Title/Subject: **EUROPEAN UNION GENERAL DATA PROTECTION REGULATION**

Applies to: ☒ faculty ☒ staff ☒ students ☒ student employees ☐ visitors ☐ contractors

Effective Date of This Revision: March 1, 2019

Contact for More Information: Roger Rehm, VP of Information Technology

☒ Board Policy ☒ Administrative Policy ☒ Procedure ☐ Guideline

---

This policy is to ensure compliance with the European Union (EU) regulations relating to the collection, storage, disclosure and use of personal data, as well as the rights of persons with regard to their data.

1. PURPOSE OF POLICY

The purpose of the policy is to ensure compliance with the EU General Data Protection Regulation (GDPR). This regulation requires that institutions that collect personal data from natural persons who are in EU member states meet certain standards, including disclosure of what information is being collected, why the information is being collected, how the information will be stored, what the information will be used/processed for and who will have access to it. The regulation also gives robust rights to the person regarding their data.

2. STAKEHOLDERS MOST IMPACTED BY THE POLICY

Any University office or unit that collects, stores or uses the data of students, faculty, staff or any other person while they are in an EU member state will be impacted by this Policy. These include, but are not limited to:

- Academic Affairs
- Enrollment and Student Services
- Office of Information Technology

3. KEY DEFINITIONS

Key definitions are found in Chapter 1 Article 4 of the GDPR Regulation. Those definitions include:

3.1 Personal data

Any information relating to an identified or identifiable natural person (‘data subject’). An identifiable natural person is one who can be identified—directly or indirectly—in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

3.2. Processing

Authority: Robert O. Davies, President
History: New Policy
Indexed as: GDPR; personal data protection; personal data privacy; data privacy

Any operation or set of operations which is performed on personal data or on sets of personal data—whether or not by automated means—such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

3.3. Consent
Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

3.4. Personal data breach
A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data transmitted, stored or otherwise processed.

3.5. Data subject
A natural person (not a corporate or other organizational entity).

3.6. European Union (EU)
Those countries that have ratified membership in the Union.

3.7. Supervisory authority
An independent public authority which is established by an EU state pursuant to the GDPR.

3.8. Legal basis
Necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

4. POLICY

4.1 Collection of personal data

4.1.1. All University activities that collect personal data from natural persons in the EU related to admission or employment shall communicate to the person the reason and purpose for collecting the information by using University-approved forms and directing such persons to the University's GDPR Compliance website. This provision shall apply to any person (student, faculty or staff) who is physically present in the EU and from whom the University is collecting personal data, regardless of the reason for the person's presence in the EU.

4.1.2. All University activities that collect personal data from natural persons in the EU **not** related to admission or employment—or otherwise collected on a lawful basis—shall obtain written consent from the person with regard to the collection of the information using University-approved forms available from the Office of the General Counsel.

4.1.3. Any personal data collected from a natural person in the EU shall be stored, secured and accessed consistent with the Office of Information Technology's data security policies.

4.2. Personal data breaches

Any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data transmitted, stored or otherwise processed shall be reported to the Supervisory Authority of the EU member state within 72 hours of notice of the breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

4.3. Data subject rights and retention of academic data

4.3.1. The individual rights of persons in the EU with regard to their personal data includes the rights of access, ratification, removal, restriction, portability, to object and to not be subject to automated individual decision making, and those rights shall be respected consistent with the procedures implementing this policy.

4.3.2. With regard to academic data—including course work attempted and/or completed, as well as grades associated with those courses—the University must preserve that data for legal and accrediting requirements. With respect to other data, the individual's right to erasure and to be forgotten will be respected consistent with the regulation and United States law.

4.4. Implementation

4.4.1. All University operations that collect data should perform an analysis to determine whether and to what extent the office collects personal data that could originate from natural persons in EU member states. Units that collect such information must document the processing and storage of the data.

4.4.2. All University contracts within those offices should be reviewed for compliance with this policy and, if non-compliant, a strategy to achieve compliance must be implemented.

4.4.3. All personnel who deal with GDPR-covered data must go through appropriate training.

4.5. Communication

All academic and administrative offices will be made aware of this policy through appropriate University mechanisms.

4.6. Exceptions

No exceptions exist for this policy.

5. ACCOUNTABILITY

Failure to adhere to this policy could result in discipline under the applicable rules, policy or contract, up to and including termination of employment.

6. FAQS

6.1. When does this policy apply?
Whenever personal data is being collected from a person who is physically present in an EU member state.

6.2. How does this policy differ from other data security policies, such as HIPAA, FERPA or GLBA?
The GDPR provides rights to individuals different from data protection laws in the United States and, in most circumstances, provides individuals with greater rights and controls over their own data.

6.3. Who should I contact with questions?
Contact the Office of Information Technology or the Office of the General Counsel with questions.

6.4. Does this policy apply to EU students and faculty when they're located in the US?
No. This policy only applies to natural persons physically in an EU member state.

6.5. Does this policy apply to US students, faculty and staff when they are in the EU?
Yes. Any natural person in the EU has the rights afforded by the GDPR while in an EU member state.

- Information regarding the GDPR
- Full text of the GDPR

Central Michigan University reserves the right to make exceptions to, modify or eliminate this policy and or its content. This document supersedes all previous policies, procedures or guidelines relative to this subject.