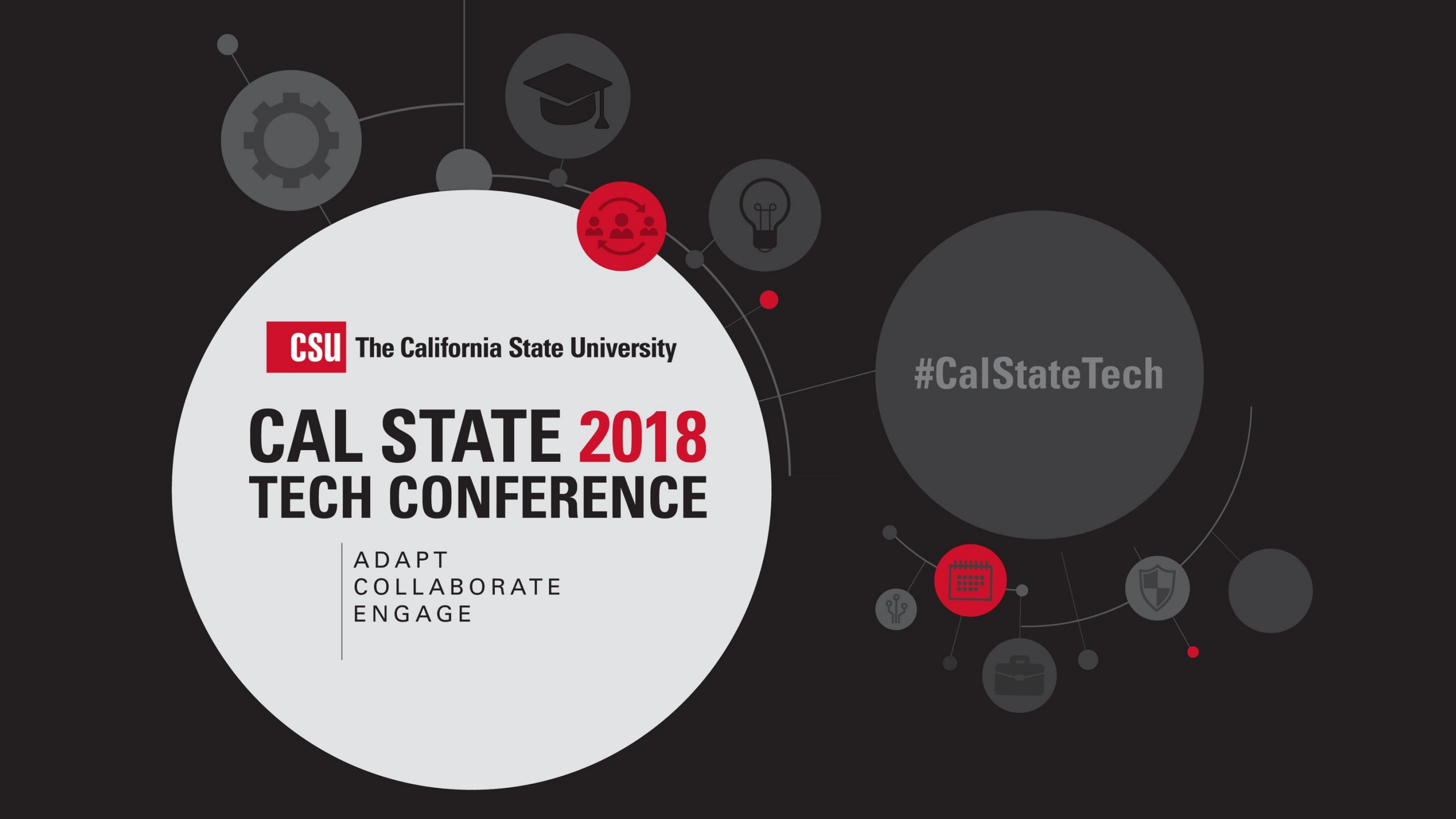

CSU The California State University
CAL STATE 2018
TECH CONFERENCE
ADAPT
COLLABORATE
ENGAGE
#CalStateTech

CSU The California State University

CAL STATE 2018
TECH CONFERENCE
ADAPT • COLLABORATE • ENGAGE

The EU General Data Protection Regulation: A Primer

Ed Hudson, CSU Chief Information Security Officer

OVERVIEW

- A Brief History of Data Protection
  - FIPPs & development of data privacy concepts
  - European Union versus U.S. approaches to data privacy
- GDPR
  - General provisions
  - GDPR versus FERPA

A Brief History of Data Protection

A BASIC OVERVIEW

- Data privacy refers to the protection of sensitive information about individuals that is collected, processed, stored and transferred by an entity
- First articulated by the US in the Fair Information Practice Principles (FIPPs) in 1973
- Led to adoption of US Privacy Act of 1974 (and thousands of subsequent statutes, regulations and laws)

See https://www.dhs.gov/publication/fair-information-practice-principles-fipps

FIPPs

- Data will not be collected absent a specific purpose
- Data will be accurate, and kept only as long as is necessary for the purpose for which it was collected
- People will be told what data is collected and how it will be used
- Data will not be shared with others without permission
- Data will be secured against unauthorized access

APPLICATION OF FIPPS IN THE US

- Sector-specific data protection
  - HIPAA (medical); FERPA (educational); GLBA (financial); FTC privacy and data safeguarding rules (commercial and credit transactions), COPPA (children), etc.
  - Many laws regulate only part of the data lifecycle (collection, processing, use, retention, transfer, disclosure, deletion)
- Federal and state laws and regulations

APPLICATION OF FIPPS IN THE EU

- EU Data Protection Directive of 1995
  - Data regulated based on its content rather than how it is used
  - Regulated all transactions regardless of industry
  - Addressed entire data management lifecycle
  - Consensus framework individually legislated by 28 member states
  - Applied to data collected in the EU

See Directive 95/46/EC at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

APPLICATION IN THE E.U.

- "Data Controller"
  - "The natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data . . . ."
- "Data Processor"
  - "A natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller."

APPLICATION IN THE E.U.

- What does "processing" cover?
  - "Processing" includes collection, retention, use, transfer, disclosure and deletion of data
  - Processing may also include inadvertent disclosure (*e.g.*, data breach)
- Who is responsible for "processing"?
  - The **data controller** retains responsibility for all data processing, regardless who does it

GDPR: THE BASICS

- Enacted as law (legally binding on all 28 member states) in April 2016
  - Uniform protections for all EU residents regardless where the data controller or processor is located
  - Shift from a “directive” to a “regulation”
  - Requires affirmative demonstration of compliance
  - Robust enforcement

GDPR: THE BASICS

- Who is subject to this law?
  - 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
  - Any entity anywhere in the world that monitors the behavior of EU residents

GDPR: THE BASICS

- Whose data does it cover?
  - Individuals physically present in the European Union, regardless of citizenship or nationality
  - EU residents anywhere in the world (except for certain types of one-off data transactions)
  - Individuals only
    - Data regarding corporations or other legal entities, such as universities or nonprofits, are not included)

See GDPR Recitation item 14 (“The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data”)

GDPR: THE BASICS

- What data is covered?
  - All personal data are subject to core protections
  - Any data that can be used (even indirectly) to identify a person
- Extra protection for “sensitive personal data” (ethnic origin, religion, political views, sexual orientation, etc.)
- Less stringent requirements for encrypted or pseudonymous data

GDPR: Personal Data

(a non-exhaustive list)

- Name, address, telephone
- Genetic data*
- Biometric data*
- Physical description
- Photographs
- Education
- Birthdate
- National origin
- Location data
- Race/ethnicity
- Religion
- Sexual orientation
- IP addresses
- Political affiliation
- Financial matters
- “Data concerning health”
- Employment history
- Online identifiers

* Where being processed in order to uniquely identify an individual

GDPR: THE BASICS

- What data management is covered?
  - Collection
  - Retention
  - Use, transfer, and disclosure
  - Deletion
  - Breaches of data (non-consented disclosure)
- Valid legal reason is required for each processing activity (and may require separate consents)

GDPR: THE BASICS

- What is the legal basis for collection?
  - Consent
  - Contract
  - Legal Obligation (Law enforcement and Govt.)
  - Vital Interest (Medical)
  - Legitimate Interest
  - Public Task
- Valid legal reason is required for each processing activity.
- DPIAs required for each activity

GDPR: THE BASICS

- What does consent mean?
  - Direct consent, freely given, for <u>each</u> transaction in which data is collected
  - Indirect consent through a contract to which the data subject is a party
  - Compliance with controller's legal obligation
- Provides strong incentive for data minimization

See GDPR Articles 13 & 14

GDPR: THE BASICS

- Consent does not include:
  - General waivers
  - Mandatory consent as condition for providing services not requiring the information
  - Overarching “check the box” transactions
  - Automatic opt-in consent with optional opt-out

See GDPR Articles 13 & 14

GDPR: THE BASICS

- Data subject's rights:
  - The "right to be forgotten"
  - Access for the purpose of examination, correction, objection and erasure (without fee, unless the request is "manifestly excessive")
  - Data portability
  - Restriction on scope of processing
  - No profiling without consent

See GDPR Articles 13 & 14

GDPR: THE BASICS

- Data Controller/Processor Required Disclosures to Data Subjects
  - Identity and contact information of controller
  - Legal basis and purpose of data collection
  - Recipients (by category) of collected data
  - Data retention and deletion policies of data controller
  - Whether data will be maintained in a third country

See GDPR Articles 13 & 14

Questions?

GDPR: THE BASICS

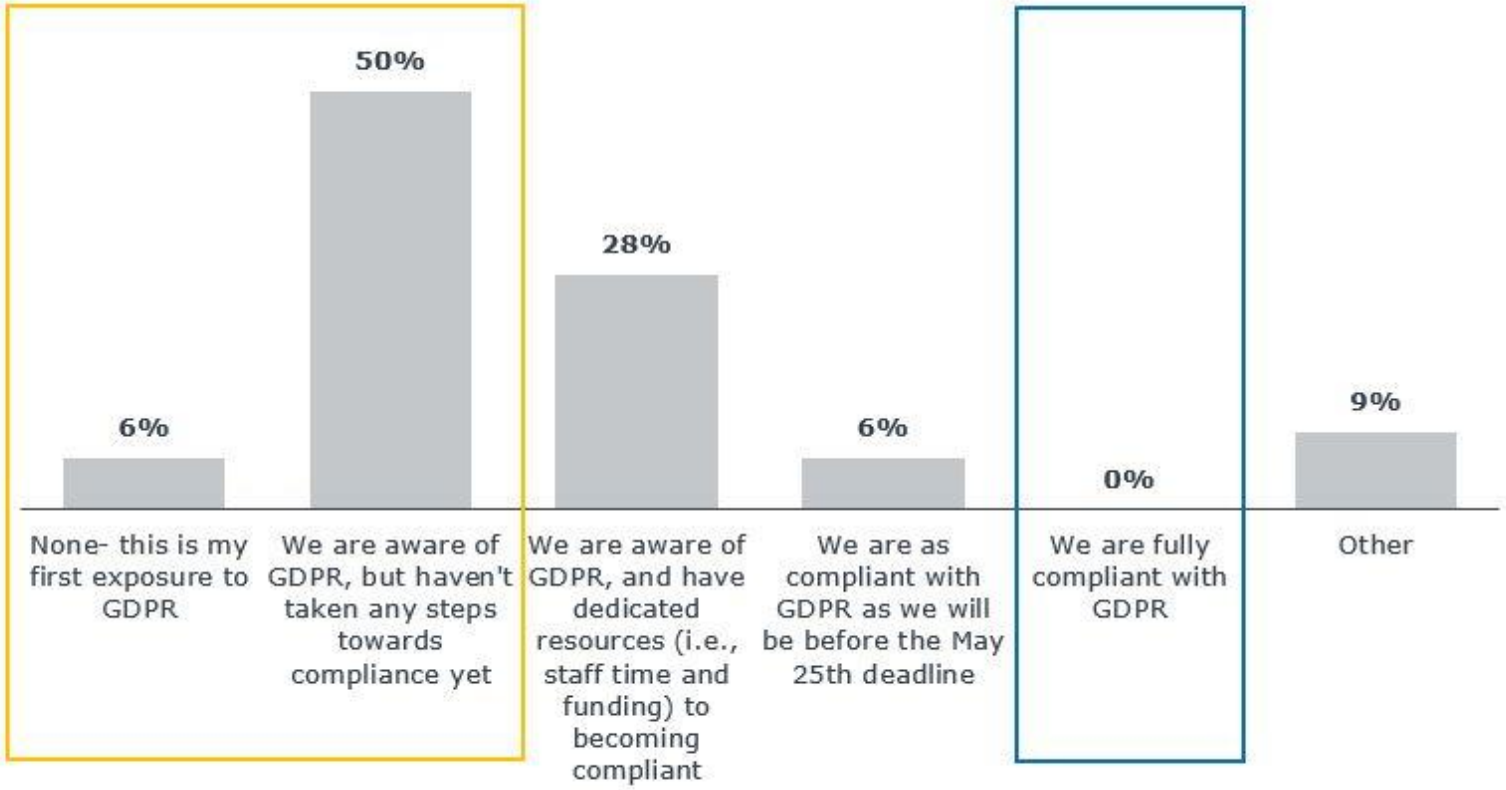
- Data Breach Notification Requirements
  - Within 72 hours of discovery
  - To the appropriate European Union member state regulatory authority (DPA)
  - With information regarding remedial steps taken in response to breach
  - With notification to data subjects “without undue delay”

See GDPR Articles 33 & 34

FERPA versus GDPR

FERPA	GDPR
• "Directory information" is public unless the data subject affirmatively opts out • Focus is on post-collection issues (who can get data, either inside or outside the University); does not address collection or retention policies	• All personal information is protected unless the data subject affirmatively consents to disclosure • 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

HIGHER ED COMPLIANCE ISSUES



Privacy, Where are we running to

- AB 375- CA Data Privacy Protection Act
  - Passed in one week
- “When data sharing helps us get what we want, we all say yes. When it’s disadvantageous, we want the ability to retract our yes, or to say no in the moment. This is why I admire the GDPR: it’s about you, the data subject, being able to decide how your information gets used. It emphasizes user control, and it requires entities that deal with personal data to be flexible.”- Rita Heimes

PRIVACY WORKING GROUP

WHO	WHAT
CISO International Programs Information Technology OGC --- Human Resources Student Affairs Academic Affairs Risk Management CMS/PeopleSoft Labor Relations	• GDPR compliance • Review of existing policies • Development of CSU privacy policy • Develop templates for campus use • Review of data classification standards • Chief Privacy Officer

Questions?