General Data Protection Regulation (GDPR) for Researchers

Kathleen Tranelli, Privacy Office
Mark Wright, Office of Counsel

November 2018

Agenda

- Scope of GDPR
- Examples
- Key Concepts
- Implications if study is subject to GDPR
- What you should do /Resources
- Questions

GDPR Scope

- GDPR applies to organizations involved in the "processing" of "personal data" of individuals located in the EEA

- Personal data includes more than health care data; GDPR is broader than HIPAA

- Personal data includes coded data a/k/a "pseudonymized" data

GDPR Scope

- Processing is defined broadly; includes both controllers and processors
- Controller: Determines the purposes and means of processing the data
- Processor: Performs analysis/processing at the direction of the controller

GDPR Scope

- Applies to organizations "established" in the EEA , i.e. that have an office or facility there

- Applies to organizations not established in the EEA where the processing activities are related to offering goods or services to or monitoring the behavior of "data subjects in the Union"

  - Data subject = any person located in EEA irrespective of nationality

Example Research Scenarios That May Trigger GDPR

- Collaborating with researchers in EEA member states
  - Serving as a participating site or core site in research sponsored by an EEA company
  - Acting as a lead site in a multi-site study involving EEA sites
- Conducting secondary research on data sets originating in EEA
- U of R can be either controller or processor depending on the research arrangement

When Does GDPR Not Apply?

- No collection of data from individuals in the EEA
- For example, studies that do not collect information that is linked to a subject's identity, such as anonymous survey- based studies in which the identities of participants cannot be tracked back to the individual
- Data that has been anonymized (no key to re-identify the data)

Key Concepts

- May only process data if a specified "lawful basis" exists
  - E.g. Consent, legitimate interests, public interest
    - There are issues with consent as a basis

- Transfer of data from EEA to US requires an additional lawful basis
  - Express consent or
  - Model Contract Clauses
    - Core terms not negotiable; may require governing law / jurisdiction in EEA

Implications if GDPR applies

- Right to complain to EEA supervisory authority and private right of action
- Potential for substantial fines / penalties
- Data breach notification
  - Within 72 hours to the data processing authority in the relevant country; “without delay” to subjects
- Accountability and record keeping requirements

Implications if GDPR applies

- Broad rights for data subjects:
  - Transparency
  - Access
  - Rectification
  - Erasure
  - To restrict processing
  - Portability
  - To object to processing
  - To withdraw consent

Implications if GDPR Applies

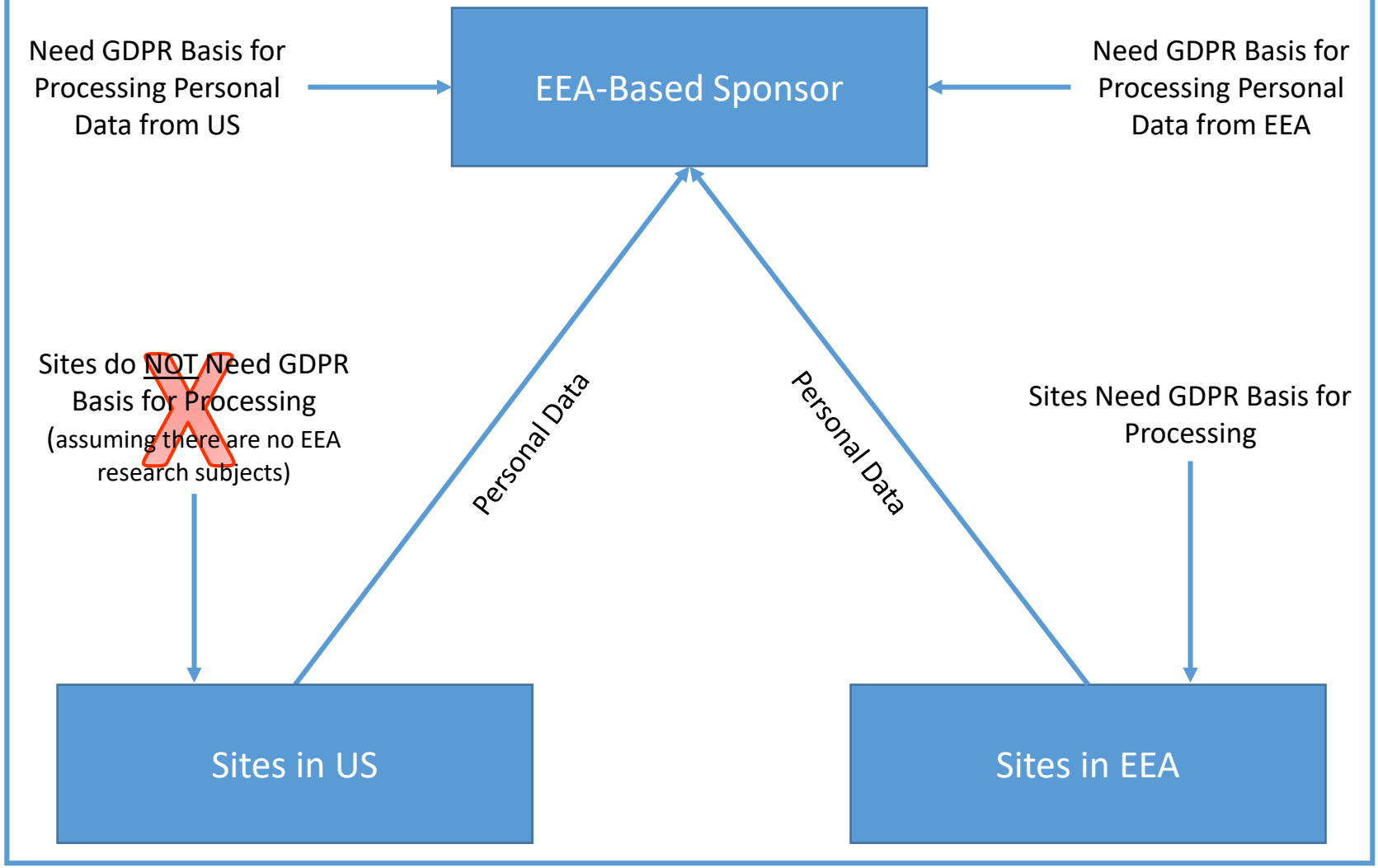
- IT Systems
  - Need to be configured to honor data subjects rights
    - Tracking of data to make it available, ability to delete data
  - Need to meet GDPR security standards
    - Compliance with UR IT standards for PHI, e.g. encryption, is a good starting point, but don't assume your system is compliant
    - Coding data where possible is wise, although not a "safe harbor" as in HIPAA
- Contracts
    - Depends on particular scenario; careful analysis needed
- Vendor Management

Implications if GDPR Applies

- Data subjects must be provided a Notice of their rights
  - Identity and contact details of the controller
  - Purposes and lawful basis for processing data
  - Period of time for which data will be stored or criteria used to determine period
  - Right to request erasure of personal data
  - Transfer of data from EU to U.S. and basis to legitimize transfer
  - Right to lodge complaint with EU data protection authorities

- Implications for Informed Consent forms

GDPR Application to Multi-Site Trial



What You Should Do/ Resources

- Write to research-gdpr@rochester.edu or contact one of us if you
  - Have a study that might trigger GDPR
  - Receive a communication that mentions GDPR and requests a change to informed consents or notices
  - Are asked to change or enter contract due to GDPR, or have a contract that mentions EEA/EU data
- See Q&As at http://www.rochester.edu/ohsp/documents/ohsp/pdf/policiesAndGuidance/Guideline_for_GDPR_QA_for_researchers.pdf


Questions