RUTGERS UNIVERSITY
Office for Research

WORKSHEET: GDPR Compliance - Data Protection And Privacy		
NUMBER	DATE	PAGE
11.201 (HRP-335)	5/1/2024	Page **1** of **2**

The purpose of this worksheet is to provide support and guidance for IRB Reviewers, Staff, and Researchers to determine whether the proposed human research must adhere to the General Data Protection Regulation (GDPR). This European Union regulation establishes and enhances protections for the privacy and security of personal data about individuals residing within the European Economic Area (EEA). This WORKSHEET does not need to be completed or retained.

1. When Does GDPR Apply: Compliance with GDPR is required when Sections (1a) **AND** (1b) below apply to the research:

☐ **(a) The research plans to obtain or process data from or about individuals who are residents of an EEA member state** (*GDPR Art 3*): The study proposes to obtain (intentionally or unintentionally) identified or identifiable information from or about living individuals ***who reside*** in an EEA member state at that moment their data is obtained.
NOTE: GDPR protects the data of individuals who reside in an EEA member state regardless of their nationality, citizenship, or immigration status.
NOTE: The regulation applies to any organization worldwide which obtains or processes identified or identifiable data belonging to EEA residents.

European Economic Area (EEA): The EEA includes European Union (EU) countries and Iceland, Liechtenstein and Norway.

EEA 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 and Sweden. Also, Iceland, Liechtenstein and Norway. Switzerland and the UK are not members of the EEA or EU but have similar data protection regulations.

There are **dependent territories/countries** that are technically in the EU though not in Europe that are governed by GDPR, some of these include: Azores, Canary Islands, Guadeloupe, French Guiana, Madeira, Martinique, Mayotte, Reunion, and Saint Martin and others. Make sure to check if a location is a territory of a country located in the EEA.

Brexit and GDPR Regulations 2021: The United Kingdom (UK) left the EU in Dec 2020 and is no longer considered a Member State. The UK has already agreed that GDPR will be absorbed into UK domestic law as part of the European (Withdrawal) Agreement. GDPR compliance for the UK will continue to be required for all past and present research studies.

NOTE: GDPR applies to research conducted with or about EEA residents **on-board vessels** registered to EEA Countries at the time of data collection which travel in international waters or airspace (*GDPR Article 3.3*).

☐ **(b) The research plans to obtain or process "Personal Data" or "Special Category Data" (as defined by GDPR), or biospecimens.**
NOTE: Read carefully the definitions of key terms provided below as GDPR does not define key terms in the same fashion as the U.S. GDPR is broader and covers/protects information not covered by HIPAA or usual U.S. traditions around use of data in research.

"Personal Data" (GDPR Art 4.1) – is any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together or can lead to the identification of a particular person, also constitute personal data.
NOTE: GDPR **applies** to data that the U.S. would otherwise consider 'de-identified' by some pseudonymizing scheme, such as 'key-coding'. See Section 2c below for the definition of **pseudonymization** (GDPR Article 4(5) and Article 29 Working Party Opinion 05/2014).

"**Special Category Data"** (GDPR Art. 9) - sensitive personal information which merits greater data security protections, such as data revealing racial or ethnic origin, political opinions, religious beliefs, data concerning health, a person's sex life or sexual orientation, or genetic or biometric data that is processed for the purpose of uniquely identifying an individual.

Biospecimens—material collected from the human body—are considered to contain **personal data** relating to an identified or identifiable natural person (GDPR Art. 2) as DNA, intrinsic to biospecimens, is a unique code that will always link to only one person.

Processing (GDPR Article 4.2): "...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 [...]". An non-exhaustive series of examples include: "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". **NOTE:** Researchers who receive identified or identifiable data collected by other organizations to analyze, process or store in some way, are considered Processors and, as such, must comply with the requirements of GDPR.

2. When Does GDPR Not Apply: Compliance with GDPR is not required if any of the following apply to the research:

☐ The research does not plan to obtain data from or about individuals residing in EEA member states.

☐ The research plans to process identified or identifiable data of residents of EEA members states **who were not EEA residents** at the time of data collection (for example, data was obtained from or about individuals while they resided in the U.S., before they returned or changed their residence to an EEA member state.)

☐ The research plans to obtain or process **only anonymous or anonymized data** from or about residents of EEA member states. GDPR does not apply to data that does not relate to an identified or identifiable person or to data rendered anonymous in such a way that the data subject is not or no longer identifiable.

In order for data to be considered **anonymous or anonymized**, direct and indirect personal identifiers must be removed and technical safeguards have been implemented such that data can never be re-identified. (That is, there is zero risk of re-identification.) According to GDPR, anonymized data does not fall within the GDPR because it is no longer considered "personal data" (GDPR Recital 26).

NOTE: Pseudonymization is not the same as **anonymization**. Pseudonymization is the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information. Pseudonymization strategies, such as key coding data, reduce the linkability of a dataset with the original identity of a data subject, and is accordingly a useful security measure, but risk of re-identifiability remains. As such, when the research proposes to obtain, process or control pseudonymized (i.e., coded data), **GDPR applies** (Article 29 Working Party Opinion 05/2014).

3. Actions: Select the appropriate action based on your determination from Sections 1 and 2 above.

☐ **If GDPR Applies to the Research:** Visit the Rutgers IRB's GDRP Guidance Webpage for an itemized list of protocol design and consent informational elements which must be addressed in the study to comply with GDPR from an IRB perspective.

☐ **If GDPR Does Not Apply to the Research**: **STOP**. The IRB does not require additional protections outlined in the protocol plan or appear in the consent document to comply with GDPR. **NOTE:** There may be GDPR requirements that apply to your research, which are outside the IRB's purview. Contact Rutgers University Ethics and Compliance (https://uec.rutgers.edu/programs/gdpr/) for assistance.

Notes:
(a) GDPR Regulations: https://gdpr-info.eu/
(b) GDPR Definitions: https://gdpr-info.eu/art-4-gdpr/
(c) GDPR Regulations as interpreted for UK data handlers by the UK Information Commissioner's Office (ICO) https://ico.org.uk
(d) GDPR European Data Protection Board (EDPB): Advisory Board (Formerly the Article 29 Working Party) https://edpb.europa.eu/edpb_en
(e) GDPR's description of Identifiable Data (Known as "Personal Data" in GDPR Art 4) is broader than the "Common Rule": HHS regulations, (45 CFR Part 46.102(e)).
(f) GDPR governs key-coded data "pseudonymized data" where data collectors do not have access to a key code needed to re-identify the coded data. This type of data is not exempt from the regulation.
(g) If data is anonymized after collection, it cannot be excluded from GDPR regulations.
(h) Biospecimens cannot be de-identified or anonymized under GDPR because they contain genetic material (DNA) which falls under "Personal Data" (GDPR, Art 4(1)).
(i) GDPR does not apply to the collection of fully anonymous data (as defined by GDPR Recital 26).
(j) Do not confuse pseudonymization with encryption, a data protection technique which is also recommended by the GDPR but is something entirely different.
(k) GDPR and HIPAA Data: GDPR sets standards for all sensitive personal data, while HIPAA deals with only Protected Health Information (PHI). HIPAA standards are limited to health information held by Covered Entities like doctors, employers who offer health benefits or insurance companies. Business Associates – like shredding companies, IT companies, or transcription services are regulated by HIPAA. The GDPR, however, applies to all organizations dealing with personal data.