GDPR 101: An Overview of the EU's General Data Protection Regulation

Brad Judy and Sarah Braun – Office of Information Security, System Administration

GDPR Overview

General Data Protection Regulation is privacy legislation in the European Union that was passed in 2016 and took effect in May, 2018. It outlines a definition for personally identifiable information, establishes individual privacy rights, enumerates valid business reasons for PII handling, and sets a number of expectations for organizations handling PII.

PII

- Data from which a living individual is identifiable (by anyone) directly or indirectly (name, ID number, location, physical, physiological, genetic, mental, economic, cultural or social identity, etc.)
- Special category for highly sensitive information (race/ethnicity, religion/philosophy, genetic/biometric, health, sexual orientation, political views, trade union membership, etc.)

Individual rights

- Withdraw consent for PII processing
- Request copy of all of their data
- Request the ability to move their data to a different organization
- Request to delete information that is no longer relevant
- Request corrections to inaccurate information

Scope

- Applies to EU residents
    - Does not apply to EU citizens while they reside in the US
    - Does apply to US citizens when they provide PII while located within the EU

Impact to CU

Direct impacts – CU maybe directly bound to GDPR compliance through research grants and contracts or administrative contracts with service providers.

Indirect impacts – GDPR sets new standards for privacy rights around the world and our community members will have higher expectations about their privacy rights. It is quickly redefining privacy best practices

Broader Influence

Raises the bar for privacy standards and laws. GDPR is viewed as the current standard for modern privacy laws. Most notably, the focus is shifted to the individual's privacy rights rather than just an organization's responsibilities. It directly extends reach outside the EU borders by leveraging a business's EU presence to apply fines. It indirect has a broad reach by influencing both national and local/regional privacy laws around the world.

California Consumer Privacy Act – California passed a new privacy law in 2018 that takes effect in 2020. It borrow from GDPR in the individual privacy rights focus

Colorado Consumer Privacy Law – Colorado law was updated in 2018 but is still an older style bill focused more on data breach response obligations and not on personal privacy rights.

Other countries – Many other countries have privacy laws with a variety of scopes. As new ones emerge, we can see the influence of GDPR. Brazil passed a new privacy law this year that is influenced by GDPR and becomes effective in 2020.

Privacy basics checklist

- ☐ **Do you need to collect personal information?** – Ensure there is a true business need for the information.
- ☐ **Are you only requesting the minimum information required?** – Resist the temptation to collect additional information that you "might" need in the future.
- ☐ **Are you informing the individual why you need it and what it will be used for**? If the information will be handled by a third-party, is that clearly disclosed?
- ☐ **Have third-parties involved in handling personal information been properly vetted and is appropriate contract language in place?** Information security office can assist.
- ☐ **Is personal information properly secured?** Follow CU security standards and consult with the information security office. Most notably, **limit access to personal information to only those who need to know**.
- ☐ **Do you have a data retention plan that includes a schedule to delete personal information when it is no longer needed?** Have a plan for deleting old information and have processes that ensure information is cleaned up according to that plan
- ☐ **Are you aware of any regulatory or contractual requirements regarding privacy or security?** Be sure you know your obligations and come up with processes to meet them. This may mean meeting specific security standards, minimum/maximum data retention requirements or other required steps.
- ☐ **Know how you will handle privacy related questions and requests.** Privacy@cu.edu can assist or connect you with others at CU to help with privacy concerns.