COLUMBUS STATE UNIVERSITY

Policy Name:	EU General Data Protection Regulation Compliance Policy[1]
Policy Owner:	Office of General Counsel
Responsible University Office:	Office of General Counsel; University Information & Technology Services
Approval Date:	January 10, 2020
Effective Date:	January 10, 2020
Revisions:	None
Policy Number:	TBD
Related Policies:	USG-BOR Records Retention Schedules

I. PURPOSE AND SCOPE OF POLICY

In order for Columbus State University (CSU) to educate its foreign and domestic students both in class and on-line, engage in world-class research, and provide community services, it is essential and necessary that CSUC has a lawful basis, to collect, process, use, and/or maintain the personal data of its students, employees, applicants, research subjects, and others involved in its educational, research, and community programs. These activities include, without limitation, admission, registration, delivery of classroom, on-line, and study abroad education, grades, communications, employment, applied research, development, program analysis for improvements, and records retention.

CSU takes seriously its duty to protect the personal data it collects or processes. In addition to CSU's overall data protection program, the European Union General Data Protection Regulation (EU GDPR) imposes obligations on entities, like CSU, that collect or process personal data about people in the European Union (EU). The EU GDPR applies to personal data CSU collects or processes about anyone located in the EU, regardless of whether they are a citizen or permanent resident of an EU country. Among other things, the EU GDPR requires CSU to:

1. be transparent about the personal data it collects or processes and the uses it makes of any personal data;
2. keep track of all uses and disclosures it makes of personal data; and
3. appropriately secure personal data
4. and give users the right to require CSU to remove their personal data from all CSU systems

[1] This Policy has been implemented pursuant to the University's Policy on Policies, Section VIII, Interim or Emergency Policies.

This policy describes CSU's data protection strategy to comply with the EU GDPR. This policy applies to the personal data and sensitive personal data protected by the EU GDPR and all CSU Units who collect or process personal data and sensitive personal data protected by the EU GDPR.

II. DEFINITIONS

Collect or Process Data: Collection, storage, recording, organizing, structuring, adaptation or alteration, consultation, use, retrieval, disclosure by transmission/dissemination or otherwise making data available, alignment or combination, restriction, erasure or destruction of personal data, whether or not by automated means.

Consent of the data subject means 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.

Consent: Under the EU GDPR:

1. Consent must be a demonstrable, clear affirmative action.
2. Consent can be withdrawn by the data subject at any time and must be as easy to withdraw consent as it is to give consent.
3. Consent cannot be silence, a pre-ticked box or inaction.
4. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.
5. Request for consent must be presented clearly and in plain language.
6. Maintain a record regarding how and when consent was given.

Controller: The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Identified or Identifiable Person: An identified or identifiable 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, psychological, genetic, mental, economic, cultural or social identity of that person.
Examples of identifiers include but are not limited to: name, photo, email address, identification number such as ID#, Account (User ID), physical address or other location data, IP address or other online identifier.

Lawful Basis: Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:

1. The data subject has given consent to the processing of his or her personal data for one or more specific purposes;

2. Processing is 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;
3. Processing is necessary for compliance with a legal obligation to which the controller is subject;
4. Processing is necessary in order to protect the vital interests of the data subject or of another natural person;
5. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
6. Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party.

Legitimate Interest: Processing of personal data is lawful if such processing is necessary for the legitimate business purposes of the data controller/processor, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.

Personal Data: Any information relating to an identified or identifiable person (the data subject).

Processor: Special categories of personal data that require consent by the data subject before collection or processing are:

Sensitive Personal Data: Data falls under the following categories:

1. Racial or ethnic origin
2. Political opinions
3. Religious or philosophical beliefs
4. Trade union membership
5. Genetic, biometric data for the purposes of uniquely identifying a natural person
6. Health data
7. Data concerning a person's sex life or sexual orientation

III. POLICY

A. Lawful Basis for Collecting or Processing Personal Data: CSU has a lawful basis to collect and process personal data. Most of CSU's collection and processing of personal data will fall under the following categories:

1. Processing is necessary for the purposes of the legitimate interests pursued by CSU or by a third party.
2. Processing is 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.
3. Processing is necessary for compliance with a legal obligation to which CSU is subject.

4. The data subject has given consent to the processing of his or her personal data for one or more specific purposes.

There will be some instances where the collection and processing of personal data will be pursuant to other lawful bases.

B. Data Protection & Governance: CSU will protect all personal data and sensitive personal data that it collects or processes for a lawful basis. Any personal data and sensitive personal data collected or processed by CSU shall be:

1. Processed lawfully, fairly, and in a transparent manner
2. Collected for specified, explicit, and legitimate purposes, and not further processed in a manner that is incompatible with those purposes
3. Limited to what is necessary in relation to the purposes for which they are collected and processed
4. Accurate and kept up to date
5. Retained only as long as necessary
6. Secure

C. Sensitive Personal Data & Consent: CSU must obtain consent before it collects or processes sensitive personal data.

D. Individual Rights: Individual data subjects covered by this policy will be afforded the following rights:

1. information about the controller collecting the data
2. the data protection officer contact information (if assigned)
3. the purposes and lawful basis of the data collection/processing
4. recipients of the personal data
5. if CSU intends to transfer personal data to another country or international organization
6. the period the personal data will be stored
7. the existence of the right to access, rectify incorrect data or erase personal data, restrict or object to processing, and the right to data portability
8. the existence of the right to withdraw consent at any time
9. the right to lodge a complaint with a supervisory authority (established in the EU)
10. why the personal data are required, and possible consequences of the failure to provide the data
11. the existence of automated decision-making, including profiling
12. if the collected data are going to be further processed for a purpose other than that for which it was collected.

PROCEDURES

A. Data Governance: All CSU Units who collect or process personal data protected by the EU GDPR must document the lawful basis for the collection or processing of personal data and sensitive personal data they collect or process, why they collect it, and how long they keep it.

All data at CSU shall be kept in compliance with the USG-BOR Records Retention Schedules.

B. Privacy Notice: CSU's Privacy Notice to data subjects must specify the lawful basis for CSU to collect or process personal data and include:

1. whether their personal data are being collected or processed and for what purpose
2. categories of personal data concerned
3. to whom personal data is disclosed
4. storage period (records retention period)
5. existence of individual rights to rectify incorrect data, erase, restrict or object to processing
6. how to lodge a complaint
7. the source of the personal data (if not collected from the data subject)
8. the existence of automated decision-making, including profiling

C. CSU's Privacy Notice: A link to the CSU Privacy Notice is available on the footer of all CSU websites—"Privacy Policy": https://webs.columbusstate.edu/web_privacy_policy.php

D. Individual Rights: Any individual wishing to exercise their rights under this policy should contact University Information and Technology Services: https://webs.columbusstate.edu/web_privacy_policy.php

E. Data Protection:

1. Security of Personal Data - All personal data and sensitive personal data collected or processed by any CSU Units under the scope of this policy must comply with the security controls and systems and process requirements and standards of NIST Special Publication 800-171.

2. Breach Notification - Any CSU Unit that suspects that a breach or disclosure of personal data has occurred must immediately notify CSU's Chief Information Security Officer in the Department of Information and Technology Services.

IV. RELATED BOARD OF REGENTS' POLICIES

USG-BOR Records Retention Schedules

V. LINKS

Columbus State University EU GDPR Model Consent Form
EU General Data Protection Regulation (EU GDPR)
Columbus State University Privacy Notice
Columbus State University Data Protection Safeguards
Columbus State University Controlled Unclassified Information Policy
NIST Special Publication 800-171