

EU GDPR: The General Data Protection Regulation

A Brief Overview

Duke Privacy

The General Data Protection Regulation

Became effective May 25, 2018.

**Formally codifies privacy as a
fundamental right and protects the flow
of personal data.**

GDPR Requirements:

- **Have a legal basis for processing the personal information of covered data subjects.**
- **Have a legal basis for transferring the personal information of covered data subjects to the U.S.**
- **Document and provide data subjects specific notice of processing and transfer activities and the legal bases to do so.**
- **Respond to data subjects' rights requests.**
- **Provide notice of breaches of personal data.**

The GDPR Applies to Entities

- Established in the European Economic Area (the 28 EU states plus, Iceland, Liechtenstein and Norway) who process personal data of EA/EEA data subjects.
- Outside of the EEA who process the personal data of EA/EEA data subjects in the course of offering goods or services (even when free) or where behavior of the data subjects is monitored.



Personal Data is Defined Broadly

- **“Personal data”:**

Any information relating to an identified or identifiable natural person. (GDPR Art. 4(1))

- **“Special categories of personal data”:**

Race, ethnicity, political opinions, religious or philosophical beliefs, trade union membership, health, sexual orientation or sex life. (GDPR Art. 9(1))

The GDPR Applies to Two Groups

- A “controller” is an entity that, alone or jointly with others, determines the purposes and means of processing data. (GDPR Art. 4(7))
e.g., acting as a collaborator as part of a research project.
- A “processor” is an entity that processes personal data on behalf of the controller. (GDPR Art. 4(8))
e.g., acting as a fee-for-service laboratory.

How the GDPR Applies to Universities in the U.S.

GDPR applies if:

The university has an establishment in the EEA and acts as a data controller or processor

The university offers goods or services to individuals in the EEA

The university monitors the behavior of individuals in the EEA

Application Examples

Establishment:

- Study Abroad programs

Offering of goods and services:

- Recruiting students and faculty in the EEA.
- University press or corporate education targeting customers in the EEA.

Monitoring behavior:

- Online education programs that include participants in the EEA and use cookies to track student participation.
- Tracking giving history of alumni and other donors in EEA member states.

Legal Bases to Process Personal Data

- The data subject has given consent to processing.
- The processing is necessary for the performance of a contract to which the data subject is a party.
- The processing is necessary for compliance with a legal obligation.
- The processing is necessary to protect vital interests of the data subject or a natural person.

Legal Bases to Process Personal Data

- The processing is necessary for a task carried out in the public interest.
- The processing is necessary for the 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.

Legal Bases to Process Special Categories

- The Data Subject has given explicit consent of the data subject to processing.
- The processing is necessary to protect the vital interests of the data subject or another natural person where the data subject is physically or legally incapable of giving consent.
- The processing is necessary for reasons of public interest in the area of public health.
- The processing is necessary for scientific or historical research purposes.

Legal Bases for Data Transfer

- **Explicit consent of the data subject to the transfer of personal data to the U.S.**
- **Model contractual clauses – impose certain requirements of EU data privacy law with respect to data transferred under contract.**
- **Data transfers necessary to protect the “vital interests” of the data subject - generally considered to be “life and death” situations.**
- **Codes of Conduct**
- **Binding Corporate Rules and Privacy Shield – *not applicable to Duke***

The GDPR provides the following rights for individuals:

- The right to be informed.
- The right of access.
- The right to rectification.
- The right to erasure.
- The right to restrict processing.
- The right to data portability.
- The right to object.
- Rights in relation to automated decision making and profiling.



Data Protection Officer

The GDPR requires that data controllers and processors with core activities that put them in scope designate a Data Protection Officer (DPO) to oversee the measures taken for GDPR compliance.

The Duke DPO is:

David J. Falcone

Director of Privacy, Ethics and Compliance

University Compliance Officer

Questions?

Contact Duke Privacy:

privacy@duke.edu