KENNESAW STATE UNIVERSITY
OFFICE OF RESEARCH
Research Compliance

IRB Guidance:

General Data Protection Regulation (GDPR)

INTRODUCTION

When conducting research in the European Union, Kennesaw State (KSU) Faculty/staff/students, or any other agents of KSU, are expected to comply with General Data Protection Regulation.

I. European Union Law and the EEA

A. What is GDPR?

The European Data Protection Regulation (GDPR) is applicable as of May 25th, 2018 in all member states to harmonize data privacy laws across Europe. It imposes new strict rules for controlling and processing person information.

Countries that have adopted the GDPR include all of EU as well as Iceland, Lichtenstein, and Norway. All together, they are referred to as the European Economic Area (EEA).

All Countries in the EEA:

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

*Countries that are not part of the EU.

The U.S. Department of Health and Human Services, through OHRP provides a compilation of guidances on the implementation and use of GDPR, which may vary from country to country. Go to https://www.hhs.gov/ohrp/international/gdpr/index.html for more information.

The GDPR applies to processing of personal data by an individual or legal entity. Processing is very broad and can cover anything that is done with personal data including any automated or manual manipulation. This includes collecting, recording, organizing, structuring, storing, adapting, altering, retrieving,

consulting, using, disclosing, disseminating, making available, aligning, combining, restricting, erasing, or destroying data.

B. What is Personal Data?

Personal data means any information relating to an identifiable person in the EEA. This can include email and physical addresses as well as on-line identifiers such as IP addresses and cookies. There are additional protections (i.e., special categories) for data that is sensitive in nature and carries the potential risk to harm an individual's privacy. Special Categories include information or data about an individual's health, genetics, race, ethnicity, political opinions, religion, and sexual orientation.

Generally processing of health, genetic, and biometric data is prohibited unless:

a. The subject has provided explicit consent
b. The subject has made the information publicly available; or
c. The processing is otherwise permitted by law (e.g., legally required, required for treatment, etc.).

C. Types of Data:

Studies that are HIPAA compliant may not necessarily be GDPR compliant. GDPR goes a bit beyond HIPAA.

Anonymized data – data that has all direct and indirect identifiers permanently removed and it is impossible to re-identify. GDPR does not apply to this type of data.

Pseudonymous data – data that can no longer be attributed to a specific subject without the use of additional information. Any additional data must be kept distinctly separate and is subject to technical measures to ensure no individual can be identified. Therefore, under the GDPR, pseudonymous data refers to data from which identifiers in a set of information are replaced with artificial identifiers, or pseudonyms, that are held separately and subject to technical safeguards, this includes coded data. GDPR does apply to this type of data as it is considered identifiable.

II. The Use and Processing of Data

A. Consent and the Right to be Forgotten

Data can be used in scientific research with the freely given, specific, informed, unambiguous, express written consent of the individual data subject. The consent documentation must include a well-described purpose for the scientific research and must be clearly distinguishable from other matters. Guidance suggests that while the initial consent may be broad in nature, the subjects would then be given the opportunity to consent to each individual use of the collected data as the new purpose becomes clear.

Under the GDPR, individuals have the right to be forgotten or the right of erasure. This means that upon the withdrawal of consent at any time, the controller should delete or anonymize the personal data immediately and its use of the data for the research study should stop. However, if the data needs to be

retained after consent is withdrawn, the informed consent form must specify as such and indicate at the outset that, even if consent is withdrawn, the entity will retain the data for another identified lawful basis.

However, this does not mean that the controller can swap from consent to another lawful basis. When data is processed for multiple purposes, the controller must be clear at the outset about which purpose applies to each element of data and which lawful basis is being relied upon.

B. Scientific Research Purpose – No Consent

GDPR permits processing of special categories of personal information for scientific or historical research purposes. Under this mechanism, use must be limited such that it is proportionate to the aim pursued, respects the essence of the fundamental right to data protection, and provides for suitable and specific measures to safeguard the fundamental rights and the interests of the subject. This implies that where the research purposes can be fulfilled by further processing which does not require the identification of data subjects then the research shall be fulfilled in a manner that does not permit such identification.

C. Public Health Purpose – No Consent

GDPR further permits the use of special categories of personal information on the basis of necessity of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices. This basis for processing most directly authorizes health professionals to use special categories of personal data to protect public health in epidemics, pandemics, or other imminent safety threats in connection with drugs or devices.

D. Subject's Rights

The GDPR provides individuals with a variety of rights relating to their personal data. Many of these rights are similar to those afforded under the Common Rule, such as the right to receive detailed notices about the collection and use of data, the right to access data, and the right to object. In addition, the GDPR provides subjects with the right to be forgotten/to erasure and the right to reject automatic profiling.

The right to be forgotten provides subjects with the ability to request complete removal of their data at any time upon request, subject to certain limitations. The right to reject profiling may impact studies that use algorithms to determine eligibility. Such requests must be dealt with on a case-by-case basis and researchers should contact the IRB at irb@kennesaw.edu for assistance with responding to such requests.

E. Notice of Privacy

A controller must provide the subject with a notice of the controller's privacy practices. This notice must be:

a. concise, transparent, intelligible, and easily accessible

b. written in clear and plain language, particularly if addressed to a child; and
c. free of charge.

Generally, the notice must answer the who/what/why/where/when/how questions related to data collection and use such as:

- What information is being collected/processed?
- Who is collecting/processing it (including contact information)?
- How is it collected/processed?
- Why is it being collected/processed, including the lawful basis?
- How will it be used?
- How will it be stored and for how long?
- Who will it be shared with (including third-parties)?
- What will be the effect of this on the individuals concerned?
- Is the intended use likely to cause individuals to object or complain?
- Will it be transferred to a third country and, if so, what is the lawful basis for such transfer?
- The data subjects must also be informed of their rights to request access, rectification, erasure or restriction of processing, to object to processing, and the right to data portability.

F. <u>Requests to Add Consent Language</u>

In general, investigators will not be collecting or processing personal data on individuals located in the EU as part of their participation in this study. As a result, the GDPR is not applicable to research activities at KSU and the KSU IRB is not in a position to approve the proposed changes to the consent form. These changes will be removed during pre-review.

We do note that our consent documents are written in such a way to confirm that subjects have freely and explicitly given specific, informed, and unambiguous written consent to the collection and processing of their data. If a sponsor wishes to provide a separate notification to subjects, the sponsor may create a separate privacy notification for use at our site that is (1) distinct from the consent document; (2) does not include signature lines; and (3) does not reference our privacy officer as a contact for questions about GDPR. Questions should be directed to a contact provided by the sponsor.

III. Enforcement and Discipline

A. **<u>Data Breaches</u>**

In the case of a personal data breach, data controllers shall without undue delay notify the appropriate regulator of the breach. The regulation goes on to state that, where feasible, this notification should take place no later than 72 hours after the breached party has become aware of the incident.

Further, if it is determined that the breach is likely to result in a high risk to an individual's rights and freedoms, such individual must also be notified of the breach. Internally, the research leaders should immediately contact the Office of Legal Affairs.

B. Penalties

Fines are administered by individual member state supervisory authorities and vary depending on the type and scope of violation. There are two tiers of administrative fines that can be levied:

- Up to €10 million, or 2% annual global turnover – whichever is higher.
- Up to €20 million, or 4% annual global turnover – whichever is higher.

The fines are based on the specific articles of the Regulation that the organization has breached, taking into account certain aggravating and mitigating circumstances. Infringements of the organization's obligations, including data security breaches, will be subject to the lower level, whereas infringements of an individual's privacy rights will be subject to the higher level.