THE GENERAL DATA PROTECTION REGULATION ("GDPR")
IN HUMAN SUBJECTS RESEARCH ("HSR")

What is the GDPR?

Effective May 25, 2018, the GDPR standardizes* data protection laws across all European Union ("EU") countries, as well as Iceland, Lichtenstein, and Norway (collectively, the "European Economic Area" or "EEA") and imposes strict new rules on processing personal information relating to individuals and organizations physically located in the EEA, regardless of citizenship.

Countries in the European Economic Area

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

* Each country implements the GDPR differently and country-specific guidance can be found in the *HHS Compilation of European GDPR Guidances, available at https://www.hhs.gov/ohrp/international/gdpr*.
**Denotes countries that are not part of the EU

Research involving the collection of personal data on individuals within the EEA, whether through in-person or electronic methods (e.g., online or email), may implicate the GDPR. The main areas of impact are changes to the consent process, modified contractual language in research and vendor agreements, increased data protection and technical security requirements, and prompt breach notification requirements (72 hours).

For studies involving EEA study subjects, an EEA sponsor, and/or an EEA subsite(s), including where JHU acts as a data coordinating center or lead site for a multi-site study with EEA sites, researchers should connect with the applicable research administration and IRB offices as soon as possible.

What is "Personal Data"?

Under the GDPR, "personal data" is very broadly defined to mean any information relating to an identifiable person in the EEA, including name, email and physical address, government issued identifiers, and online identifiers (e.g., IP addresses and cookies). Additional protections are given to "special categories" of personal data due to their sensitive nature and potential risk of harm to an individual's privacy. Criminal records are also subject to heightened protection.

Data collected in the course of research often includes "special categories" of personal data, including information about a data subject's health, genetics, race or ethnicity, political opinions, religion, and sexual orientation. In general, processing of health, genetic, and biometric data is prohibited unless 1) the data subject has provided explicit consent, 2) the data subject has made the information publicly available, or 3) the processing is otherwise permitted by law (e.g., necessary for medical treatment, legally required, for scientific research purposes).

Identifiable, De-Identified/Coded, and Anonymous Personal Data

The information protected under the GDPR extends beyond that protected under the Health Insurance Portability and Accountability Act ("HIPAA") and data protection measures that are HIPAA compliant are not necessarily GDPR compliant.

The GDPR does not apply to "anonymized" data, meaning all direct and indirect personal identifiers have been permanently removed. This is a very high standard and most research data will not satisfy the standard to take it outside the GDPR. Data that is "de-identified" under HIPAA is likely not "anonymized" under the GDPR.

The GDPR may apply to "pseudonymized" or "coded" data, meaning data that can no longer be attributed to a specific data subject without the use of additional information. This is true even if JHU does not have any ability to re-identify the subject or any access to the key linking the data to the subject's identity. Data that is "de-identified" under HIPAA is likely pseudonymized, and therefore, identifiable personal data under the GDPR.

Data 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 connect with the applicable IRB for assistance with responding to such requests.

Penalties for Non-Compliance

Fines for non-compliance are tiered, but can be up to the greater of 20 million euros and 4% of the JHU's annual revenue.

Practical Steps for Researchers

If your study involves the collection of personal data of individuals located in the EEA, whether directly or indirectly or through in-person or electronic methods, researchers should:

1. As soon as possible, connect with the applicable research administration office and IRB.
2. Design and implement a protocol which:
    a. Embeds data protection considerations at an early stage, not retrospectively. For example, if possible, collect only de-identified or pseudonymized data at the outset.
    b. Collects only the absolute minimum personal data necessary for the study. For example, if using an online survey tool, change default settings so that IP addresses are not collective if they are not required for the study.
    c. Minimizes the scope of use of personal data.
    d. Retains personal data for only as long as necessary.
    e. Maintains complete and accurate records of processing activities on personal data (e.g., details of any other recipients, any transfers within or outside the U.S., record retention period, details of security measures).
    f. Permits researchers to respond to data subject requests. For example, record and store data in such a way that would permit removal upon request.
    g. Establishes and maintains appropriate data security measures, taking into account the nature, scope, context, and purposes, as well as the risks (likelihood and severity).
    h. Establishes a system to identify and respond to a data breach.
3. Incorporate the appropriate consent process and documents.
4. Require collaborators, study sites, vendors, third-party websites and tools, and apps to be GDPR-compliant. Contracts may need to include certain clauses.
5. In the event of a data breach, notify the Office of the General Counsel **immediately** at 410-516-8128. The GDPR requires JHU to respond within 72 hours, when required.