General Data Protection Regulation (GDPR)

Molly M. Theodossy
Director of Compliance and Policy Programs

UCDAVIS
UNIVERSITY OF CALIFORNIA

What is GDPR?

- GDPR replaces existing EU privacy regulations, with the goal of establishing a single set of privacy laws across the European Economic Area (EEA).
- GDPR becomes effective on May 25, 2018.
- The regulation enhances individuals' fundamental rights to privacy and applies to data processed in the offering of goods or services to individuals located in the EEA, and the monitoring of behavior of individuals in the EEA.
- "This Regulation applies to the **processing** of **personal data** wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a system." *(Article 2)*

What is Personal Data?

"'Personal data' means any information relating to an identified or identifiable natural person ('data subject')" *(Article 4)*

Specifically includes:

- Name
- Identification number
- Location data
- Online identifier
- One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

What is Processing?

"'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means" *(Article 4)*

Specifically includes:

- Collection
- Recording
- Organization
- Structuring
- Storage
- Adaptation or alteration
- Retrieval
- Consultation
- Use
- Disclosure by transmission, dissemination or otherwise making available
- Alignment or combination
- Restriction
- Erasure
- Destruction

Examples of Processing

Per the European Commission:

- Staff management and payroll administration
- Access to/consultation of a contacts database containing personal data
- Sending promotional emails
- Shredding documents containing personal data
- Posting/putting a photo of a person on a website
- Storing IP addresses or MAC addresses
- Video recording (CCTV)

Principles Relating to Processing

- Lawfulness, fairness, and transparency
  - Clear, concise communication
- Purpose limitation
  - Use limited to purpose communicated
- Data minimization
  - Minimum data required for purpose
- Accuracy
  - Correct and complete
- Storage limitation
  - Keep only as long as needed
- Integrity and confidentiality
  - Security
- Accountability
  - Demonstrate compliance

Rights of Data Subjects

- Transparency
  - What data will be collected?
  - How will it be processed?
  - What is the basis for lawful processing?
  - How can data be corrected/accessed/erased?
  - All rights written in plain language.
- Information and access
  - How data is being processed and access to all data and information.
- Rectification and erasure
  - Request correction or supplement incomplete data.
  - “Right to be forgotten.”
- Objection and automated processing
  - Objection to direct marketing, or can be based on personal circumstances.
  - Can request human review of data when there is a legal effect on data subject.

Conditions for Processing

Processing shall be lawful only if and to the extent that at least one of the following applies:

- Consent from data subject
  - Freely given, specific, informed, unambiguous
  - Provided through clear affirmative action (e.g., opt-in checkbox)
  - Can be withdrawn—processing must stop
  - Data subject must be at least 16 years old
- Contract to which data subject is party
- Legal obligation under Union or Member State law
- Protection of the vital interests of individual(s)
  - For example, humanitarian purposes, emergencies, disasters
- Public interest/authority vested in controller by Union or Member State law
- Legitimate interest of controller
  - Generally when there is no impact on data subject
  - Requires balancing test to compare legitimate interest of controller to rights/interests of data subject

Special Categories of Personal Data

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data
- Health data
- Sex life or sexual orientation

Challenges to Compliance

- GDPR is a complex law and many aspects of its application and enforcement have not yet been determined.
- Some decisions are still pending at UCOP regarding implementation across the system.
  - Data Protection Officer or EEA representative appointment
  - Breach reporting procedures, including reporting to EEA supervisory authorities
  - Update Appendix DS
  - General guidance

Next Steps

- Inventory of Activities
  - What presence do we have in Europe?
  - What goods or services does UC offer to data subjects in the EEA?
  - In what instances is UC monitoring behavior of individuals located in the EEA?
  - In what instances do we rely on vendors or third parties to provide goods or services to data subjects in the EEA/monitor behavior of individuals in the EEA?
  - When do we receive personal data from the EEA?
  - When do we transfer data to the EEA?
  - What data do we have?
  - Self-assessment survey available at https://privacy.ucdavis.edu/form/gdpr-data-inventory.
- Determine basis for lawful processing when subject to GDPR.
- Develop processes for maintaining records of processing activities and consents for processing.

Next Steps

- Review privacy policies and revise as necessary to reflect rights of data subjects.
- Implement appropriate technical and organizational security measures.
- Document steps taken for GDPR compliance.
- Consider need for Data Protection Impact Assessment (DPIA) for data categories likely to result in high risk to rights and freedoms of data subjects.
- Monitor EEA regulatory bodies and Working Party for further guidance.

Thank you!

Questions?
https://privacy.ucdavis.edu/gdpr
privacy@ucdavis.edu

UCDAVIS