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

Megan Stoll, Assistant University Counsel, Office of University Counsel
Dave Grogan, Associate Director, University Ethics & Compliance Office

November 9, 2018
This presentation will answer 3 questions:

What is the GDPR?

When does GDPR affect research at U of I?

What GDPR compliance tools does U of I have?
1. What is the GDPR?
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)
- Can apply to data controllers/processors outside the EEA
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)

Think HIPAA but for **ALL** personal data!

- 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)
GDPR restricts processing and transferring PD.

**Special categories of PD** – need **explicit consent** to process [Art. 9]
- 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 natural person
- **Health data**
- Data concerning a person’s **sex life** or **sexual orientation**

**Criminal convictions or offenses** – generally **cannot** collect this information at all [Art. 10]

**Transferring** personal data to another controller or processor generally requires a **data processing agreement (DPA)** [Art. 28]
2. When does GDPR affect research at U of I?
GDPR sometimes applies to data controllers and processors located outside the EEA, like U of I.

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

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

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

- **Controller or processor inside the EEA**
  - Any processing of personal data of persons anywhere in the world
  - E.g., through wearable devices, cookies and other trackers

- **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

E.g., participation in clinical trial; providing analysis of survey responses

**GDPR sometimes applies to data controllers and processors located outside the EEA, like U of I.**
<table>
<thead>
<tr>
<th>Scenario – If you want to:</th>
<th>Yes</th>
<th>No</th>
<th>Depends</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conduct an online survey involving research subjects worldwide</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Survey students from the EU while attending a psychology class in Urbana</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interview research subjects in Germany, Norway and Switzerland</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use personal data about Malaysians provided by a collaborating university in Italy</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Conduct a clinical study for a French pharmaceutical company using U.S. citizen research subjects</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data scrape the social media accounts of persons in the EEA for publicly available data</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
PIs should think about GDPR in 5 situations.

In these situations, PIs should use one of the tools that U of I has developed for determining whether GDPR applies.

1. Primary data collected from persons physically located in EEA
2. Secondary data obtained by PI from entity in EEA about individuals located anywhere
3. Data will be scraped from accounts or websites of persons or entities in EEA
4. Collaborating researchers/parties in EEA are providing their personal data
5. Personal data collected by any of the above methods will be shared outside of U of I
3. What GDPR compliance tools does U of I have?
U of I has various GDPR compliance tools.

- Flowchart
- Self-Assessment Online Tool*
- Template DPAs
- U of I GDPR website*
- Notice and consent templates

* Coming soon
U of I has developed 2 tools to help determine whether GDPR applies to your research.

- **Flowchart** available in Box

- **Self-Assessment Online Tool**
  - Online tool developed by OVCR’s Research Application Development team (*coming soon*)
Part I - Will PI collect Personal Data (PD) directly from persons in the EEA?

- Start
  - Will PI collect PD directly from persons in EEA?
    - Yes: Is PD being collected truly anonymous?
    - No: Is the PD being collected via a one-time survey?
  - No: Questions about criminal convictions or offenses (Art. 10 GDPR)
    - Yes: Any Special Categories of PD (Art. 9 GDPR)
      - Yes: For Online Surveys, use TEMPLATE #3
      - No: Will any incentive, report, analysis or follow-up be given to research subjects?
        - Yes: Will PD from this before be combined with PD about the research subjects from any other source?
          - No: The GDPR does not apply to this one-time survey
          - Yes: For Paper Surveys, use TEMPLATE #4
        - No: For Verbal Surveys, use TEMPLATE #5
          - Yes: Will PI be processed only on list of I serviers?
            - Yes: Does I of I have CDP, DPA or 3rd party processing PD?
              - No: Request contract office enter into CDP DPA
              - Yes: TEMPLATE A
            - No: To Part II

Part I of V of the flowchart
• Allows PI to self-assess whether GDPR applies
• Works on desktop and mobile devices
• Creates printable report
• Identifies required notice & consent templates
• Identifies required DPA templates
Self-Assessment Tool Report Example

You can choose to show all your answers or just the conclusions.

You can name the report.

You can add notes.

You can export the survey answers and conclusions to a spreadsheet.

Displays GDPR requirements for each part (other parts would appear below).

<table>
<thead>
<tr>
<th>Part 1 - Person in EEA</th>
<th>Part 2 - Entities in EEA</th>
<th>Data Scraping</th>
<th>Collaborators in EEA</th>
<th>Sharing PD</th>
<th>Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**The GDPR applies.** Specifically, because you indicated in Part 1 that you are directly asking persons in the EEA for their PD, you must first notify the data subjects and seek their consent. To assist, the following templates include the required notice/consent verbiage. Template 3 (for online surveys), Template 4 (for paper surveys), Template 6 (for verbal surveys). The templates are available from OP RB.

**The GDPR applies.** Your answers to Part 1 indicate the GDPR applies to your research, that the U of I will act as a data controller, and that your research data will be processed by a 3rd party. However, you also indicated the U of I does not have a DPA with the 3rd party. To ensure the PD you collect is properly secured by the 3rd party, contact the contract office you normally deal with and ask them to obtain a C2P DPA with the 3rd party if one does not already exist. The contract office should use DPA Template A.
Resources & Points of Contact

- EU GDPR
- EU GDPR Box Folder
- University Ethics & Compliance Office
  - Dave Grogan: 217-300-1862
  - Donna McNeely: 217-206-6202
- University Counsel
  - Megan Stoll: 312-996-7762
  - Steve Anderson: 217-333-0560