UCDAVIS LEGAL GUIDE

# European Union General Data Protection Regulation (GDPR) Overview

**What is the GDPR?**
The GDPR is a European Union law that is mainly intended to protect personal data privacy. It restricts the ways that collectors and processors of personal data can collect, process, and share that personal data.

**When does the GDPR apply to the University of California?**
The GDPR likely applies to UC in such areas as admissions (students applying from the European Economic Area, or EEA), Study Abroad programs, patients in the EEA (medical record transfers/second opinions), research subjects (telehealth studies), and similar circumstances. The GDPR generally applies where:

- An organization collecting data maintains an "establishment" (business incorporation, physical location, etc.) within the EEA
- Goods or services are offered to data subjects located in the EEA
- The behavior of a data subject in the EEA is monitored
- Personal data is transferred from inside the EEA to outside the EEA

**What does the GDPR require?**
The GDPR requires a variety of steps to ensure that the collecting, storing, and processing of personal data complies with the law. If you think the GDPR applies to the work you do at UC Davis, or to the information you process as an employee, then you should consult with the Campus Privacy Officer (privacy@ucdavis.edu). An abbreviated and incomplete list of some of the main requirements of GDPR is included here:

**Lawful basis for processing:** To process any personal data covered under the GDPR, there must be a lawful basis for the processing. Any of the following qualifies:

- For the performance of a contract with the data subject
- To comply with a legal obligation
- To protect the vital interests of the data subject or a natural person (i.e., to avoid risk to life or serious harm)
- To perform a task carried out in the public interest or exercise of official authority
- For legitimate interest, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

**Legitimate purpose and no further processing:** Personal data collected must be for a specified, explicit, legitimate purpose that is identified at the time of collection. There must be no further processing. (Some exceptions exist for archiving for public interest, scientific or historical research, or statistical purposes.)

**Limited data collection:** Personal data collection must be adequate, relevant, and limited to what is necessary.

**Limited, accurate, and secure storage:** Data stored must be stored accurately, and no longer than necessary. Storage and processing must be secure (in certain cases, this could require encryption or pseudonymization).

**Data subject rights:** Data subjects generally have rights to the following:

- Notice as relates to details related to the data collection and purposes

- Access to (and copies of) their data
- Rectification of their inaccurate data
- Data portability (ease of transfer) of their data
- Erasure of their data
- Objection to processing of their data when the legal basis of processing is based on public interests or the controller's legitimate interests.

**Security, data inventory, and impact assessments:** The GDPR also requires:

- An inventory and record of processing activities
- Complete "Data Impact Assessments"
- General security and data protection to be ensured by design
- Contract clauses that specifically relate to the GDPR.

**Further Resources:**

- EU GDPR official text: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679
- UC FAQ: https://ucnet.universityofcalifornia.edu/news/2018/05/notice-on-general-data-protection-regulation.html
- UC Davis GDPR simplified flier: https://privacy.ucdavis.edu/sites/g/files/dgvnsk1756/files/inline-files/GDPRSimplified.pdf
- UC Davis GDPR Privacy Office resources: https://privacy.ucdavis.edu/gdpr