Data Privacy and GDPR
Executive Overview
Information Technology Services, March 27, 2018

University of San Diego

General Data Protection Regulation

GDPR A New Challenge

- General Data Protection Regulation (GDPR) was established by the European Parliament and Council
  - ✓ to attempt to harmonize data privacy laws across Europe*
  - ✓ to protect and empower all EU citizens' and their data
  - ✓ to reshape the way organizations across the region approach data privacy
  - ✓ to give the right of erasure of one's own private data
  - ✓ To address the security practices at companies that hold massive amounts of personal information (Equifax, Alibaba, Facebook, Google, Amazon, etc.)
- GDPR focuses on the protection of personal information
  - ✓ Personal data is defined (Article 4(1)) as "any information relating to an identified or identifiable natural person"
  - ✓ It also includes any individual piece of information that can be tied back to a person by itself or in combination with other pieces of information.

University of San Diego

* White & Case Consulting explain that the GDPR fails to fully "harmonize" data privacy laws due to the fact that the GDPR allows each of the 28 EU member state Data Protection Authorities (DPA) to define their own parameters for data privacy matters related to Chapter 17 of the GDPR.

GDPR: Who Does it Impact?

It's not just organizations located in the European Union. It's any organization that has any data on any person living in the EU.

Steps toward GDPR Compliance

1. Awareness: Ensure that decision makers and key people at USD are aware of the European Union GDPR and that it is going to impact the way the university collects, stores, protects and processes EU subject data.

2. Documentation: USD is required to document the personal data that is held on EU data subjects, where it came from, how it is used, and who we share it with. This is being done through an information audit on the way USD collects, stores, protects and processes EU subject data.

3. Information and Privacy Statement: USD will need a new Privacy Statement/Notice to inform people of how USD intends to process/use an individuals data. This statement will need to address the "legal basis" for processing the data, specify retention periods in clear and understandable language. A clear statement and reasoning will need to be developed that explains why certain data will be retained in perpetuity (e.g. student enrollment and academic record data).

4. Rights of Data Subjects: The regulation calls for the implementation on new rights such as the right to access, right to be forgotten, the right to data portability, the right to object, the right to revoke consent, and the right to restrict processing.

5. Designate a Data Protection Officer: Organizations will need to appoint a Data Protection Officer (DPO) with understanding of IT Security solutions and practices (USD Information Security Director).

University of San Diego

Steps toward GDPR Compliance

6. Third-party Management: Vendors, data providers/suppliers, and outsourced system providers, should be required to protect personal data and should be monitored to ensure that they do so.

7. Privacy by Design: As USD plans for a new technology or service there will need to be consideration on data-protection requirements from the initial stages of the planning and development process or as a new product of technology is assessed.

8. Data Breaches: GDPR stipulates that data breaches resulting in risk to individuals' rights and freedoms should be reported to authorities within 72 hours, and subsequently to the data subjects. USD may need to update our Information Security Incident Response Policy.

9. IT Security: USD is required to protect data through means such as encryption and have effective operational procedures and policies for managing data. IT Security monitoring solutions such as intrusion detection and prevention systems are required.

University of San Diego

TERRITORIAL SCOPE

EU Establishments

Non-EU Established Organizations
Offer goods or services or engaging in monitoring within the EU.

THE PLAYERS

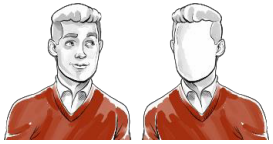
Data Subjects

Data Controllers

Data Processors

Supervisory Authorities

PERSONAL DATA



Identified **Identifiable**

SENSITIVE DATA

Racial or Ethnic Origin

Religious or Philosophical Beliefs

Genetic Data

Political Opinions

Biometric Data

Trade Union Membership

Health

Sex Life

RESPONSIBILITIES OF DATA CONTROLLERS AND PROCESSORS

Security

Data Protection Officer (DPO)

Designate DPO if core activity involves regular monitoring or processing large quantities of personal data..

Record of Data Processing Activities

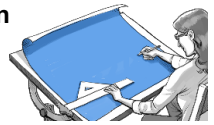
Maintain a documented register of all activities involving processing of EU personal data.

Data Impact Assessment

For high risk situations

Data Protection by Design

built in starting at the beginning of the design process



LAWFUL PROCESSING

Collection and processing of personal data must be for "specified, explicit and legitimate purposes" – with consent of data subject or necessary for

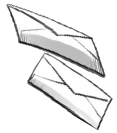
- performance of a contract
- compliance with a legal obligation
- to protect a person's vital interests
- task in the public interest
- legitimate interests

CONSENT

Consent must be freely given, specific, informed, and unambiguous.

GDPR

DATA BREACH NOTIFICATION

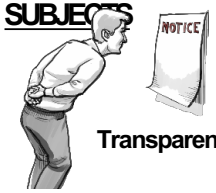


A *personal data breach* is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

If likely to result in a high privacy risk → notify data subjects

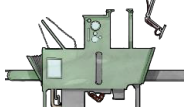
Notify supervisory authorities no later than 72 hours after discovery.

RIGHTS OF DATA SUBJECTS



Transparency

Automated Decision-Making



"Right not to be subject to a decision based solely on automated processing, including profiling."

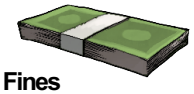
Right to Erasure

Access and Rectification

Purpose Specification and Minimization

Right to Data Portability

ENFORCEMENT



Fines

Up to 20 million euros or 4% of total annual worldwide turnover. Less serious violations: Up to 10 million euros or 2% of total annual worldwide turnover.

Effective Judicial Remedies: compensation for material and non-material harm.

INTERNATIONAL DATA TRANSFER

Adequate Level of Data Protection

Binding Corporate Rules (BCRs)

Privacy Shield

Model Contractual Clauses

TEACHPRIVACY

www.teachprivacy.com

Workforce awareness training by Prof. Daniel J. Solove

Privacy Reality and US Universities

- "No US university will be compliant with GDPR on the effective date (of May 25, 2018)." – Ivy League CIO
- "The compliance process for public entities requires the EU to work through the US State Department and we don't believe either the EU or state department are going to get into a battle over this with universities." – CIO from Major US Research University and Leader of Higher Education Information Security Council
- SoCal Higher Education CIO Alliance (20+ Universities) concluded that taking a "wait and see" approach to GDPR compliance is the most prudent and common course of action. This is based on the fact that many universities already have security solutions in place along with policies and practices to protect personal information.
- "We feel that it won't be long before California, NY, or Mass. implement something like GDPR so we want to move towards being able to fulfill this requirement over the next 12-24 months." – CIO and CISO from Carnegie R1 Institution.
- "However, as set out in (GDPR) Chapter 17, there are several areas that remain unharmonised. In these areas, compliance requirements continue to vary from one Member State to the next." Case & White Consulting

University of San Diego

USD Plans for Improved Data Privacy

1. ITS Working Group formed to identify work to enhance data privacy practices with the goal of making incremental progress toward GDPR compliance.

2. Implement Storage Level Encryption for ALL USD enterprise systems and data by August 31, 2018 (part of NetApp storage replacement project). This supplements or replaces existing application and database encryption technologies.

3. Data Protection Officer (DPO) will start work on June 4th, 2018. At universities and small organizations the role of DPO can be part of the Information Security Director position.

4. Data Identification Framework is being used to gather a list of all data sources and types that enter USD systems/databases.

5. Data Assessments using the Identification Framework, there will be a series of meetings with USD business units that will document all data sources, data types, and variables associated with individuals'. Documentation will be prepared on how data is obtained, secured and the use/purpose of the data. Business units involved with data assessments include but are not limited to Undergraduate Admissions, Graduate Admissions, Law School Admissions, Alumni Relations, Parent and Family Relations, Financial Aid, International Center, Payroll, Human Resources, Career Services, Student Health Center, IRP, etc.

University of San Diego

USD Plans for Improved Data Privacy

6. Data Flow Diagrams may be developed from Data Assessments to document how personal data is shared/passed and stored among various USD enterprise systems.

7. Privacy Statement/Policy USD will need to draft a privacy policy or a notification that can be used to inform individuals of how the university secures and protects their personal information. The privacy notification will serve as part of a user consent agreement specific to their data.

8. Incident Response Policy will be reviewed and updated, as needed, to reflect any new requirements for breach notifications and compliance with US and other laws.

9. Consent Tracking systems are being assessed and a determination will be made as to whether an internally developed consent tracking system may suffice or if the university will have to purchase a third-party solution to track consent.

10. Data Retention and Preservation rules will need to be clearly defined and articulate data that USD will retain permanently. For example, rules to retain data on students' and their academic record, degrees, graduation date, etc. will need to be defined.

11. Data Limitation rules will need to be assessed to determine the risks of retaining data that may have limited or no use to the university.

University of San Diego

USD Plans for Improved Data Privacy

12. Third-party Vendors Documentation will be prepared for the practices that companies use to store and secure university data. Specifically this refers to the practices of vendors that offer Software as a Service, cloud providers, and hosted solutions that are located outside USD data centers.

13. Data Subject Rights will be reviewed and potential solutions identified. This may include documentation on the ways users may review their personal information, rectify any errors, request that certain types of data to be deleted/erased and define formats to allow for portability of personal data (DPO contact on website).

14. Awareness will be raised through this presentation and summary documentation of data privacy publications provided to the University Executive Cabinet. ITS will create a website to explain USD's data privacy efforts and policy; GDPR information will be listed on that site.

University of San Diego