Don’t Bite Off More Than You Can Chew: 
Taking a Risk-Based Approach to GDPR Compliance 
and Key Tools to Help You Get There

Presenters

Megan Stoll
Assistant University Counsel
Office of University Counsel
University of Illinois System

Dave Grogan
Associate Director of University Compliance
University Ethics & Compliance Office
University of Illinois System
What we will talk about today.

Why we care about a European regulation

A risk-based approach to tackling the GDPR

Tools to kick-start your GDPR efforts

Why we care about a European regulation
GDPR is a comprehensive regulation protecting the personal data of certain natural persons.

What does it protect?
- **Personal data (PD)** – any information relating to an identified or identifiable natural person (if someone, somewhere, has a key to re-identify data, it is protected)

When is it effective?
- **Now!** (since 5/25/2018)

Why do we care?
- **Steep fines:** Up to €20 million or 4% of global revenue (whichever is greater)

### Key Terms
- **Controller** – person or entity that determines the purposes and means of the processing of PD
- **Processor** – person or entity that processes PD on behalf of controller
- **Processing** – any operation or set of operations performed on PD or sets of PD (e.g., collection, recording, storage, use)

The GDPR is the law of the land in the European Economic Area (EEA).

EEA = EU + Iceland + Liechtenstein + Norway

- The European Union (EU) consists of 28 countries
- UK is keeping GDPR regardless of Brexit
The GDPR may apply to your university even though it is established outside the EEA.

**Applicability (a.k.a. jurisdictional reach)**

- **Controller or processor outside the EEA**
  - Offering of goods or services (even if free) to persons in the EEA
  - Monitoring of behavior (including online activity) of persons in the EEA

- **Controller or processor inside the EEA**
  - Any processing of personal data of persons anywhere in the world

- **E.g., admission, participation in clinical trial; study abroad**
- **E.g., through wearable devices, cookies and other trackers**

The GDPR gives data subjects a number of rights.

- **Notice** (Art. 13 & 14)
- **Access** (Art. 15)
- **A copy** (Art. 15)
- **Correction** (Art. 16)
- **Completion** (Art. 16)
- **Erasure** (Art. 17)

- **Restriction** (Art. 18)
- **Notice of changes to recipients** (Art. 19)
- **Portability** (Art. 20)
- **Object** (Art. 21)
- **No decisions based solely on automated processing** (Art. 22)

It's like HIPAA and FERPA on steroids
The GDPR restricts processing and transferring PD.

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Special category PD</strong></td>
<td>Need <em>explicit consent</em> to process</td>
</tr>
<tr>
<td>• Data revealing <strong>racial</strong> or <strong>ethnic</strong> origin, <strong>political opinions</strong>, <strong>religious</strong> or <strong>philosophical</strong> beliefs, or <strong>trade union membership</strong></td>
<td></td>
</tr>
<tr>
<td>• <strong>Genetic</strong> data, <strong>biometric</strong> data for the purpose of uniquely identifying a person</td>
<td></td>
</tr>
<tr>
<td>• <strong>Health</strong> data</td>
<td></td>
</tr>
<tr>
<td>• Data concerning a person’s <strong>sex life</strong> or <strong>sexual orientation</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Criminal convictions</strong></td>
<td>Generally cannot process at all</td>
</tr>
<tr>
<td><strong>Transferring PD</strong></td>
<td>Generally requires a <strong>data protection agreement (DPA)</strong> to transfer to another controller or processor</td>
</tr>
</tbody>
</table>

**A risk-based approach to tackling the GDPR**
We took a risk-based approach to GDPR compliance.

**Method**
Created a team with Privacy & Information Security Officers, University Counsel, and stakeholders at each university to augment existing policies and procedures and facilitate GDPR compliance.

We charted a 3-phase approach to GDPR compliance.

**Phase I**
- Read the GDPR!
- Initial risk assessment
- Stakeholder meeting
- Stakeholder survey
- Initial working groups
- Implement baseline measures

**Phase II**
- Expanded working groups
- Foundation and Alumni Alliance
- Address department webpage specific notice and consent requirements
- Outreach and training

**Phase III**
- Policy and procedure development and alignment
- Governance and oversight mechanism
- Complete open items from Phase II
Our initial risk assessment determined that the following units were potential GDPR stakeholders:

- Alumni relations
- Dean of Students
- Financial Aid
- Foundation
- Graduate admissions
- Healthcare
- Housing

- HR
- Information technology (including website design)
- International programs
- Marketing
- Online learning

- OVCR and PIs
- Payroll & employee benefits
- Purchasing
- Registrar
- Undergraduate admissions

*This is not a comprehensive list.

We held an initial System-wide stakeholder meeting to help coordinate our GDPR efforts.

- We invited representatives from every stakeholder and held the meeting via Skype
- We provided an overview of the GDPR to create a baseline level of understanding and gave everyone access to a GDPR resource folder in Box
- We told stakeholders what was coming and that we needed their help
We asked units to complete a survey to identify the scope of potential GDPR impact.

We tailored a NACUA / University of Chicago survey for our 3 universities.

We used distribution of the survey to create awareness at the dean level.

We received over 80 responses from a wide range of colleges, departments, and units.

We now appreciate the GDPR covers more than just people in the EU.

European Union (EU) General Data Protection Regulation (GDPR) Survey

Beginning on May 25, 2018, some University of Illinois units and departments will experience an expansive EU data privacy regulation known as the EU GDPR. The regulation, as defined in the GDPR, applies to institutions or entities that control or process personal data about individuals who are in the EU. There are significant fines for noncompliance.

The GDPR defines personal data as “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.”

If you are storing, processing, or otherwise using any personal data of individuals in the EU, we need to understand how and why and make sure we comply with the GDPR when it applies.

To help determine whether the GDPR applies to your unit/department, please complete the following survey (one survey per unit/department). If necessary after assessing your responses, we will contact the person you designated below as your point of contact to set up a time to discuss the information you provide and to help develop a more detailed plan to comply with GDPR requirements.

Immediate / Visible Impact

- Supplemental Privacy Notice
- Cookie Banner
- Website notice / consent on priority websites

Working Groups:

- Admissions
- Distance learning
- International
- Contracts
- Security
- Research
- HR

Drumbeat Meetings

- Bi-weekly / monthly / quarterly meetings to drive effort
- Develop GDPR implementation milestones for overall GDPR effort and working groups
- Maintain formal meeting agendas and meeting notes to show progress and due diligence

University of Illinois System
Tools to kick-start your GDPR efforts

Unless otherwise noted, the following tools are available in Box. Email GDPRrequest@uillinois.edu from your .edu address for access.

These tools do not constitute legal advice. Legal questions should be directed to your institution’s legal counsel.

We welcome feedback/improvements!
Develop an implementation roadmap to guide your way.

- Identify priority tasks, establish due dates, and assign responsibility
- Give working groups concrete guidance
- Include stakeholders and subject matter experts on working groups; make sure both participate in meetings

Your GDPR Magna Carta – Explaining how your institution addresses the GDPR.

- Most important programmatic element
- Deployed to all university websites via the U of I standard privacy notice

Explains what personal data we process, the legal basis, how we share personal data, and identifies data subjects’ rights and how to exercise them
A cookie-banner can be the most visible evidence of good-faith efforts to promote privacy.

- Initially deployed cookie banner only to GDPR priority websites
- Once we worked out implementation issues, expanded to all our websites
- We use commercial vendor but your web developers may be able to produce in-house

For study abroad in the EEA, request travelers’ consent before they leave to process their special category data.

- Personal data collected in the U.S. before departing is not subject to GDPR
- Personal data may need to be sent back to your university once students & faculty are in the EEA
- Examples include health and conduct related information
- Request students and faculty provide consent before leaving U.S.
- The notice & consent form we developed is loosely based on a NACUA template
- Our form is available in Box

Click on the image of the form to access it in Box.
Research may be your most significant GDPR risk, so it is worth investing time and effort into compliance.

In these situations, PIs need to determine whether the GDPR applies.

1. Primary data collected from persons physically located in the EEA
2. Secondary data about persons in the EEA previously collected by the PI for other research or by other persons or units at the university
3. Secondary data obtained by PI from entity in EEA about individuals located anywhere
4. Data will be scraped from accounts or websites of persons or entities in EEA
5. Collaborating researchers/parties in EEA are providing their personal data
6. Personal data collected by any of the above methods will be shared outside the university

We developed a flowchart you can adapt to address the 6 situations where a PI must determine if the GDPR applies to research data.

Part I - Will PI collect Personal Data (PD) directly from persons in the EEA?

The 6-part flowchart is available in Box.
The flowchart helps determine if the GDPR applies and what notice / consent and data protection agreements are required.

You can use the flowchart to develop an online tool specific to your institution’s research portfolio.

- Allows PI to self-assess whether GDPR applies
- Identifies required notice & consent templates
- Identifies required DPA templates
- Creates a printable report
- Works on desktop and mobile devices
- Demo only – not sharable

All templates are available in Box.
GDPR rights requests will come, so you need to have a procedure ready to address them.

University of Illinois has received over 40 “right to be forgotten” requests from deseat.me citing Article 17 of the GDPR

We developed procedures for handling the requests, building on existing FERPA and HIPAA procedures

Working with Registrar’s Office, we developed a form to help confirm requestor’s identity under Article 12 before initiating a records search

Promote GDPR awareness and train your employees so that they know what to do.

Website

• A GDPR website can guide people to resources
  • The University of Illinois GDPR website has both public & password-protected pages
  • A GDPR website likely will be the 1st stop for employees searching for how your institution addresses GDPR

Email

• Use emails to target various constituencies
  • We use messages from senior executives to convey the importance of GDPR to a wide audience

Presentations

• Live, targeted presentations are very effective for promoting awareness at all levels of the organization
  • We use area-specific presentations (e.g., research, contracts, IT, deans)
## Resources & Contact Information

<table>
<thead>
<tr>
<th>Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Unless otherwise noted, the tools from this presentation are available in Box</td>
</tr>
<tr>
<td>• Email <a href="mailto:GDPRrequest@uillinois.edu">GDPRrequest@uillinois.edu</a> from your .edu address for access</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Contact Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Dave Grogan</td>
</tr>
<tr>
<td>• <a href="mailto:dgrogan@uillinois.edu">dgrogan@uillinois.edu</a></td>
</tr>
<tr>
<td>• 217-300-1862</td>
</tr>
<tr>
<td>• Megan Stoll</td>
</tr>
<tr>
<td>• <a href="mailto:mjsoll2@uillinois.edu">mjsoll2@uillinois.edu</a></td>
</tr>
</tbody>
</table>

Disclaimer: Answers to legal questions often depend on specific facts, state and local laws, and institutional policies and practices. These PowerPoint slides and comments of the presenters do not constitute legal advice. Legal questions should be directed to your institution’s legal counsel.

**University of Illinois System**