KENNESAW STATE UNIVERSITY

Policy Title	EU General Data Protection Regulation Compliance Policy
Issue Date	May 25, 2018
Effective Date	May 25, 2018
Last Updated	May 1, 2023
Responsible Office	Office of the Vice President of Information Technology and Chief Information Officer
Contact Information	Office of the Vice President of Information Technology and Chief Information Officer, Office of Cybersecurity Phone: 470-578-6620 Email: ocs@kennesaw.edu

1. Policy Purpose Statement

Kennesaw State University (KSU) has a lawful basis to responsibly collect, process, use, and/or maintain the confidential personal data of its students, employees, applicants, research subjects, and others involved in its educational, research, and community programs. The European Union General Data Protection Regulation (EU GDPR) imposes obligations on entities, like Kennesaw State University, that collect or process confidential personal data about people in the European Union (EU). This policy describes Kennesaw State University's data protection strategy to comply with the EU GDPR.

2. Background

The EU GDPR came into force on May 25th, 2018. Among other things, the EU GDPR requires Kennesaw State University to: a) be transparent about the confidential personal data it collects or processes and the uses it makes of any confidential personal data; b) keep track of all uses and disclosures it makes of confidential personal data; and c) appropriately secure confidential personal data.

3. Scope (Who is Affected)

Any KSU department or individual collecting or processing confidential personal data of a covered individual, *anyone* located in the EU. The EU GDPR applies to the confidential personal data Kennesaw State University collects or processes about anyone located in the EU, regardless of whether they are a citizen or permanent resident of an EU country.

4. Exclusions or Exceptions

Kennesaw State University has a lawful basis to collect and process confidential personal data. Most of Kennesaw State University's collection and processing of confidential personal data will fall under the following categories:

a. Processing is necessary for the purposes of the legitimate interests pursued by Kennesaw State University or by a contracted third party.
b. Processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering a contract.

c. Processing is necessary for compliance with a legal obligation to which Kennesaw State University is subject.
d. The data subject has given consent to the processing of that individual's confidential personal data for one or more specific purposes.

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

5. Definitions and Acronyms

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, or erasure or destruction of confidential personal data, whether or not by automated means.

Consent: Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which that individual, by a statement or by a clear affirmative action, signifies agreement to the processing of confidential personal data relating to him or her.
Under the EU GDPR:

a. Consent must be a demonstrable, clear affirmative action;
b. 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;
c. Consent cannot be by silence, a pre-ticked box, or inaction;
d. 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;
e. Request for consent must be presented clearly and in plain language; and
f. Record regarding how and when consent was given must be maintained.

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 confidential personal data.

Kennesaw State University Unit: A Kennesaw State University college, school, office, or department.

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 KSU identification, KSU account (e.g., NetID), or physical address or other location data.

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

a. The data subject has given consent to the processing of that individual's confidential personal data for one or more specific purposes;
b. 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;
c. Processing is necessary for compliance with a legal obligation to which the controller is subject;

d. Processing is necessary in order to protect the vital interests of the data subject or of another natural person;
e. 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; and/or
f. Processing is necessary for the purposes of the legitimate interests pursued by the controller or by contracted third party.

Legitimate Interest: Processing of confidential 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 confidential personal data.

Processor: A natural or legal person, public authority, agency, or other body who processes personal data on behalf of the controller.

Confidential Personal Data: Special categories of information related to an identified or identifiable person that require consent by the data subject before collecting or processing are:
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.

6. Policy

KSU will obtain consent before it collects or processes such confidential personal data. Data collected or processed by Kennesaw State University shall be:
a. Processed lawfully, fairly, and in a transparent manner;
b. Collected for specified, explicit, and legitimate purposes, and not further processed in a manner that is inconsistent with these purposes;
c. Limited to what is necessary in relation to the purposes for which they are collected and processed;
d. Accurate and kept up-to-date;
e. Retained only as long as necessary in alignment with university retention and disposition standards; and
f. Secured to industry best practices and standards.

7. Associated Policies/Regulations

a. USG BOR Records Retention guidelines: All data at KSU shall be kept in compliance with the BOR policy.
b. Kennesaw State University's Privacy Statement: KSU's Privacy Statement to data subjects must specify the lawful basis to collect or process confidential personal data. A link to the KSU Privacy Statement is available on the footer of all KSU websites.

8. Procedures Associated with this Policy

a. Security of Confidential Personal Data: All confidential personal data collected or processed by any Kennesaw State University Unit under the scope of this policy must comply with the security controls and process required by the Kennesaw State University Data Security Policy.
b. Breach Notification: Any KSU Unit that suspects that a breach or disclosure of confidential personal data has occurred must immediately notify the KSU Office of Cybersecurity via a

service ticket.

9. Forms Associated with this Policy

a. EU GDPR Legitimate Interest Form (Available from the Division of Legal Affairs.)
b. EU GDPR Model Consent Form (Available from the Division of Legal Affairs.)

10. Violations

Any individual wishing to make a complaint or exercise their rights under this policy may do so by submitting a Service Request with the Office of Cybersecurity.

11. Review Schedule

The Office of Cybersecurity will review the EU General Data Protection Regulation Compliance Policy annually.

At Kennesaw State University, institutional policies that have undergone the established shared governance review and feedback process are presented to the President and Provost for final approval. The signatures below indicate this institutional policy has been reviewed and approved by the President and Provost.

DocuSigned by:
Dr. Kathy Schwaig July 11, 2023
11EA3F49C7FD4B9...
Dr. Kathy S. Schwaig,
President
Kennesaw State University

DocuSigned by:
Ivan Pulinkala July 11, 2023
02FA0CC7B24D4B3...
Dr. Ivan Pulinkala
Provost and Senior Vice President for Academic Affairs
Kennesaw State University