

- *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 impact University of Arizona human subjects researchers include:

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

- *Legitimate Interests* means the processing of personal data is necessary for the researcher's 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. Specific 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 sexual activities 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 memberships. Personal data relating to criminal convictions and offences are ***not*** included, but similar extra safeguards apply to its storage and use.

- *Pseudonymized Data* means coded data, and it is considered to be personal data subject to the protections of GDPR. ***This is in contrast to the Common Rule, which generally does <u>not</u> protect such information as "identifiable private information" provided that certain steps are taken to prevent the researcher from obtaining the means to link the code to the subject's identity.***

- *Privacy Notice* is a GDPR-specific term that refers to the notification required for the collection and transfer of the data of identifiable persons. ***For HSPP purposes, the Informed Consent Form serves as the Privacy Notice. The University of Arizona has a GDPR-specific Consent Addendum that includes the language necessary to satisfy the requirements of the GDPR Privacy Notice.***

HSPP Procedures related to GDPR Requirements

When a study is subject to GDPR requirements, the following is required upon submission to the HSPP:

- The IRB Protocol document must include information about the:
  - proposed usage and storage of the data, including an expected future use;
  - period for which the data will be stored, or the criteria used to determine that period; and
  - a statement that data will be deleted or anonymized immediately if a participant withdraws their consent.

- *GDPR Consent Addendum* which includes information about:
  - the period for which the data will be stored;
  - any future use of the data; and
  - the fact that consent may with withdrawn at anytime and the data will be deleted.

European Union General Data Protection Regulation Requirements

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.

- For an online survey, use an active ("opt-in") informed consent. Under the GDPR, consent must be freely given, specific, informed, unambiguous, and explicit.

- 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 their data removed.

It is the responsibility of the Principal Investigator to determine whether their study demands adherence to the GDPR requirements. For further assistance, investigators can reference the Department of Health and Human Services Office for Human Research Protections guidance on GDPR or contact the HSPP directly.