

SUNY's Guidance on the European Union General Data Protection Regulations (GDPR)

(Selected items)

1. Overview of the GDPR:

The General Data Protection Regulations ("GDPR") were adopted by the European Commission in order to strengthen and unify data protection for all individuals within the European Union ("EU").

GDPR became effective on May 25, 2018 and applies in European Economic Areas ("EEA") which includes the EU members + Iceland, Liechtenstein and Norway. For purposes of this Guide, references to EU will include EEA.

2. The GDPR:

- Extends jurisdiction with extra-territorial applicability;
- Provides for penalties for non-compliance;
- Establishes stronger conditions for seeking informed, explicit consent;
- Provides additional rights for data subjects, including mandatory data breach notification and data erasure ("right to be forgotten"); and
- Generally requires that information of data subjects be stored in a secured fashion.

3. When Is GDPR Triggered?

There are generally three Buckets of Data:

- A. Information Transmitted from EU to US institution - e.g., application for admission
- B. Information Gathered from EU resident while at institution (student or employee)
- C. Information Transmitted from EU to US Institution after termination of association with US institution - e.g., Alumni data

Generally, Buckets A and C are covered by GDPR but Bucket B is not, unless data ultimately bleeds over into Bucket C.

GDPR also applies if an entity is monitoring behavior within the EU, which is why we have developed an acknowledgement/consent form for our students to sign before going to the EU. (See Sec. VI below).

4. Information Covered under GDPR:

There are two types of information that are covered under GDPR:

- A. Personally identifiable information which mirrors that covered under FERPA
- B. Sensitive Information - race, ethnicity, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

For general personal data, campuses just need a legitimate business purpose to collect it.

For sensitive information (described above), campuses need consent from the data subject to collect it.

For the right to be forgotten, if there is a legitimate business purpose to maintain the data, campuses do not have to honor such requests.

For "sensitive information", we must honor withdrawal of consent unless there is another EU/GDPR lawful purpose to otherwise utilize the data.

Campuses should develop internal procedures on how to respond to requests to be forgotten and general inquiries under GDPR.

8. Research:

The GDPR may be applicable to a range of research activities:

1. University conducts research in the US in which participant data is transmitted to sponsors, servers, or data core facilities in the EU;
2. Research studies that collect data online from EU residents may be subject to GDPR;

GDPR considers key-coded data to be "personal data" and refers to key-coded data as "pseudonymized data." This contradicts the position under many US research and privacy laws, such as the Common Rule and HIPAA; pseudonymized data are considered identifiable personal data and therefore remain subject to GDPR protections; even if the person who holds the data does not have access to the key needed to link the data to the data subject's identity.

GDPR does not apply in the following instances:

1. No collection of personal data from individuals in the EU; For example, studies that do not collect information that is linked to a subject's identity, such as anonymous survey based studies in which the identities of participants cannot be tracked to the individual;
2. Data that has been anonymized -no key created to re-identify individuals from the data.

See here for additional guidance for researchers which SUNY intends to adopt for its campuses: <https://www.ucl.ac.uk/legal-services/ucl-general-data-protection-regulation-gdpr/guidance-notices-ucl-staff/guidance-researchers>