University of Wisconsin-Oshkosh
Institutional Review Board (IRB)

STANDARD OPERATING PROCEDURES (SOP)	
SOP Number: 11 Effective Date: October 31, 2019 Last Reviewed: October 31, 2019 Prepared By: Kelly Schill & Crystal Wagner	**Title:** **Guidance on the General Data Protection Regulation (GDPR)**

I. What is the General Data Protection Regulation (GDPR)?

General Data Protection Regulation (GDPR) is a European Regulation which became effective on May 25, 2018. GDPR provides protections for privacy and security of personal data of natural persons located (living or traveling) in the European Economic Area (EAA).

The GDPR protects personal data by:

1. Establishing the circumstances under which it is "lawful" to collect, use, disclose, destroy, or otherwise process personal data, including when conducting research activities;
    a. A "lawful basis" includes the following circumstances:
        i. When required for:
            1. a contract, public interest, to comply with a law, to protect an individual's life, for the legitimate interests of a third party (no sensitive data)
        ii. Freely given consent for a specific purpose has been provided
2. Establishing certain rights of individuals, including rights to access, amendment, and erasure;
3. Requiring personal data controllers and processors to implement appropriate technical and organizational security measures to ensure a level of data security that is appropriate to the risk to personal data;
    a. Controllers: The legal entity who, alone or jointly with others, determines the purposes and means of the processing of personal data.
        i. Example: The sponsor of a research study or the PI of investigator initiated research
    b. Processors: A legal entity who processes personal data on behalf of the controller.
        i. Example: The PI of an industry sponsored research study, clinical research coordinators, database administrators
        ii. Processing of data involves any of the following: adapting, altering, collecting, combining, consulting, destroying, disclosing, erasing, organizing, recording, retrieving, storing, structuring, and using
    c. Processors and Controllers must take the following measures:
        i. Limit access to the data
        ii. Code or encrypt the data where possible
        iii. Limit processing to only the necessary data
        iv. Retain the data for the least amount of time possible
        v. Incorporate data protection into the processing tasks

4. Requiring notification to data protection authorities and affected individuals within 72 hours following the discovery of a personal data breach.
    a. Data breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored, or otherwise processed.
    b. Any data breach occurring on a GDPR covered study must be reported within 24 hours upon identification to the UW System Legal Counsel and the IRB.

II. What Constitutes Personal Data Under GDPR?

Personal data is defined in GDPR as any information that contains identifiers related to an identified or identifiable natural person, otherwise known as a data subject. Examples of personal data include a person's name, email address, government issued identification, photographs, IP address or cookies, work records/income, test answers, or other unique personal identifiers.

1. Sensitive Data Categories and GDPR
   GDPR lists some special categories of personal data considered to be sensitive in nature and a greater risk for privacy harm: Race/ethnicity, political opinions, religious or philosophical beliefs, trade union membership, income, genetic data, biometric data, health data, data concerning a person's sex life or sexual orientation
    a. **If sensitive data is being processed, explicit consent for those data elements is required.** (i.e., waiver of consent is not allowable)
    b. Although not specifically listed under special categories in the regulation, the use of criminal records requires explicit consent
2. Coded or Pseudonymized Data and GDPR
   Of significance to the research community, GDPR considers "pseudonymized data" (e.g., coded data) to be "personal data" even when one lacks access to the key-code required to link data to an individual data subject. This is in contrast to U.S. research and privacy laws such as the Common Rule and HIPAA.
3. Anonymous Data and GDPR
   Studies that do not collect information that is linked to a subject's identity, such as anonymous surveys, in which the identities of subjects cannot be traced are not subject to GDPR. However, under GDPR, a key-code cannot exist to re-identify data in order for the data to be considered anonymous. If a key-code exists, the data is considered personal data.

III. To Whom Does GDPR Apply?

1. GDPR applies to:
    a. Those who offer goods or services to persons in the European Union (EU) or European Economic Area (EEA)
        i. See Appendix A: European Union (EU) Countries and European Economic Area (EEA)
        ii. EEA= European Union (EU)+ Iceland, Liechtenstein, Norway, and UK.
    b. Those who monitor the behavior of individuals in the EEA
        a. For example, monitoring patients once they return to EEA
    c. Those who collect, control and process data about persons in the EU/EEA
        iii. Regulation is unrelated to citizenship

2. Examples of when GDPR may apply to human subjects research in the U.S. (Including, but not limited to):
    a. Studies sponsored by companies/industry in the EU/EAA
    b. International research involving human subjects in an EU/EAA country in which researchers collect, process, or store personal data.
        i. All international research must comply with the local regulations or laws of the located country.
    c. Web-based research in which researchers collect, process, or store the personal data of participants in the EU/EAA
        i. Example: data collection from social media sites or online survey research
        ii. IRB suggests collecting the minimum amount of personal/demographic data necessary to complete the study or collecting anonymous data when possible. Note: Many online survey sites, including Qualtrics, collect personal data including IP addresses by default so it is important to review the settings prior to distribution.
    d. Transmission of personal data when traveling/visiting EEA country
    e. Studies with long-term follow-up of participants currently residing in the EU/EAA
    f. Long-term biometric monitoring studies involving participants currently residing in the EU/EAA
3. Examples of activities that are NOT subject to GDPR:
    a. Collection of identifiable personal data from individuals who are EEA citizens but are physically located in the United States at the time of data collection

IV. Data Subjects' Rights under GDPR:

A data subject is defined in the GDPR as any natural person or legal entity from whom data is being collected. Data subjects have the following rights:

1. **The right to object:**
   Data subjects must have a genuine choice to accept or decline without detriment the terms offered.
2. **The right to be informed:**
   The following information must be provided to an individual whose personal data is being collected, used, or accessed for research:
    a. The existence of the right to withdraw consent without detriment and how they can exercise that right.
    b. Specific purpose of the use of the data.
    c. What type of data will be collected/used.
    d. The legal basis for using the data.
    e. How long the data will be stored.
    f. Who will have access to the data.
    g. Data protection rights.
    h. Where they can protest or complain the use of their data and the protection of such data.
    i. Contact information for the institution and, if required, a data protection officer.
3. **The right to a notice:**

Data subjects have a right to be informed that their data was collected, where and how it was collected, and for what purpose. Data subjects should also be given notice when personal data is modified and erased.

4. **The right to access:**
   Data subjects have the right to request a free electronic copy of the personal data that was collected from them.
5. **The right to data portability:**
   Data subjects have the right to obtain, transfer, and use their personal data for other purposes of their own desires. This protects subjects from proprietary lock-in as this requires the data not be incompatible with other platforms, preventing a shift in control of the data from the subjects to the processor.
6. **The right to privacy by design:**
   Personal data must be restricted in access to only those data subjects have agreed may have access. Adequate and reasonable security measures must be in place.
7. **The right to restrict processing:**
   Data subjects have the right to cease their data from being further distributed or processed.
8. **The right in relation to automated decision-making and profiling:**
   Data subjects must be offered a degree of control of their data and its processing. Data can only be automated by prior consent of the subject whose data is being automated.
9. **The right to erasure:**
   Data subjects have the right to have any records of their personal data destroyed if desired.
10. **The right to rectification:**
    If any breach of agreement occurs that violates the rights of a data subject, that subject has the right to corrective measures being taken by the responsible party.

V. Impact on the Consent Process:

GDPR permits researchers to rely upon consent from research subjects as a lawful basis for processing personal data for research purposes typically under 'public interest' as the most appropriate legal basis. A waiver of the consent process is not allowable.

Consent Process

To obtain a valid consent for processing an individual's personal data for research purposes under GDPR, the consent must be:

1. **Freely Given:** An individual must have a realistic choice--the realistic ability to refuse or withdraw consent without detriment. Coerced consents by individuals in a position of authority are not compliant with GDPR. Withdrawal of consent must be as easy as giving consent.
2. **Clear Language:** The consent must be in clear and plain language, intelligible, and easily accessible.
3. **Specific on Purpose:** The consent must include a specific, transparent statement of each purpose of the study including the rights articulated above. This must also include specific reference for any future use of the data.
4. **Fully Informed:** An individual must be informed of the nature and extent to which he or she is consenting of data collection activities and use of collected data.

5. **Unambiguous Indication/Affirmative Consent:** GDPR requires a statement or clear, affirmative act—resulting from deliberate action—that indicates that the data subject has agreed to the proposed collection and processing of data activities. Silence, prechecked boxes, and inactivity (all considered passive consent) are not considered to be consent.
6. **Reversible:** An individual must be able to withdraw any degree of their consent at any time for any reason without detriment.
7. **Granular:** An individual must be allowed to give separate consent for distinct personal data processing operations.

Required Elements of Consent to Comply with GDPR

1. Name and/or title of the data processor (Principal Investigator) and any others who will have access to the data
2. Purpose and basis for processing the subject's data
3. Type of data to be processed, including listing of special categories considered to be sensitive:
    a. 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
4. The right to withdraw from the research and the mechanism to withdraw
5. Information regarding automated process of data for decision making about the individual, including profiling
6. Data security provisions, including storage and transfer of data
7. Length of data storage (can be indefinite)
8. Whether and under what conditions data may be used for future research, either related or unrelated to the purpose of the current study

Secondary Research Consent

Secondary research also requires a "lawful basis" for processing of personal data and consent. Sensitive data must be explicitly detailed in the consent document. The purpose of the secondary research must be compatible with the initial purpose when consent was not obtained initially.

Definition of Child for GDPR and Consent Considerations:

GDPR defines a child (for the purposes of using or accessing personal data) as an individual under the age of 16. For any personal data collected regarding a child under the age of 16, the "holder of parental responsibility" must explicitly consent to the collection or use of that child's data. Individual countries may choose to lower the age below 16 within their own jurisdiction, but it cannot be lowered below the age of 13.

VI. Importance of Compliance for UW Oshkosh:

Failure to follow the GDPR places the University at risk of noncompliance, monetary fines, and reputational harm. Fines associated with noncompliance can be up to 20 million Euros or 4% of the University's prior financial year worldwide annual revenue.

Appendix A: European Union (EU) and European Economic Area (EEA)

European Union (EU) member countries:

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

European Economic Area (EEA)

Iceland
Liechtenstein
Norway
All the countries in the EU

Note: The United Kingdom is expected to continue to be a member of EEA into 2019. Switzerland is not a member of the EEA.

References

- Article 29 Working Party guidelines on consent under Regulation 2016/679, revised and adopted on 10 April 2018: (https://iapp.org/media/pdf/resource_center/20180416_Article29WPGuidelinesonConsent_publishpdf.pdf). Accessed 8/2/2019.
- Does GDPR regulate my research studies in the United States? (https://www.mwe.com/en/thought-leadership/publications/2018/02/does-gdpr-regulate-researchstudies-united-states). Accessed 8/2/2019.
- GDPR interactive searchable version online: (https://gdpr-info.eu/). Accessed 8/2/2019.
- GDPR pdf English version of regulation: (http://data.consilium.europa.eu/doc/document/ST5419-2016-INIT/en/pdf). Accessed 8/2/2019.
- Guidance for General Data Protection Regulations (GDPR) compliance in the conduct of human research: (https://irb.northwestern.edu/sites/irb/files/documents/GDPR%20Guidance_0.pdf). Accessed 8/2/2019.
- Guidelines on consent under Regulation 2016/679: (https://www.mayerbrown.com/files/uploads/Documents//PDFs//2017//December//wp259_enpdf__2_.pdf). Accessed 8/2/2019.
- Healthcare researchers prepare for GDPR: What does GDPR mean for health care researchers? (http://www.kantarhealth.com/docs/whitepapers/healthcare-researchers-prepare-for-gdpr.pdf?sfvrsn=10). Accessed 8/2/2019.
- New draft consent guidelines under the GDPR: What you need to know. (https://www.mayerbrown.com/publications/detailprint.aspx?publication=14187). Accessed 8/2/2019.
- New draft guidelines on GDPR consent requirement's application to scientific research: (https://biglawbusiness.com/new-draft-guidelines-on-gdpr-consentrequirements-application-to-scientific-research/). Accessed 8/2/2019.
- Personal data: Definition: (https://www.cnil.fr/en/personal-data-definition). Accessed 8/2/2019.
- A primer on the use of personal data from the European Union: (http://rgs.usu.edu/irb/guidelines/). Accessed 8/2/2019.
- Roles and responsibilities of principal investigators/co-investigators: (https://www.umass.edu/research/policy/pi-and-co-pi-roles-and-responsibilities). Accessed 8/2/2019.
- General Data Protection Regulation (https://privacy.ucdavis.edu/gdpr). Accessed 8/14/2019.
- The European Union (EU) General Data Protection Regulation (http://www.irb.pitt.edu/GDPR). Accessed 8/15/2019.
- IRB Guidance: GDPR and Research at UW (https://kb.wisc.edu/page.php?id=89204) Accessed 8/15/19