# GDPR: A Development and Integration Perspective

**Bo Pitsker, UCOP**
Enterprise Security Architect
Bo.Pitsker@ucop.edu

August 15, 2018

# Agenda

- Meeting objectives
- Presenter background
- Concluding remarks
- Q & A
- Other Resources

# Introduction

- Security and Privacy are *always* requirements for developers and integrators
- UC has adopted ISO/IEC 27001/2 as a security standard
- UC has also adopted the NIST Cybersecurity framework (CSF)
- We are committed to strict adherence to laws, regulations and best practices for security

# What is the GDPR, and Why Should You Care?

- The General Data Protection Regulation (GDPR) is an EU law to protect privacy and give individuals more control over their data
- GDPR is special because:
  - It protects EU residents *worldwide*
  - It creates unique rights for persons to control their personal data
  - It targets any organization doing business with EU residents, even without a presence in the EU; e.g. recruiting EU students

# Why does GDPR apply to UC?

- UC does business in Europe
- UC markets to EU residents
- EU citizens and residents come to UC
- UC systems and applications contain personal data of EU citizens and residents
- UC students, faculty and staff go to Europe

***Failure to comply with GDPR can result in fines up to 4% of annual revenue!***

# Key definitions

- Data Subject - “A natural person whose personal data is processed by a controller or processor”
- Data Controller - “The entity that determines the purposes, conditions and means of the processing of personal data”
- Data Processor - “An individual or organization that processes data on behalf of the data controller”

# Key definitions (cont.)

- Personal Data - “Any information related to a natural person or ‘Data Subject’, that can be used to directly or indirectly identify the person”
- Special Categories of Data - “Special category data is personal data which the GDPR says is more sensitive, and so needs more protection”
  - Race -Ethnic origins - Trade unions - Genetics
  - Religion - Biometrics - Health - Sex life/orientation
- Consent - “Freely given, specific, informed and explicit consent by statement or action signifying agreement to the processing of their personal data”

# GDPR-specific Requirements for Developers and Integrators

- Privacy by Design (PBD) - The general principle is that systems and applications must be designed for privacy and security
- Lawful basis for processing – personal data cannot be processed without a lawful basis
  - For developers, this usually means *consent,* but could be *legal* or *contractual*
  - Other basis includes: contract, legal obligation, vital interests or a public task

# **GDPR-specific Requirements for Developers and Integrators** (cont.)

- The right to be informed – GDPR requires explicit and detailed disclosure of the collection and use of personal data
  - May be done by administrative processes external to the application, but not recommended
  - Cannot be a monolithic, legalistic statement
  - Must be timely – Presented at time of collection, or within a month if data acquired from other sources
  - Must be accessible at all times

# Consent – Based on the right to be informed, *consent* is required before processing and

- Must be unambiguous and affirmative
- Cannot be obtained by “opt-out” or pre-filled “opt-in” methods
- Must be obtained separately from any terms of service agreements
- Must be obtained for each distinct stage of processing
- Must be recorded for audit and compliance purposes
- Must be possible to withdraw consent at any time

# Data subjects have the right to access and review their personal data at any time to

- Confirm that their data has or is being been processed
- Validate the accuracy of the data (see the “the right to rectification”)
- Determine that their data is being processed lawfully
- Make decision about whether to continue to permit processing (see the “the right to erasure”)

# Data subjects have the right to access and review their personal data at any time to

- Confirm that their data has or is being been processed
- Validate the accuracy of the data (see the “the right to rectification”)
- Determine that their data is being processed lawfully
- Make decision about whether to continue to permit processing (see the “the right to erasure”)

# Conclusion

- Security is driven by business needs
- Enterprise architecture provides the basis for security transformation
- Frameworks establish the means to organize and prioritize the work of security
- The UC EA team and ITAC have established a process and a body of work for security
- We are here to help (and we're not from the IRS!)

# Q & A

# For more information

**Presenter**

Bo Pitsker, Enterprise Security Architect

Bo.pitsker@ucop.edu

510-587-6490

**UC EABoK**

sp.ucop.edu/sites/its/apptech/enterprisearchitecture/EABoK/default.aspx

If unable to access, contact Jerome McEvoy, jerome.mcevoy@ucop.edu

**Information Technology Architecture Committee (ITAC)**

spaces.ais.ucla.edu/display/ucitag/Home