



I. Policy Title

EU General Data Protection Regulation Compliance Policy

II. Policy Purpose and Statement

Lawful Basis for Collecting or Processing Personal Data:

FVSU has a lawful basis to collect and process personal data. FVSU's collection and processing of personal data will generally fall under the following categories (this is a non-exclusive list):

- a. Processing is necessary for the purposes of the legitimate interests pursued by FVSU or by a 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 FVSU is subject.
- d. The data subject has given consent to the processing of his or her special categories of sensitive personal data for one or more specific purposes.

III. Policy Application and Effective Date

- a. This policy applies to all external and internal FVSU Community.
- b. This policy is effective August 16, 2018.

IV. 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 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- b. Consent can be withdrawn by the data subject at any time and must be as easy to withdraw consent as it is to give consent.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 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.
- 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 personal data.
FVSU Unit	A FVSU college, office or department.
Identified or Identifiable Person	<p>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.</p> <p>Examples of identifiers include but are not limited to: name, photo, email address, identification number such as FVSU ID# or Account#, user ID, physical address or other location data, Internet protocol (IP) address or other online identifier</p> <p>Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:</p> <ol style="list-style-type: none"> a. The data subject has given consent to the processing of his or her 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; f. Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party.
Lawful Basis	
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 Processor	<p>Any information relating to an identified or identifiable person (the data subject).</p> <p>A natural or legal person, public authority, agency or other body who processes personal data on behalf of the controller.</p> <p>Special categories of sensitive personal data that require consent by the data subject before collecting or processing are:</p> <ol style="list-style-type: none"> 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 g. Data concerning a person's sex life or sexual orientation
Special Categories of Sensitive Personal Data	

Withdrawal of Consent FVSU must have a process for individuals who request to withdraw their consent.

V. Policy

Overview

The European Union has passed a data privacy regulation that is applicable throughout the entire [European Union \("EU"\)](#), and to those who collect personal data about people in the EU. The European Union General Data Protection Regulation ("GDPR") imposes obligations on entities, like Fort Valley State University ("FVSU" or the "University"), that collect or process personal data about people in the EU. The GDPR applies to personal data collected or processed about *anyone located in the EU*, regardless of whether they are a citizen or permanent resident of an EU country.

In order for FVSU to educate its foreign and domestic students, both in class and online, and engage in world class research, it is sometimes necessary to collect, process, use, and/or maintain the personal data of its students, employees, applicants, research subjects, and others involved in its educational and research programs. FVSU takes seriously its duty to protect the personal data it collects or processes. In addition to FVSU's overall data protection program, FVSU must make sure it complies with the dictates of the GDPR. Among other things, the GDPR requires FVSU to:

- a. be transparent about the personal data it collects or processes and the uses of any personal data
- b. keep track of all uses and disclosures it makes of personal data
- c. appropriately secure personal data

This policy describes FVSU's data protection strategy to comply with the GDPR.

Data Protection & Governance

FVSU will protect all personal data and special categories of sensitive personal data that it collects or processes for a lawful basis. Any personal data and special categories of sensitive personal data collected or processed by FVSU 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, kept up to date and properly secured
- e. Retained only as long as necessary and in accordance with the University System of Georgia Board of Regents [USG-BOR Records Retention Schedules](#).

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 (if assigned)
- c. the purposes and lawful basis of the data collection/processing
- d. recipients of the personal data

- e. if FVSU intends to transfer personal data to another country or international organization
- f. the period the personal data will be stored
- g. 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
- 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 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

FVSU Data Collection

FVSU collects information from individuals or entities when they access any FVSU website. Information that is collected from this contact is the contactor's IP address, date and time of the website access along with the web pages(s) visited. In addition, FVSU may also collect any information that it receives from a visitor's web browser, including browser type and version, and operating system. This information helps us understand aggregate uses of our site, track usage trends and improve our services.

The following is a typical log entry when someone visits our website:

```
73.207.112.121 130.207.244.191 - - [01/Jun/2015:13:12:49 -0400] "GET
/sites/default/files/uploads/images/admissions_graduate_0.jpg HTTP/1.1" 200 35380
"http://www.gatech.edu/admissions" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_3)
AppleWebKit/600.6.3 (KHTML, like Gecko) Version/8.0.6 Safari/600.6.3"
```

Cookies

Cookies are files that many websites transfer to users' web browsers to enable the site to deliver personalized services or to provide persistent authentication. The information contained in a cookie typically includes information collected automatically by the web server and/or information provided voluntarily by the user. Our website uses persistent cookies in conjunction with a third-party technology partner to analyze search engine usage and web traffic patterns. This information is used in the aggregate to monitor and enhance our web pages. It is not used to track the usage patterns of individual users.

Security

Our information security officer within our Information Technology Department is committed to ensuring the security of your information. We have put in place reasonable physical, technical and administrative safeguards designed to prevent unauthorized access to or use of the information collected online.

Sharing your information

We will not share your information with third parties except:

- a) as required by law;
- b) as necessary to protect University interests;
- c) as necessary to further University research efforts pursuant to approvals from appropriate data stewards and the IRB, and/or
- d) with service providers acting on our behalf who have agreed to protect the confidentiality of the data.

Links to other websites

This site may contain links to other websites not affiliated with FVSU. We are not responsible for the privacy practices of these other sites. We encourage you to read the privacy statements of other sites for assurance that their practices safeguard your privacy.

Legal Notice

Notwithstanding any language to the contrary, nothing contained herein constitutes nor is intended to constitute an offer, inducement, promise, or contract of any kind. The data contained herein is for informational purposes only and is not represented to be error free. Any links to non-Fort Valley State

University information are provided as a courtesy. They are not intended to nor do they constitute an endorsement by the Fort Valley State University of the linked materials.

Responsible Party

Any questions or concerns regarding this policy, or to report a suspected instance of noncompliance, should be directed to the Chair of the Institutional Review Board (IRB), the Chief Compliance Officer, and/or the Chief Legal Officer.

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 FVSU disciplinary procedures, as well as personal civil and/or criminal liability.

Enforcement of the GDPR will be carried out by the appropriate Data Protection Authority within the European Union. SU must obtain consent before it collects or processes special categories of sensitive personal data.

VI. Forms

N/A

VII. Appendices

N/A

VIII. Related Resources

IX. Responsible Party

Questions regarding this policy should be directed to:

Job Title:

Department: Legal Affairs and Risk Management

Phone: 478-445-4284

Email:

Fax: