GDPR Overview

**What is GDPR?**

The General Data Protection Regulation (GDPR) comes into effect on 25t May 2018.

It standardizes and strengthens the right of all European Citizens to data privacy. GDPR emphasizes transparency, security and accountability for organizations that collect, use, share and store personal data.

While many of the main concepts and principles of GDPR are much the same as those in our current FERPA and Privacy Act laws, GDPR introduces new elements and significant enhancements which Centre College is required to accommodate.

**What this means to Centre College**

Centre College looks to attract a diverse faculty, staff and student body and this includes citizens from the European Union. We are also very proud of our Study Abroad and Internship programs which can bring US citizens to the European Union during their academic career. Centre College must ensure we comply with the GDPR for both our EU citizens but also for US citizens during their stay in EU countries.

**What is Centre College doing about GDPR?**

Centre College is developing guidance for staff, faculty and students who will be affected by GDPR. This will include crating forms to track students notification of our policies, procedures to challenge data and a data map for all privacy data stored and used by the College.

For further information, please contact Andrew Ryan, Chief Information Officer at andrew.ryan@centre.edu

**Why is GDPR Important**

Centre College processes significant amounts of personal data about its applicants, students, staff, faculty, alumni, and many others. People are increasingly aware of their rights and expect organizations like Centre College to protect their personal data.

The GDPR significantly increases the obligations and responsibilities for organizations like us in how we collect, use and protect personal data. At the Centre of the new law is the requirement for organizations to be fully transparent about how they are using and safeguarding personal data, and to be able to demonstrate accountability for their data processing activities.

**Key GDPR Changes**

The GDPR introduces a number of changes to data protection practices and will require the College to review and revise its approach to data handling. Key changes include:

1. **Privacy notices**: more detailed privacy notices are required, which explain the purpose and legal basis behind processing activities
2. **Accountability**: stronger requirements to demonstrate compliance; record-keeping regarding all data processing activities;
3. **Privacy by Design and Default** should be the norm;
4. **Data Protection Impact Assessments (DPIAs):** mandatory for all new processing activities where privacy risks are high
5. **Sensitive personal data**: now includes genetic and biometric data
6. **A broader definition of personal data:**now includes ID numbers, IP addresses and reversibly anonymized (‘pseudonymised’) data
7. **Consent**: must be ‘opt-in’ (rather than being assumed from lack of action), freely given, informed and specific to named processing activities; data subjects will be able to withdraw consent at any time
8. **Right to be forgotten**: data subjects can request that their data is deleted in some circumstances
9. **Right to data portability**: data subjects can request their data in a portable format, in order to move it to another data controller
10. **Subject Access Requests**: individuals still have a right to request access to their personal data held by an organization; this can no longer be charged for; the response time limit is reduced from 40 days to one month
11. **More restrictive rules around the use of child data:**restricts the age at which individuals can lawfully give consent, introduces rules for the language used in consent requests targeted at children and regulates the way online services obtain children’s consent.
12. **International transfers**: new rules for transfers outside the European Economic Area (EEA)
13. **Breach notification**: must notify the Data Protection Commissioner within 72 hours of becoming aware of a data protection breach
14. **Fines**: tougher financial penalties (fines of up to 4% of annual global turnover or €20 million (whichever is greater));

Updated: May 2018