University of CINCINNATI

EU's General Data Protection Regulation (GDPR)

The **General Data Protection Regulation (GDPR)** is the European Union's (EU) privacy regulation. GDPR was designed to harmonize data privacy laws across the EU, and requires organizations to protect personal data they acquire from individuals located in the EU. GDPR provides individuals with greater control over how their personal data is collected and used.

Whom does GDPR protect?

GDPR protects personal data of individuals, referred to as "data subjects," located in the EU. GDPR protects the personal data of anyone located in the EU when their data is collected or "processed," regardless of their nationality, citizenship, or permanent place of residence.

What data is covered by GDPR?

GDPR applies to information that directly or indirectly identifies or could identify an individual. This includes, but is not limited to, name, address, phone number, date of birth, email address, identification number (e.g., driver's license number, Social Security number or M number), IP addresses, cookie identifiers, device information, advertising identifiers, financial information, geo-location information, social media information, consumer preferences, race, ethnicity, sexual orientation, and political affiliation.

To whom does GDPR apply?

GDPR applies to any organization—located within or outside of the EU—that collects and processes the personal data of individuals, such as offering goods and services or collecting online data. Organizations who collect and maintain personal data are "data controllers," and organizations who process the data are "processors."

What is meant by "Processing" Data?

"Processing" is virtually any use of an individual's personal data. Processing is any operation performed with personal data or with sets of personal data, whether or not by automated means. This includes

collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, transmission, dissemination or otherwise making available, as well as erasure or destruction.

Remember, GDPR applies even when the processing of data takes place outside of the EU.

What rights are provided by GDPR?

GDPR provides individuals in the EU with significant rights over how their personal data is used, including how it is collected, processed, and transferred by data controllers and processors.

Under GDPR, EU data subjects have the right to:

- Access any personal data that an organization has collected about the individual;
- Know the reason an organization is processing the individual's personal data and the categories of personal data that an organization processes;
- Correct any errors in personal data collected or processed by an organization;
- Know how long an organization will store the individual's personal data;
- Under certain circumstances, require the organization to permanently delete the individual's personal data (this right is sometimes referred to as the right to be forgotten or the right to erasure);

From an organizational perspective, GDPR requires significant data protection safeguards and imposes a number of obligations. For example, the organizations must:

- Have a legal basis for collecting and processing the personal data of EU data subjects; document the legal basis; collect and use data only when a legal basis exists, and only to the extent of that legal basis;
- Minimize the collection and processing of personal data whenever possible;
- Protect any personal data that it collects and uses;

- Conduct an assessment to determine any risks and privacy impacts related to collecting and processing the personal data of data subjects, implement a plan to mitigate those risks and impacts, and continuously monitor both the risks and the mitigation plan for change;
- Maintain a breach notification policy, and notify authorities of any breach.
- When consent is the basis for processing personal data, the use of the data must be limited to the scope of the consent. To complete a consent form click here: GDPR Consent Form

When consent is the basis for processing personal data, the use of the data must be limited to the scope of the consent.

Does GDPR impact UC?

GDPR applies to UC in certain situations. Since GDPR protects the data of individuals located in the EU, regardless of their citizenship or permanent place of residence, UC's collection of personal data from individual in the EU may be subject to GDPR. This may include members of the UC community who are vising the EU or residing (permanently or temporarily) in the EU, and EU residents who attend or work for UC.

Examples of GDPR's potential application to UC:

Student applicant:

A prospective student who lives in the European Union and applies to U.C. The data they provide may be subject to GDPR.

Faculty:

A faculty member travels to the European Union to complete work for UC. If, for example, the faculty member is hospitalized while in the EU, the transfer of information about this event (i.e. accident reports, time off from work statement) from the EU to UC may be subject to GDPR.

Study abroad:

Data generated about a UC student while they are physically located in the EU may be subject to GDPR. Students sign a consent for release of specific categories of data prior to travel.

Questions:

Lorren Ratley, U.C. Director of Privacy
Lorren.Ratley@uc.edu
(513) 558-2733

Resources:

Protection of Personal Data in the EU
General Data Protection Regulation
European Commission-Data Protection
GDPR (Searchable Feature)
GDPR Guide