# 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 | PoT C.r |

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 online 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 u10.6 ( -1.31-4.34.6.6 (n)13.(,)a)10.6 (t)-3 (i(t)-5.-0.004 Tc 0.006 Tw 0.859 0 Td [(1 .9 (

retained after consent is withdrawn, the informed consent form must specify as such and indicate at the outset that, even if consent is withdrawn, the entity will retain the data for another identified lawful basis.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

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:

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.