European Union’s General Data Protection Regulation

How is ECU Affected?

-Don Sweet, CIO
Who represents the European Union:

<table>
<thead>
<tr>
<th>Country</th>
<th>Country</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>Austria</td>
<td>Germany</td>
<td>Poland</td>
</tr>
<tr>
<td>Belgium</td>
<td>Greece</td>
<td>Portugal</td>
</tr>
<tr>
<td>Bulgaria</td>
<td>Hungary</td>
<td>Romania</td>
</tr>
<tr>
<td>Croatia</td>
<td>Ireland</td>
<td>Slovakia</td>
</tr>
<tr>
<td>Cyprus</td>
<td>Italy</td>
<td>Slovenia</td>
</tr>
<tr>
<td>Czech Republic</td>
<td>Latvia</td>
<td>Spain</td>
</tr>
<tr>
<td>Denmark</td>
<td>Lithuania</td>
<td>Sweden</td>
</tr>
<tr>
<td>Estonia</td>
<td>Luxembourg</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>Finland</td>
<td>Malta</td>
<td></td>
</tr>
<tr>
<td>France</td>
<td>Netherlands</td>
<td></td>
</tr>
</tbody>
</table>
What is the GDPR?

General Data Protection Regulation or GDPR
(effective May 25, 2018)

GDPR is a new data protection law for all entities (including higher education) that process the personal data of natural persons located within the European Union, thereby protecting their fundamental rights.

The GDPR has specific rules that we must adhere to that are different than U.S. data privacy laws. Compliance is key for constituents, supporters and donors living on European soil.
In other words:

For East Carolina University, “natural persons” are:

- ECU students in study abroad programs in the EU
- Faculty (ECU or those hired within the EU)
- Staff and other personnel (ECU or those hired w/in the EU)
- Third parties including local contractors, donors, etc. within the EU
- Natural persons in the EU applying/enrolling to ECU or taking online classes from ECU and residing in their EU country
- Natural persons from the EU playing sports for ECU
- ECU researchers sharing personal data with those in the EU
What represents “personal data”:

Any information relating to the identity or identifiable attributes (such as name, location, IP addresses, images, etc.) of all natural persons residing in the EU are covered.

Includes other factors specific to the physical, physiological, genetic, mental, economic, personal preferences, interests, reliability, behavior, cultural or social identity of a “natural person.”
What represents “personal data”:

*continued... Additional stringent rules for processing special categories of personal data concerning:*

- Race or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetics or biometrics
- Health
- Sex life/sexual orientation
- Criminal record
8 Data Protection Principles


1. Process data fairly and lawfully
2. Used for limited, specifically stated purpose – not in a manner incompatible with the purpose
3. Used in adequate, relevant manner
4. Must be accurate and kept up-to-date
5. Kept no longer than is absolutely necessary
6. Processed in accordance with the rights of the data subject
7. Appropriate measures against data breach, accidental loss, destruction or damage
8. Not transferred outside the EU without protection or consent
What if we do not address the GDPR?

• Financial penalties up to $24M or 4% of annual revenue imposed by National Data Protection Agency (NDPA)

• NDPA can request an audit at any time addressing how we are in compliance

• Reputational damage to ECU
To comply with the GDPR...

We need a Data Governance Framework that ensures data is secured from unauthorized access

• Who’s responsible for implementing & maintaining data policies and processes?

We are presently implementing an Enterprise Data Governance Program
To comply with the GDPR...

We need a Data Governance Framework that ensures data is secured from unauthorized access

• Where is data physically stored?
• How is access to data controlled?
• Are staff trained to handle data securely?
• Is external testing done to confirm data security?
To comply with the GDPR...

Must have IT policies that address the following:
• What is acceptable usage of IT infrastructure by staff?
• Passwords & procedures to grant and rescind system access?
• Email containing sensitive data can’t be sent to private email addresses.
• Use of removable media (USBs, etc.)
• Remote access to systems
To comply with the GDPR...

Use of multiple mitigating security controls to protect resources and data:

System-oriented Security:
- Firewalls Yes
- Network monitoring Yes
- Email filtering Yes
- Web filtering Yes via Cisco “Umbrella” Tool
- Intrusion detection system Yes
- Anti-virus protection Yes
- Software patching Yes
- User access controls Yes
- Data encryption Yes (planned for all ECU computers)
To comply with the GDPR...

It’s really all about the consent...

Data subjects must give consent in all cases “by a clear affirmative action establishing a freely given, specific, informed and unambiguous indication of the individual’s agreement to their personal data being processed... such as a written statement.”

We do not have this process and it must be developed.
To comply with the GDPR...

... more about the consent...

• Burden of proof lies with ECU

• Data subjects must be able to withdraw consent at any time – easily!

• Must obtain parental consent for data subjects under the age of 16
To comply with the GDPR...

Privacy Notice

A formal privacy notice is required stating:

• How personal data is used
• Retention periods for the data
• Legal basis for processing the data
• Where complaints can be filed

Must use plain, clear language and notice must be easily assessible!
What should we be doing now?

1. Thoroughly understand the components of GDPR
2. Appoint a Data Protection Officer (*owner of GDPR*) *
   *dedicated, dual-role or outsourced*
3. Appoint a GDPR Project Manager/Hire Consultant
4. Document all affected areas within ECU
5. Perform Gap Analysis
6. Formally map affected Data Flows (*internal & external*)
7. Ensure 3rd party vendors are compliant
8. Ensure individual rights (*see next slide*)
9. Adopt “Privacy by Design” (*need formal policy*)
10. Develop a comprehensive implementation plan
Ensure Individual Rights:

- Right of access to personal data
- Right of rectification of their data
- Right to data portability
- Right to withdraw consent
- Right to restrict/block/suppress processing of data
- Right to erasure/to be forgotten (data)
- Right to complain; judicial remedy; representation; and compensation
End of Presentation