Agenda

- Purpose
- Privacy Basics Review
- GDPR Review
- California update
- Questions, discussion
Privacy Fundamentals

• Privacy: **Control** over our domains (body, territory, communication, associations, data)
  • Data privacy: Control over how your data are collected, used, and shared
GDPR: Background Review

• European Union’s General Data Protection Regulation
  • Relevant to individuals in 30 EEA Member States (EU members plus Iceland, Liechtenstein, and Norway)
  • UK has very similar regulations
  • Generally:
    • Handling personal data is illegal unless specifically legal
    • Be clear and transparent about processing
    • Gives rights to individuals
Due to competing goals, GDPR is both broad and vague, but it follows certain principles:

- **Empower individuals** (data subjects’ rights)
- **Lawfulness, fairness, and transparency**
- **Purpose limitation** (specified, explicit, and legitimate purposes)
- **Data minimization** (adequate, relevant, and limited amount)
- **Accuracy**
- **Storage and retention limitation**
- **Security**
- **Accountability**
GDPR: Scope Review

- Applies to: “Entities…processing…personal data”
  - WHO: “Entities”
    - Relevant to UC San Diego if:
      - Offering goods or services (payment not required) to individuals in the EU,* or
      - Monitoring behavior of individuals in the EU*
  - WHEN: “Processing”
  - WHAT: “Personal data”

*Note: this is location-based, not citizenship or residency*
GDPR: Definitions Review

**PROCESSING:** Any operation performed on personal data, such as:

- Collecting
- Recording
- Organizing
- Structuring
- Storing
- Adapting or altering
- Retrieving
- Consulting
- Using
- Disclosing
- Making available
- Aligning or combining
- Restricting
- Erasing or destroying
• **PERSONAL DATA:** Any information related to an identified or identifiable person, in particular by reference to an identifier, such as:
  - A name
  - An ID number
  - Location data
  - An online identifier, or
  - One or more factors specific to:
    - Physical
    - Physiological
    - Genetic
    - Mental
    - Economic
    - Cultural
    - Social identity of that person

• Special considerations given to **SENSITIVE TYPES OF PERSONAL DATA:** data about crimes, data of minors, and special categories
• **PERSONAL INFORMATION**: Information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household
  
  • Definition is even broader than GDPR!
  
  • Includes such things as alias; device info; browsing and search history; interactions with a website, app, or ad; inferences drawn from any such information that reflects “preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes” and “audio, electronic, visual, thermal, olfactory” info!
• Processing must be lawful and based on one of the following:
  • Consent
  • Contract with data subject
  • Legal obligation, as defined by EU or Member State law
  • Vital interests of data subject (life or limb)
  • Public interest or official authority, as defined by EU or Member State law
  • Legitimate interest of controller or third party
GDPR: Consent Review

- Must be freely given, specific, informed, unambiguous, and clear indication of wishes
- Distinguishable from other matters
- Must be as easy to withdraw consent as it is to give it!
- What's **NOT** consent
  - Blanket consent
  - Bundled in clickwrap
  - Silence/inactivity
  - Pre-ticked boxes
  - Conditioning service on data that is not necessary for performance
GDPR: Responding to Data Subject Requests

- Data Subjects’ Rights
  - Transparency and right to be informed
  - Right to access own data
  - Right to rectify
  - Right to restrict processing
  - Rights regarding automated decision-making
  - Right to erasure (“right to be forgotten”)
  - Right to data portability
  - Right to controllers facilitating rights

- 30 days to respond; 2 additional months, if necessary or if complex request
• Data subjects requests must be communicated to vendors/service providers
  • Note: Trackability obligation!
  • IT involvement is key!

• The rights are NOT absolute
  • Contact privacy office, counsel, or records administration
GDPR: Requirements of Particular Processing

- Maintain written record of processing activities specifying
  - Name and contact of controller
  - Purpose of processing
  - Categories of data subjects
  - Categories of personal data
  - Categories of recipients
  - Transfers to third countries
  - Retention period
  - Description of security measures

Translation: Basically, “Do a processing inventory and a data map; document!”
• Build privacy into requirements-gathering and design stages of projects (privacy-by-design)
• Minimize data
  • Required info vs. nice-to-have
• Implement appropriate security measures
• Respond to data subject requests within a month*
• Use suppliers providing appropriate compliance
• Execute special contracts with partners
• Transfer outside EU only under certain conditions

*Do NOT take any action based on a data subject request without consulting with privacy office, counsel, or records administration
GDPR: Why Should We Care?

- Fines of up to €20,000,000 (~$23.5M) or 4% of total worldwide yearly revenues, whichever is higher
- Inability to collaborate with entities that comply with GDPR
- Inability to transfer data from the EU
- Private claims for compensation from data subjects
- Scrutiny and audits of all data practices by data protection authorities

- Also... preparation for what's on the horizon...
Sweeping California privacy law passed in June 2018; effective January 2020

- Does not apply directly to much of what UC does

- Many of the same principles as GDPR:
  - California residents protected with respect to “any information that relates” to them
  - Requires data maps, inventories, and records in many circumstances
  - Update policies
  - Update systems and processes to protect privacy
  - Specifies methods of data subject requests and a clear “do not sell my data” link on websites

Shameless Plug

• Get your staff, researchers, and students trained on privacy
  • The UC San Diego Privacy 101 Workshop is open to all of UC and the public
GDPR: Resources

- **Primary**
  - European Data Protection Board [website](https://edpb.europa.eu) (for interpretations and standard contract clauses)

- **Guides, slides, and surmise**
  - Trusted CI: NSF Cybersecurity Center of Excellence, [GDPR Webinar](#) (May ‘18) and [slide deck](#) (special thanks to Scott Russell)
  - EDUCAUSE [GDPR Resource library](#)
  - Institute of Fundraising, “[Connecting People to Causes: A Practical Guide to Fundraising Research](#)”
  - SuperOffice.com: [GDPR for Marketing: The Definitive Guide for 2020](#)

- **Examples**
  - Cambridge University [toolkit](#) and [Data Protection webpage](#) (great source for privacy statement language)
  - Juro.com [privacy statement](#) (great example of layered, easy to understand privacy statement)

- **UCOP General Counsel Advisories** (contact Privacy Office)
Suggestions, comments, questions

Pegah K. Parsi, JD MBA
Campus Privacy Officer
pparsi@ucsd.edu
privacyofficer@ucsd.edu
858-822-4439
privacy.ucsd.edu

@UCSD_Privacy