The GDPR and Research: What you need to know*

- **What is the General Data Protection Regulation (GDPR)?**
  The GDPR is a privacy act in the European Union (EU) and European Economic Area (EEA) countries which regulates the collection, use, and security of personal data. The full regulation and other helpful information can be found here: https://gdpr-info.eu/

  A list of EU and EEA countries can be found here: https://www.gov.uk/eu-eea

- **How does the GDPR impact research?**
  Since the GDPR applies to personal data collected in, or transferred from, any EU or EEA country, research conducted in these locations or with persons in those locations are subject to this regulation. This means that there are additional consent and data protection elements beyond what is typically required by the IRB at UCCS which you will need to consider while designing and conducting your research.

  In general, the GDPR applies to the collection and use of personal data:
  1. Through activities within the borders of EEA countries; or
  2. That is related to offering goods and services to EEA residents; or
  3. That involves monitoring the behavior or EEA residents.

- **What activities are typically subject to the GDPR?**
  1. Activities involving identifiable information if personal data is being collected from one or more research participants ***physically located*** in the EU/EEA at the time of data collection (even if the participant is NOT an EU/EEA resident).
  2. Activities involving the transfer of personal data collected under the GDPR from an EU/EEA country to a non-EEA country.

  Note that citizenship **does not matter** in terms of the GDPR, it is the location of the data to be collected or transferred. For example, data collected from EU or EEA citizens who are in the US **are not** subject to the GDPR. Similarly, data collected from a U.S. citizen who resides in the EU/EEA **will be** subject to the GDPR.

- **What are examples of activities that are NOT subject to the GDPR?**
  Activities involving collection of identifiable personal data from individuals who are ***physically located within the United States*** at the time of data collection (even if the participant is an EU/EEA citizen).

- **What types of data does the GDPR cover?**
  The GDPR regulates the collection and use of personal data which is defined as "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, in particular by reference to an identifier such as a name, an identification number, location data, an online

identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;" (From GDPR Article 4, 1).

The GDPR does not regulate anonymous data, or any data where all identifiers have been removed irreversibly and the data are not coded. Under the GDPR coded, or pseudonymized data, **does not meet** the threshold of anonymous data and **are subject** to all the restrictions of the GDPR. Data can be made anonymous if all identifiers are removed and no code exists to re-identify the data.

- **What are some other data concerns to be aware of?**

  Certain types of data referred to as "sensitive personal data" require additional data security measures due to their nature and risk to participants if there is a data breach. These include data about health, genetics, race/ethnicity, biometrics, sexual orientation/sexuality, political affiliation/opinions, religious affiliation/beliefs, and trade union membership.

- **What participant rights under the GDPR do you need to consider?**

  1. Participants have the right to access their data
  2. Participants can request corrections to their data
  3. Participants can request to withdraw participation AND to have their data purged (right to be forgotten)
  4. Participants can request to have their data transferred to a third party

- **What additional information is required in consent documentation due to the GDPR?**

  1. Consent must be affirmative and specific, and be able to be revoked
  2. Consent must be documented
  3. Subjects must be fully informed of all procedures; deception cannot be used if collecting personal data
  4. All data being collected must be specifically listed, as well as all processes and procedures related to data collection
  5. A statement of subjects' rights to have their personal data removed from the study (prior to any anonymization)
  6. A statement regarding if data will be removed or transferred from the EU/EEA
  7. A statement regarding any third parties who have access to or are involved with the data (i.e. Qualtrics, Survey Monkey, etc.)
  8. A statement about the right to file a complaint with the data protection authority
  9. Please feel free to reach out to privacy@cu.edu or irb@uccs.edu for assistance developing consent form language related to GDPR

- **What do I do if there is a data breach?**

  Data breaches must be reported to the appropriate authorities and effected participants within 72 hours of discovery of the breach. **If you suspect or experience a breach, please contact the IRB irb@uccs.edu and OIT (719) 255-4357 immediately.**