**The General Data Protection Regulation**

The General Data Protection Regulation or GDPR will come into effect on May 25 of 2018. It has the potential to significantly alter the way businesses handle and store data. The primary objective of GDPR is to strengthen security and privacy protection for individuals.

The main points of the GDPR is the severity of the potential fines and new requirements such as

breach notification, right to access, right to be forgotten, and user consent.

It primarily focuses on personal data, with extra protection for ‘sensitive personal data’.

Personal data includes data that can be used to identify a person, such as email and physical addresses online identifier, e.g. an IP address. Sensitive personal data includes ethnic origin, religion, health, biometric, genetic, political views, etc.

The GDPR applies to any entity in the EU, any entity in the EU that controls or processes data of any individual , any entity anywhere in the world that offers goods or services to individuals in the EU, or any entity anywhere in the world that monitors the behavior of EU residents.

The GDPR includes all the processes associated with the collection, retention, use, transfer, disclosure, deletion and data breach or unauthorized disclosures. Transfer of data from/to the US across EU borders requires additional certifications, such as a Privacy Shield certification.

An important aspect of GDPR is individuals consent for their use of personal information and excludes general waivers, “check the box” or automated opt-in consent with optional opt-out. In addition individuals have the “right to be forgotten”, and rights of access for the purpose of examination, correction, objection and erasure, the right to limit scope of processing and no profiling without consent.

|  |  |
| --- | --- |
| FERPA | GDPR |
| “Directory information” is public unless the data subject affirmatively opts out | All personal information is protected unless the data subject affirmatively consents to disclosure |
| Focus is on post-collection issues (who can get data, either inside or outside the University); does not address collection or retention policies | Must disclose all data collection and retention policies to data subject, including who in the University has non-consensual access to data and how data will be used |

From CSU - OGC presentation to ISO – 12-2017