EUROPEAN UNION GENERAL DATA PROTECTION REGULATION COMPLIANCE

Area:	Office of the President	Number:	n/a
Applies to:	All faculty and staff	Issued:	August 16, 2018
Sources:	EU General Data Protection Regulation (EU GDPR)	Revised:	
	GSOU Privacy & Legal Statement	Reviewed:	
	USG BoR Records Retention Schedule	Page(s):	5
Policy Owner:	Office of Legal Affairs		

I. Purpose

Georgia Southern University is an institute of higher education involved in education, research and community development. In order for Georgia Southern University 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, and Georgia Southern University 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.

Georgia Southern University takes seriously its duty to protect the personal data it collects or processes. In addition to Georgia Southern University's overall data protection program, the European Union General Data Protection Regulation (EU GDPR) imposes obligations on entities, like Georgia Southern University, that collect or process personal data about people in the European Union (EU). The EU GDPR applies to personal data Georgia Southern 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 Georgia Southern University 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;
3. appropriately secure personal data.

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

II. Policy Statement

Lawful Basis for Collecting or Processing Personal Data

Georgia Southern University has a lawful basis to collect and process personal data. Most of Georgia Southern University'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 Georgia Southern University 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 Georgia Southern University 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.

Data Protection & Governance

Georgia Southern University 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 Georgia Southern University 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.

Sensitive Personal Data & Consent

Georgia Southern University must obtain consent before it collects or processes sensitive personal data.

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 Georgia Southern University 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.

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

III. Definitions

Collect or Process Data – Collection, storage, recording, organizing, structuring, adaptation, or alteration, consultation, use, retrieval, disclosure by transmission/dissemination or otherwise make data available, alignment or combination, restriction, erasure or destruction of 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 personal data relating to him or her. Under the EU GDPR:

- Consent must be a demonstrable, clear affirmative action.
- 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.
- Consent cannot be silence, a pre-ticked box or inaction.
- 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.
- Request for consent must be presented clearly and in plain language.
- 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 Unit - 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 Eagle ID#, Eagle 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:

- The data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- 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;
- Processing is necessary for compliance with a legal obligation to which the controller is subject;
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- 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;
- 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 – A natural or legal person, public authority, agency or other body who processes personal data on behalf of the controller.

Sensitive Personal Data – Special categories of personal data that require consent by the data subject before collecting or processing are:
- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic, biometric data for the purposes of uniquely identifying a natural person;
- Health data;
- Data concerning a person's sex life or sexual orientation.

IV. Exclusions

This policy applies to the personal data and sensitive personal data protected by the EU GDPR and all Georgia Southern University units who collect or process personal data and sensitive personal data protected by the EU GDPR. There are no exclusions or exceptions to the policy.

V. Procedures

Georgia Southern University's Privacy Notice to data subjects must specify the lawful basis for Georgia Southern University to collect or process personal data and include:
- whether their personal data are being collected or processed and for what purpose;
- categories of personal data concerned;
- to whom personal data is disclosed;
- storage period (records retention period);
- existence of individual rights to rectify incorrect data, erase, restrict or object to processing;
- how to lodge a complaint;

- the source of the personal data (if not collected from the data subject);
- the existence of automated decision-making, including profiling.

A link to the Georgia Southern University Privacy Notice is available on the footer of all Georgia Southern University websites – Privacy & Legal Statement.

Any individual wishing to exercise their rights under this policy should contact the Office of Internal Audit, Risk & Compliance at RiskCompliance@georgiasouthern.edu.

Any Georgia Southern University unit that suspects that a breach or disclosure of personal data has occurred must immediately notify Georgia Southern Information Security at security@georgiasouthern.edu.

To report suspected instances of noncompliance with this policy, please contact the Office of Internal Audit, Risk & Compliance at RiskCompliance@georgiasouthern.edu. or visit Georgia Southern University's *Ethics & Compliance Reporting Hotline*, a secure and confidential reporting system, at: https://georgiasouthern.alertline.com/gcs/welcome.