European Union General Data Protection Regulation (GDPR)

Northwestern
Agenda

• Welcome & Introductions

• What is GDPR and how may it impact the University

• Plan of action

• Your role

• Next steps
The GDPR Team

Project Team:

Marcia Isaacson (Compliance)
Priya J. Harjani (Office of General Counsel)
Tom Murphy (Northwestern IT)

Working Group:

Ann K Adams (Research)
Pamela S Beemer (Human Resources)
Carl J Cammarata (Feinberg School of Medicine)
Jacqualyn F. Casazza (Registrar)
Mike Daniels (ASRSP)
Janet L. Dobbs (Global Marketing)
Melanie Earle (Compliance)
Luke Figora (Risk Management)
Celina A Flowers (Provost)
Julie Anne Friend (Global Safety & Security)
Karey Fuhs (Undergraduate Learning Abroad)
Lester Greenman (NUIT)
Heather Harlan (Investments/Real Estate)
Amy Lammers (Admissions)
Kathleen E. Murphy (Research)
Heather Ruggio (Alumni Relations and Development)
Ravi S Shankar (International Office)
Kelly Stack (Global Marketing and Communications)
Sara West Tully (Undergraduate Learning Abroad)
Elements of the Regulation

• Principles relating to the processing of data (Art 5-11)

• Rights of the data subject (access to personal data, rectification and erasure) (Art 12-23)

• Responsibilities of Controller and Processor (maintaining records, security, breach notification, data protection officer) (Art 24-43)

• Transfers of personal data to third countries (ensuring 3rd country compliance) (Art 44-50)

• Remedies, liability, and penalties (Art 77-84)

• Specific processing situations (historical or scientific research, journalistic purposes, academic artistic or literary expression, statistical purposes) (Art 85-91)
The Regulation

• Goal of the GDPR: To harmonize the regulations and protections for individuals with respect to data processing and to safeguard the free flow of information between member states of the European Union (EU).

• Principles:
  • Personal data shall be processed lawfully, fairly and in a transparent manner
  • Collected for specified, explicit, and legitimate purpose and not further processed in a manner that is incompatible with that purpose
  • Limited to what is necessary in relation to purpose processed
  • Accurate and kept up to date
  • Kept for no longer than needed
  • Processed in a manner that ensures appropriate security

• There are special rules for processing special categories of personal data, such as racial or ethnic origin, political options, religious or philosophical beliefs.

• There is an exception for research (Article 89 (2))

• Sanctions: Fines up to 20M Euros or 4% of annual worldwide turnover.

• GDPR enforcement will begin May 25, 2018.

• Regulation can be found at: https://gdpr-info.eu
Jurisdiction

• The GDPR applies to the processing of personal data in the context of activities of an establishment of a controller or a processor in the EU, regardless of whether the processing takes place in the Union or not.

• The GDPR applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union; where the processing activities are related to:
  • The offering of goods or services irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
  • The monitoring of their behavior as far as their behavior takes place within the Union.
Definitions (Article 4 GDPR)

- **Personal Data**: Any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural 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, physiological, genetic, mental, economic, cultural or social identity of that natural person.

- It can include anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address.

- **Processing**: Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

- **Controller**: The person, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

- **Processor**: The person, agency or other body which processes personal data on behalf of the controller.
Examples of Northwestern Activities that might be subject to the regulation

- **Students**: Soliciting and receiving applications for admission; payment of tuition; study travel to EU as part of a program
- **Research**: Data collected directly or indirectly (from third parties or through data sets) about persons located (permanently or temporarily) in the EU
- **Faculty**: Collaborations with EU institutions or faculty
- **Employment**: Recruitment of faculty or staff in EU; employment of persons in EU on permanent or temporary basis
- **Fundraising**: Soliciting or receiving donations from persons in EU
- **Online learning** platforms/online education
- **Websites**: capturing information about people living in EU/cookies
- **Processing of data** by NU for controllers or processors located in the EU
- **Marketing**: NU apps or other goods and services to persons in the EU
Northwestern GDPR Project: Goal and Approach

**Goal:** Northwestern University will review GDPR requirements, and develop a risk-based compliance strategy and corresponding compliance program.

**Approach:**

- **People**
  - Engage the right stakeholders, document GDPR roles & responsibilities

- **Policy**
  - Provide privacy statements and supporting templates & documentation

- **Process**
  - Assess and address processes in support of compliance

- **Technology**
  - Identify possible technical solutions to further enable compliance
In Scope:
• Identify relevant GDPR requirements and prioritize key compliance components and activities, such as:
  • Identifying potential populations affected
  • Identifying potential functional/business areas affected
  • Identifying common elements and categories, with particular focus on special categories of personal information
  • Understanding the purpose and use of the data that is processed and identifying the legal basis for it
  • Identifying relevant data flows
  • Developing a GDPR data registry
  • Developing privacy statements, a privacy policy, and key compliance activities for impacted processes
• Identify other processes affected by GDPR and develop or update relevant documentation and processes
• Develop a website and toolkit to disseminate information and facilitate compliance
• Strive to identify potential GDPR compliance technical needs and/or solutions.
• Draft recommendations for a sustainable on-going GDPR compliance program

Out of Scope:
• Development and implementation of technical solutions to address GDPR requirements
Project Activities

**Working Group Participation**
- Actively participate in all-stakeholder (or break away group) meetings and contribute to the progress of the project
- Provide input to the design of ongoing GDPR program
- Review regular status reports and stay informed of project developments
- Serve as a on-going GDPR liaison for your part of the organization

**Process & document development and review**
- Identify data flows potentially regulated by GDPR
- Actively participate in working sessions to document and analyze processes in your organization that may be impacted by GDPR
- Utilize and take ownership of on-going processes and documentation developed by the project (data flow template, etc.)
## Next Steps

<table>
<thead>
<tr>
<th>Activities</th>
<th>Key Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Email to stakeholders, letting them know working group exists</td>
<td></td>
</tr>
<tr>
<td>• Distribution of data inventory questionnaire</td>
<td></td>
</tr>
<tr>
<td>• Analyze results of questionnaire, categorize data</td>
<td></td>
</tr>
<tr>
<td>• <strong>Develop small working groups to consider and address each category of data and other common issues</strong></td>
<td></td>
</tr>
</tbody>
</table>

Schedule monthly working group sessions

Develop a website and toolkit to disseminate information and facilitate compliance

Review priority project work (ex: mapping data flows for data registry)

Identify other potential stakeholders
Questions and Answers