UNIVERSITY SYSTEM OF GEORGIA
Legal Affairs

270 Washington Street, S.W.
Atlanta, Georgia 30334

PHONE (404) 962-3255
FAX (404) 962-3264
USG-LEGAL@USG.EDU

M E M O R A N D U M

TO: Presidents
Vice Presidents of Academic Affairs
Vice Presidents of Student Affairs
Chief Auditors
Chief Business Officers
Chief Human Resource Officers
Chief Information Officers
Chief Legal Officers

FROM: USG Office of Legal Affairs

DATE: May 16, 2018

SUBJECT: EU General Data Protection Regulation (GDPR)

As many of you know and have asked our office about, new data privacy rules will take effect in the European Union on May 25, 2018. Known as the General Data Protection Regulation (GDPR), this directive will also have compliance implications for USG Institutions. This memorandum seeks to educate USG constituents about GDPR implications and provide guidance on compliance with GDPR.

What Does the GDPR Do?

The GDPR does two things: (1) it explicitly confers numerous rights upon data subjects located in the European Union (EU), and (2) it requires covered organizations to put significant safeguards in place regarding the use and processing of personal data of EU subjects (failure to do so can result in enforcement action and a very significant financial penalty of up to 4% of a violating entity's revenue).

Personal Protections Under the Regulation

Under the regulation, covered individuals have the right to, among other things:

- Access any data that an organization has collected about the individual;
- Know why an organization is processing the individual's personal data and the categories of personal data that an organization processes;
- Correct any errors in personal data collected or processed by an organization;
- Know how long an organization will store the individual's personal data; and
- Under certain circumstances, require the organization to permanently delete the individual's personal data (this right is sometimes referred to as the "right to be forgotten" or the "right to erasure").

Obligations for Organizations

GDPR imposes a number of obligations upon the organizations that are subject to it. Notable requirements include that the organization:

- Have a legal basis for collecting and processing the personal data of EU data subjects, document that legal basis, and only collect and use data when a legal basis exists;
- Minimize the collection and processing of personal data whenever possible;
- Protect any personal data that it collects and uses;
- Conduct an assessment to determine any risks and privacy impacts related to collecting and processing the personal data of data subjects, implement a plan to mitigate those risks and impacts, and continuously monitor both the risks and the mitigation plan for change;
- Conduct a data protection impact assessment for special categories of high-risk data collection and processing; and
- Have a breach notification policy and notify authorities within 72 hours of learning of the breach.

Organizations located within the EU must comply with the GDPR, as do organizations, **regardless of where they are located**, that offer goods or services to or collect data on people in the EU. For example, among other things, the latter would include USG Institutions that accept applications from EU subjects or maintain data on institution students studying abroad in the EU.

GDPR Terms to Know

GDPR uses several defined terms that have special meaning within the regulation:

- A *controller* is an organization that directs the collection of personal data from a data subject. For example, in our context, an institution directing the collection of admissions related data.
- A *processor* is an organization that uses or processes personal data from a data subject at the direction of a data controller. For example, in our context, an institution using collected admissions related data. An institution can be both a processor and a controller.
- A *data subject* is an identified or identifiable natural person. In our context this could include a prospective student, student, or faculty member physically located in the EU.
- *Personal data* is any information about an identified or identifiable data subject. It can include direct identifiers like name, address, email address, and national identification numbers or indirect identifiers like location data or IP address. (Note: this list of data elements is not exclusive, and the definition of "personal data" under GDPR should be considered in the broadest possible context.)

The Onus Is on the Organization Collecting the Data

Both controllers and processors must implement policies and practices to ensure that a data subject's privacy rights are not violated. As mentioned earlier, GDPR specifies that data controllers and processors must have a documented legal basis for collecting and processing the personal data of EU data subjects. There are two basic categories of legal basis: (1) consent from the data subject, and (2) one of the specified business reasons for processing data.

Organizations must specifically be able to point either to consent or to one of the stated business purposes as the organizations' reason for processing data. The GDPR consent requirements are very specific and limit the use of personal data for uses other than those specifically stated in the consent document. For that reason, generally speaking, most organizations will want to be able to identify one of the stated business reasons for processing the personal data of an EU data subject.

Impact on USG Institutions

GDPR poses a concern for U.S. higher education institutions, particularly in those instances where colleges and universities interact with EU data subjects. These interactions must be fully understood, documented and assessed for GDPR applicability. For instance:

- Does GDPR apply if an institutional website is merely accessible in the EU via the internet? ***Probably not.***
- Does it apply to the collection of IP address information from that same website to feed subsequent faculty and staff talent management or student recruitment activities? ***Maybe***.
- Does it apply to talent management and recruitment activities specifically directed at EU data subjects? ***Probably***.
- Does it apply to a U.S. institution's EU-based study abroad programs? ***Most likely***.

What Should Our USG Institutions Do to Prepare?

The first step is to understand where the institution is collecting and using personal data collected from EU data subjects. Included in this review should be an analysis of the types of personal data being collected, and, where possible, minimize or eliminate certain types of personal data collection.

Under GDPR, obtaining the appropriate consent to the collection of personal data is crucial. Just as crucial is providing a mechanism by which a person may withdraw that consent. Finally, each institution will also need to adopt a compliance policy for GDPR and a privacy notice. As the regulation becomes operative, and there is experience on how it is being applied relevant to the USG context, adoption of a systemwide policy may be forthcoming.

Our colleagues in Legal Affairs at Georgia Tech have spent a tremendous amount of time and effort in researching and preparing for the implementation of GDPR. They have graciously provided us with the following draft forms and consented to these being shared with all USG Institutions as sample documents to consider utilizing to help with institutional compliance with GDPR. These sample documents may be downloaded via http://bit.ly/usg-gdpr as well as via Georgia Tech's Legal Affairs website.

- **Data Steward Questionnaire** (to be used to assist an institution in determining where data subject to the GDPR is being collected);
- **Lawful Basis Questionnaire** (to be used to determine if there is a legitimate interest in collecting the data);
- **Consent for Collection and Processing of Sensitive Personal Data** (to be obtained from EU data subjects);
- **Procedures for Withdrawal of Consent** (GDPR allows a data subject the option to withdraw consent);
- **Procedures for Exercise of Individual Rights** (includes the "right to be forgotten");
- **EU GDPR Compliance Policy**; and
- **Privacy Notice**

Note that the penalties for noncompliance with the GDPR are substantial, so it is imperative that each USG Institution take the necessary steps toward compliance. While on its face the GDPR may seem onerous, its main focus represents simple good data collection policy – collect only that data that you really need and for which you have a legitimate interest to collect.

Please contact Daryl Griswold or Edward Tate in the USG Office of Legal Affairs with any questions.