WHAT INVESTIGATORS NEED TO KNOW ABOUT THE GDPR

1. What is the GDPR?
   The General Data Protection Regulation (GDPR) is a European law that establishes protections for the privacy and security of Personal Data, and establishes, in part, the circumstances under which it is lawful for a research investigator from outside the European Union (EU) or other European Economic Area (EEA) states to collect and process a person’s Personal Data when in connection with either of the following:
   - The monitoring of that person’s behavior while in the EU/EEA
   - The offering of goods or services to that person while in the EU/EEA

   Under the GDPR investigators must implement security measures for such subjects’ Personal Data appropriate to the level of risk, and follow strict rules of informed consent.

2. To what does the GDPR apply?
   The GDPR applies to a subject’s Personal Data collected in, or transferred from, any European Union or other European Economic Area state, regardless of the subject’s nationality.

3. Is my research subject to the GDPR if I am conducting it in the United States?
   Yes: The GDPR applies to research being conducted outside of the European Union (EU) or other European Economic Area (EEA) states if its subjects include nationals and/or non-nationals physically present in the EU/EEA states at the time the Personal Data is being collected.

4. To whom does the GDPR apply?
   The GDPR applies to European Union (EU) and other European Economic Area (EEA) nationals and non-nationals physically present in EU/EEA states when they are specifically being targeted.

   Current European Union states include: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and the United Kingdom.

   Current other European Economic Area states include: Iceland, Liechtenstein, and Norway.

   Note that other states may adopt the GDPR or similar regulations in the future; for example, the United Kingdom has indicated its intent to adopt the GDPR once it has exited from the European Union.

5. Does the GDPR apply to European Union (EU) and other European Economic Area (EEA) state nationals if their personal data is being collected in the US?
   No: The GDPR only applies to individuals who are physically present in an EU/EEA state; therefore, EU/EEA nationals whose physical presence is outside of an EU/EEA state at the time their personal data is being collected are not covered by the GDPR.

6. What does the GDPR mean by Personal Data?
   Under the GDPR, Personal Data refers to any information that relates to an identified or identifiable living person – a person who can be identified, directly or indirectly, by one or more identifiers.

   In addition, the GDPR designates Special Categories of Personal Data (requiring heightened protections), defined by the GDPR as potentially sensitive data including, but not limited to, racial or ethnic origin; data concerning health; data concerning a person’s sex life or sexual orientation; genetic data and biometric data used to uniquely identify an individual; and data regarding a person’s political opinions, religious or philosophical beliefs, or trade union membership.

   Examples of identifiers include, but are not limited to: names, identification numbers, location data, online identifiers, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person. (Note that identifiers are not limited to those specified by HIPAA.)
7. Are coded data considered Personal Data?  
Yes: The GDPR considers coded data (which it calls Pseudonymized Data) to be Personal Data as the code makes identification of a subject possible. Note that the investigators themselves do not need to have access to the code required to link the data to individual subjects; as long as a code exists, the data are considered Personal Data.

8. Are anonymous data considered Personal Data?  
No: The GDPR does not consider anonymous data to be Personal Data. This includes what the GDPR refers to as Anonymized Data, where all personal identifiers have been irreversibly removed and the data are not coded.

9. Does the GDPR, like HIPAA, allow for the de-identification of Personal Data?  
No: Unlike HIPAA, the GDPR does not provide specific methods for the de-identification of Personal Data or the category of a limited data set: Data are either identifiable or anonymous as defined above.

10. What does the GDPR mean by Monitoring Behavior?  
While the GDPR does not directly define the monitoring of behavior, guidance indicates it refers to such things as the tracking or profiling of subjects. Examples of behavior monitoring may be tracking subjects’ physical activity through the use of a mobile device, tracking subjects’ buying habits electronically for the purpose of predicting their preferences, or continued observation of subjects as part of post-discharge care in a clinical study.

11. What does the GDPR mean by Offering Goods or Services?  
While the GDPR does not directly define the offering of goods or services, guidance indicates that offering compensation for participation in a research study may qualify. In addition, there may be times when simply granting a subject the opportunity to participate in a research study may qualify (e.g., in a clinical trial).

Note that the offering of goods and services must be targeted: simply recruiting subjects through, for example, a website accessible to individuals within a European Union (EU) or other European Economic Area (EEA) state does not necessarily qualify as the “offering of goods or services” as intended by the GDPR. However, if the website is translated into an EU/EEA state language other than English (for the purpose of recruiting EU/EEA state members), or if compensation is offered in an EU/EEA currency (for the purpose of recruiting EU/EEA state members), the research may be considered to be subject to the GDPR.

12. Are there special considerations that need to be made regarding children?  
Yes: The GDPR stipulates that the age of consent is 16 and that if a subject is below the age of 16, consent from the child’s parent or legally authorized guardian is required. Member states may provide by law for an age of consent as low as 13 for children in their state, though no state has yet provided such a law.

That an individual is of the age of consent must be verifiable – a simple check box is not acceptable. Likewise, the authority of the parent or legal guardian must be verifiable if the child is below the age of consent.

13. May I use deception or incomplete disclosure in my research?  
No and Yes: Because of the GDPR’s emphasis on fully informed consent of subjects, deception is not to be used in research involving the collection of personal data.

Incomplete disclosure may possibly be used if the subjects are informed prospectively, via the consent process, 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. Note that this will be considered on a case-by-case basis and the justification for its use will be carefully considered.

14. What do I do if there is a data breach for research subject to the GDPR?  
The GDPR has specific and strict rules regarding data breaches. If a data breach occurs on research subject to the GDPR, the breach must be reported to the Brandeis University Office of the General Council and the IRB administrator within 72 hours of the discovery of the breach. Your report should include: the type of breach; the nature, sensitivity, and volume of Personal Data; the severity of the possible consequences for subjects; and the ease with which subjects may be identified.

15. What happens if I don’t comply with the GDPR?  
Fines associated with noncompliance under the GDPR can be up to €20 million (in excess of $20 million).
16. How do I comply with the GDPR?
1. If you are conducting research subject to the GDPR, you must outline in detail in your IRB application:
   • Your use of active explicit consent (subjects must opt-in to participate in your research – opt-out procedures are not acceptable and statements such as ‘By clicking on the continue button you consent to participate in this research’ are not acceptable)
   • How you will ensure consent is freely given with no possibility for perceived coercion
   • That you will allow your subjects to withdraw consent (as easily as it was to give it) at any time
   • That you will allow your subjects the option to have their data expunged (prior to anonymization)
   • That you have procedures in place to expunge a subject’s data in the event a subject so requests
   • That you will allow your subjects access to their data if they choose, as well as explain how it can be accessed
   • A comprehensive data management and security plan, with special considerations for Special Categories of Personal Data
   • How you will demonstrate consent was obtained for all subjects, regardless of how it was obtained
2. In addition to the elements of informed consent outlined in 45 CFR 46, you must comply with additional GDPR informed consent requirements, which include:
   • A detailed list of the types of data to be collected
   • An estimate of the time each subject will spend participating in the research
   • A statement regarding the subject’s right to withdraw consent at any time, as well as how
   • A statement regarding the subject’s right to have their data expunged (prior to anonymization), as well as how
   • A statement regarding the subject’s right to have access to their data free of charge, as well as how
   • An explanation regarding who will have access to the data
   • Information regarding data security, including the storage and transfer of data
   • A statement outlining how long data will be stored
   • A statement that the data will be removed from European Union or other European Economic Area states
   • A statement regarding any third parties (e.g., Qualtrics, transcription services, etc.) who will be involved in the processing of the data
   • A statement regarding the right to file a complaint with the data protection authority
3. You must request consent for the use of a subject’s Personal Data separately from consent to participate in the research.

17. Some Useful Language for Consent to the Collection, Use, and Processing of Personal Data
I hereby consent to the collection, use, and processing of my personal information as outlined and described above.

I have been encouraged to ask questions, have received satisfactory answers to my questions, and understand my rights as outlined in this consent form.

I understand that my participation is voluntary and that I may withdraw my personal information at any time without reason or penalty, and that I may request access to my personal identifiable information at no cost.

I give consent for my personal information to be transferred overseas, and more specifically to the United States of America, even if this country is not considered by the EU authorities to be a privacy safe harbor.
Resources:


https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679

GDPR Searchable Version:

https://gdpr-info.eu

EU GDPR Portal:

https://www.eugdpr.org

Article 29 Data Protection Working party: Guidelines on consent under Regulation 2016/679:

http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

HHS: Attachment B – European Union’s General Data Protection Regulations:


Information Commissioner’s Office (UK): Guide to the General Data Protection Regulation:


GDPR EU.org: GDPR Overview

https://www.gdpreu.org

GDPR EU.org: Right of Access to Data Defined:

https://www.gdpreu.org/the-regulation/list-of-data-rights/right-of-access/

GDPR EU.org: Right to Erasure of Data Defined:

https://www.gdpreu.org/the-regulation/list-of-data-rights/right-to-erasure/

GDPR EU.org: Consent Defined

https://www.gdpreu.org/the-regulation/key-concepts/consent/