UC and the General Data Protection Regulation

ITPS, May 31, 2018

Robert Smith

Systemwide IT Policy

Disclaimer

- GDPR is an evolving topic
  - GDPR has multiple/competing goals
- Regulators are updating guidance
  - Many things not defined, some have guidance, some not
  - Member states have flexibility
- UC is in the midst of mapping out a strategy
- The level of impact to UC is being studied and will drive investment

What is the GDPR?

- General Data Protection Regulation
- Intends to harmonize data privacy laws across Europe
  - Individual rights > Data Controller rights
- Repeals and replaces the Data Protection Directive 95/46/EU
  - Increased territorial scope
  - Increased penalties
  - Strengthens consent requirements
- Took effect on May 25, 2018 - Passed in April 2016
- Higher education is not the target, but is impacted
- Data collected in the European Union Economic Area (EEA) about 'natural persons' is in scope
  - Probably further processing of older GDPR data after 5/25/18 is in scope too
  - EEA = EU + Norway, Iceland and Lichtenstein
  - UK will enact same/similar regulation

USA vs EU Privacy Regulation

USA

- Laws create a right of privacy where it is needed – sectoral approach
  - Health: HIPAA
  - Students: FERPA
  - Financial: GLBA, FCRA
  - Marketing: TCPA, TSR, CAN-SPAM
- State laws like CMIA - The Confidentiality Of Medical Information Act (CMIA)
- Thinking: Does anything say we can't?

EU/EAA

- Privacy is a fundamental and uniform right
- Umbrella regulation
  - Broad scope
  - Broad responsibilities
- Thinking: You can't unless something says specifically you can

Requires different thinking!

GDPR in one slide
EU General Data Protection Regulation

- Effective date – May 25, 2018
- Core principles
  - Lawfulness (legal basis)
  - Transparency
- Participants
  - Data subjects = natural persons in EEA
  - Data controllers
  - Data processors
  - Supervisory Authorities
- All personal data – special rules for 'sensitive data'
  - Broader than US – e.g., IP address
- Explicit consent freely given & revoked
- Data subjects have rights
  - Transparency, Erasure, Rectification, Specific and Minimal, Portability
- Limits automated processing impacting individuals
- GDPR follows the data!
  - Impacts big data where ID is possible
- Data breach notification 72 hours after discovery
- Fines up to €20M ($28M+) or 4% revenue
- Things UC (probably) must do
  - ~~Appoint a Data Protection Officer~~ (UC probably not processing on a "large scale")
  - Inventory and record processing activities
  - Data Impact Assessments for high risk processing
  - Security and data protection by design – process and systems
  - Have contract clauses
  - Create consent forms, notice practices and "lawful basis"
  - Support data subject rights
  - Support notification requirements

Is UC in scope for GDPR?

- An "establishment" in the EEA
  - Operating an office in the EEA
- Processing activities relate to:
  - **Offering of goods and <u>services</u> to data subjects located in the EEA**
    - Recruiting students, faculty, staff, athletes
    - Consultative services to health care providers or patients
    - Online learning/websites
    - Financial aid
  - **Monitoring data subjects' behavior where behavior takes place in the EEA**
    - Research of individuals located within the EEA
    - UC students, staff and faculty while they are abroad
- **Or the transfer of personal data from EEA outside EEA**
  - Transfer of medical records
  - EEA students coming to UC
  - Clinical research results from EEA sites

Fundamental Rights Summary

- Personal data must be:
  - Processed pursuant to a lawful basis
    - Contract is preferred method
  - Collected for specified, explicit and legitimate purposes; no further processing
    - Exception: archiving for public interest, scientific or historical research purposes or statistical purposes
    - Research may have some flexibility
  - Adequate, relevant and limited to what is necessary
  - Accurate
  - Kept in a form permitting identification for no longer than necessary
  - Secure
- Most important data subject rights
  - Notice, Consent, Objection, Transparency, Erasure, Rectification, Specific and Minimal, Portability

Steps for UC: Measured Approach

- UC should continue conducting business
  - At the same time, take the next sensible steps
  - Solidify compliance and operational responsibilities
  - (See next slide)
- Remember, consent cannot be satisfied by asking individuals to agree to "any and all purposes."
  - Opt-out provisions will also not meet GDPR consent requirements.
  - Consent should only be used as a lawful basis if no other lawful basis may be relied upon.
- The new IS-3 is a good foundation for the data security requirements

This is a work in progress.
Systemwide workgroup → Locations.

Steps for Location: Compliance

- Consult advisories
  - Conducting a GDPR Analysis, GDPR Decision tool, Legitimate Interests Assessment, Complying with Consent Requirements
- Complete an inventory of processing – "record of processing"
  - Develop processes for maintaining records of processing activities and consents for processing, use the Record of Processing Advisory and Record of Processing template
- Update contracts as necessary
  - Where a UC supplier accesses or uses personal data from the EEA to perform a service for UC: Appendix Data Security + Appendix DS Amendment 2
  - Where UC receives data from the EEA collected from another institution/company in the EEA: standard clauses approved by the EU Commission
- Consider need for Data Protection Impact Assessment (DPIA) for data categories likely to result in high risk to rights and freedoms of data subjects
- Update consent forms, notices to comply with GDPR
- Develop breach reporting procedures: reporting to EEA supervisory authorities and data subjects – plan to use the new UC Incident Response Standard
- Implement appropriate technical and organizational security measures

This is a work in progress.

University of Michigan …

- It will take some time for organizations around the world to sort through, understand, and determine the implications of the GDPR requirements, as well as figure out how best to meet them. Watch for more information as the university's GDPR working group goes about its work.

A measured approach …

Questions

Hillary Noll Kalay
Counsel, Health Law
Office of the General Counsel
Telephone: 510-987-0355
hillary.kalay@ucop.edu

Robert Smith
ITS
Systemwide IT Policy
510-587-6244
robert.smith@ucop.edu

Scott Seaborn
Systemwide Privacy Manager
510-987-0459
Scott.Seaborn@ucop.edu

D'Arcy Myjer
Director of Compliance, Ethics,
Compliance & Audit Services
510-987-0887
D'Arcy.Myjer@ucop.edu

https://ucop.box.com/v/uc-internal-use-gdpr
Enter: UCGDPR

GDPR in short
If you need wording – use this

- The European Union's General Data Protection Regulation (GDPR) is a new privacy law that governs the use of personally identifiable information. The GDPR grants certain legal rights to people whose personal data is being collected and processed and imposes legal responsibilities on entities that control or process personal data.
- In general, the GDPR covers the storage or use of personal data for University functions or activities that 1) take place in the EU; 2) involve outreach to people in the EU to offer goods or services; or 3) track people in the EU online or involve the control or processing of data relating to people in the EU.

Statement you can use for Units

- GDPR may have implications for your unit if your Unit collects, processes, or stores (or uses a third party to collect, process, or store) personal data from individuals in the European Union. The GDPR defines "personal data" very broadly such that the term includes names, addresses, phone numbers, national IDs, IP addresses, profile pictures, personal healthcare data, educational data, and any other data that can be used to identify an individual.
- GDPR concerns the personal data of individuals in the European Economic Area (EEA), which includes EU countries as well as Iceland, Norway, and Lichtenstein. So when we say the EU, we mean all of the above countries or EEA.

What is Personal Data?

Personal data - Article 4(1) defines “personal data” as follows

- ‘personal data’ means **any information relating to an identified or identifiable natural person** (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Behavioral analysis – Recital 24

- The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the **monitoring of the behaviour of such data subjects** in so far as their behaviour takes place within the Union. In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of **profiling** a natural person, particularly in order to take decisions concerning her or him or for **analyzing or predicting her or his personal preferences, behaviors and attitudes**.

Examples of common GDPR Identifiers

Personal data

- Name
- Identification number
- Location data (Address, GPS, etc.)
- Online identifier (handle, e-mail)
- One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity
- Online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags.
- Behaviors
- **Any information relating to an identifiable person** who can be directly or indirectly identified in particular by reference to an identifier.

Special

- Racial or ethnic origin
- Political opinions
- Religious/philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data
- Health-related data
- Sex life/sexual orientation
- Criminal convictions and offenses

There is no safe harbor in GDPR!

What is the EEA?
European-Union Economic Area

- **European Union**
  - Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden
- **Additional countries:**
  - Iceland, Liechtenstein, Norway
- **United Kingdom**

Data Subjects
“natural persons” in the EEA

- **Art. 3 GDPR, Territorial scope, (2)**
  - **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.**

Simple GDPR summary

- **General Data Protection Regulation (“GDPR”)**: A privacy law of the European Union that governs the use of personally identifiable information. It concerns the personal data of individuals in the European Economic Area (EEA), which includes EU countries as well as the United Kingdom, Iceland, Norway, and Lichtenstein. The GDPR defines "personal data" very broadly such that the term includes names, addresses, phone numbers, national IDs, IP addresses, profile pictures, personal healthcare data, educational data, and any other data that can be used to identify an individual. It addresses multiple issues, such as the rights of data subjects, consent, and purpose of use.

Lawful basis under GDPR

- Performance of a contract
- Legitimate interest
- Compliance with legal obligations (EU/EEA)
- Consent
- Public interest/official capacity
- Protection of vital interests of a natural person