

UC San Diego

VENDOR REVIEWS AND PRIVACY CAMPUS LISA OCTOBER 2021

Pegah K. Parsi, Campus Privacy Officer
she/her/ella

KUMEYAAY LAND ACKNOWLEDGEMENT

The UC San Diego community holds great respect for the land and the original people of the area where our campus is located. The university was built on the unceded territory of the Kumeyaay Nation. Today, the Kumeyaay people continue to maintain their political sovereignty and cultural traditions as vital members of the San Diego Community. We acknowledge their tremendous contributions to our region and thank them for their stewardship.

Objectives

- Quick review of privacy and personal data
- What needs privacy review?
- Understand preliminary questions to ask project leaders and vendors
- Myths and FAQs
- Questions and dialogue

Privacy Fundamentals Review

- Privacy:
 - Not just about confidentiality/secretcy
 - Ability to **exercise control** over one's self and understand the decisions made about one's self, including about one's:
 - Body
 - Territory and space
 - Communications
 - Personal data



Privacy Fundamentals (cont'd)

Relationship between privacy and security



- Security plays an important role in the protection of privacy; however...
- Privacy can't be achieved solely by securing personal data (think ethical use, consent, rights to data)
- And sometimes, the two concepts are in conflict! (consider airport security, surveillance cameras, email monitoring, DLP programs)

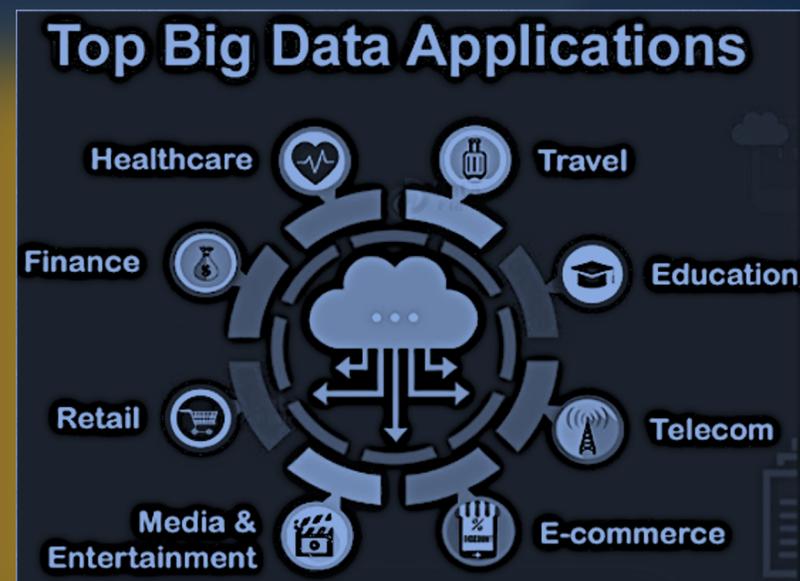
Third party reviews

- Third party engagements -- paid and unpaid – can pose risks to and are reviewed for myriad things, like:
 - Accessibility
 - Export control
 - Fair labor practices
 - Financial and legal risks
 - Security
 - AND privacy



Third party reviews

- Security reviews third party's security practices to ensure they meet the UC standards for the sensitivity level of the data or system
- The Campus Privacy Office reviews the **entire project** (the vendor and our implementation, our data handling practices) to protect individuals, ensure ethical data practices, and comply with laws and policies (for all non-UCSD Health)



What needs a privacy review?

- Any campus project where the third party handles, collects, processes, maintains, creates, transfers, etc. **P-3 or P-4 personal data**
- **Existing vendors** used in **new context** involving P-3 or P-4 personal data on campus
- **Material changes** to a campus project; the type or volume of data involved; population of data subjects; or vendor's practices



NOTE: UCSD Health projects should contact the Health Sciences Office of Compliance and Privacy.

What does privacy review for?

- Compliance with laws and policies
 - Allowable uses and disclosures
 - Consent/notice requirements
 - Contractual requirements
 - Training requirements
 - Privacy impact assessments, if required
 - Appropriateness of the disclosure limitation methods (e.g., anonymization, differential privacy, masking)



What else does privacy review for?

- Ethical considerations, including data ethics
 - Reuse/sale of data, incl. “de-identified” data
 - Transparency and communicating your purpose
 - Whether third party creates profiles of individuals
 - AI and algorithmic bias
 - Disparate impact on certain populations
 - Normalizing surveillance



Why you should care...

- Litigation risk
- Reputational risk
- Easier to frontload than retrofit
- Increased interest in privacy following high profile breaches
- Regulatory move toward deleting inappropriately collected/handled data (e.g., without notice)
- It's the right thing to do



Some privacy questions (internal)

- Questions for our own UCSD units (in addition to regular security and accessibility questions):
 - What data are provided? How detailed are reports?
 - What population's data are involved? Where are they geographically?
 - Does data move into or out of the United States? If so, where to/from?



Some privacy questions (vendor)

- Questions for vendors and UCSD units:
 - Does the vendor use this data for any other purpose? To train its algorithm? For facial recognition?
 - Who de-identifies the data? How? By what standards? What do they (or you) use “de-identified/anonymized” data for?
 - With whom do they/you share data (including “de-id’ed” data)?



Some privacy questions (vendor)

- Questions (cont'd)
 - Does the vendor have a documented policy for reviewing its code and processes for bias?
 - Do they create a profile of users?
 - Do they combine this data with data from other sources?
 - Do they share with other entities that combine this data with other sources?



FAQs

- How do I get a privacy review?
 - privacy.ucsd.edu → Forms & Templates → Vendor Privacy Risk Form (pilot)

The screenshot shows the UC San Diego Privacy website. The page title is "PRIVACY" and the logo "UC San Diego" is in the top right. A navigation menu includes: What is Privacy, Policies, Guiding Principles, ISPC, Trainings, Services, GDPR, COVID-19, Forms & Templates, and Contact. The breadcrumb trail is "HOME / Forms & Templates". The main heading is "Forms & Templates" with a list of five links: 1. [DATA SUBJECT REQUEST TO RESTRICT, OBJECT TO, OR DELETE PERSONAL DATA](#), 2. [LETTER OF RECOMMENDATION RELEASE FORM](#), 3. [ACCESS WITHOUT CONSENT \(email \[ucsdprivacy@ucsd.edu\]\(mailto:ucsdprivacy@ucsd.edu\)\)](#), 4. [VENDOR PRIVACY RISK FORM \(pilot\)](#), and 5. [SYLLABUS PRIVACY MODEL/TEMPLATE](#). A sidebar on the left contains links for Privacy, What is Privacy, Policies, and Guiding Principles.

- When should I ask for a privacy review?
 - The sooner in your project/program design the better, but certainly before you sign a contract, implement the program, or transfer data.

FAQs

- **What happens at the end of a privacy review? Does the Campus Privacy Office have to approve my project?**
 - The Campus Privacy Office provides a written determination that the project, as described, results in low, moderate, or high privacy risk to individuals and to the university and provides recommendations on specific controls that may mitigate risk.
- **How long does a privacy review take?**
 - It depends on the complexity of the project and how long it takes the unit and vendor to provide responses to the Vendor Privacy Risk form. The sooner you start, the better.

FAQs

- **Are privacy reviews only needed for software purchases?**
 - No. Reviews are NOT limited to software purchases! Other services, for example, photography, paper storage, security cameras, conference administration, and translators all have privacy issues.
 - Also, reviews are NOT limited to purchases at all! Freebies and off-the-shelf products also present concerns.
- **Security already reviewed my project. Isn't that enough?**
 - No. Privacy and security reviews have some commonalities, but they are different. Privacy reviews for such things as consent, notice, data ethics, and AI bias. Plus, privacy is increasingly a very complex and rapidly-changing field. The best place for the latest in privacy law updates is with the Campus Privacy Office.

FAQs

- *[Insert other UCs/departments/university here]* is already using the service. Isn't that enough?
 - No. Context of use matters!
 - Plus, privacy reviews are relatively new in higher ed (but not in industry!) and not all places review to the same standards or at all.
- **The IRB reviewed my project. Isn't that enough?**
 - No. The UCSD IRB does not review for privacy compliance. Plus, privacy is increasingly a very complex and rapidly-changing field. The best place for the latest in privacy updates is with the Campus Privacy Office.

FAQs

- We are only giving FERPA directory information (e.g., names and email addresses) to the third party. Do we need a privacy review?
 - It depends. If the vendor's software logs locations, date-time stamps, device IDs, or IP addresses, they are handling sensitive data. These are all considered sensitive under various privacy laws (including in California!). Takeaway: Don't just think about what you are handing to the vendor, but consider ALL of the personal data the vendor will have on an individual.

Shameless Plug

- The UC San Diego **Privacy 101 Workshop** are free and open to all of UC and the public

The screenshot shows the UC San Diego Privacy website. The header includes the 'PRIVACY' logo and the 'UC San Diego' name. A navigation menu lists: What is Privacy, Policies, Guiding Principles, ISPC, Trainings, Services, GDPR, COVID-19, Forms & Templates, and Contact. A search icon is also present. The main content area is titled 'Trainings' and includes a sub-section for 'Training and awareness'. It lists two main training categories: 'Privacy 101 Workshop' and 'General Data Protection Regulation (GDPR) Primer'. The 'Privacy 101 Workshop' section lists dates and times for sessions from 04/22/21 to 11/18/21. The 'GDPR Primer' section notes that registration is required via the UC Learning Center. A sidebar on the left contains a menu with items: Privacy, What is Privacy, Policies, Guiding Principles, ISPC, Trainings (highlighted), Services, GDPR, and COVID-19. An illustration of a laptop with various data icons is shown on the right side of the page.

PRIVACY UC San Diego

What is Privacy Policies Guiding Principles ISPC Trainings Services GDPR COVID-19 Forms & Templates Contact

HOME / Trainings

Privacy

What is Privacy

Policies

Guiding Principles

ISPC

Trainings

Services

GDPR

COVID-19

Trainings

[Training and awareness](#) (check back for updates)

- Privacy 101 Workshop:** Open to UC and the public. This is a prerequisite for any of the other trainings (registration required via [UC Learning Center](#); if you are unable to register through the UC Learning Center, email ucsdprivacy@ucsd.edu to be added to the list. Non-UCSD please register through [Eventbrite](#))
 - 04/22/21: 8:45 AM - 12:00 PM (Zoom)
 - 05/18/21: 8:45 AM - 12:00 PM (Zoom)
 - 06/23/21: 12:45 PM - 4:00 PM (Zoom)
 - 07/22/21: 12:45 PM - 4:00 PM (Zoom)
 - 08/18/21: 8:45 AM - 12:00 PM (Zoom)
 - 09/28/21: 12:45 PM - 4:00 PM (Zoom)
 - 10/26/21: 12:45 PM - 4:00 PM (Zoom)
 - 11/18/21: 8:45 AM - 12:00 PM (Zoom)
- General Data Protection Regulation (GDPR) Primer** - (registration required via [UC Learning Center](#); if you are unable to register through the UC Learning Center, email ucsdprivacy@ucsd.edu to be added to the list) Non-UCSD please register through [Eventbrite](#).

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](https://twitter.com/UCSD_Privacy)



UC San Diego