

MAINE COMMUNITY COLLEGE SYSTEM

INFORMATION TECHNOLOGY

Section 908

SUBJECT: EUROPEAN UNION GENERAL DATA PROTECTION REGULATION COMPLIANCE

PURPOSE: To provide guidance and create uniform standards and procedures for the collection and storage of personal data protected by the EU General Data Protection Regulation

A. Introduction

The European Union (“EU”) General Data Protection Regulation (“GDPR”) unify data privacy laws across the EU and protect the data privacy of individuals physically present in the EU. The purpose of this policy is to provide guidance and uniform standards and procedures for compliance with the requirements of the GDPR.

B. Application

This policy applies to MCCC’s collection and storage of personal information of individuals physically present in the EU, including MCCC students and employees, without regard to place of permanent residence.

C. Definitions

For purposes of this policy, the following terms have the following meanings:

1. “Collect or process data” means the 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.
2. “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. In addition:
 - a. Consent can be withdrawn by the data subject at any time with the same ease as to give consent;
 - b. Consent cannot be given through silence, a pre-checked box or inaction;

- c. 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;
 - d. Request for consent must be clear and in plain language; and
 - e. A record must be maintained memorializing how and when consent was given.
3. “Controller” means 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.
 4. “Identified or identifiable person” means a person who can be identified, directly or indirectly, in particular by reference to an identifier, including but not limited to name, photo, email address, physical address or other location data, identification number, user ID, IP address, or other online identifier; or one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of that person.
 5. “Personal data” means any information relating to an identified or identifiable person (the data subject).
 6. “Processor” means a natural or legal person, public authority, agency or other body who processes personal data on behalf of the controller.
 7. “Sensitive personal data” means the following special categories of personal data that require consent by the data subject before collecting or processing:
 - a. Racial or ethnic origin;
 - b. Political opinions;
 - c. Religious or philosophical beliefs;
 - d. Trade union membership;
 - e. Genetic, biometric data for the purposes of uniquely identifying a natural person;
 - f. Health data; and
 - g. Data concerning a person’s sex life or sexual orientation.

D. Lawful Basis for Collecting or Processing Personal Data

Personal data on individuals located in the EU may be collected and processed if 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; or
2. Processing is necessary for:
 - a. Purposes of the legitimate interests pursued by MCCS or by a third party, except where such interests are overridden by the

interests or fundamental rights and freedoms of the data subject which require protection of personal data;

- b. Performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;
- c. Compliance with a legal obligation to which M CCS is subject;
- d. Protection of the vital interests of the data subject or of another natural person; or
- e. Performance of a task carried out in the public interest or in the exercise of official authority vested in M CCS.

E. Data Protection & Governance

Personal data on individuals located in the EU 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 data are collected and processed;
- 4. Accurate and, where necessary, kept up to date;
- 5. Retained only as long as necessary; and
- 6. Processed in a manner that ensures appropriate security.

E. Sensitive Personal Data

M CCS must obtain consent from the data subject before collecting or processing sensitive personal data.

F. Individual Rights of Access

Individual data subjects covered by this policy have the right to obtain from M CCS confirmation as to whether or not his or her personal data are being processed, and, if yes, access to the personal data and the following information:

- 1. The purposes and lawful basis of the data collection/processing;
- 2. The recipients or categories of recipients of the personal data;
- 3. The categories of personal data at issue;

4. The envisaged period the personal data will be stored;
5. 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;
6. The existence of the right to withdraw consent at any time;
7. The right to lodge a complaint with a supervisory authority established in the EU;
8. Why the personal data are required, and possible consequences of the failure to provide the data;
9. The existence of automated decision-making, including profiling;
10. Whether MCCS intends to transfer personal data to another country or international organization;
11. Whether the collected data are going to be further processed for a purpose other than that for which it was collected;
12. Information about the controller collecting the data; and
13. Data protection officer contact information (if assigned).

G. Additional Procedures and Forms

Additional procedures and forms specific to compliance with the GDPR are set forth in Section VIII of the Information Technology Procedures Manual and shall include at a minimum:

1. Legal Requirements;
2. Data Protection and Governance;
3. Privacy Notice;
4. Consent;
5. Individual Rights;
6. MCCS Roles and Responsibilities;
7. Data Protection;
8. Breach Notification; and
9. Verification requirements.

REFERENCES: European Union General Data Protection Regulation

DATE ADOPTED: June 13, 2018