# EU General Data Protection Regulation Compliance Policy

Type of Policy: Administrative
Effective Date: TBD
Last Revised: TBD

**Policy Owner**: UITS
**Policy Contact**: Stephen Gay, Executive Director and Chief Information Security Officer

## 1. Reason for Policy

Kennesaw State University ("Kennesaw State University" or the "University") is an institute of higher education involved in education, research and community development. In order for Kennesaw State University to educate it's foreign and domestic students both in class and on-line, engage in world-class research, and provide community services, it is essential and necessary, and Kennesaw State University has a lawful basis, to 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. These activities include, without limitation, admission, registration, delivery of classroom (including on-line, and study abroad) education, grades, communications, employment, applied research, development, program analysis for improvements, and records retention.

Kennesaw State University takes seriously it's duty to protect the confidential personal data it collects or processes. In addition to Kennesaw State University's enterprise security program, 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"). The EU GDPR applies to 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. 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
c) appropriately secure confidential personal data

This policy describes Kennesaw State University's data protection strategy to comply with the EU GDPR.

## 2. Policy Statement

### 2.1 Lawful Basis for Collecting or Processing Confidential Personal Data

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 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 Kennesaw State University is subject.

d) The data subject has given consent to the processing of his or her 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.

### 2.2 Data Protection & Governance

Kennesaw State University will protect all confidential personal data that it collects or processes for a lawful basis. Any confidential personal 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 incompatible with those 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 in alignment with university retention standards

f) Secured to industry best practices and standards

### 2.3 Confidential Personal Data & Consent

Kennesaw State University must obtain consent before it collects or processes confidential personal data.

### 2.4 Individual Rights

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

a) information about the controller collecting the data

b) the data protection officer contact information (or designated Controller)

c) the purposes and legal basis/legitimate interests of the data collection/processing

d) recipients of the confidential personal data

e) if Kennesaw State University intends to transfer confidential personal data to another country or international organization

f) the period the confidential personal data will be stored

g) the existence of the right to access, rectify incorrect data or erase confidential personal data, restrict or object to processing, and the right to data portability

h) the existence of the right to withdraw consent at any time

i) the right to lodge a complaint with a supervisory authority (established in the EU)

j) why the confidential personal data are required, and possible consequences of the failure to provide the data

k) the existence of automated decision-making, including profiling

l) if the collected data are going to be further processed for a purpose other than that for which it was collected

**Note: Exercising of these rights is a guarantee to be afforded a process and not the guarantee of an outcome.**

## 3. Scope

This policy applies to confidential personal data protected by the EU GDPR and all Kennesaw State University Units who collect or process confidential personal data protected by the EU GDPR.

## 4. 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 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 he or she, 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:<br>a) Consent must be a demonstrable, clear affirmative action.<br>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.<br>c) Consent cannot be silence, a pre-ticked box or inaction.<br>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.<br>e) Request for consent must be presented clearly and in plain language.<br>f) 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 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.<br>Examples of identifiers include but are not limited to: name, photo, email address, identification number such as KSU ID#, KSU Account (NetID), physical address or other location data. |
| **Lawful Purpose** | Processing of confidential personal data shall be lawful only if and to the extent that at least one of the following applies:<br>a) The data subject has given consent to the processing of his or her confidential personal data for one or more specific purposes;<br>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;<br>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;<br>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;<br>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:<br>a) Racial or ethnic origin<br>b) Political opinions<br>c) Religious or philosophical beliefs<br>d) Trade union membership<br>e) Genetic, biometric data for the purposes of uniquely identifying a natural person<br>f) Health data<br>g) Data concerning a person's sex life or sexual orientation |

## 5. Procedures

| **5.1 Data Governance** | |
|---|---|
| **Document Lawful Basis for Collection or Processing** | All Kennesaw State University Units who collect or process confidential personal data protected by the EU GDPR must document the lawful basis for the collection or processing of confidential personal data they collect or process, why they collect it, and how long they keep it |

| | |
|---|---|
| | All data at Kennesaw State University shall be kept in compliance with the USG-BOR Records Retention Schedules. |

| 5.2. Privacy Notice | |
|---|---|
| | Kennesaw State University's Privacy Notice to data subjects must specify the lawful basis for Kennesaw State University to collect or process confidential personal data and include:<br>a) whether their confidential personal data are being collected or processed and for what purpose<br>b) categories of confidential personal data concerned<br>c) to whom confidential personal data is disclosed<br>d) storage period (records retention period)<br>e) existence of individual rights to rectify incorrect data, erase, restrict or object to processing<br>f) how to lodge a complaint<br>g) the source of the confidential personal data (if not collected from the data subject)<br>h) the existence of automated decision-making, including profiling<br><br>A link to the Kennesaw State University Privacy Notice is available on the footer of all Kennesaw State University websites – "Legal & Privacy Information": http://legal.kennesaw.edu |

| 5.3 Consent | |
|---|---|
| **Document** | Kennesaw State University Units must obtain affirmative consent before it collects or processes confidential personal data. |
| **Withdrawal of Consent** | Kennesaw State University units must have a process for individuals who request to withdraw their consent. |

| 5.4 Individual Rights | |
|---|---|
| **Rights** | Any individual wishing to exercise their rights under this policy may do so by submitting a Service Request with the Office of Cybersecurity at service@kennesaw.edu |

| 5.5 Data Protection | |
|---|---|
| **Security of Confidential Personal Data** | All confidential personal data collected or processed by any Kennesaw State University Units under the scope of this policy must comply with the security controls and systems and process required by the Kennesaw State University Data Security Policy: https://policy.kennesaw.edu/content/data-security-policy |
| **Breach Notification** | Any Kennesaw State University Unit that suspects that a breach or disclosure of confidential personal data has occurred must immediately notify the Kennesaw State University Office of Cybersecurity via a service ticket at service@kennesaw.edu |

## 6. Forms

| Title | Link |
|---|---|
| EU GDPR Legitimate Interest Form | [add link to Legitimate Interest Form] |
| EU GDPR Model Consent Form | [add link to Consent Form] |
| | |

## 7. Frequently Asked Questions

For Frequently Asked Questions about EU GDPR compliance at Kennesaw State University, see website here: https://gdpr.kennesaw.edu

## 8. Responsibilities

### 8.1.Responsible Party:

#### Kennesaw State University Units

To document the legitimate interest and/or consent of confidential personal data collected or processed pursuant to this policy.

To cooperate with Kennesaw State University when individuals inquire about their confidential personal data collected or processed pursuant to this policy (See Section 2.3).

To immediately notify and cooperate with the Kennesaw State University UITS Office of Cybersecurity relating to any data breach: https://uits.kennesaw.edu/ocs

### 8.2.Responsible Party:

#### Kennesaw State University

To field inquiries about confidential personal data collected from individuals while in the EU (See Section 2.3).

To coordinate with Legal Affairs and Kennesaw State University Unit in responding to inquiries about confidential personal data collected from individuals while in the EU.

### 8.3.Responsible Party

#### KSU UITS Office of Cybersecurity

To answer questions about and review data security measures.

To address data breach notification.

## 9. Enforcement

Violations of the policy may result in loss of system, network, and data access privileges, administrative sanctions (up to and including termination or expulsion) as outlined in applicable Kennesaw State University disciplinary procedures, as well as personal civil and/or criminal liability.

To report suspected instances of noncompliance with this policy, please contact The Kennesaw State University Office of Cybersecurity via a service ticket at service@kennesaw.edu

## Related Information

| Resource | Link |
|---|---|
| EU General Data Protection Regulation (EU GDPR) | https://www.eugdpr.org |
| EU GDPR FAQs | https://gdpr.kennesaw.edu |
| Kennesaw State University Legal & Privacy Notice | http://www.legal.kennesaw.edu |
| Kennesaw State University Data Security Policy | https://policy.kennesaw.edu/content/data-security-policy |
| USG-BOR Records Retention Schedules | http://www.usg.edu/records_management/schedules |
| | |

## 10. Policy History

| Revision Date | Author | Description |
|---|---|---|
| XX-XX-XXXX | Kennesaw State University | New Policy |