Published on *University of Colorado* (https://www.cu.edu)

EU General Data Protection Regulation (GDPR) Compliance [1]

The General Data Protection Regulation “GDPR” is a European Union “EU” regulation, that the European Parliament passed in April 2016 to govern the processing and movement of EU resident’s personal data.

International laws, like the EU GDPR, may become requirements for CU departments through contracts and agreements with third-parties or partners in other countries. For example, a research partner in the EU might require that all work be compliant with the EU GDPR. If you have an agreement that requires compliance with the EU GDPR, contact your campus information security, privacy or compliance team for guidance.

The EU GDPR went into effect on May 25, 2018 and replaced the 1995 Data Privacy Directive. The new regulation has a broader territorial scope and more significant fines (up to $20 million) for violations than prior EU law. The GDPR applies to entities located outside of the EU that handle personal data about EU residents when offering them services or monitoring their behavior.

The EU GDPR sets a broad definition for personal information and establishes a variety of requirements regarding the handling of EU residents' personal information. Note that the law specifically applies to EU residents rather than citizens. It does not apply to EU citizens while they reside in the United States. However, it does apply to United States Citizens when they provide data to the University while temporarily located in the EU.

At a high level, GDPR addresses the following requirements:

- Data processing must be lawful, meaning that one of the following apply:
  - Consent for processing was obtained from the individual(s)
  - A legitimate interest exists – details are further defined in the law
  - A contractual relationship exists – data processing is done to meet the obligations of a contract
- Data collected must be adequate, relevant and proportionate
- Data must be retained only as long as necessary and must be secure
- Data transfer restrictions exist outside of the EU
- Notice must be provided to individuals about how data will be processed and used

In addition, data subjects have a number of rights, including the:

- Right to be informed
- Right to access their data
- Right to correct data
- Right to request deletion of data

Questions

Contact the Office of Information Security at privacy@cu.edu [2] if you have questions or concerns about the GDPR, how it may apply to your department or inquiries related to personal data that may be collected and processed by the University of Colorado.

Resources

- GDPR full text [3]
- EDUCAUSE - The General Data Protection Regulation Explained [4]
- International Association of Privacy Professionals (IAPP) [5]
- College and University Professional Association for Human Resources (CUPA-HR) [6]

Updated August 27, 2024

Groups audience:
Office of Information Security

Source URL:https://www.cu.edu/security/eu-general-data-protection-regulation-gdpr-compliance

Links
[1] https://www.cu.edu/security/eu-general-data-protection-regulation-gdpr-compliance
[2] mailto:privacy@cu.edu [3] https://gdpr-info.eu/ [4] https://er.educause.edu/articles/2017/8/the-general-data-protection-regulation-explained
[5] https://iapp.org/media/pdf/resource_center/GDPR_AWARENESS_GUIDE._092717.pdf
[6] https://www.cupahr.org/data-privacy-gdpr/