General Data Protection Regulation

Purpose

The purpose is to outline the policy and procedures for compliance with the European Union (EU) and Economic Area's (EEU) General Data Protection Regulation, which became effective May 25, 2018.

Policy | Special Categories | Consent | Inadvertent Activation | Penalties | Data Breach Reporting | Procedures

Definitions

Anonymized Data is data in which there are no identifiable persons, i.e., all personal identifies have been removed.

Controller is a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the "processing" of personal data.

Identifiable 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, online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person. 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 but not below the age of 13.

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 affect human research are:

- ***Consent* -** the individual gives clear permission for an investigator to process his/her personal data for a specific purpose

- ***Legitimate interests*** **-** the processing is necessary for an investigator'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 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 (e.g. IP address or cookie identifier), or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.

Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Processor is a natural or legal person, public authority, agency or other body which is "processing" personal data on behalf of a controller.

Pseudonymised Data is coded data and is personal data subject to the protections of the GDPR. This is in contrast to the Common Rule (45 CFR 46), which generally does not protect such information as "identifiable private information," provided that certain steps are taken to prevent the investigator from obtaining the means to link the code to the subject's identity.

Privacy Notice is another GDPR-specific term that refers to the notification required for the collection and transfer of the data of identifiable persons (e.g., informed consent form).

Policy

The General Data Protection Regulation (GDPR) is a European law which establishes data protections for privacy and security of **personal data** about individuals **located in** or **transferred from** the European Union and European Economic Area (EEA), regardless of the citizenship status of the individuals. Specifically, these areas include 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

The GDPR applies to the collection and use by a controller or processor (e.g., research investigator) of all personal information, whether directly or indirectly identifiable, which is collected in or transferred from, any of the above countries.

The GDPR does not apply to the collection or use of information which is anonymized. However, the GDPR uses a high standard for anonymization. All direct and indirect identifiers of an individual must not be present, and the investigator must implement safeguards that ensure that the data can never be re-identified. For data to be truly anonymized under GDPR, the anonymization must be irreversible.

The GDPR is related to research because:

1. It establishes the circumstances under which it is lawful to collect, use, disclose, destroy, or otherwise process "personal data."
2. It establishes certain rights of individuals in the EEA, including rights to access amendment, and erasure (right to be forgotten).
3. It requires researchers to implement appropriate technical and organizational security measures to ensure a level of data security that is appropriate to the risk of the data.
4. It requires notification to data protection authorities and affected individuals within 72 hours following the discovery of a personal data breach, which is a security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

Special Categories of Personal Data

These categories require additional protection, and individuals must explicitly consent to the use of data about:

- Race or ethnic origin
- Health
- Genetics
- Biometrics for identification purposes
- Sex life or sexual orientation
- Political opinions
- Religious or philosophical beliefs
- 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.

CONSENT REQUIREMENTS UNDER GDPR

The GDPR requires a legal basis to collect and process (i.e. analyze) personal data of a data subject in the EEA. The investigator must provide the data subject with specific information in a **notice of privacy** and, under certain circumstances, must also obtain the **explicit consent** of the data subject for certain processing activities. An informed consent form serves as the privacy notice.

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

1. **Freely given:** The individual must be given a realistic choice and ability to refuse or withdraw consent without detriment. Individuals in a position of authority cannot obtain consent, nor can consent be coerced.
2. **Specific:** The consent must include explicit, transparent and contain the:
    1. Identity of the Principal Investigator
    2. Purpose of the research
    3. Types of data collected, including any special categories of data
    4. Right to withdraw and the mechanism for withdrawal
    5. Information on who will have access to the data
    6. Time period for which data will be stored (can be indefinite)
    7. Information regarding data security, including storage and transfer of data

        8. Information regarding automated process of data for decision making about the individual, including profiling (e.g., assignment to treatment or placebo)
        9. Whether and under what conditions data may be used for future research, either related or unrelated to the purpose of the current study
3. **Informed:** An individual must be informed of the risks, how their data will be safeguarded, their rights in relation to the research, and how to exercise those rights.
4. **Unambiguous:** Consent must be granted through a statement or clear affirmative action.

Additionally, there are certain rights that data subjects have:

1. The right of access to their data
2. The right to request corrections to their data
3. 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:
    1. The need to protect scientific research if deletion would render impossible or seriously impair the research objectives; or
    2. 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
4. The right of data portability, such as to request transfer of their personal information to a third party (e.g., personal physician) in a format suitable for re-use

Since GDPR requires that the specific purpose is disclosed, the IRB will be unable to approve deception research or research involving incomplete disclosure if the study is subject to GDPR.

INADVERTENT ACTIVATION OF GDPR

Some research activities are more likely to collect personal data from EEA data subjects without the intent to do so. For instance, data collected from social media, crowdsourcing, or other online survey platforms could easily contain personal data from subjects located in the EEA at the time of collection.

Investigators need to verify where data is coming from by, for example, including a screening question asking whether potential subjects are located in an EEA country. In this case, researchers can disqualify a potential subject, thereby preventing their enrollment, or they may ensure the consent form complies with GDPR.

PENALTIES FOR NONCOMPLIANCE

Failure to follow GDPR's regulations if they apply puts an institution at risk of noncompliance, monetary fines, and reputational harm. Fines associated with noncompliance under the GDPR can be up to twenty million Euros or 4% of an institution's prior financial year worldwide annual revenue.

Data Breach Reporting

The GDPR imposes strict rules and timelines regarding report of data breaches. Any data breach occurring on a project involving GDPR-covered research must be reported within 24 hours upon discovery of the breach to **Ms. Leslie W. Christianson, Assistant Provost,** at 570-348-6211, x. 2492 or lchristianson@maryu.marywood.edu, in addition to any report that must be made to the IRB (see IRB's Mandatory Reporting policy). The following information should be communicated:

- Type of breach
- Nature, sensitivity, and volume of personal data
- Severity of consequences for individuals
- Number and characteristics of affected individuals
- Ease of identification of individuals

- IRBNet number and study title

Procedures

1. The investigator submits an application form and all required materials to the IRB or ERC via IRBNet following instructions on the respective website.
2. In addition to what is indicated in the application form and informed consent template, the investigator includes:
    1. Whether and under what conditions data may be used for future research, either related or unrelated to the purpose of the current study;
    2. A statement that if a subject withdraws consent, that his/her data will be deleted or anonymized immediately, unless providing another legal basis to retain it;
    3. Information about data security;
    4. The right of the subject to have access to, request corrections in, or transfer his/her data;
    5. If applicable, specific information about automated individual decision-making, including profiling (e.g., assignment to treatment or placebo).
3. The investigator reports any breaches within 24 hours of their discovery to Ms. Tammy J. McHale, VP for Business Affairs and Treasurer, at 570-348-6222 or tmchale@marywood.edu, as well as to the IRB (see Mandatory Reporting Policy).

Resources

General Data Protection Regulation

Portal for GDPR Information at Eugdpr.org

GDPR Recommendations from Secretary's Advisory Council on Human Research Protections

Guidance from University of Madison-Wisconsin

History

05/24/2018 - Created

07/30/2019 - Updated with additional definitions and requirements

02/17/2021 - Updated to reflect a change in the contact person for breach reporting

02/22/2021- Updated to reflect a change in the contact person for breach reporting