General Data Protection Regulation (GDPR) Summary

What is General Data Protection Regulation (GDPR)?

- A data protection law passed by the European Union (EU) that imposes strict new rules on maintaining and processing personally identifiable information on residents of 28 EU Member States.
- It extends the protection of personal data and data protection rights by giving EU residents more control over how organizations use their data. GDPR applies to all organizations holding and processing EU resident’s personal data, regardless of geographic location. This would include those organizations outside the EU. Note the law applies to EU residents (as opposed to only EU citizens).
- GDPR was introduced to specify how consumer data should be used and protected in today’s digital environment, therefore the primary focus is on companies like Facebook, Google, and Amazon. However, the regulation also applies to colleges and universities which provides their own set of goods and services.
- The regulation goes into effect May 25, 2018.

Fundamental differences in philosophy and focus between the U.S. and EU

- Data privacy
  - U.S. = A consumer right
  - EU = A fundamental human right
- Consent
  - FERPA - Focuses on obtaining authorization to disclose contents of a record
  - GDPR - Involves not only the ability to disclose data but the ability to collect, retain, and delete data. The entire lifecycle of the data may be affected.

Key Features/Enhancements of GDPR

<table>
<thead>
<tr>
<th>Territorial reach</th>
<th>Applies to all organizations holding and processing EU resident's personal data, in connection with offers of goods and services and the monitoring of behavior, regardless of the organization’s geographic location.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy by design</td>
<td>Calls for inclusion of data protection from the onset of designing systems, implementing appropriate technical and infrastructural measures.</td>
</tr>
<tr>
<td>Enhanced individual rights</td>
<td>Greater transparency on collection and use of data at time of collection, easier cheaper redress for complaints. Current agreement between EU and U.S. Privacy Shield security framework structure is currently what has been negotiated - requirements include more robust protection in the form of written commitments and assurances (e.g., requires annual self-certification by organizations, privacy policies on website, prompt response to complaints). Also the right to deletion and correction of data (known colloquially as the right to be forgotten), right to complain, right to receive information about what was collected in a structured way.</td>
</tr>
<tr>
<td>Expanded definition of personal data</td>
<td>Unique online identifiers (IP addresses, mobile device identifiers such as geolocation data, biometric data, etc.).</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Consent</td>
<td>Must be specific to each data processing operation; must be intelligible and easily accessible form using clear, plain language.</td>
</tr>
<tr>
<td>Breach notification</td>
<td>Has a definition of personal data breach; requires data breaches to be reported to European national state authorities within 72 hours.</td>
</tr>
<tr>
<td>Organizational requirements</td>
<td>Administrative compliance on data processing; requires documentation on policies, impact assessments. It is a thought process on risk and how to mitigate it.</td>
</tr>
<tr>
<td>Penalties</td>
<td>Failure to comply could lead to fines of up to 4 percent of global turnover or €20 Million, whichever is higher.</td>
</tr>
</tbody>
</table>


**Within higher education, what populations are affected by this regulation?**

- Students who are residents of the EU
- Domestic students in study abroad programs in the EU
- Faculty, staff and other personnel (hired locally or posted to the EU)
- Third parties in general (i.e. EU contractors, EU donors, EU researchers)
- Others...?

**Implementation considerations around consent and personal rights**

- How do we need to alter our operational processes?
- Implement special practices just for EU students? faculty? staff? Apply to all or take a segmented approach?
- How do we identify privacy requirements?
- How/when to obtain authorizations? Identify milestones during a record’s lifecycle.
- How do we systematize these practices?
- How extensive are required audit trails?
- What are our notification requirements?

For more information, refer to https://www.eugdpr.org/