SOP-R-012: TC IRB Standard Operating Procedure (SOP) for General Data Protection Regulation (GDPR) Compliance

Purpose
This SOP outlines the procedures to ensure compliance with the General Data Protection Regulation (GDPR) for research involving personal data from individuals located in the European Economic Area (EEA).

Scope
This SOP applies to all researchers at Teachers College who conduct research involving the collection, use, processing, or transfer of personal data from individuals located in the EEA.

Definitions
- **GDPR:** European law that protects the privacy and security of personal data from individuals in the EEA.
- **EEA Countries:** 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 United Kingdom*.
    - **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, but the UK has the independence to keep the framework under review.*
- **Personal Data:** Any information relating to an identified or identifiable individual.
- **Special Categories of Data:** Sensitive data including racial or ethnic origin, political opinions, religious beliefs, health data, genetic data, etc.
- **Data Controller:** The entity that determines the purposes and means of processing personal data.
- **Data Processor:** The entity that processes data on behalf of the Data Controller.
- **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.
    - *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.

Responsibilities
- **Primary Investigator (PI):** Ensure research complies with GDPR requirements, including obtaining valid consent and implementing data protection measures.
- **IRB:** Review research protocols to ensure GDPR compliance and provide guidance to researchers.
- **Teachers College Information Technology (TCIT):** Assist with aspects of GDPR compliance and data protection agreements.

Teachers College, Columbia University
Institutional Review Board
525 W. 120th St. Box 151, New York, NY 10027
212-678-4105 | IRB@tc.edu | RH 13 | tc.edu/IRB

Procedures

1. Determining GDPR Applicability

1.1 The PI must determine if the research involves personal data from individuals located in the EEA by addressing the following questions:

- Will personal data be collected from individuals in the EEA?*
- Will personal data be collected from EEA citizens when they are in the United States?*
- Does the data include personal or sensitive personal information?
- Will the research involve monitoring the behavior of individuals in the EEA?
- Will the study use cookies or other online tracking tools to collect data from individuals in the EEA?
- Does the study involve collaboration with an institution based in the EEA?

If the answer is "**yes**" to any of these questions above, GDPR likely applies.

***NOTE:** *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.*

2. Informed Consent

2.1 Obtain explicit, informed consent from participants by including the following elements in the consent form:

- Purpose of data collection.
- Types of data collected, including any sensitive categories.
- Rights of data subjects under GDPR (access, rectification, erasure, restriction, data portability, withdrawal of consent).
- Data protection measures.
- Data sharing and transfer details, including safeguards for transfers outside the EEA.
- Duration of data retention.

2.2 Refer to the TC IRB GDPR Consent Notice Template for specific language to include.

3. Data Collection and Processing

3.1 Collect only the minimum necessary personal data to achieve research objectives.

3.2 Consider anonymizing or pseudonymizing data where possible.

3.3 Implement technical and organizational measures to protect personal data (e.g., encryption, access controls).

4. Data Subject Rights

4.1 Ensure procedures are in place for participants to exercise their GDPR rights, including:

- Access to their data.
- Correction of inaccuracies.
- Requesting deletion of their data.
- Restriction of data processing.
- Withdrawal of consent.

5. Data Transfer

5.1 If personal data will be transferred outside the EEA, ensure appropriate safeguards are in place (e.g., Standard Contractual Clauses, Privacy Shield).

Teachers College, Columbia University
Institutional Review Board
525 W. 120th St. Box 151, New York, NY 10027
212-678-4105 | IRB@tc.edu | RH 13 | tc.edu/IRB

6. Data Retention

6.1 Specify the duration for which personal data will be retained and ensure it complies with TC IRB's Data Sharing, Requests, & Encryption policies.

7. Data Breaches

7.1 In the event of a data breach, immediately notify the IRB and TC IT to take appropriate actions.

8. IRB Review Process

8.1 Use the TC IRB GDPR Compliance Reviewer Determination Checklist to review protocols for GDPR compliance.

8.2 Confirm that all required elements are included in the consent form and protocol.

8.3 Provide feedback and require modifications if necessary to ensure compliance.

9. Training and Resources

9.1 Provide training to researchers on GDPR requirements and data protection best practices.

9.2 Refer researchers to the TC IRB Guidance for Researchers: EU General Data Protection Regulations for detailed guidance.

10. Compliance Monitoring

10.1 The IRB will conduct periodic audits to ensure ongoing compliance with GDPR requirements.

10.2 Non-compliance will be addressed in accordance with Teachers College policies and procedures.

Contacts

- **IRB Office:** irb@tc.edu
- **TC IT:** privacy@tc.columbia.edu

References

- TC IRB Guidance for Researchers: EU General Data Protection Regulations
- TC IRB GDPR Consent Notice Template
- TC IRB GDPR Compliance Reviewer Determination Checklist
- General Data Protection Regulation @ TC — GDPR
- General Data Protection Regulation (GDPR)
- The European Data Protection Board
- SACHRP's Attachment B - European Union's General Data Protection Regulations

Teachers College, Columbia University
Institutional Review Board
525 W. 120th St. Box 151, New York, NY 10027
212-678-4105 | IRB@tc.edu | RH 13 | tc.edu/IRB