



**FAMU**

FLORIDA A&M UNIVERSITY

**ENTERPRISE RISK  
MANAGEMENT**  
DIVISION OF AUDIT

**Psst!**

# Privacy in Higher Education

---

Risk Bulletin #2023-ERM-01

---

July 19, 2022



## Overview of Privacy in Higher Education

The passage of the General Data Protection Regulation (GDPR) brought privacy to leaderships' attention at organizations across the globe. Multiple states and countries have passed or are currently preparing comprehensive data privacy and security legislation. For example, in the United States, the California Consumer Privacy Act (CCPA) was passed following GDPR. Since 2013, 41 states have enacted more than 120 supplemental laws, according to Huron report, [Shades of Gra: Evolution of Data Privacy Standards in Higher Education](#).

The growing number of privacy laws and regulations that higher educational institutions must understand and comply with is only half the privacy battle. Higher education institutions are rapidly forming partnerships with third-party vendors, integrating artificial intelligence and data analytics tools into research, business, and academic processes, and allowing a variety of smart and personal technology to be utilized on campuses. While all of these may help push universities into new frontiers of innovation, efficiency, and competitiveness, they all come with a variety of privacy and ethical concerns that institutions must find a way to meet the needs of their stakeholders while maintaining public trust and reducing liability to their organizations.

In 2020, EDUCAUSE and Huron conducted a data privacy study, [The Evolving Landscape of Data Privacy in Higher Education](#). This study provided the following higher education privacy insights:

- 62% of institutions have created privacy officers or privacy officer positions. With the exception of those employed at highly mature privacy organizations, respondents cited additional staffing as the number-one resource they desired. For those who wear a privacy hat among many others, other duties often precluded them from spending sufficient time developing more than the most rudimentary privacy resources.
- A great deal of time and effort is required to create and distribute all the necessary privacy policies and to build privacy awareness campaigns and trainings for faculty and staff.
- Noted a lack of privacy discussions in contact-tracing planning meetings. As institutions continue to collect and store personal data to ensure a safe and secure presence on campus, privacy professionals should be consulted to help institutions be transparent about their data processes and to ensure the privacy of individuals is safeguarded.
- Privacy concerns arise when staff, faculty, and students work and learn from home including issues of equity, sharing of private information during business calls, recording of students' names, faces, and home environments, and sharing of information during online proctoring of exams.
- Proactively creating a privacy program and policies based on the institution's underlying values, which then lay the groundwork for meeting or exceeding future laws and regulations, is one of the best ways to prepare an institution for any such future legislation.
- Students are not well informed about how institutions use their data.



- Both new and old privacy offices in higher education will need to conduct privacy and security risk assessments, both within an institution when people and offices are working with PII and with outside vendors and third-party solution providers that also require data access to fulfill their services.

## Chief Risk Officer Recommended Actions

- Perform an enterprise-wide privacy assessment to review privacy practices at FAMU and develop recommendations for improving FAMU's privacy governance and programming.
- Establish a privacy officer position, or integrate role responsibilities into a current position, to coordinate privacy efforts across the University.
- Clearly define ownership for key privacy areas across the University.
- Develop a comprehensive data governance program.
- Develop privacy education and awareness campaigns for students and staff. For example, adding privacy training as a module in FAMU Fundamentals 2023.
- Integrate detailed privacy reviews into procurement/contract process.

## How Privacy Impacts the University's Strategic Plan: Boldy Striking

- **FAMU Strategic Priority 2: Academic Success/Goal 3**
  - Position FAMU to emerge as a world-class leader in healthcare education, research and service to address disparities, emergent needs and advance holistic well-being.
- **FAMU Strategic Priority 5: Organizational Effectiveness and Transformation/Goal 2**
  - Optimize effectiveness of operations through enhancement of processes and innovation.
- **FAMU Strategic Priority 5: Organizational Effectiveness and Transformation/Goal 3**
  - Strengthen the University's culture of strategic decision making through promotion and enhancement of compliance, internal controls, and enterprise risk management practices with an emphasis on engagement, education, reporting, and accountability.

## Senior Leadership Team Suggested Points of Discussion

- What privacy concerns do each division have? What additional privacy concerns related to FAMU DRS should be discussed?
- What new legal or regulatory requirements related to privacy has recently been passed or is on the horizon?
- What is the University's stance on privacy and ethics when it comes to the use of artificial intelligence and data analytics?
- Who, or what team of persons, will be responsible for assessing and handling privacy incidents?
- Should a privacy committee be created? Can it be a sub-committee of the Enterprise Compliance Committee, if they do not already have one? If ECC does have a privacy compliance committee, what



have they covered and what do they plan to cover? Does SLT have additional recommendations for people who should be on this committee?

- What is the timeline for creating a data governance program?
- What privacy policies need to be reviewed or created? (i.e. work-from-home, bring-your-own-device, videoconferencing, contact tracing, privacy breach, etc.)

## Additional Privacy Resources

### [Data Defense: Privacy Protection Actions](#)

This article discusses four actions to encourage students to take for better understanding of what data are collected about them and what control they may have over the use of their private information.

### [Educause 2021: What's Next for Data Privacy and Security Laws?](#)

Higher education CISOs prepare for future privacy and security regulations. This article covers: Developing a Culture of Privacy; A High-Level View of a University's Data Inventory; What a Data Governance Framework Should Cover; and The Future of Data Privacy and Protection.

### [Protecting Both Privacy and Security in Higher Ed](#)

This article discusses how partnerships between privacy and security offices help colleges leverage and protect data without compromising confidentiality.

### [What are the elements of privacy risk management and compliance?](#)

This illustration provides guidance on developing and maintaining a structure to fully protect data privacy.

### [U.S. Data Privacy Laws in 2022: State and Federal laws that Protect Your Data](#)

This article will guide you through the U.S. data privacy laws — including both federal and state legislation — that aims to protect the data privacy rights of U.S. citizens.

Authored by:



**Deidre Melton**  
CDPSE, CRMA, CRISC, CIA, CFE, CISA, CISM, CIGI  
Associate Vice President for Audit and Chief Risk Officer  
Florida A&M University