Session T510
Demystifying General Data Protection Regulation (GDPR) Requirements for Research Institutions

Demystifying the EU data privacy law and its impact on research

James Riddle, MCSE, CIP, CPIA, CRQM
Vice President of Institutional Services
Advarra
Experience

> Over 15 years developing human research protection programs
> Assistant Director at the Fred Hutchinson Cancer Research Center
> Vice President for Operations at large independent IRB
> AAHRPP site visitor
> Published author and frequent speaker on human research protection issues

Certifications & Affiliations

> Certified IRB professional (CIP)
> Certified Professional IACUC Administrator (CPIA)
> Microsoft Certified Systems Engineer (MCSE)
> Clinical Trial Transformation Initiative, Steering Committee Member (CTTI)
> Collaborative Institutional Training Initiative, Author and HRP Steering Committee Member (CITI)
> Alliance for Clinical Research Excellence and Safety, SASI Accreditation Domain Leader (ACRES)
> Northwest Association for Biomedical Research, Emeritus Board Member (NWABR)
> IRB Advisor, Editorial Board Member
> Public Responsibility in Medicine and Research, Faculty Member and Mentor (PRIM&R)
Learning Objectives

1. Outline EU GDPR scope, key definitions and requirements, and regulatory impact on researchers and research organizations.

2. Evaluate operational implications of GDPR regarding protection parameters around informed consent, future research, research transparency, data processing and sharing, data transfer outside the EU, as well as business privacy policies and responsibilities.

3. Highlight GDPR requirements in contrast to US data privacy, security, and confidentiality regulations.

4. Offer potential solutions for updating policies, procedures, and practice for compliance with GDPR.
Agenda

• Overview of GDPR
• Definitions & Requirements
• Regulatory & Operational Implications
• Comparison of GDPR to US Regulations
• General Recommendations
Poll Question 1 – US Research Participants in EU/EEA

• Hypothetical: A research participant is enrolled in a US-based clinical trial, investigating efficacy of sensor insoles, and travels to Spain. While the participant is in Spain, data from the insoles are collected and transmitted to the study team in the US.

• Is this activity subject to GDPR?
  a) Yes
  b) No
Overview of GDPR

GDPR applies in the 28 member states of the EU and three additional countries (Iceland, Liechtenstein, and Norway) that together with the EU make up the European Economic Area ("EEA").
Where Does GDPR Apply?
Application to Organizations

GDPR applies to the processing of personal data of data subjects by a controller or processor not established in the EEA, when processing activities are related to:

• Offering of goods or services, irrespective of whether payment of the data subject is required, to such data subjects in the EEA, or

• Monitoring of data subjects’ behavior as far as their behavior takes place within the EEA.
Poll Question 2 – EEA Citizen in a Clinical Trial in the US

• *Hypothetical:* An investigator in the US initiates a research study domestically and enrolls an EEA citizen at her US research clinic.

• **Research data collected in the US from this participant is:**
  a) Automatically subject to GDPR
  b) Not subject to GDPR
  c) Only subject to GDPR if the citizen is from the EU
  d) Only subject to GDPR for data transfers from the US to non-EEA countries
Penalties & Consequences

Failure to comply with GDPR has significant consequences. Fines of up to 4% of a sponsor’s global revenue can be assessed depending on the scope of the violation, including the provisions on subject access and right to erasure.
Definitions & Requirements
Data Subject

“An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or by one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.”
Personal Data

• Any information relating to an identified or identifiable natural person ("data subject").

• **Special categories of personal data, include:**
  
  “…data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation…”

The collection of special categories of personal data is prohibited by the GDPR, unless an exception condition is met, which includes the data subject giving their explicit consent for the collection of these categories of data.
Data Controller & Processor

**Controller**

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.

**Processor**

A natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.
Processing Data

Processing is defined by GDPR as

“...any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction”.

Any activity that affects the data from a clinical trial during its entire life-cycle, from its collection by the sites as source data to its reporting, aggregation, analysis, and destruction.
Anonymized & Pseudonymized Data

- GDPR does not apply to anonymized data

Anonymization is judged on a facts and circumstances test, taking into account “all the means reasonably likely to be used . . . [e]ither by the controller or by another person to identify the natural person directly or indirectly.”

- Pseudonymized data is considered personal data under GDPR

The processing of personal data in such a manner that the personal 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 Principles

- Lawfulness, fairness, transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability*
Regulatory & Operational Implications
Authority to Process Personal Data

- **Processing personal data under GDPR requires a legal basis:**
  - *Specific* consent of the data subject
  - Performance of a contract to which the data subject is a party
  - Compliance with a legal obligation
  - Protection of vital interests of the data subject or a natural person
  - Task carried out in the public interest
  - Legitimate interests of the controller or a third party, except where such interests are overridden by the interest or fundamental rights and freedoms of the data subject
Basis to Process Special Categories of Personal Data

- Processing this special class of personal data under GDPR requires a unique basis:
  - *Explicit* consent of data subject
  - Vital interests of data subject where incapable of giving consent
  - Manifestly made public by the data subject
  - Substantial public interest
  - Preventive medicine, diagnosis, or healthcare
  - Necessary for scientific or historical research purposes
  - Public interest in the area of public health
Authority to Transfer Personal Data

GDPR requires a legal basis for the transfer of personal data from the EEA to jurisdictions that do not have commensurate level of data protection.

Transfer requirements apply even if GDPR does not apply directly to receiving party!

- Explicit consent
- Performance of a contract between data subject and controller...
- Important reasons of public interest
- Establishment, exercise, or defense of legal claims
- Protection of vital interests
- Standard contractual clauses, binding corporate rules, codes of conduct
Controller/Processor Obligations

Records of Processing Activities
- Purpose (or categories) of processing
- Categories of
  - Data subjects
  - Personal data
  - Recipients
- Limitations on retention
- Technical and organizational security measures
- Third-country transfer

Representative in the EU
- More than occasional
- Inclusive of special categories of data on a large scale
- Risky

Data Protection Officer (DPO)
- Core activity
- Large scale
- Involves regular & systematic monitoring or special categories of data
Data Subject Consent – Working Party (WP) Guidance

The WP issued guidelines on GDPR data subject consent, including:

• Consent has 4 elements:
  1. Freely given
  2. Specific
  3. Informed
  4. Unambiguous indication by a statement or a clear affirmative action

• Consent should be as easy to withdraw as to give.
Consent – WP Guidance – Research Implications

• GDPR does not preempt/substitute for regulations governing clinical trials.
• If details of research are not known at outset, updates regarding details of the research should be provided to subjects as the information becomes known so that subject can determine whether to exercise right to withdraw.
• Make available a “Comprehensive research plan” to data subjects at outset.
• Future uses involving special categories of data will need to meet a more rigorous standard for consent.
• No research exception for withdrawal of consent.
Poll Question 3 – Basis for Processing Personal Data

• Which basis could justify the processing of ethnic origin in a research study subject to GDPR?

  a) Explicit consent only
  b) Legitimate interest of commercial sponsor
  c) Specific consent only
  d) Public health
Notice to Data Subjects

GDPR requires controllers to provide data subjects with notice regarding the processing of their personal data. Relevant notice elements for research include:

- Identity and contact details of controller, controller's data protection officer, and controller's EU representative (where applicable).
- Purposes and legal basis for processing data under EU law.
- Period of time for which data will be stored or criteria used to determine period.
Data Subjects Rights

Access

Rectification

Portability

Restriction

Erasure

Objection
Data Processing Transparency: Research Data Sharing

**GDPR transparency** requirements apply irrespective of the legal basis for processing and relate primarily to the notice requirements.

- With a legal basis other than consent, controllers should consider including, in their notice, a compatibility analysis as to how any further processing is consistent with the original purpose.

**Research transparency** could be challenged by GDPR and will require additional justification where the data is not anonymized.

- Clinicaltrials.gov
- US NIH – GWAS, dbGAP
- Health Canada – Public Release of Clinical Information (Draft Guidance)
- EMA – Policy 0070
Poll Question 4 – IRB Responsibilities

• *Hypothetical*: An IRB receives a research informed consent form also containing GDPR language for processing a participant’s personal data.

• **Which section(s) of the research ICF is the IRB required to review for regulatory compliance?**
  a) Confidentiality
  b) HIPAA
  c) GDPR
  d) Both A & C
Comparison of GDPR to US Regulations
Common Rule

- Informed consent
- Readily ascertainable
- May not apply to coded data
- Retention of identifiable data permissible after withdrawal

GDPR

- Specific/explicit consent
- Identity determined, directly or indirectly, by reasonably likely means
- Applies to pseudonymized data
- No research exception for withdrawal of consent
HIPAA

In contrast to HIPAA, GDPR:

• Focuses on the data subject.
  > Private right of action.
• Permits processing of public personal data.
• Has no safe harbor that lists specific identifiers that if excluded would render a dataset anonymous.
• Does not have the concept of a Limited Data Set.
• Has right to erasure.
• Has right to access personal data, as long as the request does not adversely affect the rights and freedoms of others.
• Has more subjective breach thresholds and quicker turn around times for processing data requests and for breach notification/communication.
General Recommendations
General Recommendations

1. Consent to the full extent required by parallel clinical trial regulations will be necessary, even where GDPR consent is identified as basis for processing.

2. For IRBs reviewing ICFs that include GDPR language, determinations should be clear that IRB review does not assure GDPR-compliance.

3. Consider alternative basis for processing personal data, including scientific research or public interest.

4. Transfers of personal data from EU to US require a legal basis, including explicit consent or contractual clauses.
5. Assess controller/processor status for each anticipated processing of personal data, including clear identification of each entity’s responsibilities and obligations under GDPR.

6. Data privacy info should be provided to research participants for GDPR-compliant studies, highlighting personal data use and flow.

7. Secondary research uses and brief compatibility analysis should be included in notices of privacy practices.

8. Keep only that minimum personal data necessary to fulfill the purpose and delete or anonymize the data when no longer needed for that purpose.
General Recommendations

9. Document internal assessment of need for an EU representative, a DPO, and/or a DPIA.

10. Evaluate existing HIPAA procedures, privacy policy (notice), contracts, and informed consent form templates (if applicable) for GDPR gap analysis.
Wrap Up
Thank you!

Questions?

James Riddle, MCSE, CIP, CPIA, CRQM

Vice President of Institutional Services

Advarra

james.riddle@advarra.com