UNLV | Office of RESEARCH INTEGRITY HUMAN SUBJECTS

Guidance – Research and GDPR

General Description

General Data Protection Regulation (GDPR) is a European law that went into effect on May 25, 2018. It established data protections for privacy and security of personal data about individuals located in the European Economic Area (EEA). This allows people to have more control over their personal data and that businesses benefit from a level playing field.

When it applies / context

GDPR will apply if you collect personal data/information from research subjects who are physically located in the EEA. The participant does not need to be an EEA resident. However if EEA residents are physically located in the United States (or another country not in the EEA), GDPR does not apply. The EEA includes the following countries:

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

Considerations & Best Practices

Considerations

What is identifiable personal data under GDPR?

"Personal data" is any information relating to an identified or identifiable natural person ("data subject"). An identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, identification number, online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.

"Special categories" of personal data require a higher level of protection due to their sensitive nature and consequent risk for greater privacy harm. This includes information about a data subject's health, genetics, race or ethnic origin, bio-metrics for identification purposes, sex life or sexual orientation, political opinions, religious or philosophical beliefs, or trade union membership. Although criminal convictions and records are not considered "special categories" of personal data, this information is subject to amplified protections under the GDPR.

Anonymized Data: The GDPR does not apply to data that have been anonymized. However, under GDPR, there is no de-identified (or "anonymized") safe harbor akin to HIPAA. Whether data can be considered anonymized, and therefore not subject to GDPR, must be determined based on the facts and

circumstances, considering all the means reasonably likely to be used, either by the person in control of the data ("controller") or by another person, to identify the natural person, directly or indirectly.

Coded or Pseudonymized Data: Data that has been "pseudonymized" (coded data - can no longer be attributed to a specific data subject without the use of key-code information that is kept separately) remains personal data that *is* subject to GDPR.

What is required if you will be conducting research and it is subject to GDPR?

Consent must be **freely given, specific, informed** and **unambiguous** as to the data subject's wishes by a **statement** or by a clear **affirmative action**:

- **Freely given** means the individual must have a realistic choice, or the realistic ability to refuse or withdraw consent. Individuals in a position of authority cannot obtain consent, nor can consent be coerced.
- **Specific** means the consent must be explicit and transparent and contain the following information:
    - Identity of the Principal Investigator
    - Purpose of the data collection
    - Types of data collected, including listing of any special categories of data
    - The right to withdraw from the research and the mechanism for withdrawal
    - Identify who will have access to the data
    - Time period for which data will be stored (can be indefinite)
    - Information regarding data security, including storage and transfer of data
    - Information regarding automated process of data for decision making about the individual, including profiling
    - Information regarding data security, including storage and transfer of data
    - Whether and under what conditions data may be used for future research, either related or unrelated to the purpose of the current study
- **Informed** means that subjects are made aware of the risks, how their data will be safeguarded, their rights in relation to the research (as described below), and how to exercise those rights.
- **Unambiguous** means consent is given through a statement or clear affirmative action.
    - This may be by a written or oral statement or other affirmative act demonstrating consent. For instance, checking a box can indicate consent, while silence or pre-ticked boxes that require unchecking (opting out) cannot.
    - Investigators should be able to demonstrate that a particular subject consented to the research. Consent records, including time and date of consent, must be maintained for each data subject.
    - If the consent form serves multiple purposes, the request for consent must be clearly distinguishable within the document.

- ***There is no ability for the IRB to waive informed consent under GDPR.***

Additionally, there are certain rights that data subjects have:

- The right of access to their data
- The right to request corrections to their data
- The right to withdraw and to request erasure of their data. In this case, data may be retained only if it is anonymized or if another legal basis exists to retain the data. This may include:
  - The need to protect scientific research if deletion would render impossible or seriously impair the research objectives; or
  - The need to protect the public health by ensuring the accuracy and quality of data related to medical care or to investigational drugs and devices
- The right to request transfer of their personal information to a third party (such as a personal physician) in a format suitable for re-use

Best Practices

How do I inform subjects?

As a part of the consent process, you will provide the GDPR Addendum to subjects, which is a separate section in the consent form. This must be signed in order to satisfy the requirement of a clear affirmative action.

Resources

European Commission 2018 reform of EU data protection rules. Retrieved July 9, 2019, from https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en