**TC IRB Guidance for Researchers: EU General Data Protection Regulations (GDPR) Compliance**

**Purpose**

This document assists investigators at Teachers College in determining whether The General Data Protection Regulation (GDPR) applies to their research projects, provides an overview of the regulation in the context of research, and offers points of contact for questions.

**Key Terms and Definitions**

1. GDPR: The General Data Protection Regulation (GDPR) is a European law that came into effect on May 25, 2018, establishing 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.
2. EEA Countries: 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**\***.
   1. **\***The United Kingdom is an outlier: Although the UK has departed from the EU as of January 2021, The GDPR is retained in domestic law as the [UK GDPR](https://ico.org.uk/for-organisations/data-protection-and-the-eu/data-protection-and-the-eu-in-detail/the-uk-gdpr/), but the UK has the independence to keep the framework under review.
3. Personal data. The term ‘personal data’ means any information concerning or relating to a living person who is either identified or identifiable (such a person is referred to as a ‘data subject’). An individual could be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier (such as an IP address), or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual. It is not necessary to have a name associated with the information. If the information, taken in the aggregate, could be used to identify a person, it is personal data protected by the GDPR.
   1. Personal data protected by the GDPR is much broader than Protected Health Information (PHI) protected by HIPAA or other types of personal information protected in the United States, such as Social Security numbers and financial account numbers.
4. Specialized categories of data: Health data, biometric data, Genetic data, Data about sex life or sexual orientation, race or ethnicity, political opinions, religious or philosophical beliefs, trade union membership.
5. Data Controller: Decides how and why the data is collected. The owner(s) of the data.

Examples: In clinical research, the sponsor is a controller if they design the study protocol, which determines how/and why the data is collected.

1. Data Processor: Collects or does anything with the data on behalf of the controller.
2. Processing: The term “processing” refers to any operation or set of operations performed on personal data. Processing includes storing, collecting, retrieving, using, combining, erasing, and destroying personal data, and can involve automated or manual operations.
3. Automated Processing: According to the GDPR, automated processing involves any form of processing of personal data that is carried out without human intervention. This includes activities where personal data is processed through automated means such as algorithms, artificial intelligence, or software applications to perform tasks like analyzing, predicting, or making decisions based on the data.
   1. Profiling: A specific type of automated processing that involves using personal data to evaluate certain aspects of an individual, such as their performance at work, economic situation, health, preferences, interests, reliability, behavior, location, or movements.

**What activities fall under GDPR?**

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

1. Collecting personal data from individuals in the EEA in relation to offering goods or services, including research.
2. Processing personal data by an organization established in the EEA.
3. Monitoring the behavior of individuals in the EEA.

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

The physical location of a data subject determines the applicability of the regulation. Personal data of an individual who is physically located within the EEA countries at the time of data collection (whether the participant is not a citizen or resident of an EEA country), is covered under the GDPR.

The personal data of an individual who is physically located anywhere outside of the EEA at the time of data collection (even if the participant is a citizen of an EEA country) is not covered under the GDPR. However, if the personal data of this individual is subsequently processed (e.g., used, stored, or shared) after their return to the EEA, such data may be within the scope of the GDPR.

**EXAMPLES:**

* Human subjects research conducted on location in any EU/EEA member country.
* Remote or virtual interviews or focus groups involving EU/EEA residents.
* Secondary research use of previously collected personal data about EU/EEA residents.
* Web-based recruitment or surveys that target or enroll EU/EEA residents within or outside of the EU/EEA.

Table 1: The GDPR applies to the following EEA countries

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

**If the data will be anonymous or de-identified, would GDPR still apply?**

Unlike U.S. regulations, GDPR does not use the word “de-identified,” but rather “pseudonymized” and “anonymous,” both of which have specific definitions.

* **Pseudonymized data** likely are subject to GDPR if the research team had a role in the initial collection of the data with identifiers and had access to the identifiers.
* **Anonymous data** are not subject to GDPR.

Table II: Data Type and GDPR Applicability

| **Data Type** | **Description** | **Regulation** |
| --- | --- | --- |
| **Identifiable Data** | Personal data collected from individuals who are, at the time of data collection, physically present in any of the EEA countries | Regulated by GDPR***\**** |
| **Pseudonymized (Coded data)** | - “*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*." | GDPR Article 4(5) |
| - Re-identification of individuals is possible through the use of additional information. | 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*.” | GDPR Recital 26 |
| - Re-identification of individuals is NOT possible. | Not regulated by GDPR. |

***\* GDPR can apply to data collected by a TC affiliate, or data collected by a third party and sent to TC researchers for analysis as part of a collaboration, from a data bank or repository, or pursuant to any other agreement or arrangement.***

**Process for Evaluating GDPR Applicability**

The following questions should be addressed in the protocol to determine whether GDPR applies to your study. If GDPR applies, the GDPR data consent form should be utilized. Contact the IRB office if you have any questions.

1. Will Teachers College collect or use the personal data of research subjects physically located in the EEA at any time of data collection?
2. Does the data include personal or sensitive personal information (e.g., national identification number, date of birth, address, photos, cookie IDs, exam info)?
3. Does Teachers College intend to recruit and enroll research subjects located in an EEA country in connection with the research study?

If you respond "**yes**" to questions 1-3 above, GDPR likely applies.

If you respond "**yes**" to questions 4-6 below, reach out to Teachers College Information Technology (TCIT) at [privacy@tc.columbia.edu](mailto:privacy@tc.columbia.edu) to discuss whether additional actions are required.

1. Will Teachers College monitor the behavior of research subjects located in an EEA country through an app or wearable devices?
2. 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?
3. Does the study team have a collaborator based in the EEA or hired the services of an organization within the EEA to assist with the study?

**Consent Requirements under GDPR**

GDPR requires researchers to obtain valid consent for the collection and use of personal data for research purposes. Consent must be:

* The individual must have a realistic choice, or the ability to refuse or withdraw consent without detriment.
* The consent must include a specific, transparent statement of each purpose of the study, what personal data elements are being collected, and the rights articulated above.
* Individuals must be informed of the nature and extent of data collection activities and the use of data.
* GDPR requires a clear affirmative act indicating an agreement to the proposed data processing activities.

**Special Categories of Personal Data**

The GDPR includes more stringent protections for "special categories" of personal data that merit a higher level of protection due to their sensitive nature and consequent risk of greater privacy harm. This includes information about a data subject’s:

* 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

Although criminal convictions and records are not considered special categories of personal data, this information is also subject to greater protection under the GDPR.

**Special Cases: Incomplete Disclosure and/or Deception**

If GDPR applies to your study, designs involving deception cannot be conducted due to the GDPR’s requirements for affirmative and informed consent. Incomplete disclosure may be used under specific conditions and must be justified on a case-by-case basis.

**Rights of Research Subjects under GDPR**

Research subjects have several rights under GDPR, including:

* **Access and Review:** The right to be provided all the personal data the study has about them and to review it.
* **Correction:** The right to have inaccuracies in their personal data corrected.
* **Erasure:** The right to require that all their personal data be deleted.
* **Restriction of Processing:** The right to require that the processing of identifiable personal data be restricted or halted.
* **Withdrawal of Consent:** The right to withdraw consent at any time.
* **Data Portability:** The right to move their personal data from one location to another.
* **Notification before Data Collection:** The right to prior notification before data collection.
* **Reject Automated Profiling:** The right to reject automated profiling.

**Anonymized Data**

Anonymized information is not personal data under the GDPR and is not subject to GDPR. The focus is on the possibility of reidentification either by the controller or another person.

**EXAMPLE:** *A survey conducted using Qualtrics or another third-party online survey tool where the researcher receives assurances that the data is not linked to any IP address or other identifiable information; or paper records where no information about the participant is collected or recorded.*

**What can I do to make my project GDPR-compliant?**

1. Collect the absolute minimum personal/demographic data needed.
2. Consider designing the study such that it can be done anonymously or record no identifying information.
   1. Many online survey sites collect personal information, including IP addresses, by default. Since IP addresses are considered identifiable information, make sure that you need to collect this information for your study. If not, disable this feature. We strongly recommend using REDCap or Qualtrics as an online survey platform. If other electronic systems are used, consult the IRB office for guidance.
3. Use active informed consent. Under the GDPR, consent must be freely given, specific, informed, unambiguous, and explicit.
   1. Following informed consent language, a button stating “click to proceed to the survey” or similar is considered active consent for these purposes. Silence, pre-ticked boxes, and inactivity do not meet the standard for active consent under the GDPR.
4. Verify that contracts with any third-party website or software applications include language clarifying GDPR roles and responsibilities and specifying mechanisms to be used for global data transfers. If you wish to use any other services or software solutions, a data processing agreement will need to be in place.
5. For research where identifiable data will be collected, include an executable plan to restrict processing or remove data in the event participant request to have their data removed.
   1. The informed consent document must notify the participant that their participation is voluntary and that they may leave the study at any point; however, the informed consent need not describe how the data erasure will take place if requested. It is sufficient if these procedures are in place and available internally.

**Who is responsible for GDPR compliance when relying on another IRB?**

Compliance with GDPR 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 and be mindful of any contract terms. The IRB of record, whether another institution or a commercial IRB, should typically set the standard for what is needed to be GDPR compliant.

**How does GDPR affect secondary research?** The data controller of the initial dataset is responsible for meeting secondary research requirements. If the TC study is the data controller for the initial dataset, researchers must ensure the following:

* 1. The [TC IRB GDPR Consent Notice Template](https://docs.google.com/document/d/15sdEj0ktHijAq0IwJu_lUggZiA8z6nhp?rtpof=true&usp=drive_fs) includes language for secondary research.
  2. Ensure secondary research purposes are compatible with the original purposes for which the data was collected.
  3. Obtain explicit consent from data subjects for secondary research, if required.

**Consequences of non-compliance**

Non-compliance with a protocol or consent requirement is managed by the IRB. Non-compliance with data handling or other violations of the privacy policy is managed by TC IT in accordance with applicable policies.

In the event of a data breach or suspected loss of data, or if an individual covered by the GDPR contacts you at any point after data collection and asks for their data to be erased, immediately notify the IRB and the TC IT so that appropriate steps can be taken at the College level and proper, timely response and support may be provided.

**IRB Application Information: Requirements**

1. **Description of Data Collection and Processing:**
   * Specify if personal data from individuals located in the EEA will be collected.
   * Detail the types of personal data to be collected, including any sensitive personal data.
   * Explain the purpose of data collection and how the data will be used in the research.
2. **Legal Basis for Data Processing:**
   * Identify the legal basis for processing personal data under GDPR (e.g., explicit consent, performance of a contract, legitimate interest).
     + For research involving human participants, informed consent is considered the lawful basis for collecting and processing personal data.
3. **Data Protection Measures:**
   * Describe the technical and organizational measures implemented to protect personal data (e.g., encryption, access controls).
   * Explain procedures for pseudonymization or anonymization of data, if applicable.
4. **Data Subject Rights:**
   * Outline how the rights of data subjects under GDPR will be addressed, including:
     + Right to access
     + Right to rectification
     + Right to erasure
     + Right to restrict processing
     + Right to data portability
     + Right to withdraw consent
5. **Data Transfer:**
   * Indicate if personal data will be transferred outside the EEA and the safeguards in place for such transfers (e.g., Standard Contractual Clauses, Privacy Shield).
6. **Data Retention:**
   * Provide the duration for which personal data will be retained and the criteria used to determine this period.
7. **Template Text for IRB application (to be included under Section IV Confidentiality Procedures & Participant Privacy):**

* This research involves the collection and processing of personal data from participants located in an EEA country [specify country (ies]. Teachers College (TC) is responsible for both collecting and processing this data. The legal basis for collecting and processing this data is explicit consent obtained by the TC PI from the participants. The personal data collected includes [specify types of data, e.g., academic performance, socio-economic background, survey responses].
* Participants will be informed of their rights under GDPR in the consent document, including access, correction, erasure, restriction, data portability, and withdrawal of consent.
* ***If automated processing is involved***: Automated decision-making will be used to analyze academic performance data to identify trends. Participants have been informed of their right to object to such processing and request human intervention.
* The personal data collected will be identifiable at the point of collection. De-identification measures will be applied once the data is processed and analyzed, ensuring that the data cannot be traced back to individual participants before any potential data transfer outside of the EEA.
* ***If data transfer is involved:*** Any transfer of de-identified data to Teachers College in the United States will be covered by appropriate Data Use Agreements (DUAs) or Material Transfer Agreements (MTAs) to ensure compliance with GDPR and to safeguard the confidentiality of the data.

**Consent Document Information: Requirements**

1. **Purpose of Data Collection:**
   * Clearly state the purpose for collecting and using personal data in the research study.
2. **Types of Data Collected:**
   * Specify the types of personal data being collected, including any sensitive data categories.
3. **Rights of Data Subjects:**
   * Inform participants of their GDPR rights, including:
     + Right to access their data
     + Right to correct inaccuracies
     + Right to request deletion of their data
     + Right to restrict or object to processing
     + Right to data portability
     + Right to withdraw consent at any time without affecting the lawfulness of processing based on consent before its withdrawal.
4. **Data Security Measures:**
   * Briefly explain the measures taken to protect their data (e.g., pseudonymization, encryption).
5. **Data Sharing and Transfer:**
   * Inform participants if their data will be shared with third parties or transferred outside the EEA, including the safeguards in place.
   * These safeguards may include Standard Contractual Clauses (SCCs), encryption of data during transfer, pseudonymization of personal data, and strict data access controls to ensure only authorized personnel have access to your data.
   * Regular audits and monitoring should also be conducted to ensure compliance with GDPR, and data processing agreements should be established with all third-party service providers involved in the transfer and processing of data.
6. **Duration of Data Retention:**
   * Indicate how long their data will be retained and the reasons for this retention period.
7. **Contact Information:**
   * Provide contact details for the data protection officer or the person responsible for data privacy within the research team, and how participants can exercise their rights.
8. **Template Text for Consent Forms:** Please refer to the [TC IRB GDPR Consent Notice Template](https://docs.google.com/document/d/15sdEj0ktHijAq0IwJu_lUggZiA8z6nhp?rtpof=true&usp=drive_fs) for the information to be included as part of the main consent form and under the PROTECTION OF YOUR CONFIDENTIALITY section.

**Resources & References**

* [TC IRB GDPR Consent Notice Template](https://docs.google.com/document/d/15sdEj0ktHijAq0IwJu_lUggZiA8z6nhp?rtpof=true&usp=drive_fs)
* [TC IRB GDPR Compliance Reviewer Determination Checklist](https://docs.google.com/document/d/1jGVsxId6D0xrfOgmbwNtXjZs_CJAroF-?rtpof=true&usp=drive_fs)
* [General Data Protection Regulation @ TC — GDPR](https://www.tc.columbia.edu/gdpr/)
* [General Data Protection Regulation (GDPR)](https://gdpr-info.eu/)
* [The European Data Protection Board](https://edpb.europa.eu/)
* [SACHRP’s Attachment B - European Union's General Data Protection Regulations](https://www.hhs.gov/ohrp/sachrp-committee/recommendations/attachment-b-implementation-of-the-european-unions-general-data-protection-regulation-and-its-impact-on-human-subjects-research/index.html)

**GDPR Frequently Asked Questions (FAQs)**

1. **Does GDPR apply if a TC researcher collects data from participants located in the EEA?**

* Yes, GDPR applies if personal data is collected from participants physically located in the EEA, regardless of their nationality or residency.

1. **Does GDPR apply if the research is conducted online, and the participants are in the EEA?**

* Yes, GDPR applies to online data collection from individuals who are physically in the EEA at the time of data collection.

1. **If a TC researcher is processing previously collected de-identified data from an EEA country, does GDPR apply?**

* GDPR may not apply to fully anonymized data where re-identification is not possible. However, pseudonymized data (where re-identification is possible with additional information) is subject to GDPR. For example, a research study collects data from participants at various universities on their dietary habits and fitness routines, and the dataset removes all direct identifiers like names, student IDs, and specific ages. However, if only one participant in the study is a vegan triathlete from a small university, that participant might still be identifiable through the combination of these unique characteristics, making the data pseudonymized rather than fully anonymized.

1. **Does GDPR apply to a study involving U.S. citizens traveling in the EEA who participate in research activities?**

* Yes, GDPR applies to any individual located in the EEA at the time of data collection, regardless of their citizenship.

1. **Does GDPR apply if a TC researcher collaborates with an institution based in the EEA?**

* Yes, if the collaboration involves collecting, processing, or sharing the personal data of individuals in the EEA, GDPR applies. A data transfer agreement may be required.

1. **If a TC researcher uses an EEA-based service provider for data processing, does GDPR apply?**

* Yes, if the service provider processes the personal data of individuals in the EEA, GDPR applies, and a data processing agreement should be in place.

1. **If a study monitors the behavior of participants in the EEA using apps or wearable devices, does GDPR apply?**

* Yes, monitoring the behavior of individuals in the EEA through apps or wearable devices falls under GDPR.

1. **Does GDPR apply if personal data is transferred from the EEA to the USA for analysis?**

* Yes, transferring personal data from the EEA to the USA requires compliance with GDPR, including ensuring appropriate safeguards like Standard Contractual Clauses or Privacy Shields.

1. **Does GDPR apply to research conducted entirely within the USA involving only U.S. residents?**

* No, GDPR does not apply to research activities conducted entirely within the USA with participants who are not located in the EEA.

1. **Does GDPR apply to anonymous data collected from EEA participants?**

* No, GDPR does not apply to anonymous data where re-identification of individuals is not possible.

1. **If a TC researcher receives de-identified data from an EEA collaborator, does GDPR apply?**

* GDPR may not apply if the data is fully anonymized. However, if the data is pseudonymized and can be re-identified, GDPR would apply.

1. **Does GDPR apply if an EEA participant moves to the USA after data collection?**

* GDPR applies to the data collected while the participant was in the EEA. Post-collection, the data remains subject to GDPR regardless of the participant's relocation. The key point is that the data was collected while the participant was within the EEA, and thus, it remains protected under GDPR regardless of subsequent relocation.

1. **Does GDPR apply to publicly available data from the EEA used in research?**

* GDPR may not apply if the data is genuinely public and does not involve any processing that identifies or can re-identify individuals.

1. **Is it possible to apply for a waiver to the application of GDPR?**

* No. The GDPR does not provide a procedure to be exempted from its requirements.

1. **What steps should a PI at TC take to ensure GDPR compliance?**

* The PI should:
* Determine if the research involves personal data from the EEA.
* Identify the legal basis for processing personal data.
* Implement appropriate data protection measures.
* Inform participants of their rights under GDPR.
* Ensure proper data transfer agreements are in place if applicable.
* Seek IRB approval and include GDPR-specific consent language.

1. **Who can I contact at TC for GDPR-related questions?**

* For GDPR-related questions, contact the IRB office at [irb@tc.edu](mailto:irb@tc.edu) or the TC IT at [privacy@tc.columbia.edu](mailto:privacy@tc.columbia.edu).