Verrill

Verrill

EU General Data Protection Regulation (GDPR) - Compliance Challenges for Institutions

Andrew P. Rusczek, Esq.
Partner

1

Agenda

- Current Landscape
- Crosswalk with HIPAA
- Key Definitions
- Territorial Scope
- "Legal Bases" for Processing
- Key Controller and Processor Obligations
- Top 4 Difficult Situations for Institutions

Verrill

2

Verrill

Current Landscape re: EU Data Protection Laws

- EU Data Protection Directive
  - Approved October 24, 1995, and applied until May 25, 2018
  - Implemented in different ways by each of the EU member states
  - **Generally applied to non-EU controllers that "made use of equipment" in the EU**
- EU General Data Protection Regulation (GDPR)
  - Approved May 24, 2016 and applied as of May 25, 2018
  - **Generally applies to non-EU controllers or processers that (1) offer goods or services within the EU or (2) monitor the behavior of individuals within the EU**
  - Penalties up to the **greater of** €20,000,000 or 4% of the total worldwide annual turnover (revenue) of the preceding financial year

Verrill

3

Crosswalk Between HIPAA and the GDPR

HIPAA Term		GDPR Term
Covered Entity	→	Controller
Business Associate	→	Processor
Use Disclosure	→	Processing*
Protected Health Information	→	Personal Data (including pseudonymised)
De-identified	→	Anonymised

* Special rules apply to transfers of personal data out of the EU (a particular type of processing).

Verrill

4

Verrill

Key Definitions – Personal Data

- **Personal data** – any information relating to an identified or "identifiable natural person"
  - Generally interpreted to include **coded data**, also referred to as "pseudonymised data" under the GDPR
  - In the research context, personal data is **not** limited to data of research participants, but also includes data of investigators, study staff, and other individuals
- The GDPR does not apply to the processing of anonymous information, including for statistical or research purposes
  - **But no de-identification safe harbor like HIPAA!**

Verrill

5

Key Definitions – Special Categories of Data

- Data revealing/concerning:
  - **Health**
  - Racial or ethnic origin
  - Political opinions
  - Religious or philosophical beliefs
  - Trade union membership
  - **Genetic information**
  - Biometric information (when processed for the purpose of uniquely identifying a natural person)
  - A natural person's sex life or sexual orientation

Verrill

6

Verrill

Territorial Scope

- **For entities outside the EU** – the GDPR applies to the processing of **personal data of data subjects in the EU** by a controller or processor **not established in the EU**, where the activities relate to:
  - **Offering goods or services to** such data subjects in the EU (regardless of payment from the data subject)
  - **Monitoring of their behavior** as far as the behavior takes place in the EU
- **For entities in the EU** – the GDPR applies to the processing of personal data **in the context of the activities of an establishment of a controller or a processor in the EU**, regardless of whether the processing takes place in the EU

Verrill

7

Bases for Lawful Processing of Personal Data

- Different requirements for different types of processing:
  - Processing of regular personal data
  - Processing of special categories of personal data
  - Transfer of personal data out of the EU

Verrill

8

Verrill

Key Controller Obligations*

- Develop and maintain a written record of processing activities
- Identify applicable bases under the GDPR for all processing activities
- Draft/provide required disclosures to data subjects
- Implement technical and organizational measures (including policies)
- Execute GDPR Data Processing Agreements with vendors
- Facilitate the exercise of data subject rights
- Notify relevant EU supervisory authorities and/or data subjects of data breaches
- Determine whether to appoint an EU legal representative
- Determine whether to appoint a Data Protection Officer
- Determine whether to conduct any Data Protection Impact Assessments

* Not an exhaustive list.

Verrill

9

Key Processor Obligations*

- Refrain from processing personal data except on instructions from the controller or as required by EU law
- If authorized by the controller to use subcontractors, ensure that subcontracts flow down required data processing clauses
- Notify the controller of breaches without undue delay
- In similar circumstances as applicable to controllers:
  - EU legal representative
  - Data Protection Officer
  - Written record of processing activities
  - Technical and organizational measures (including policies)

* Not an exhaustive list.

Verrill

10

Verrill

Top 4 Difficult Situations for Institutions

1. Standard Contractual Clauses
2. EU Sponsor for a U.S.-Based Study
3. Data Protection Officer
4. No Consistency

Verrill

11