Guidance for EU General Data Protection Regulations (GDPR) compliance in the conduct of human research.

What is the GDPR?

The General Data Protection Regulation (GDPR) is a European law that went into effect on May 25, 2018 and establishes protections for the privacy and security of "personal data" from or about individuals in the European Economic Area ("EEA") and certain non-EEA organizations that process personal data of individuals in the EEA.

The purpose of this document is to assist investigators in determining whether this regulation may apply to their research project. The document provides an overview of the regulation in the context of research, a series of questions to consider for whether GDPR may apply to a specific study, and recommended points of contact if there are questions. Definitions and more information about the regulation are provided at the end.

Overview:

What activities fall under GDPR?

GDPR protects data from or about individuals. At a high level, the following types of activities would fall under the GDPR:

1. Collecting personal data/information from individuals while they are in the EEA in relation to offering goods or services, including research.
2. Processing personal data/information, when data are processed by an organization that is established in the EEA.
3. Where an entity processes personal data/information in relation to monitoring the behavior of individuals in the EEA.

The term, "processing" data under GDPR includes a broad set of activities that generally pertain to working with the data in any way, including collecting, storing, sharing, analyzing, or archiving information.

Why might GDPR affect my research if I am based in the United States?

Your research may be affected by GDPR if the research procedures collect information or data (either in person or online) from an individual who is performing (or completing) the research activity in one of the European Economic Area countries referenced below. **This location is unrelated to citizenship or residency.**

Countries within the EEA include: Austria, Belgium, Bulgaria, Czech Republic, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, United Kingdom.

If the data will be anonymous or deidentified, would GDPR still apply?

Unlike U.S. regulations, GDPR does not use the word "de-identified," instead using "pseudonymized" and "anonymous," both of which have specific definitions.

Anonymous data are not subject to GDPR. Deidentified (or pseudonymized) data likely are, but *may* not be subjected to GDPR provided the research team did not have a role in the initial collection of the data with identifiers and will not have access to the identifiers going forward. A data transfer agreement may be applicable.

De-identified	• Data / information that neither identifies nor provides a reasonable basis to identify an individual. • Requires a formal determination by an expert opinion, or requires the removal of specific identifiers and an absence of actual knowledge that the information could be used to identify the subject. • Re-identification of individual is possible through use of a code or other record.	HIPAA Privacy Rule *Not regulated by HIPAA.*
Pseudonymized	• "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, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. • Re-identification of individual possible through use of additional information.	GDPR Article 4(5) *Regulated by GDPR.*
Anonymized	• "Information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable." • Re-identification of individual is NOT possible.	GDPR Recital 26 *Not Regulated by GDPR.*

What if we are relying on another IRB to be the IRB of record, who is responsible for GDPR compliance?

Compliance with GDPR regulations as they apply to a project is a shared responsibility starting with the study team and PI. The PI and study team must assess the study to determine whether GDPR may apply to the project, and if sponsored, be mindful of any contract terms Sponsored Research may make the team aware of.

Once it is determined that GDPR does apply to a project, the IRB of record, whether another institution or a commercial IRB, should typically set the standard for what is needed to be GDPR

compliant. For example, the IRB may require use of specific language regarding use of data in a consent form.

However, everyone should be mindful of complexities that compliance with GDPR may add to a research project and should raise questions if the Northwestern site is collecting, receiving, storing, or managing (processing) data in any way that is affected by GDPR.

What are the consequences of non-compliance?

Non-compliance with a protocol or consent requirement would be managed by the IRB. Non-compliance with data handling or other violations of privacy policy would be managed by University Compliance in accordance with applicable Handbooks.

Process for evaluating GDPR applicability when submitting the protocol and consent.

The following questions should be adequately addressed in the protocol.

Review the questions below to assist in determining whether GDPR applies to your study.

- **If you respond "yes" to questions 1-3, GDPR likely applies.**
- **If you respond "yes" to questions 4-6, reach out to privacy@northwestern.edu to discuss whether additional actions are required.**

If GDPR applies, the GDPR data consent form should be utilized. Contact the IRB office if you have any questions.

1. Will Northwestern collect or use the personal data of research subjects physically located in the EEA at any time of data collection (regardless of the research subject's country of residence or citizenship)?

2. Does the data include personal information (for example, national identification number, date of birth, address, photos, cookie IDs, exam info, and so on) or sensitive personal information (for example, racial or ethnic origin, religion, medical info, sexual orientation)?

3. Does Northwestern intend to recruit and enroll research subjects who are located in an EEA country in connection with the research study?
   a. If so, which country(s)?
   b. If so, which types of data?

If so, please describe the type of data that will be collected as part of the study to assist in determining whether these data are covered by GDPR.

Note: If you are using a local service or company to collect those data from participants in the EEA, a data transfer agreement may be required. Please contact SR for help with that determination.

4. Will Northwestern monitor the behavior of research subjects located in an EEA country through an app or any other use of wearable or smart devices (e.g., cell phones, tablets, or other electronic devices)?

If "yes," then describe:

5. Will the study team use cookies or other online tracking tools to collect and/or monitor the online behavior of identifiable research subjects located in the EEA who may use a website related to the research study? Use of tracking technologies collecting identifiable information should be explicitly stated in the protocol document and consent form, as applicable.

6. Does the study team have a collaborator based in the EEA and/or have we hired the services of an organization within the EEA to assist with this study? Make it clear whom the sponsor of the study is. A data transfer agreement may be required if you are using a local service or company to collect data from participants in the EEA; please contact SR for help with that determination

Consent requirements under GDPR:

GDPR permits researchers to rely upon consent from research subjects as a lawful basis for processing Personal Data for research purposes. It is important to distinguish between *informed consent* for purposes of research studies and consent for collection and use of personal data under the GDPR. To obtain a valid consent for collection and/or use of data for research purposes under GDPR, the individual's consent must be:

a. **Freely given**: The individual must have a realistic choice, or the realistic ability to refuse or withdraw consent without detriment. Similar to US law, coerced consents are not compliant with GDPR.

b. **Specific**: The consent must include a specific, transparent statement of each purpose of the study, what personal data elements are being collected, and including the rights articulated above. This includes specific reference for "future use" of the data.

c. **Informed**: An individual must be informed of the nature and extent to which the individual is consenting to what data collection activities and to what use of data.

d. **Clear and Unambiguous**: GDPR requires a statement or "clear affirmative act" that indicates the individual has agreed to the proposed processing of data activities. Silence, pre-checked boxes and inactivity (passive consent) are not allowed for the purposes of consent.

The mechanism for obtaining consent may vary based on the type of data collected.

When possible, do not collect sensitive information. The GDPR includes more stringent protections for the following "special categories" of personal data:

- Racial or ethnic origin
- Political opinions

- Religious or philosophical beliefs
- Trade union membership
- Physical or mental health information
- Sex life and sexual orientation
- Genetic and biometric data

Special cases: Incomplete disclosure and/or deception.

If GDPR applies to your study, study designs involving deception cannot be conducted due to the GDPR's requirements for affirmative and informed consent to the use of their data.

If your study design requires incomplete disclosure, additional procedures must be followed to ensure consent requirements are met. For example, if the subjects are informed prospectively of the use of incomplete disclosure and consent to its use; are fully debriefed; and their right to withdraw their data is reiterated after the debriefing, then incomplete disclosure may be used. Note that this will be considered on a case-by-case basis and the justification for its use will be carefully considered.

Anticipate how the exercise by research subjects of their special rights under the GDPR may impact your study. Your study will need to provide a process for research subjects to exercise their rights under the GDPR. You should also evaluate what the impact of exercising those rights will be on the adequacy of the research data.

Their rights will include:

- *Access and review.* The right to be provided all the personal data the study has about them and to review it.
- The right to have any inaccuracies in their personal data corrected and, if the information is incomplete, completed.
- *Erasure, right to be forgotten.* The right to require that all of their personal data be deleted.
- The right to require that the processing of identifiable personal data be restricted or halted while the processing of the information is being contested.

The GDPR provides an exception to the right to be forgotten if exercise of the right is "likely to render impossible or seriously impair the achievement of the objectives of the research."

APPENDIX:

Additional Information GDPR Details

GDPR, or Regulation (EU) 2016/6793 of the European Parliament and of the Council, is an EU legislation that protects natural persons with regard to the processing of personal data and on the free movement of such data. The GDPR is designed to protect the privacy of individuals in the EEA and to reshape the way organizations with operations or customers in the EU approach data privacy and data portability.

As such, the GDPR:

1. Establishes the circumstances under which it is lawful to collect, use, disclose, destroy or otherwise "process" Personal Data, including when conducting research activities;

2. Establishes certain rights of individuals in the EEA, including rights to access, amendment and erasure (referred to as the right to be forgotten)

   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 study team may need to delete or anonymize the personal data immediately and its use of the data for the research study should stop. Consult with privacy@northwestern.edu before doing so. 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;

3. Requires Personal Data controllers and processors to implement appropriate technical and organizational security measures to ensure a level of data security that is appropriate to the risk to Personal Data; and

4. Requires notification to data protection authorities and affected individuals following the discovery of a "personal data breach," which is breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

B. Who is protected by GDPR:

All "data subjects" who are in any EEA country for any reason. The application of GDPR is unrelated to citizenship. For example: U.S. citizens traveling to Spain could be 'data subjects' and would be protected by GDPR.

C. **Definitions**:

1. Personal Data:

   Personal data are all information which is related to an identified or identifiable natural person.

Those impacted are identifiable if they can be identified, especially using assignment to an identifier such as a name, an identifying number, location data, an online identifier or one of several special characteristics, which expresses the physical, physiological, genetic, mental, commercial, cultural or social identity of these natural persons. In practice, these also include all data which are or can be assigned to a person in any kind of way. For example, the telephone number, credit card or personnel number of a person, account data, number plate, appearance and customer number of address are all personal data.

Since the definition includes "all information," one must assume that the term "personal data" should be as broadly interpreted as possible. This is also found in case law of the European Court. These include also less-clear information, such as recordings of work times which include information about the time when an employee begins and ends his work day, as well as breaks or times which do not fall in work time. Also, written answers from a test-taker and any remarks from the test about these answers are "personal data" if the test-taker can be theoretically identified. The same also applies to IP addresses. If the processor has the legal option to oblige the provider to publish additional information which can identify the user who is behind the IP address, this is also personal data. In addition, one must note that personal data need not be objective. Subjective information such as opinions, judgements or estimates can be personal data. Thus, this includes an assessment of creditworthiness of a person or an estimate of work performance by an employer.

Last but not least, the law states that the information for a personnel reference must refer to a natural person. In other words, data protection does not apply to information about legal entities such as corporations, foundations and institutions. For natural persons, on the other hand, protection begins and is extinguished with legal capacity. A person obtains this capacity with his birth, and loses it upon his death. Data must therefore be assignable to specific or specifiable living persons for reference to a person.

Data is not "Personal Data" merely because it concerns a citizen of an EEA country. Instead, the data must concern an individual <u>located</u> in an EEA single market country unrelated to whether that person is a citizen or not of that country. There is agreement that individually identifiable data collected from an EEA citizen at a location in the United States will be subject to United States law and not GDPR. However, if the organization or the researcher continues to monitor the person citizen after returning to the EEA then GDPR does apply.

"Special Data"

2. 'Controller' means the 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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

3. ‘Processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. For example, a sponsor of a research study would typically be a “controller” and the PI would be the processor. For a self-initiated study the PI would be the controller and the processor.

4. ‘Recipient’ means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

5. ‘Consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her (see additional information below regarding “rights”.)

6. ‘Personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

7. ‘Genetic data’ means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

8. ‘Biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic (finger print) data.

9. ‘Data concerning health’ means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

D. <u>What is the reach of GDPR</u>:

The GDPR applies to research located within the EEA and to research located outside of the EEA if they offer “goods or services” to, or monitor the behavior of EEA data subjects within the EEA. It applies to all collecting, processing and holding the personal data of data subjects residing in the EEA and is unrelated to where the company’s (or researcher’s) resides. The GDPR has direct reach to a controller or processor organization located in the United States or otherwise outside the EEA if the organization:

1. Creates an establishment in the EEA;

2. Offers “goods or services” (even if free) to individuals in the EEA, such as by advertising in the EU. The “offering of goods or services” is more than mere access to a website or email address, but the purposes of considering “goods and Services” as it relates to research, some research may meet the definition of “offering goods and services” and some may not. Depending on the study, “goods and services” may be as simple as the ‘opportunity to participate’ in a research unrelated to compensation though compensation is typically viewed as “offering goods and services.”

3. Monitors the behavior of individuals in the EEA, such as by continuing to monitor patients after they return to the EEA as part of, for example, post-discharge care. The monitoring of behavior will occur, for example, where individuals are tracked on the internet by techniques that apply a profile to enable decisions to be made/predict personal preferences, etc. This means in practice research outside the EEA that is targeting consumers or participants in the EEA will be subject to the GDPR.

E. Penalties for non-compliance:

fines are the primary method of dealing with non-compliance with the specific guidance

F. Data Subject’s Rights under GDPR:

1. Right of Access: Data Subject Access Requests (DSAR) – e.g. “What do you know about me?”

2. Right to Erasure/Right to be Forgotten – e.g. “Remove me from your database”

3. Right to Rectification which is the right “Amend or correct my details.” This is a “data subject’s” right under GDPR but it is not clear this would apply to research although it could easily be interpreted to apply to research subject pools or registries.

4. Right to Restrict Data Processing – e.g. “Stop filming me”

5. Right to Withdrawal of Consent – “I don’t want to do this survey anymore”

6. Right of Data Portability – e.g. “‘Move my personal data from one location to another location. (This is a data subject’s right under GDPR but it is not clear this would apply to research.)

7. Strengthened right to prior notification before data collection.

8. Right to Reject Automated Profiling: This is a new concept under the GDPR. Profiling is automated processing that is used to evaluate personal aspects of an individual, e.g. being refused insurance based on automated algorithm. It is not known at this time if this would impact automatic profiling for eligibility / screening for a study or even the emerging research that is designed specifically to improve methods of profiling as it relates to health risks or even consumer behavior.

What about anonymous data? Can personal data be de-identified for future use?

Anonymized information is not personal data under the GDPR.

This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes. Under the Regulation, anonymous information neither identifies an individual nor makes it possible to identify an individual.

The focus is on the possibility of reidentification either by the controller or by another person to identify the natural person directly or indirectly. Generally, EEA data protection authorities deem data to be de-identified if there is no reasonable means through which someone who has access to the data could use the data to re-identify an individual who is the subject of the data. It seems as though de-identification under GDPR would be similar to de-identification under HIPAA or any sensitive data set: for example: for key-coded data to be de-identified the holder of the data must not have access to the re-identification key or possess any other means to re-identify the individuals who are the subjects of the data. This is not different from what is usual practice in the United States except that the definition of identifiers is more broadly defined.

Resources:

Barnes, M.; et al. (2018): New Draft guidelines on GDPR consent requirement's application to scientific research. (https://biglawbusiness.com/new-draft-guidelines-on-gdpr-consent-requirements-application-to-scientific-research/).

Broccolo, B. M.; et al. (2018): Does GDPR Regulate My Research Studies in the United States? (https://www.mwe.com/en/thought-leadership/publications/2018/02/does-gdpr-regulate-research-studies-united-states).

GDPR interactive searchable version online: (https://gdpr-info.eu/).

GDPR pdf English version of regulation: http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf

"Guidelines on consent under Regulation 2016/679": https://www.mayerbrown.com/files/uploads/Documents//PDFs//2017//December//wp259_enpdf__2_.pdf

Mayer Brown Legal Update] (12-2017): New draft consent guidelines under the GDPR: What You Need to Know. https://www.mayerbrown.com/publications/detailprint.aspx?publication=14187

Santos, J. (12-2017): Healthcare researchers prepare for GDPR: what does GDPR mean for health care researchers? Kantar Health (http://www.kantarhealth.com/docs/white-papers/healthcare-researchers-prepare-for-gdpr.pdf?sfvrsn=10).