GDPR @ HARVARD

General Data Protection Regulation

I. GDPR Overview

II. IRB’s role / ESTR

III. Information Security’s role / Data Safety

IV. Negotiator’s role / Research Agreements

V. Questions?

GDPR OVERVIEW

Definitions and Principles

GDPR and Research

- GDPR applies to data on living individuals located in the European Economic Area (EEA) and the UK ("Personal Data")
- Restricts "Processing" of Personal Data
  - ***Processing*** *is a general term describing the use of Personal Data, including collecting, analyzing, exchanging, etc.*

Important Definitions:

- **Personal Data:** Any information relating to an **identified or identifiable** living person
- Includes data that is directly or **indirectly identifiable**, such as "Pseudonymized Personal Data", i.e. coded data, or data that could be re-identified by a collaborator
- Definition states "**any information**," so must assume that the term "Personal Data" should be broadly interpreted
- **Special Categories of Personal Data:** Special Categories may require additional data security measures, including an elevated Data Security Level

Special Categories:

- *Racial / ethnic origin*
- *Political opinions*
- *Religious / Philosophical beliefs*
- *Genetic or biometric*
- *Health (mental or physical)*
- *Sex life / sexual orientation*
- *Trade Union membership*
- **Data on criminal activities are similarly restricted*

Important Definitions:

- **Controller:** person or organization which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data
  - Engaged in the research and research plan = **Harvard is a Data Controller, as we conduct research, not services**
  - Can have co-controllers (i.e. may be more than one controller in a project)
    - *Often requires a data use agreement (DUA) or collaboration agreement*
- **Processor:** person or organization which Processes Personal Data on behalf of the Controller
  - Vendor or contractor (e.g. survey company, software company)
    - *Typically provides services*
    - *Must work with Strategic Procurement prior to signing anything, to ensure correct contractual language is used*

Important Definitions:

- **Pseudonymization and Anonymization:**
  - Personal Data which have undergone Pseudonymization, which could be attributed to a natural person by the use of additional information is still Personal Data
    → **Pseudonymized data is Personal Data, and is subject to GDPR**
  - To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, either by the controller or by another person to identify the natural person directly or indirectly
    → **If you will not receive identifiers, but your collaborator has a key (or identifiers), you are receiving Pseudonymized Data, not Anonymized, and GDPR still attaches**
  - GDPR does not apply to Anonymous Information, i.e. 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 no longer identifiable
    → **GDPR does not apply to Anonymized Data**

Important Definitions:

- **Lawful Basis:** Processing activities must qualify for a Lawful Basis (essentially, an exception), otherwise you cannot Process data
  - Criteria for Special Categories are more demanding
  - Harvard typically elects to utilize “consent” as a Legal Basis for research projects: ‘
    - Provides documentation that data subjects were informed of the purpose of the study, as well of their rights
    - Qualifies as Lawful Basis for Special Categories and non-Sensitive Personal Data
    - Must be unambiguous, freely given, informed, specific, demonstrable
    - Consent should include specifics of study, including any Special Categories involved
  - Exchanging Personal Data also requires a Lawful Basis, which is why we must incorporate Standard Contractual Clauses (“SCCs” i.e. template GDPR language) into Research Agreements (and vendor agreements)

Important Definitions:

- **Data Minimization:** data collected and processed should not be held or further used unless it is essential for purposes that were clearly stated at beginning of study
  - **Data collection and processing should be adequate & relevant**: Scope of processing should be supported by documentation – both internal (Info Security, IRB, OSP/ORA, OVPR) and info provided to data subjects
  - **Data collection and processing should be limited to what is necessary:** This theme is prevalent throughout GDPR. There must be a specific, explicit purpose for each datapoint collected, and each processing activity
  - **Pseudonymization** and/or **Anonymization** are recommended throughout GDPR
    - Delete identifiers and/or datapoints that "link" to an individual as soon as they're no longer needed
    - Maintain identifiers separate from working/research data whenever possible

IRB’S ROLE

System of Record: ESTR

Human Subjects Research must be submitted for IRB review in ESTR

- Based on the information submitted in ESTR, **the IRB will determine if the study is Sensitive or Non-sensitive**
- **GDPR regulated studies are Sensitive,** and therefore must also be reviewed in Data Safety Application
  - *Sensitive data = DSL 3+ data*
- **If you don't believe your project rises to the level of Humans Subjects research, but you're accessing foreign data, it still must go through the Data Safety Application.**

OVPR's GDPR Ancillary Review

- **Lifecycle of data:**
  - *Who's accessing the data and identifiers*
  - *When the data will be fully Anonymized or destroyed*
- **Whether appropriate Research Agreement is in place**
  - *GDPR requires that Standard Contractual Clauses (SCCs) be included in GDPR agreements*
- **Whether participants are explicitly and comprehensively informed of project specifics**
  - *Intended uses of data, and datapoints involved*
  - *Parties involved*
  - *Timeline*

INFORMATION SECURITY ROLE

System of Record: Data Safety Application

Personal Data is Sensitive data, requiring Info. Security review

All regulated data is Data Security Level 3-5, i.e. Sensitive Data

Examples of regulated data:

- Personal Data under GDPR
- Data provided under a contract (e.g. DUA, Collaboration Agreement, NDA, MTA, etc.)
- Foreign data
- Student data
- Health data

All studies involving Sensitive data must be submitted for Info. Sec. Review in the Data Safety Application, to ensure compliance with Enterprise Security Policy & Research Data Security Policy

ENTERPRISE INFORMATION SECURITY POLICY

DSL2 - Unpublished **non-sensitive** research data, whether identifiable or not. Active research data at Harvard is at least DSL2 until published.

DSL3 - **Sensitive Data:** Some regulated data, or data that could be damaging to the subject's financial standing, career or economic prospects, personal relationships, insurability, reputation, or be stigmatizing

DSL4 - **Sensitive Data** that could place the subject at risk of significant criminal or civil liability or data that require stronger security measures per regulation

Must be submitted in Data Safety

Info. Security review in Safety Application

Info Security reviews studies in the Data Safety Application

- Automatically routed to local Info. Security
- Submission must include comprehensive description of data, including source, other parties and relevant contracts/agreements
  - *If your project includes a Research Agreement or vendor agreement, make sure it is referenced or included!*
  - *You must highlight that data is coming from a foreign source*
- Related reviews in the portal (Agreements, Safety, ESTR) must be linked via "Manage Related Projects"

Take a look at the Harvard Research Data Security Policy for more info

Managing Related Projects

- **Can occur from any application – ESTR, Safety, or Agreements** (not specific to Info Security Review/Data Safety)
- **Linking related projects is required** before the IRB will approve a Sensitive study, as they need to confirm Info Security's approval of data management plan
- Also required before ORA/OSP will sign DUA, as negotiators need to confirm Info Security (and possible the IRB) have approved

NEGOTIATORS' ROLE

Agreements Application/DUAs, MTA, NDA, Collaboration Agreement, etc.

GDPR requires an agreement for the transfer of Personal Data

GDPR requires Controllers and Processors to have contractually predetermined roles and responsibilities, therefore **Harvard requires that any exchange of Personal Data be done under a Research Agreement,** or vendor agreement

- Researchers (faculty, students, etc.) may not sign any Research Agreements involving the exchange of data – only ORA/OSP Negotiators can!
- All such agreements must also be submitted in the Data Safety Application

Policy: Negotiating and Signing Authority for Agreements Related to Research

GDPR requires an agreement for the transfer of Personal Data

What should you do if your study involves a transfer of Personal Data from or to a third party?

For example:

- From Oxford to Harvard
- From Harvard PI in Paris, to Tokyo

If third party is **collaborating** in the research: Work with the Negotiators from ORA/OSP. If the appropriate agreement is a DUA, submit in the Agreements-DUA Application

If third party is a **vendor**: Work with Strategic Procurement

Reviews of transfers of Personal Data in Agreements Application

- Once researcher submits DUA request in the **Agreements Application,** it will automatically be assigned to Negotiator
  - **Only Negotiators may draft and sign Research Agreements!**
  - Negotiators will not sign unless Info. Security has approved (and IRB, if human subjects research)
- Requests for review of collaboration agreements should be submitted directly to the relevant negotiating office
- Negotiators have templates that include GDPR's Standard Contractual Clauses, which outline relevant requirements and ensure both parties are compliant

Reviews of transfers of Personal Data

Standard Contractual Clauses:

- Negotiators are familiar with the applicability of the SCCs, and will determine when they're required for a Research Agreement
- The new SCCs (post *Schrems* case) require:
  - Personal Data be completely Anonymized, or destroyed once the purpose of the data transfer has been fulfilled (at latest, end of the PoP)
  - Project-specific risks be disclosed and considered for each data exchange
  - Only specific researchers (who must be listed in Data Safety and kept updated) may access the data

FINISHING UP

Reviews of transfers of Personal Data

EXAMPLE: You are collaborating with a PhD student from King's College London. She is going to send out a survey to her colleagues, focusing on their mental health during COVID. You will both have access to the survey responses and will co-publish a paper.

What reviews do you need?

- ***Data Safety:*** *regulated/Sensitive data (and also because Research Agreement is needed)*
- ***Negotiating Office*** *for Data Use Agreement/Collaboration Agreement*
- ***IRB*** *as you're accessing identifiable data for research purposes*

IN SUMMARY:
GDPR and Research:

- Personal Data requires Information Security review in the Data Safety Application
- Often requires IRB review in ESTR when Personal Data is identifiable
- Any exchange of Personal Data with a third-party requires a Research Agreement (negotiated by ORA/OSP) or vendor agreement (negotiated by Strategic Procurement)
- Manage Related Projects (i.e. link related reviews in the system)!!

THANK YOU

QUESTIONS?

Rachel_talentino@Harvard.edu