IRB Guidance for General Data Protection Regulations (GDPR)

GDPR, or Regulation 2016/6793 of the European Parliament and of the Council, is a European Union (EU) legislation that protects natural persons with regard to the processing of their personal data. GDPR replaces the EU Data Protection Directive. It is designed to update and harmonize data privacy laws across the countries of the European Economic Area (EEA), which includes the 27 countries for the EU plus three countries (Norway, Iceland and Liechtenstein). Countries that belong to 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 and United Kingdom.

Notes: GDPR is very broad and this guidance document is limited to considerations for researchers. Contact ETSU Legal for impact in other areas. In addition, this IRB guidance may change as the implementation and interpretation of GDPR evolve.

In addition, each country subject to these regulations has their own interpretation of the rules and there are not many published guidance documents to assist the IRB with interpretation. Contact ETSU Legal for guidance regarding your specific study. If you are working with a researcher in a country subject to GDPR, that researcher's IRB may also be a great source of information.

1. What is different about this rule?

Increased Scope: GDPR regulates the use, access, collection, and processing of all personal data throughout the EEA. The GDPR has an increased territorial scope, protecting the personal data of those that are present (not limited to citizens) in the EEA, and also extending to collection of that data by researchers beyond the EEA boundaries. For example, if you are located in the US but collecting data from people present in the EEA, you may be subject to GDPR. The data protection standards are designed to be very high. The GDPR applies to "all companies processing the personal data of data subjects residing in the Union, regardless of the company's location." (https://www.eugdpr.org/key-changes.html, accessed 6.13.18)

Penalties: The GDPR provides for the levying of penalties up to 20 million euros.

Consent and Rights: In addition, GDPR overlays some additional consent considerations. Consents must be compliant with GDPR and with local laws. Some of the rules are similar to ones we already have in place. For example, consent must be "clear and distinguishable" and provided in an "intelligible and easily accessible form, using clear and plain language." That should be true of all consents. However, GDPR goes further to say that "It must be as easy to withdraw consent as it is to give it." That means if consent is given by "checking a box", then the method of withdrawing has to "be as easy" as checking a box. GDPR also gives a right to notice, and requires that individuals from whom personal data are collected have a right to know that their data was collected, where and how it was collected, and for what purpose. People also have the right to request a free electronic copy of the data that was collected from them ("right to access"). In addition, GDPR gives individuals the "right to be forgotten", also known as "data erasure". Individuals have the right to have data that was collected from them to be erased, and the right to cease their data from being further distributed, including third parties that may have received their data. Other rights include the right to receive breach notifications, right to data portability, and right to privacy by design. More information about these new consent requirements and rights is provided in the next sections of this document.

2. What do I need to know as a researcher?

First, you need to know whether your study is subject to GDPR. If your study is subject to GDPR, then you need to know what responsibilities you have to people present in the EEA while collecting or handling their data. You need to know how to comply with GDPR and local country interpretations of GDPR.

3. When is a study subject to GDPR?

The first evaluation is whose data is being accessed, used, collected or processed. If your study involves research activity that is accessing, using, collecting or processing information or data in person or online from anyone (known as a "data subject") who is present in one of the countries of the European Economic Area (EEA), then your study is subject to GPDR. The GDPR is not limited to organizations located within the EEA, but it also applies to organizations located outside of the EEA if they offer goods or services to or monitor the behavior of EEA data subjects. Please note that an EEA data subject is broader than citizenship; in other words, if a US citizen is a foreign exchange student in one of the covered countries, their data is protected under GDPR.

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 of the personal data of data subjects present in the EEA and is unrelated to where the company (or researcher) is located.

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 EEA. The “offering of goods or services” is more than mere access to a website or email address, The “offering of goods or services” and targeting of individuals in the EEA would include recruitment of individuals in the EEA to participate in a research study.

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.

In addition, contractual relationships with others who are subject to GDPR could indirectly affect ETSU or its researchers.

The second evaluation is whether the data is personal and sensitive.
Any research project which uses **personal data** from a participant present in the EEA must abide by the requirements of the GDPR. **Personal data** is defined as “any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, constitute personal data.”

The following examples of personal data are listed by the European Commission:

- A name and surname;
- A home address;
- An email address;
- Income;
- An identification card number;
- An Internet Protocol (IP) address;
- A cookie ID;
- Phone identifiers; or
- Data held by a hospital or doctor which could uniquely identify a person.

Since the definition uses the word “any”, personal data must be interpreted in a very broad sense. The examples above indicate that a telephone number, an email address or even an IP address are all personal data. This is broader than the traditional U.S. interpretation of identifiable data.

If you have data which has been rendered anonymous in such a way that the individual is not identifiable, it is no longer considered personal data. Please note that for data to be truly anonymized under the GDPR, the anonymization must be irreversible.

If personal data is also **sensitive data**, it requires “special protection”. **Sensitive data** is data concerning “one’s health, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sexual orientation, biometric data, or data concerning a natural person’s sex life.”

You must obtain explicit consent to access, collect or use sensitive data. This means that the receipt of sensitive data that originates in the European Union must always be accompanied by the explicit consent of the individual, and for a specified purpose (i.e. “passive consent” is not sufficient).

4. What rules apply to consent under GDPR?

GDPR allows consent from research subjects to be a lawful basis for processing personal data for research purposes. To obtain a valid consent to processing an individual’s personal data for research purposes under GDPR, the individual’s consent must meet certain requirements. Consent is defined as “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.” Consent under the GDPR is seen as a tool that gives participants control over whether or not their personal data can be used for a research study. If that control is not present, then the GDPR considers the consent to be an invalid basis for processing of that data, which makes the activity unlawful under GDPR.

Generally, in order for consent to be an appropriate lawful basis:

- the potential participant must be offered control
- the potential participant must have a genuine choice with regard to accepting or declining the terms offered or declining them without detriment.
- the participant must have a degree of control of their data

The following information must be provided to an individual in the EEA whose personal data is being collected, used, or accessed for research:

- the existence of the right to withdraw consent and how they exercise that right
- specific purpose for the use of the data
- what type of data will be collected/used
- the legal basis for using the data
- how long the data will be stored
- who will view or use the data
- data protection rights
- whether the data will be removed from the EEA
- where they can complain their data use or protection
- contact information for the institution and, if required, a Data Protection Officer

The consent must additionally meet the requirements below.

Consent must be:

- a reversible decision
- freely given (if they can't withdraw or refuse, then it is not free. You must carefully consider areas where there is a potential imbalance of power).
- Specific*
- Informed (must provide accessible information)
- granular (allow them to give separate consent for personal data processing operations respectively)
- in clear and plain language, in easily accessible and intelligible form

*Specific: must specify purpose as a safeguard against function creep, must be granular in consent requests, and there must be a clear separation of information related to obtaining consent for data processing activities from information about other matters. If you are seeking consent for various different purposes, you should provide a separate opt-in for each purpose, to allow users to give specific consent for specific purposes. You must provide specific information with each separate consent request about the data that are processed for each purpose, in order to make data subjects aware of the impact of the different choices they have.

The decision must be given:

- by an 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. This means that consent requires a statement from the data subject or a clear affirmative act which means that it must always be given through an active motion or declaration. It must be obvious that the data subject has consented to the particular processing.
- A "clear affirmative act" means that the data subject must have taken a deliberate action to consent to the particular processing. 41 Recital 32 provides additional guidance about this. Consent can be collected through a written or (a recorded) oral

statement, including by electronic means. The use of pre-ticked opt-in boxes is invalid under the GDPR. Silence or inactivity on the part of the data subject, as well as merely proceeding with a service cannot be regarded as an active indication of choice. As a researcher, you must be able to clearly demonstrate that the person gave consent. Additional rules about consent apply to sensitive data.

- The GDPR does not allow use of pre-ticked boxes or opt-out constructions that require an intervention from the data subject to prevent agreement (for example 'opt-out boxes'). This means that a passive consent process is not allowed.

Withdrawal:

- You must ensure that consent can be withdrawn by the person as easily as they gave consent and at any given time. This does not mean that the giving and withdrawing of consent must always be done through the same action. However, when consent is obtained via electronic means through only one mouse-click, swipe, or keystroke, data subjects must, in practice, be able to withdraw that consent equally as easily.
- Additional information will be provided as ETSU receives additional legal guidance regarding situations where other rules, such as FDA, require the retention of data. Please note that this must be addressed and resolved prior to the initiation of a study, so that the consent contains all appropriate disclosures.

Please note that obtaining consent does not mean that you do not have to follow GDPR principles.

Since GDPR requires that the specific purpose(s) is disclosed, the IRB will be unable to approve deception research if the study is subject to GDPR.

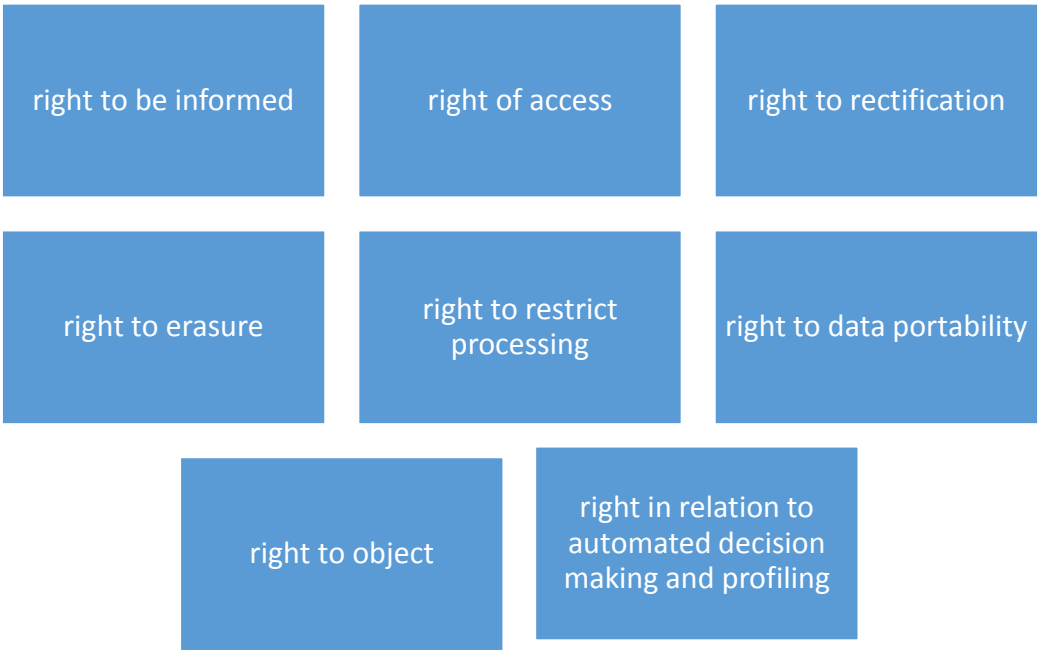
5. What if my research involves children?

The GDPR defines a child (for the purposes of using or accessing personal data) as an individual under the age of 16. For any personal data collected regarding a child under the age of 16, the "holder of parental responsibility" must explicitly consent to the collection or use of that child's data. Passive parental permission is not allowable. Please also note that individual member states may choose to lower the age below 16 within their own jurisdiction, but it cannot be lowered below the age of 13.

If your research is subject to GDPR and involves children, consult with ETSU legal.

6. What are the rules about data?

GDPR entitles the individuals to certain rights about how their data is handled. Those rights include:



In addition, GDPR permits the retention of personal data for only as long as is necessary to achieve the specific purpose for which it was collected. It must be deleted after that time.

With regard to the right to reject automatic profiling, this may have implications for researchers, for example, if algorithms are used to determine eligibility. Input from ETSU Legal will be needed if there is any question about this right and your study.

GDPR 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.

* '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. For example, a sponsor of a research study would typically be a "controller."
'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

If you are the PI of a sponsored research study, you would typically be a "processor." If you are the PI for a self-initiated study, you would be both the controller and the processor.

In addition, GDPR requires notification to data protection authorities and affected individuals following the discovery of a "personal data breach." That is defined as 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. (Submit a UPIRTSO xform to the IRB to report and obtain instructions regarding a breach)

References:

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-consentrequirements-application-to-scientific-research/), accessed 6.13.18

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-researchstudies-united-states), accessed 6.13.18

Article 29 Working Party Guidelines on Consent under Regulation 2016/679, revised and adopted on 10 April 2018, https://iapp.org/media/pdf/resource_center/20180416_Article29WPGuidelinesonConsent_publishpdf.pdf

A Primer on the Use of Personal Data from the European Union, Utah State University, http://rgs.usu.edu/irb/guidelines/, accessed 6.13.18

Guidance for General Data Protection Regulations (GDPR) compliance in the conduct of human research, Northwestern University, version date 5/25/18, https://irb.northwestern.edu/sites/irb/files/documents/GDPR%20Guidance_0.pdf, accessed 6.13.18