

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



Higher Education Compliance Conference
9:45 – 10:45 a.m.
June 10, 2019

UNIVERSITY OF ILLINOIS SYSTEM

1

1

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

UNIVERSITY OF ILLINOIS SYSTEM

2

2

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

UNIVERSITY OF ILLINOIS SYSTEM

3

3

Why we care about a European regulation

UNIVERSITY OF ILLINOIS SYSTEM

4

4

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

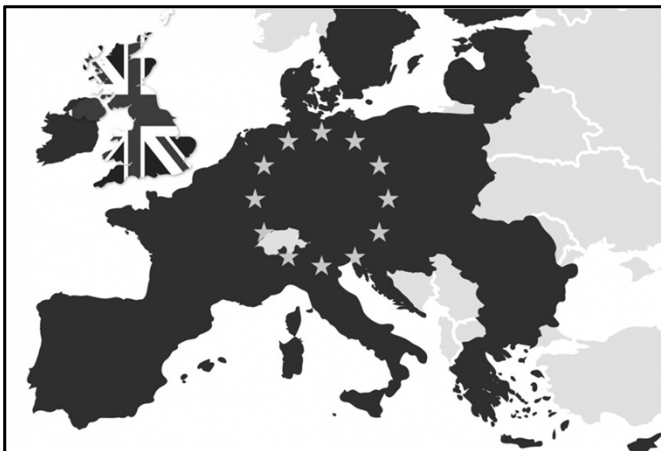
Processing – any operation or set of operations performed on PD or sets of PD (e.g., collection, recording, storage, use)

UNIVERSITY OF ILLINOIS SYSTEM

5

5

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

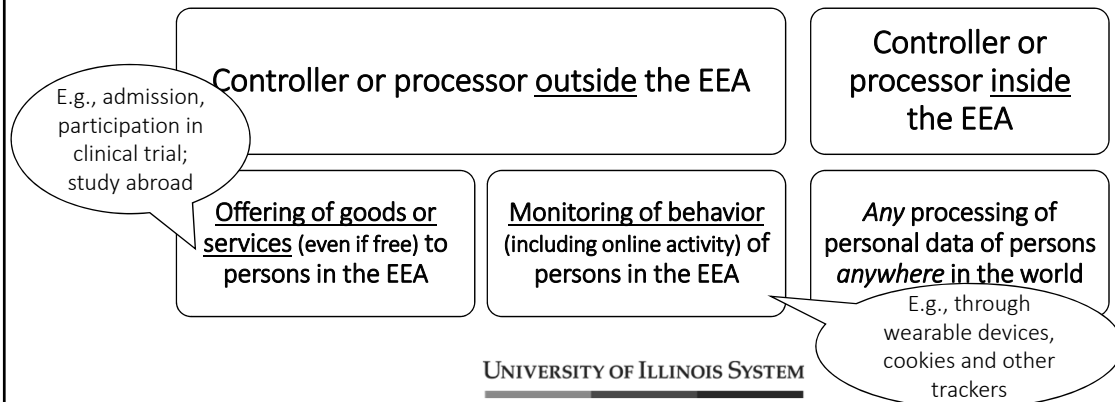
UNIVERSITY OF ILLINOIS SYSTEM

6

6

The GDPR may apply to your university even though it is established outside the EEA.

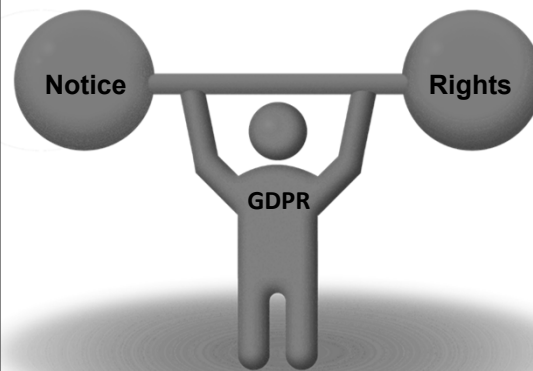
Applicability (*a.k.a.* jurisdictional reach)



7

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)



It's like HIPAA and FERPA on steroids

- **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)

UNIVERSITY OF ILLINOIS SYSTEM

8

8

The GDPR restricts processing and transferring PD.

Special category PD

Need **explicit consent** to process

- Data revealing **racial** or **ethnic** origin, **political opinions**, **religious** or **philosophical** beliefs, or **trade union membership**
- **Genetic** data, **biometric** data for the purpose of uniquely identifying a person
- **Health** data
- Data concerning a person's **sex life** or **sexual orientation**



Criminal convictions

Generally **cannot** process at all

Transferring PD

Generally requires a **data protection agreement (DPA)** to transfer to another controller or processor

UNIVERSITY OF ILLINOIS SYSTEM

9

9

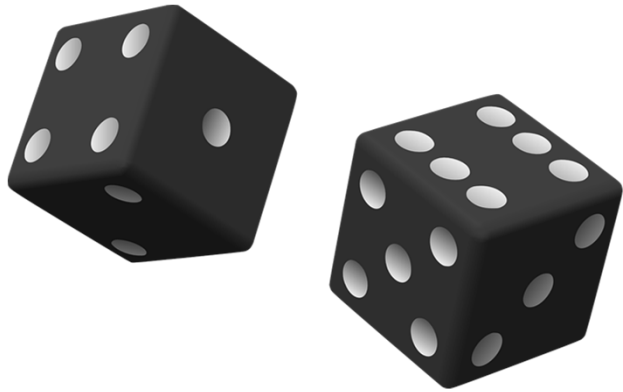
A risk-based approach to tackling the GDPR

UNIVERSITY OF ILLINOIS SYSTEM

10

10

We took a risk-based approach to GDPR compliance.



Method

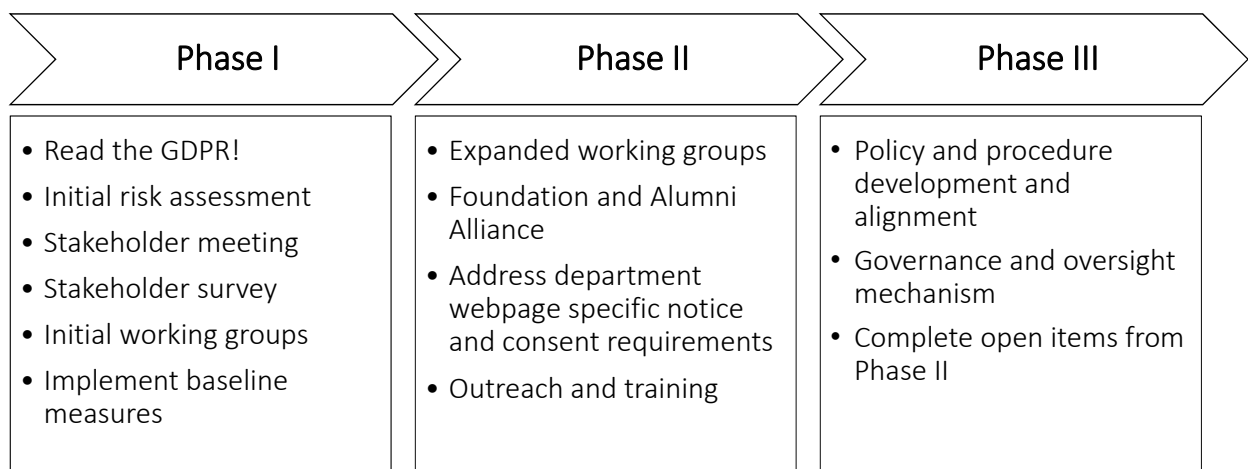
Created a team with Privacy & Information Security Officers, University Counsel, and stakeholders at each university to augment existing policies and procedures and facilitate GDPR compliance.

UNIVERSITY OF ILLINOIS SYSTEM

11

11

We charted a 3-phase approach to GDPR compliance.



UNIVERSITY OF ILLINOIS SYSTEM

12

12

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.

UNIVERSITY OF ILLINOIS SYSTEM

13

13

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

UNIVERSITY OF ILLINOIS SYSTEM

14

14

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

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

Beginning on May 25, 2018, some University of Illinois units are subject to the comprehensive EU data privacy regulation known as the EU GDPR. The regulation places obligations on persons 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 response, we will contact the person you designate 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.

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

UNIVERSITY OF ILLINOIS SYSTEM

15

15

Using the GDPR survey results, we refined our near-term GDPR approach.

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

Working Groups

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

Immediate / Visible Impact

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

UNIVERSITY OF ILLINOIS SYSTEM

16

16

Tools to kick-start your GDPR efforts

UNIVERSITY OF ILLINOIS SYSTEM

17

17

We have developed a number of GDPR tools that we are making available to you.



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!

UNIVERSITY OF ILLINOIS SYSTEM

18

18

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

EU GDPR Implementation Milestones

Milestone	Assigned To	Start Date	Due Date	Complete Date
1. Distribute surveys to all units that may be affected				
2. Sort survey responses by university				
3. Sort survey responses into 3 categories:				
a. Clearly applies (High Priority)				
b. May apply (Medium Priority)				
c. Does not apply (Low Impact)				
4. Form working groups based upon risk profiles				
a. Admissions				
b. Athletics				
c. Distance Learning				
d. International				
e. Security				
f. Research				
g. Risk				
h. Fundraising & Alumni				
5. Commence weekly drubstest meetings				
6. Review University of Illinois Web Privacy Notice				
7. Develop EU compliant privacy notice or supplemental notice				
8. Post to all university websites				
9. Review University of Illinois Web Content Policy				
10. Develop EU compliant consent checkboxes and/or banners for each webpage where personal information is collected				
a. Update all affected university websites				
11. Identify data subject rights				
a. Establish procedures for exercising them				
b. Create a policy/procedure document that can be adopted by all affected units				
12. Implement data subject rights procedures				
13. Complete training and awareness requirements				
a. Develop a plan to address requirements				
b. Develop required training				
c. Implement required training				
14. GDPR policy and procedure development and alignment				
15. Implement governance and oversight mechanisms				
16. Administrative Working Group				
a. Identify a chair or co-chairs for the Working Group				

Click on the image to access the draft roadmap [in Box](#).

19

19

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

UNIVERSITY OF ILLINOIS SYSTEM

EXECUTIVE VICE PRESIDENT/VICE PRESIDENT FOR ACADEMIC AFFAIRS

Organization Academic Affairs Programs Faculty Advisory Committee Resources RNSA UPPAC

VRRA - RESOURCES - WEB PRIVACY NOTICE

Supplemental Privacy Notice

This University of Illinois Supplemental Privacy Notice ("Supplemental Notice") supplements the University of Illinois Web Privacy Notice for certain persons in the European Economic Area ("EEA").

1. Commitment to protecting privacy and transparency

The Board of Trustees of the University of Illinois (the "University"), by and through its academic, research, and administrative units, is committed to respecting and protecting the privacy rights of persons in the EEA—comprised of the European Union ("EU") and the countries of Iceland, Norway, and Lichtenstein—pursuant to the EU General Data Protection Regulation ("GDPR"). This Supplemental Notice describes the University's commitment to the privacy of persons in the EEA.

2. Does this Supplemental Notice apply to me?

This Supplemental Notice applies to you if:

- You are a "Person" or "Data Subject"—meaning a natural person, not a corporation, partnership, or other legal entity—who is physically present in the EEA;
- It is with respect to your "Personal Information"—meaning any information relating to an identified or identifiable person—that is provided while you are physically present in the EEA;
- Such Personal Information is not earlier or later provided to the University while you are outside the EEA; and
- Such Personal Information is provided to the University:
 - During the course of the University offering you goods or services;
 - While the University is monitoring your behavior; or
 - While you are associated with any of the University's establishments in the EEA.

Please note that information pertaining to current, former, or prospective employment with the University in the United States is not considered

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

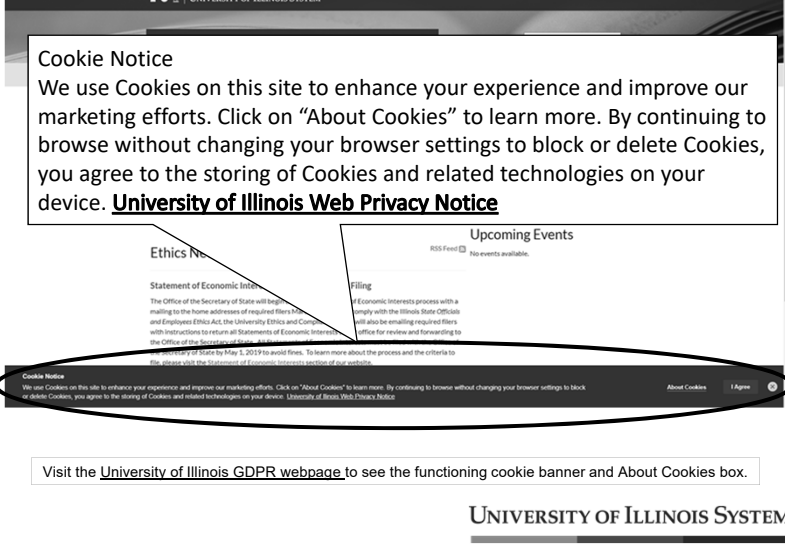
Click on website image to visit page

UNIVERSITY OF ILLINOIS SYSTEM

20

20

A cookie-banner can be the most visible evidence of good-faith efforts to promote privacy.



Visit the [University of Illinois GDPR webpage](#) to see the functioning cookie banner and About Cookies box.

- 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

21

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

Personal data collected in 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

EUROPEAN UNION GENERAL DATA PROTECTION REGULATION

ACKNOWLEDGMENT AND CONSENT

The University of Illinois (University) protects your privacy in accordance with U.S. law. In particular, the Family Educational Rights and Privacy Act (FERPA) prescribes your rights and the University's responsibilities with regard to your education records. The European Union (EU) General Data Protection Regulation (GDPR) may provide additional requirements for the University regarding the collection, use, and retention of your personal information you provide to the University, including its employees, which you are personally present in the EU during your study abroad experience.

The University may need to collect, use, and retain personal information from you, or from another entity you provide your personal information to, while you are in the EU, to ensure the study abroad program, including your safety; report with emergency or other law enforcement or emergency, law enforcement with law enforcement and other government institutions; and fulfill any other obligations for University that may have under University policy or applicable U.S. or EU law.

The University's legal basis for requesting your personal information while you are in the EU is that it is necessary for the performance of a contract between you and the University. However, certain special categories of information, such as information concerning your health, may require your consent before the University can process the information.

The University may share personal information that is collected from you while you are in the EU to the extent necessary to ensure your study abroad program. This may include sharing your personal information with education partners, contractors, or government officials on matters consistent with this notice, University policy, and applicable law. Personal information collected about you while you are in the EU may also be transferred to and retained by education partners, contractors, and University or government officials in the United States. Such transfers may be required for the performance of a contract between you and the University, which contract includes compliance with U.S. law.

If you are the victim of alleged perpetration of sexual or gender-based misconduct and/or of other criminal behavior while you are in the EU, the University will address the matter in accordance with University policy and applicable U.S. law (including but not limited to Title IX and the Clery Act). EU Member State authorities (e.g., the police) may also request under national Member State law.

Finally, with respect to personal data collected from you while you are in the EU, you have the rights of access, correction, deletion, restriction of processing, data portability, and objection. You can learn more about these rights and the circumstances under which they may be exercised by reading Article 15-20 of the GDPR ([https://gdpr.eu/article-15](#)). If you do not provide the personal information requested while you are in the EU, the University may not be able to carry out its obligations relating to your study abroad program.

Acknowledgment and Consent

I have read this notice and understand its contents. In addition:

_____ I acknowledge that the legal basis for the processing of my personal information may include that the processing is necessary for the performance of a contract between me and the University and that processing done in this basis will not be affected by my withdrawal of consent to processing.

_____ I consent to the collection, use, retention, and transfer to the United States of personal information concerning my health while I am in the EU for the purposes set forth in this notice.

_____ I consent to requests being made to appropriate University officials and/or emergency contacts if I am seriously ill or suffer an injury.

_____ I consent to the collection, use, retention, and transfer to the United States of my personal information, whether provided to me in a non-urgent situation relating to my health or otherwise, sexual or gender-based misconduct, or criminal behavior, when I am either the victim or alleged perpetrator.

_____ I understand that if the legal basis for the processing of my personal information is consent, I can withdraw my consent at any time, but doing so will not affect the processing of my personal information before my withdrawal of consent.

Facsimile signatures constitute original signatures for all purposes.

Print your name: _____ Date: _____

Signature: _____ Location at time of signature: _____

UNIVERSITY OF ILLINOIS SYSTEM

Request students and faculty provide consent before leaving U.S.

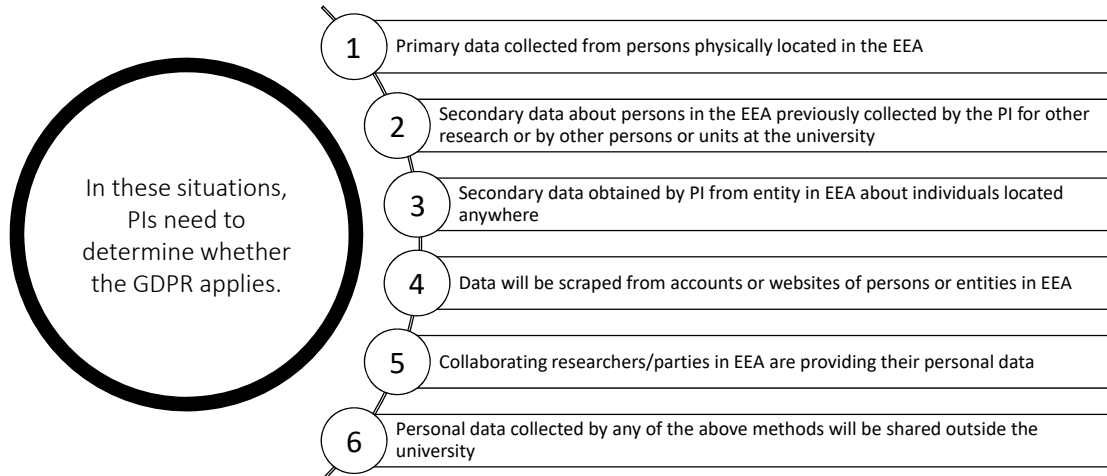
The notice & consent form we developed is loosely based on a NACUA template

Our form is available in [Box](#)

Click on the image of the form to access it in [Box](#).

22

Research may be your most significant GDPR risk, so it is worth investing time and effort into compliance.

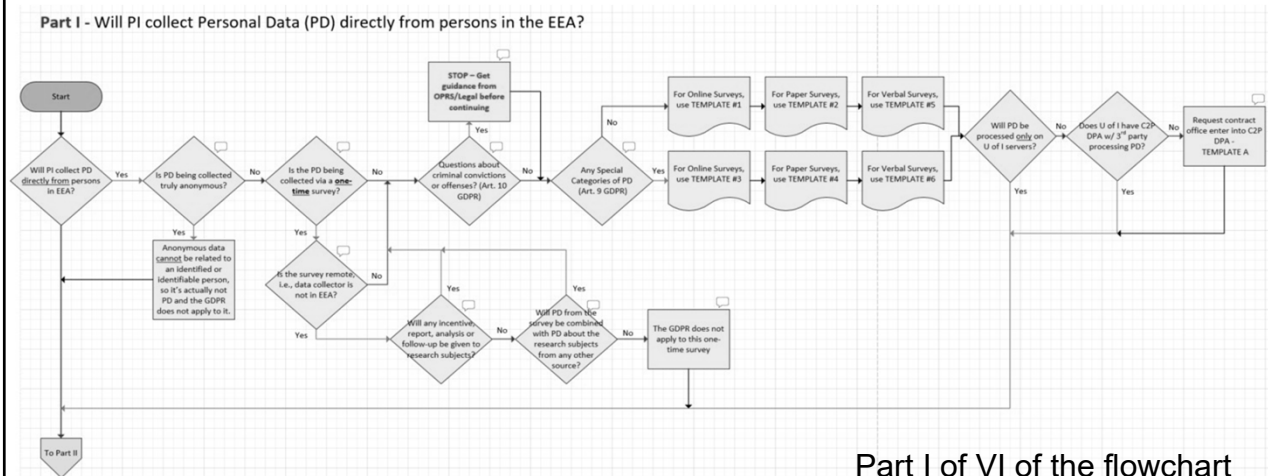


UNIVERSITY OF ILLINOIS SYSTEM

23

23

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



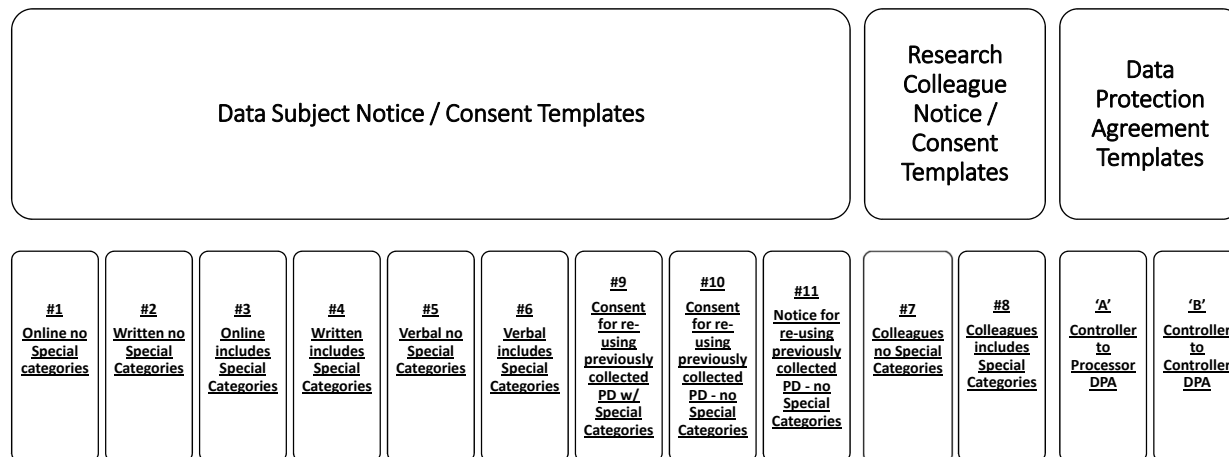
The 6-part flowchart is available in Box.

UNIVERSITY OF ILLINOIS SYSTEM

24

24

The flowchart helps determine if the GDPR applies and what notice / consent and data protection agreements are required.



All templates are available [in Box](#).

UNIVERSITY OF ILLINOIS SYSTEM

25

25

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

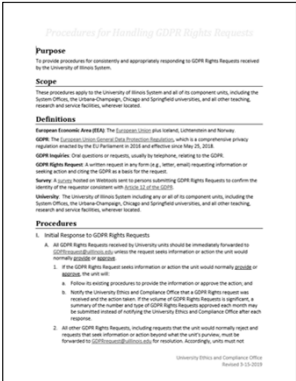
Demo only – not sharable

UNIVERSITY OF ILLINOIS SYSTEM

26

26

GDPR rights requests will come, so you need to have a procedure ready to address them.




Click on the image of the procedures to access them in Box.

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



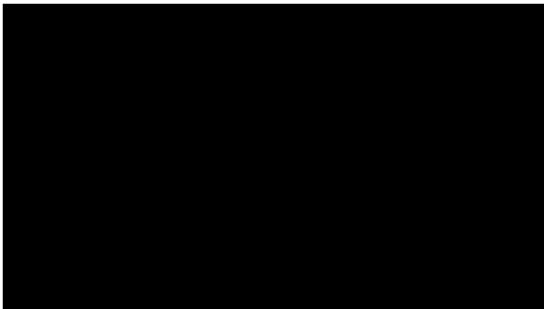
Click on the image of the identity confirmation form to access it in Box.

UNIVERSITY OF ILLINOIS SYSTEM

27

27

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



The [script for this video](#) is available in Box.

Website

- A GDPR website can guide people to resources
- The [U of I 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)

UNIVERSITY OF ILLINOIS SYSTEM

28

28

Resources & Contact Information

Resources

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



Contact Info

- Dave Grogan
 - dgrogan@uillinois.edu
 - 217-300-1862
- Megan Stoll
 - mjstoll2@uillinois.edu

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

29