Berkeley
UNIVERSITY OF CALIFORNIA

General Data Protection Regulation (GDPR) Simplified

What is the GDPR?

GDPR is a data privacy regulation. It applies to the **processing** of **personal data** related to:

- Organizations operating within the EU, even if the data processing takes place outside of the EU.
- The offering of goods and services to individuals in the EU.
- The monitoring of behavior of individuals in the EU.

The regulation takes effect on May 25, 2018, and replaces existing EU data protection directives. It is similar to existing regulations, but strengthens the rights of individuals and significantly increases fines for non-compliance.

The information contained in this document is intended to provide general information about the GDPR, but is not a comprehensive overview of this complex regulation. For additional guidance regarding specific situations or sets of data, contact the Privacy Office: privacyoffice@berkeley.edu Links to additional information and guidance are available at https://GDPR.berkeley.edu

Processing

Processing includes any action or operation an organization might take related to personal data, including but not limited to:

- Collection
- Recording
- Organization
- Storage
- Alteration
- Retrieval
- Use
- Disclosure
- Dissemination
- Erasure
- Destruction

Personal Data

Personal data is any information related to an identified, or identifiable natural person, including:

- Name
- Identification number
- Location data
- Online identifier (e.g., IP address)

- Information related to an individual's physical, psychological, genetic, mental, economic, cultural, or social identity.

Principles

At its core, the GDPR is designed to strengthen the rights of individuals to know what data is being collected about them, how that data is being used, and to have control over the use of their data; including the right to prevent organizations from processing their personal data in certain situations. The GDPR establishes the following principles:

- **Lawfulness, fairness, and transparency**
    - Requires clear and concise communication between organizations and data subjects.
- **Purpose limitation**
    - Requires organizations to use personal data only for the purposes they tell data subjects they will use it.
- **Data minimization**
    - Requires organizations to collect only the minimum personal data required to conduct business.
- **Accuracy**
    - Requires organizations to correct or supplement personal data that is inaccurate or incomplete.
- **Storage limitation**
    - Requires organizations to keep data only for as long as they need it.
- **Integrity and confidentiality**
    - Requires organizations to store data safely and securely.
- **Accountability**
    - Requires organizations to design their data management procedures in a way that enforces these principles and to be able to demonstrate compliance with the regulation.

Rights of Data Subjects

The rights of data subjects are grounded in the principles established in the regulation.

- **Transparency**
    - Data subjects have the right to understand what data will be collected, how it will be used, the lawful basis for processing, how they can access their own data, how they can correct incorrect data, how they can restrict processing of their data, how they can request

erasure of their data, and how they can object to general processing and automated processing of their data.
    - Explanation of rights must be written in clear, plain language.
- **Information and access**
    - When the data comes from the data subject, the organization must provide data subjects with information about their rights at the time they collect the data.
    - When the data is provided by another source, the information about their rights must be provided at the time the organization first contacts the data subject or first discloses the data. The information should also include the categories of personal data being processed.
    - Data subjects have the right to request access to their data. It must be provided in a common format that allows the data subject to transfer the data to another organization if desired.
    - Data subjects have the right to specific information about how and why their personal data has been processed, who has received their personal data, and how long their data will be stored.
- **Rectification and erasure**
    - Data subjects have the right for incorrect data to be corrected, and incomplete data to be supplemented, without undue delay.
    - Under certain circumstances, data subjects have the right to request their data be erased (right to be forgotten) if they no longer want their data to be processed by the controller.
    - Data subjects have the right to limit the processing of their data when they do not want their data erased but they still want the organization to continue storing the data.
- **Right to object and automated data processing**
    - Data subjects have the right to object to the processing of their data based on their particular situations.
    - Data subjects have the right to object to their personal information being processed for direct marketing purposes.
    - Data subjects have the right to object to the automated processing, including profiling, of their data if it has a legal effect on them.

Lawfulness of Processing

All processing of data must be based in one of the following conditions to be considered lawful:

- **The data subject consents to processing**

    - For consent to be valid, it must be freely given, specific, informed, unambiguous, and provided through a clear affirmative action (the data subject opts in).
    - The organization must provide a clear description of the specific purpose for processing the data, written in plain language, separate from other terms and conditions.
    - The organization must be able to demonstrate that the data subject provided consent for the processing of personal data.
    - The organization must provide a way for the data subject to withdraw consent when desired, and discontinue processing when consent is withdrawn.
    - A child must be at least 16 years old to provide consent, otherwise, consent must be provided by the parent or guardian.
- **The data subject is a party to a contract that provides for processing**
- **The controller has a legal obligation**
    - Should have a basis in Union or Member State law.
- **Processing is required to protect a vital interest,** such as for humanitarian purposes, emergencies, or disasters
- **Public interest vested in controller**
    - Should have a basis in Union or Member State law.
- **The controller has a legitimate interest in the processing**
    - For example, preventing fraud, information security, or internal administrative purposes.
    - May be used when there is no impact on data subjects.
    - The rights of the data subject to protect their own personal data may override this condition of processing.
    - Requires a balancing test to compare the legitimate interest of the organization to the rights or interests of the data subject.

How to Comply

- Complete an inventory to determine if you process data subject to the GDPR.
- Determine the lawful basis for processing the data.
- If relying on consent, determine if your systems for gaining consent are compliant with the regulation, and that you have provided a clear means for withdrawal of consent.
- Review your privacy policies and update to provide complete information as required by the regulation.
- Keep complete, accurate records of your data processing.
- Consider data protection and compliance during the development or update of any systems

you use to process data subject to the regulation.

- Document your efforts to comply with the GDPR to demonstrate a good faith effort for compliance.
- Consult with the Privacy Office privacyoffice@berkeley.edu regarding your compliance efforts.