European Union General Data Protection Regulation

- Part One: GDPR Basics
- Part Two: How the GDPR Affects Specific Areas
- Part Three: How to Update Tennessen Warnings for GDPR
- Part Four: Compliance Efforts
Part One: GDPR Basics
What is the GDPR?

- The GDPR is a Regulation of the European Union ("EU") governing the privacy and protection of data of natural persons located in EU member states.
- It went into effect on May 25, 2018, in all current EU Member States, including the United Kingdom; the European Community states (Norway, Iceland, Lichtenstein), and Switzerland.
- It applies to any person located in the EU.
- Tied to location, not citizenship.
What does the GDPR protect?

- The GDPR protects personally identifiable data of persons located in the EU.
- The data protected by the GDPR includes educational data, financial data, employment data, health data, location data, and photographs.
- This also includes de-identified data such as IP addresses and metadata if Minnesota State has legal access to other data that can connect to an individual’s identity to the de-identified data.
What is “sensitive data” according to the GDPR?

• The GDPR places additional restrictions on “sensitive” data, including:
  – data revealing racial or ethnic origin,
  – data revealing political, religious, or philosophical beliefs,
  – data revealing trade union membership,
  – identifying biometric or genetic data,
  – health data, and
  – data concerning sexual orientation or sex life.
Does the GDPR apply to Minnesota State?

- Yes, the GDPR applies to the extent that our colleges and universities collect, store, and process data on individuals located in the EU.
- The GDPR applies to any entity that collects, stores, or processes the data of persons located in the EU regardless of where that entity is located.
How can Minnesota State use data under the GDPR?

- For most data, Minnesota State needs either specific, revocable consent of the data subject, a contractual relationship with the data subject, a potential contractual relations with the data subject, or other appropriate authority.

- The GDPR places additional restrictions on “sensitive” data. Generally, sensitive data may only be used with specific, revocable, consent or to protect the vital interests of the data subject.
Deletion Requests

• The GDPR gives data subjects a right to request that an entity delete data it stores on that data subject.
• The right to erasure, or “right to be forgotten” is not absolute.
• If a campus has to keep data in order to comply with legal requirements (e.g. record retention) or fulfill the terms of a contract (e.g. admission or employment), it does not have to grant requests to erase data.
• The best practice is not to archive data that campuses no longer need for a legal or business purpose.
Data Breaches

• The GDPR requires 72 hour notice of the unauthorized disclosure of data if that data could be used to harm that individual (e.g. financial data, social security numbers, etc.), if such notice is reasonable.

• The notice goes to the regulatory agency of the nation where the affected individuals were located at the time of the breach.

• If you suspect a data breach affecting an individual located in a GDPR state when the breach occurred, please contact our Office and System Office IT Security.
Consequences of Failure to Comply with the GDPR

- Lawsuits by individuals located in Europe
- Regulatory fines and penalties
- Public relations and reputational risk
Who on our campus may have GDPR compliance obligations?

• Data Practices Compliance Officers
• International Programs Officials (International Student Issues)
• CIO’s (IT Security Concerns)
• CHRO’s (Hiring and Employee Travel)
• CFO’s (Contract Issues)
• Academic and Student Affairs (Applications)
• Alumni Relations (Solicitations)
Part Two: GDPR and Specific Areas
Students Affected by the GDPR

- Students on study abroad in Europe
- International students during semester breaks
- European applicants
- Prospective students in Europe
- Students on other school sponsored trips in Europe
Complying with the GDPR Regarding Students

• Updating travel waivers to account for GDPR (e.g. specific consent for health data, disciplinary data, contractual obligations)
• GDPR location check for international students affected by data breaches while home in Europe
• More specific warning for applicants
Employees Affected by the GDPR

- Faculty visiting European institutions
- Long-term located employees
- Employees leading official programs such as study abroad
- Employees engaging in collaborative research projects
Complying with the GDPR regarding employees

- Updated employee travel waiver
- Closer review of research contracts for GDPR considerations
- Special attention to long-term staff abroad
Updated Travel Waivers for Students and Employees

• Located on the Office of the General Counsel’s Website through SharePoint.

• Updates include:
  – Specific consent to use health data to protect vital interests
  – Specific consent to utilize data while a student or employee is abroad
GDPR and Contracts

- Contract addendum requests from current vendors
- GDPR terms in new contracts
- Contracts for operations in Europe
The GDPR requires “privacy by default” and “privacy by design.”

Minnesota State has developed a data classification program to govern how the colleges and universities maintain public, restricted, and highly restricted data.

Contracts with third parties are reviewed for data security concerns.
The data that colleges and universities collect from their websites may create GDPR compliance obligations if that data is 1) identifiable, including in aggregate, and 2) on persons located in Europe.

It is important to update Tennessen notices when collecting data if the colleges and universities are actively collecting data from persons located in Europe.

Additionally, the colleges and universities should have a full understanding of what data they are automatically collecting on their websites.
GDPR and Alumni

• The colleges and universities need to give European-based alumni the option to “opt-in” to solicitations rather than the option to “opt-out.”
• The colleges and universities should provide updated Tennessen notices as well.
Research projects involving persons located in the European Union need to be monitored to make sure that appropriate consent is granted.

The rules of informed consent may be different under the GDPR in some circumstances than the default rules in the United States.

Additionally, research contracts with European partners may require terms and conditions addressing GDPR compliance.
GDPR and Direct Services

• Direct services, such as enrolling students located in the EU in online classes, require special attention to GDPR compliance obligations.

• If your college or university is enrolling European students in online programs who are not F-1, J-1, or M-1 students based in the United States, please contact our Office.
Part Three: GDPR Updates for Tennessen
Warnings
Collection of Private Data: The Tennessen Warning Rule

• Minnesota Government Data Practices Rule
• When individuals are asked for private data about themselves (not supervisory inquiries) you must give a notice called a “Tennessen Warning.”
  – Why you are collecting the information, how information will be used;
  – Who will have access to the information;
  – Whether individual is legally required to provide the information;
  – Consequences of providing or refusing to provide the information.
Tennessen Warnings and GDPR

• Updates are required to collect data on persons located in Europe.

• Examples include:
  – Applications
  – Alumni solicitations (opt-in rather than opt-out)
  – Online information forms
  – Data collected for research purposes

• Some of this information can be provided through a standardized form or policy posted online.
The Reason You are Collecting the Data

• The reason identified must now meet one or more of the following standards for data collected from persons in Europe:
  – Fulfilling contractual obligations between the College/University and the data subject. This may include study abroad agreements, student codes of conduct, terms and conditions of employment, website terms of use, and any other contractual relationship with the data subject.
  – Consent of the data subject. The GDPR defines valid consent as written, “freely given” (i.e. not tied to a good or service), and revocable.
  – Compliance with a European legal obligation.
  – Necessary to protect the “vital interests” of the data subject or another natural person.
  – The data is necessary to perform a task carried out in the “public interest.”
  – The data is necessary for the legitimate interests of the data processor after taking into consideration the data subject’s rights to the data.
How you Plan on Using the Data

• This should include the following:
  – A clear description of how the College/University will use the data, specifically tailored to the purpose stated above.
  – An assurance that the College/University will not use the data for any other purpose.
  – A link to the appropriate records retention policy governing the data.
  – A link to the right to ask for corrections set forth in Minnesota Statutes Section 13.04 Subd. 3.
  – A link to the College/University’s data privacy related policies.
  – A notification that the data subject has the right to ask College/University to delete the data subject’s data. The College/University does not have to comply with such a request if it still needs the data for a legal or contractual purpose.
  – A notification that the data subject can avail themselves of the dispute procedures set forth in Minnesota Statutes Section 13.08 and any other legal dispute rights they have by virtue of the laws of the United States of America and any other jurisdiction.
Requirements and Consequences

• Whether the person is legally required to provide the data or may refuse to do so.
• Consequences if the person provides the data.
• Consequences if the person does not provide the data.
• The identities of people and entities that have access to the data by law.
  – All notices should include that data may be shared upon court order or provided to the state or legislative auditor.
  – Any potential public “recipients” should be listed here.
• Campuses should list contact information for the Data Practices Compliance Official.
Part Four: Compliance Efforts
Compliance Generally

- Use updated student and employee travel waivers when students and/or employees are traveling to GDPR states
- Update Tennessen notices when collecting data on persons located in the EU
- Follow data privacy best practices
- Work with the Office of General Counsel on data breaches affecting persons located in the EU or data deletion requests
- Don’t panic – the GDPR is just another compliance regime to be worked through.
GDPR Compliance Portal

- http://www.minnstate.edu/system/ogc/index.html
- Follow link to “data privacy.”
- Follow link to “European Union General Data Protection Regulation (GDPR) SharePoint Compliance Portal”
- Login to SharePoint with Star ID and Password
Contact Information

Daniel G. McCabe
Assistant General Counsel
Office of the General Counsel
–
Minnesota State
30 East 7th Street, St. Paul, MN 55101
o: 651-201-1833  |  f: 651-296-6580  |  daniel.mccabe@minnstate.edu