UNIVERSITY SYSTEM OF GEORGIA

European Union General Data Protection Regulation (EU GDPR)

RACRA Spring 2019
Macon, GA

Agenda

- Introductions
- Overview of the EU GDPR
- USG's Steps Towards Compliance
- Georgia Tech's Steps Towards Compliance
- Panel Question & Answer

Introductions

- Chris McGraw – Legal Affairs, USG
- Rose Procter – Ethics & Compliance, USG
- Susann Estroff – Legal Affairs, Georgia Tech
- Zachary Hayes – Ent. Data Mgmt., Georgia Tech

UNIVERSITY SYSTEM OF GEORGIA

Overview of the EU GDPR

Susann Estroff
Legal Affairs
Georgia Institute of Technology

EU GDPR

- Intent of the Regulation: to address the protection of natural persons **physically within the EU** with regard to the **processing of personal data** and rules relating to the free movement of such data.
- Applies to the collection and processing of personal data about anyone located in the EU (even non-EU citizens and residents)

Compliance deadline was May 25, 2018

Transparency

- The GDPR requires you to inform the data subject what **personal data** you are collecting, what you are using it for, who are you giving it to, how long you are keeping it, and how you secure it.

- Organizations must have a **lawful basis** to collect and process the personal data from the EU; must document that lawful basis; must only collect and use data when a lawful basis exists

Lawful Basis

Organizations must have a lawful basis to collect and process the personal data from the EU:

- The legitimate interests of the organization that outweigh the interests and fundamental rights and freedoms of the data subjects which require protection of the personal data
    - For Georgia Tech (and perhaps your institution), the legitimate interests are to provide educational services, employment, conduct research, development, etc.
- Pursuant to a contractual obligation
    - Example: contracts for the conduct of research
- Pursuant to consent from the data subject
    - This is for the special categories of sensitive personal data
    - GDPR gives data subjects the right to withdraw consent at any time

Personal Data

Personal data is **any information relating to an identified or identifiable person**. Identification of a person may include:

- Name
- Photo
- Email address, physical address, or other location data
- IP address or other online identifier
- Identification number (e.g., Banner ID) or a user account (Campus User ID)

Special Categories of Sensitive Personal Data

An **affirmative consent** is needed **before** collecting special categories of sensitive personal data from the EU:

- 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
- Data concerning health
- Data concerning a person's sex life or sexual orientation

Penalties for Non-Compliance

Subject to fines of up to four percent (4%) of worldwide annual turnover or € 20 million, whichever is higher.

UNIVERSITY SYSTEM OF GEORGIA

USG's Steps Towards Compliance

Rose Procter
Ethics & Compliance
University System of Georgia

STEP 1

Data Policy and Legal Notice Rewrite

Data Privacy Policy and Legal Notice

This Privacy Policy sets forth the University System of Georgia's ("USG") policy and legal notice with respect to the gathering and dissemination of information we obtain from you on USG's website located at usg.edu ("Site") and with respect to compliance (where applicable) with the European Union's General Data Protection Regulation ("EU GDPR").

USG is the operator of this Site, although software, hosting and other functions may be provided by third parties ("Service Providers"). This Privacy Policy and Legal Notice ("Policy") describes the type of information USG and its Service Providers collect from visitors to this Site, what we do with that information, and how visitors can update and control the use of information provided on this Site.

This Policy does not necessarily describe information collection policies on other sites, such as separate sites operated by our Service Providers that we do not control. Many of the resources linked from this Site are not maintained by USG. USG cannot monitor all linked resources, only those pages that fall directly within USG world-wide web structure. USG is in no way responsible for the privacy practices or the content of these linked resources, and the statements, views, and opinions expressed therein are neither endorsed by nor do they necessarily reflect the opinion of the USG. Any links to non-USG information or resources are provided as a courtesy. They are not intended to nor do they constitute an endorsement by USG of the linked materials.

This Policy may be changed from time to time and without further notice. Your continued use of the Site after any such changes constitutes your acceptance of the new terms. If you do not agree to abide by these new terms or any future terms, please do not use the Site. This site is not directed to children under 13 years of age, and children under 13 years of age shall not use this Site to submit any personal information about themselves.

Information We Gather

When you visit the Site, we may collect certain routing information, including, but not limited to, the Internet Protocol ("IP") address of your originating Internet Service Provider ("ISP"), and information provided by "cookies" stored on your hard drive. We may also collect aggregate information about the use of the Site, including, but not limited to, which pages are most frequently visited, how many visitors we receive daily, and how long visitors stay on each page. We may disclose and publish aggregate information on an aggregate basis to any party through any means, but such aggregate information will not disclose any personal information. Any information collected through this Site may also be used in aggregate by system administrators in the administration of the Site. This information helps us understand aggregate uses of our site, track usage trends, and improve our services. You may also be required to provide certain personal information in order to access various features and information on the Site. Such information may include, among other things, your name, address, and phone number. If you do not want to provide such information, you may choose not to access those features of the Site. Any personal information that you choose to provide through the Site will be protected in accordance with the provisions of this Policy.

Cookies

Cookies are small pieces of data that may be stored by a Web browser. Cookies are often used to remember information about preferences and pages you have visited. This information is stored for your convenience and also may be used in the aggregate to monitor and enhance the Site. For example, when you visit some sites on the Web you might see a "Welcome Back" message. The first time you visited the site a cookie may have been set on your computer; when you return, the cookie is read again. You can refuse to accept cookies, can disable cookies, and remove cookies from your hard drive. However, if you do not accept cookies from the Site, you may lose access to the Site or experience decreased performance of the Site.

Security and Accuracy of Confidential Information

USG does its best to ensure that the personal information obtained from you is accurate. You may review the information saved or submitted via the Site at any time up to the point when it is purged from the flat file or database. In the event that there is an error in your personal information, we will correct the information on your request.

We have put in place reasonable physical, technical, and administrative safeguards designed to prevent unauthorized access to our use of the information collected online. While we strive to protect your personal information by encryption and other means, we cannot guarantee or warrant the security of the information you transmit to us, and if you choose to use the Site, you do so at your own risk.

Please keep in mind that the information disclosed by you on our Site in certain forums – for example, information, including personal information, that you may provide to others on bulletin boards, through blogs or in chat rooms that may be available on the Site – can be collected and used by visitors to the Site.

Sharing of Information

USG is committed to maintaining the privacy of your personal information. We do not actively share personal information gathered from the Site. However, there may be some instances in which we will need to do so as required by law (including but not limited to the Georgia Open Records Act), as necessary to protect USG interests, and/or with Service Providers acting on our behalf. USG also complies with the Family Educational Rights and Privacy Act ("FERPA"), which generally prohibits (with some exceptions) the release of education records without student permission. For more details on FERPA, currently enrolled students should see their institutions' specific policies.

Questions

If you have questions about this Policy or you believe that your personal information has been released without your consent or if you wish to correct information held by USG, please contact us at https://www.usg.edu/contact.

EU GDPR Privacy Notice

Lawful Bases for Collecting and Processing of Personal Data

USG is a system of institutions of higher education involved in education, research, and community development. In order for USG and its institutions to educate its students both in class and online, engage in world-class research, and provide community services, it is essential, necessary, and USG and its institutions have lawful bases to collect, process, use, and maintain data of students, employees, applicants, research subjects, and others involved in its educational, research, and community programs. The lawful bases include, without limitation, admission, registration, delivery of classroom, online, and study abroad education, grades, communications, employment, applied research, development, program analysis for improvements, and records retention. Examples of data that USG and its institutions may need to collect in connection with the lawful bases are: name, email address, IP address, physical address or other location identifier, photos, as well as some sensitive personal data obtained with prior consent.

Please note that individual USG institutions may have their own EU GDPR privacy notices and policies posted on their websites.

Most of USG's (including its institutions') 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 USG or third parties in providing education, employment, research and development, community programs.
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 USG 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.

Types of Personal Data collected and why

USG and its institutions collect a variety of personal and sensitive data to meet one of its lawful bases, as referenced above. Most often the data is used for academic admissions, enrollment, educational programs, job hiring, provision of medical services, participation in research, development and community outreach. Data typically includes name, address, transcripts, work history, information for payroll, research subject information, medical and health information (for student health services, or travel), and donations.
If a data subject refuses to provide personal data that is required by USG or one of its institutions in connection with one of its lawful bases to collect such personal data, such refusal may make it impossible for USG or its institutions to provide education, employment, research or other requested services.

Where USG gets Personal Data and Special Categories of Sensitive Personal Data

USG and its institutions receive personal data and special categories of sensitive personal data from multiple sources. Most often, this data comes directly from the data subject or under the direction of the data subject who has provided it to a third party (for example, application for admission to a USG institution through use of a common application).

Individual Rights of the Data Subject under the EU GDPR

Individual data subjects covered by the EU GDPR (http://www.policylibrary.gatech.edu/legal/eu-general-data-protection-regulation-compliance-policy) will be afforded the following rights:

- information about the controller collecting the data
- the data protection officer contact information
- the purposes and legal basis/legitimate interests of the data collection/processing.
- recipients of the personal data
- if USG or one of its institutions intends to transfer personal data to another country or international organization
- the period the personal data will be stored
- 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
- the existence of the right to withdraw consent at any time
- the right to lodge a complaint with a supervisory authority (established in the EU)
- why the personal data are required, and possible consequences of the failure to provide the data
- the existence of automated decision-making, including profiling
- 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. Any data subject who wishes to exercise any of the above-mentioned rights may do so by making such request at GDPR@usg.edu.

Cookies

Please see the description above of "cookies" within the Privacy Policy, which is incorporated and applies equally here in regard to the EU GDPR.

Security of Personal Data subject to the EU GDPR

All personal data and special categories of sensitive personal data collected or processed by USG must comply with USG Cybersecurity Plan, as authorized by the Board of Regents Policy Manual Section 10.4 Cybersecurity: https://www.usg.edu/policies. Anyone suspecting that his or her sensitive personal data has been exposed to unauthorized access, report your suspicion to helpdesk@usg.edu. Otherwise, questions concerning GDPR can be forwarded to GDPR@usg.edu.

We will not share your information with third parties except:

- as necessary to meet one of its lawful purposes, including but not limited to,
- its legitimate interest,
- contract compliance,
- pursuant to consent provided by you,
- as required by law;
- as necessary to protect USG and/or its institutions' interests;
- with service providers acting on our behalf who have agreed to protect the confidentiality of the data.

Georgia Open Records Act

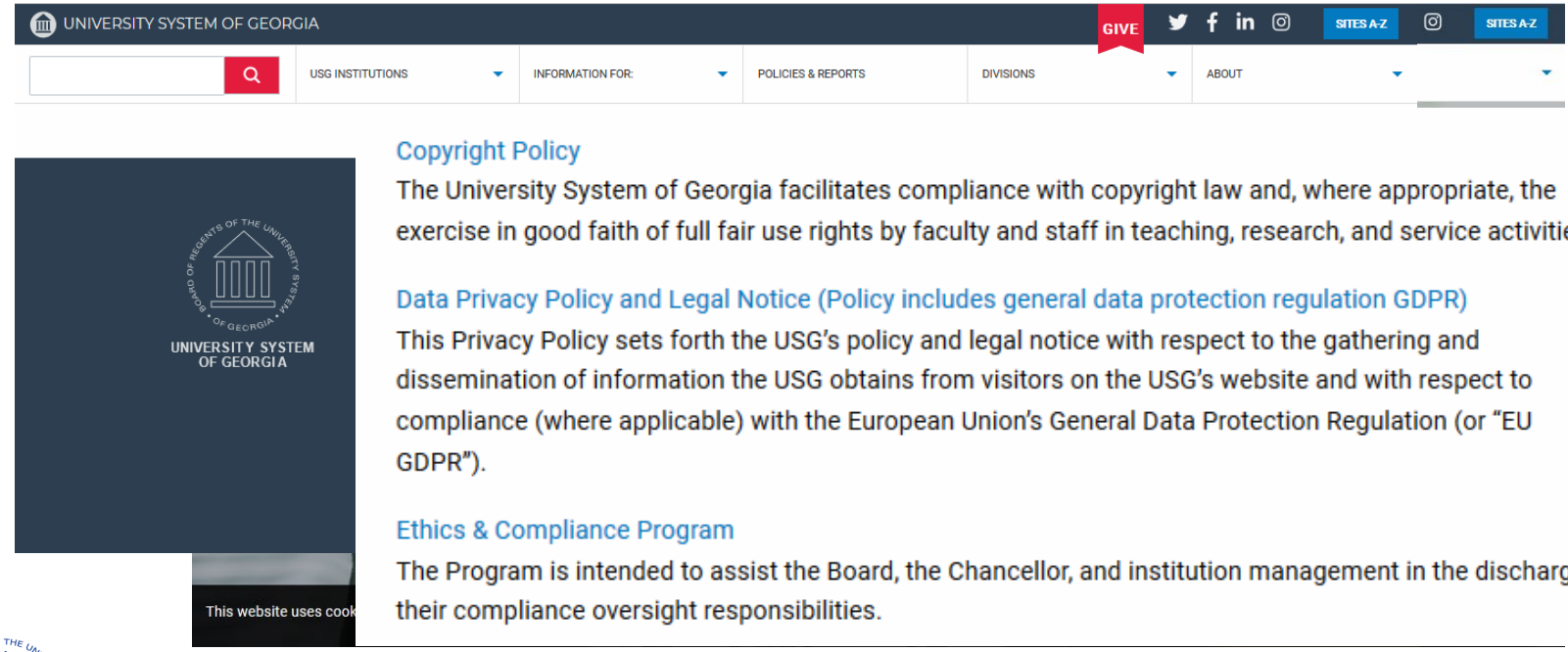
As an entity of the government of the State of Georgia, the USG and its institutions are subject to the provisions of the Georgia Open Records Act (ORA) (http://legal.gatech.edu/sites/default/files/images/1861f5609r1.pdf). Except for those records that are exempt from disclosure under the ORA, the ORA provides that all citizens are entitled to view the records of state agencies on request and to make copies for a fee.

Data Retention

USG and its institutions keep the data it collects for the time periods specified in the University System of Georgia Records Retention Schedules: https://www.usg.edu/records_management/schedules/.

STEP 2

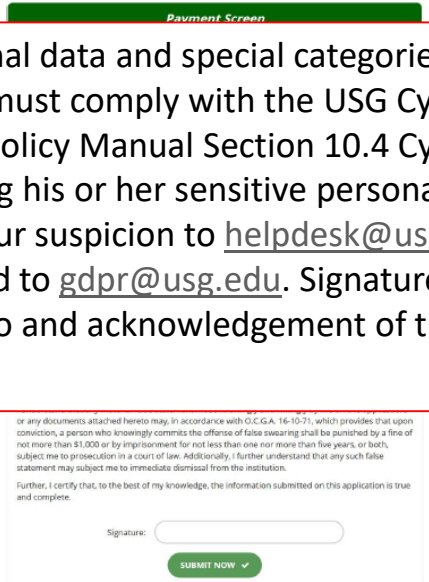
USO Website Compliance

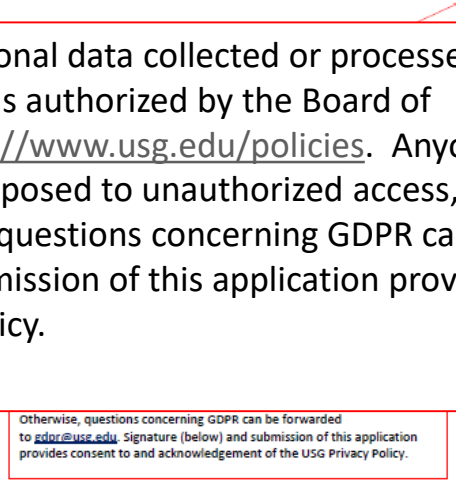


STEP 3

Student and Employee Application Compliance

All personal data and special categories of sensitive personal data collected or processed by the USG must comply with the USG Cybersecurity Plan, as authorized by the Board of Regents Policy Manual Section 10.4 Cybersecurity: https://www.usg.edu/policies. Anyone suspecting his or her sensitive personal data has been exposed to unauthorized access, report your suspicion to helpdesk@usg.edu. Otherwise, questions concerning GDPR can be forwarded to gdpr@usg.edu. Signature (below) and submission of this application provides consent to and acknowledgement of the USG Privacy Policy.





STEP 4

Data Management Review

- Where are data entry points
- Where are data stored
- How data is managed
- How data is purged

Develop processes and procedures to fulfill a request

USG Institution Websites (Homepage, HR, Admissions)

UNIVERSITY SYSTEM OF GEORGIA

Georgia Tech's Steps Towards Compliance

Zachary Hayes
Enterprise Data Management
Georgia Institute of Technology

Georgia Tech's Compliance Toolbox

Internal Collaboration

- Working Group (Legal Affairs, Ent. Data Mgmt., Cyber Security, Risk Mgmt.)
- SharePoint website

External Resources

- EU GDPR Compliance Policy
- Updated Privacy & Legal Notice
- EU GDPR website
  - Georgia Tech Compliance
  - Individual Rights
  - Questions/Support email address

Steps Towards Compliance

- Education
- Lawful Basis questionnaire
- Unit Privacy Notice template
- Consent Form template
- Legal Affairs review
- Cyber Security audit (NIST 800-171)
- Procedures manual
  - Executing Individual Rights
  - Withdrawing Consent
- Rinse and Repeat!

UNIVERSITY SYSTEM OF GEORGIA

Panel Question & Answer