The New EU General Data Protection Regulation

New EU Regulation is complex.
Containing 99 articles in its 11 chapters

Goals of GDPR:

- Increase the accountability of organizations processing personal data
- Increase control that individuals have over that processing.

General Data Protection Regulation

GDPR – Why do we care? We are not in the EU!

Territorial Scope:
This regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behavior as far as their behavior takes place within the Union. ** FERPA

Enforcement Date: May 25, 2018

- Replaces the current Data Protection Directive (1995/46/EC)

Penalties for Non-Compliance

- Organizations can be fined **up to 4% of annual global turnover** or 20 Million Euro for unlawful processing of Personal Data.

MARIST will comply with this regulation.

** **More than FERPA – that only deals with student data**
GDPR applies to all people in EU (staff, vendors, parents, both former and present)

GDPR – What is Personal Data

Some Definitions:

Personal Data = Any information relating to an identified or identifiable national person. If using a piece of data gets you to one living person, it is personal data. ** FERPA

Processing = Any operation or set of operations on personal data, whether or not automated. Collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, restriction, erasure/destruction

Data Controller = The person or organization that determines the purposes and means of processing personal data

Data Processor = The person or organization that processes personal data on behalf of the controller

Sensitive Personal Data

- Special rules apply for processing of: racial, ethnic, political, religious, trade union membership, genetic, biometric, health or sexual orientation.

- Processing of the above Sensitive Data is **prohibited** unless processing is necessary for certain specific reasons listed in Article 9 or prior consent obtained.

** **This is very different from FERPA!**
Name, Address, CWID, eMail, DOB currently considered Directory Data – NOT Personal Data!

GDPR – Rights of Individuals

Increases Control that Individuals Have Over Personal Info

Consent	➢ Companies will no longer be able to use long-winded terms & conditions. ➢ How data will be used must be given in an easily understandable form. ➢ Revoking consent must be as easy and as simple as it was to give.
Right to Access	➢ Right of individual to request confirmation as to how personal data concerning them is being processed.
Data Portability	➢ Right of individual to receive a copy of the personal data concerning them, provided free of charge and in a machine readable format.
Right to Correction	➢ Right of individual to request changes of inaccurate data. Accuracy!
Right to Erasure	➢ Entitles the individual to have his/her personal data erased when no longer needed or if processing it is unlawful. ➢ Demand further processing and dissemination of the data ceased.

FERPA

** **More than FERPA – that primarily deals only with disclosure and consent**
GDPR also deals with collection, retention and deletion

IT

GDPR – Obligations of Organization

Increases the Accountability of Organizations Processing Personal Data

Develop Processes	➢ Develop processes required to comply with all individual rights (Consent, Data Portability, Right to be Forgotten, Right to Access and Correction) ** ➢ Personal data shall be processed lawfully, fairly and in a transparent manner
Data Protection Office	➢ Assign Data Protection Officer (DPO) ➢ Assign Data Controller to oversee compliance in each processing area ➢ Provide education to Data Processors
Privacy by Design	➢ Inclusion of data protection from the onset, rather than in addition. ➢ Collect only data necessary for the stated purpose, hold only as long as needed ➢ Limit access to only those needing access and use only for stated purpose.
Record Keeping	➢ Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility.
Breach Notification	➢ Investigate and report data breach within 72 hours of discovery ➢ Mandatory when breach is likely to 'result in a risk for the rights and freedoms of individuals

** The organization must respond to requests without undue delay and **at the latest within 1 month.** If the organization doesn't intend to comply with the request, they must state the reason why.

GDPR – Obligations of Organization

Accountability of Organizations Processing Personal Data - continued

Lawful Processing	➢ The controller shall implement appropriate technical and organizational measures to ensure that processing is performed in accordance with this Regulation. ➢ Those measures shall be reviewed and updated where necessary.
3rd Party Processors	➢ Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures.
EU Representative	➢ The controller shall designate in writing a representative in the Union. ➢ The representative shall be established in one of the Member States where the data subjects, whose personal data are processed
Supervisory Authority	➢ The controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks.
Assessment	➢ Where a type of processing in particular using new technologies, the controller shall, prior to the processing, carry out an assessment. ➢ The controller shall seek the advice of the data protection officer.
Security	➢ Appropriate technical security measures put are in place, taking into account state of the art, costs of implementation, likelihood of risk and impact on data subject.

Codes of Conduct

- Encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation
- Monitoring of compliance with a code of conduct may be carried out by a body which has an appropriate level of expertise.

Transfer of Data to a Third Country or International Organization

- GDPR has specific requirements regarding the transfer of data out of the EU. One of these requirements is that the transfer must only happen to countries deemed as having adequate data protection laws.
- In general the EU does not list the US as one of the countries that meets this requirement.

https://www.privacytrust.com/privacyshield/gdpr-vs-privacy-shield.html

The EU-US Privacy Shield is a framework that protects the fundamental rights of anyone in the EU whose personal data is transferred to the United States for commercial purposes. The framework also brings legal clarity for businesses relying on transatlantic data transfers.

The new arrangement includes:

- strong data protection obligations on companies receiving personal data from the EU
- safeguards on US government access to data
- effective protection and redress for individuals
- an annual joint review by EU and US to monitor the correct application of the arrangement.

Implementing Privacy Shield Framework will reduce our likelihood of being fined.

GDPR

Who is protected by GDPR @ Marist

SIS/ Alumni	Students from the EU studying in the U.S.		
	Marist students studying abroad		
	Former students and alumni now in the EU		
HRS	Current employees in EU (Florence Faculty)		
	Former employees in the EU (including retirees)		
	Beneficiaries of employees living in the EU		
	Marist employees temporarily in EU		
Finance	Vendors		
Admissions	Applicants in the EU at time of application or have relocated since then		
SFS	Parents / Guardians residing in the EU		
Advancement	Donors in the EU		

Applies to data of subjects who are in the EU, even if in EU on a temporary basis.

http://www.aacrao.org/resources/trending-topics/gdpr/gdpr-faq

28 member states of the EU.

But what about Brexit?

The UK Government has signaled its intention to implement the GDPR.

Is it possible that similar regulations will be adapted by the U.S.?

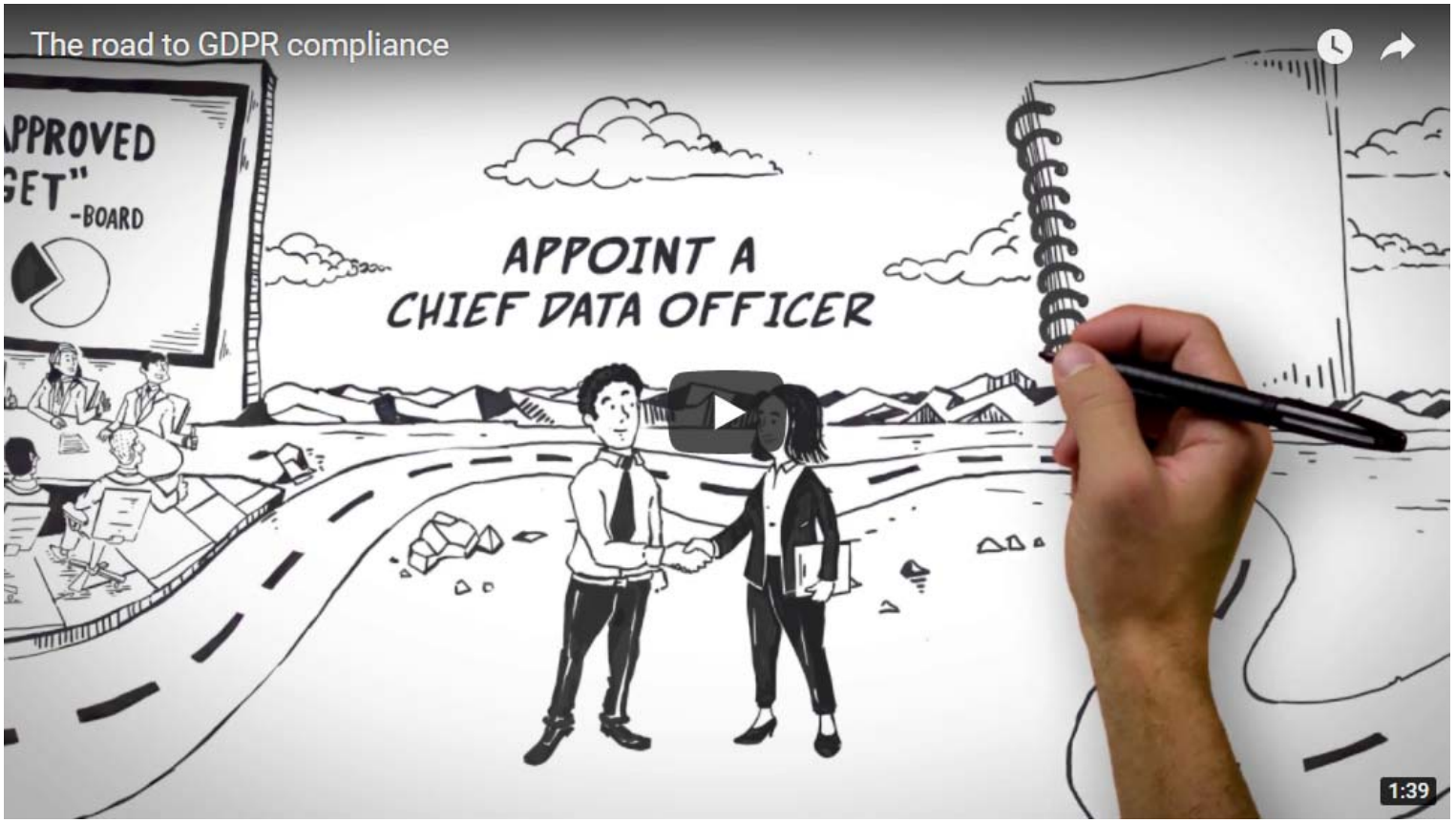
YES !

Should we extend same protections to all MARIST people?

YES !

IT

GDPR – Road to Compliance



https://youtu.be/1xy_afgALSI

GDPR – How do we get to Compliance at Marist

Campus Wide Effort - WE EACH HAVE A ROLE!

- Technical Steering Committee
- Data Protection Officer
- Data Controllers
- Information Technology
- Data Processors

- Compliance policies and procedures development will be lead by the Data Protection Office.
- Data Stewarts / Data Controllers will be provided guidance.
- Operationally implicit GDPR polices will be developed with the departments.

IT