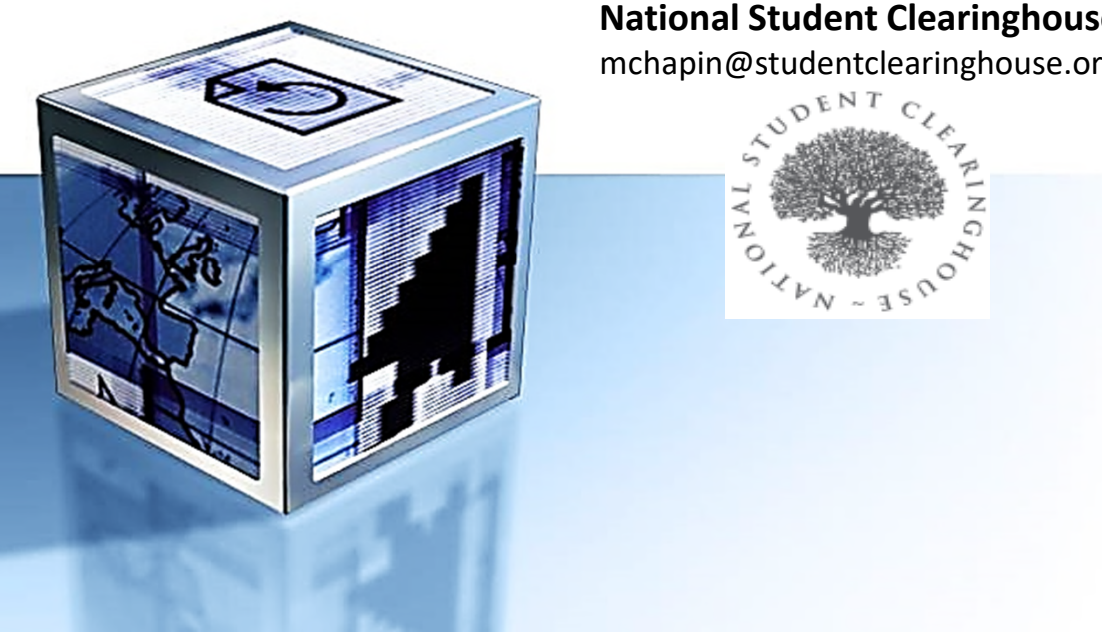
EU General Data Protection Regulation

Mary Chapin
Vice President &
Chief Legal Officer
National Student Clearinghouse
mchapin@studentclearinghouse.org

Julia Funaki
Associate Director
AACRAO
funakij@aacrao.org

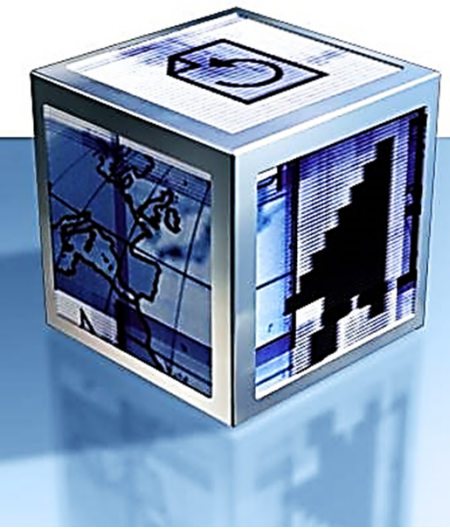
Melanie Gottlieb
Deputy Director
AACRAO
gottliebm@aacrao.org



SPRING 2018 DATA SUMMIT
BEST PRACTICES IN EDUCATION DATA SYSTEMS
MAY 2 – 4, 2018 | WASHINGTON, D.C.

Topics

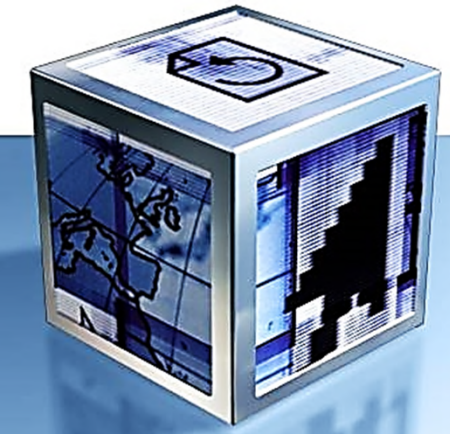
- AACRAO GDPR Survey
- Overview of EU General Data Protection Regulation
  - Key Definitions
  - Extraterritorial Scope
  - GDPR Fundamentals
- Preparation and Strategies for Compliance
- Case Studies



Audience Polling Questions 1-3

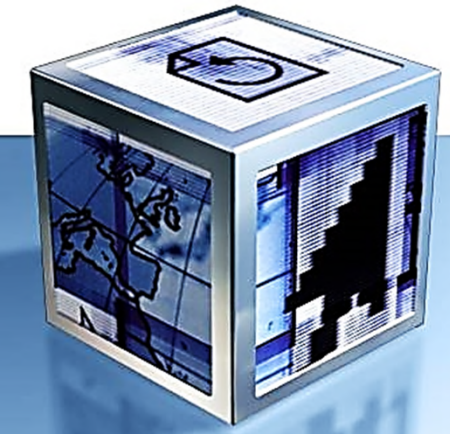
Join at Slido.com

Event Code #D210

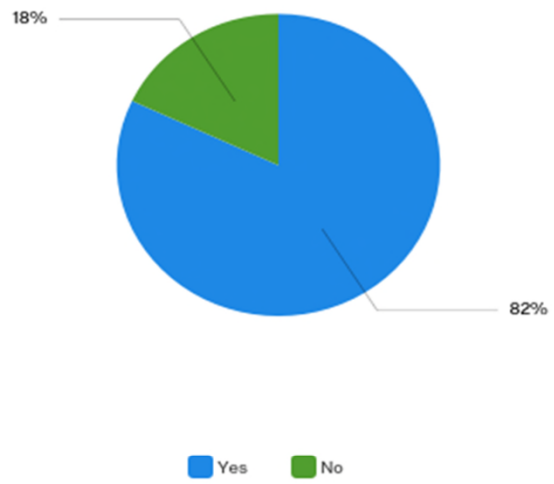


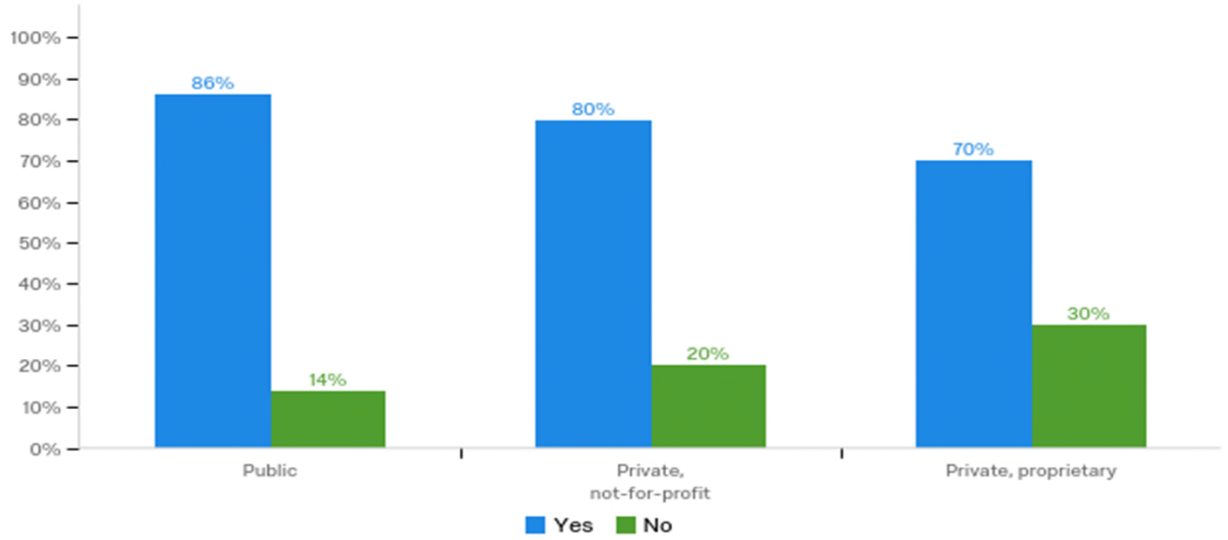
AACRAO Survey April March/April 2018

- Respondent breakdown:
  - 400 responses
    - 60% Private nonprofit institutions
    - 37% Public Institutions
    - 3% Proprietary Institutions

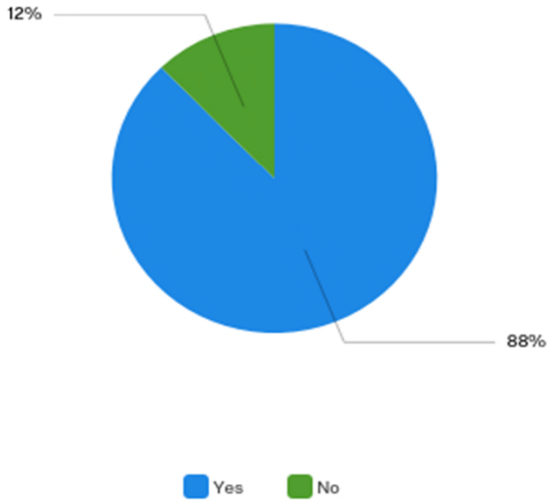


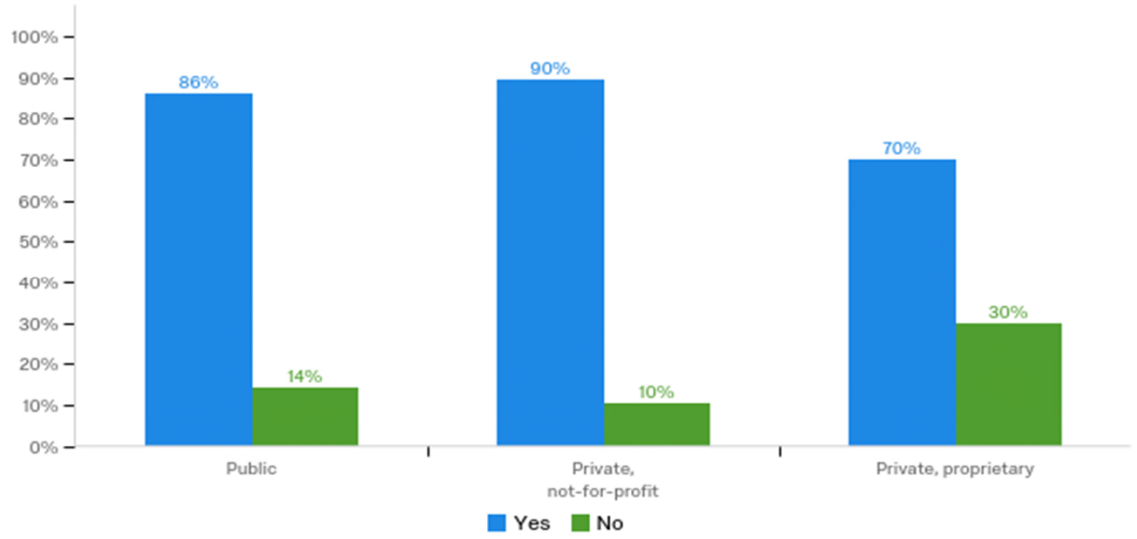
AACRAO Survey: GDPR Awareness Levels





AACRAO Survey: Does GDPR Apply ?



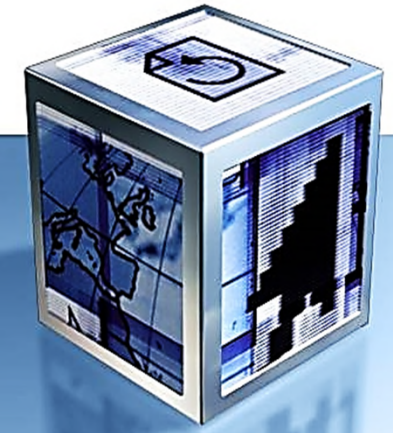


AACRAO Survey: Top Concerns

Answer	%
Right to erasure /to be forgotten	**60%**
Ability of the institution to successfully identify all data paths	**42%**
Availability of human resources to implement policy measures	**33%**
Institutional Prioritization of Compliance to GDPR	**29%**
Security of data processing	19%
Data protection by design	18%
Availability of financial resources to implement policy measures	16%
Identification of Controller/Processor roles and appropriate contracts regarding GDPR compliance	16%
Records of processing activities	14%
Data protection impact assessment	14%
Fines	14%
Breach notification	10%
Institutional Reputation (if non-compliant)	10%

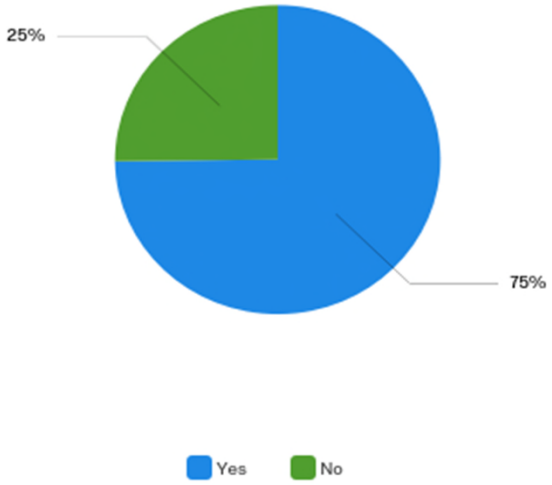
OVERVIEW OF THE EU GDPR – Background

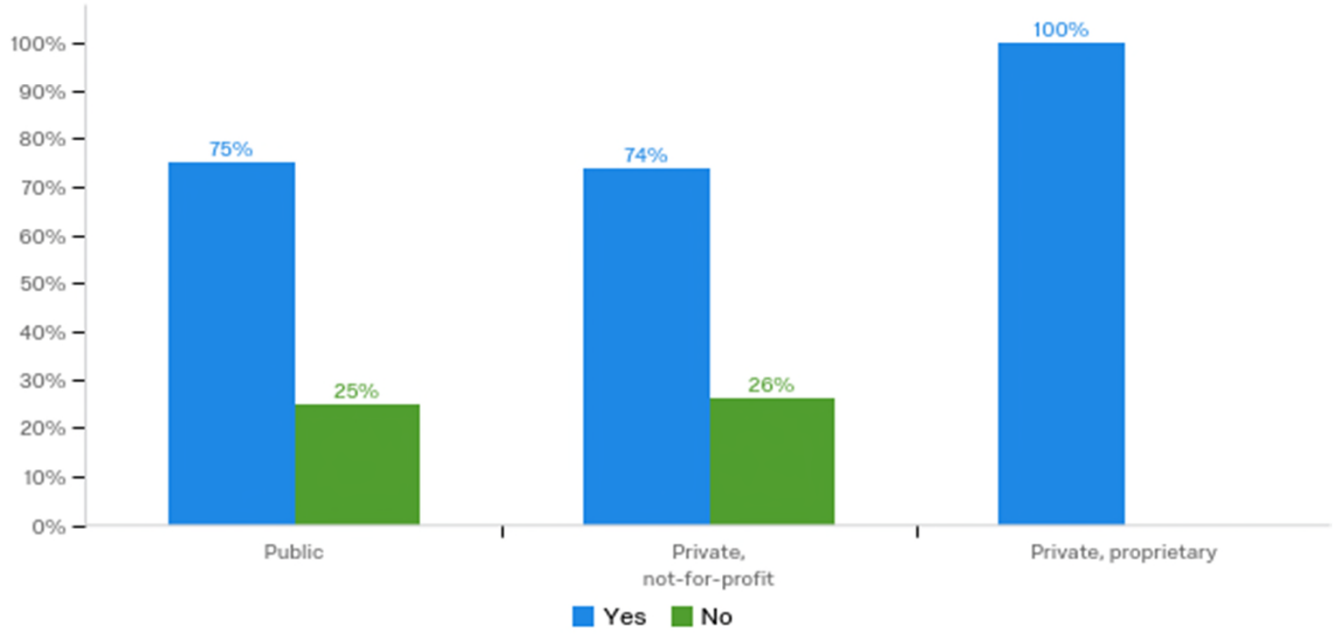
- Replaces current 1995 EU Data Protective Directive
  - *Harmonizes* the data protection laws and makes them legally binding across 28 member states
- Significantly expands personal privacy rights (fundamental rights and freedoms [1]) with regard to processing of and free movement of personal data
  - Acknowledges these rights of natural persons in the EU irrespective of nationality of data subject
- May 25, 2018
- Fines – Very Significant



1 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2016.202.01.0389.01.ENG&toc=OJ:C:2016:202:TOC

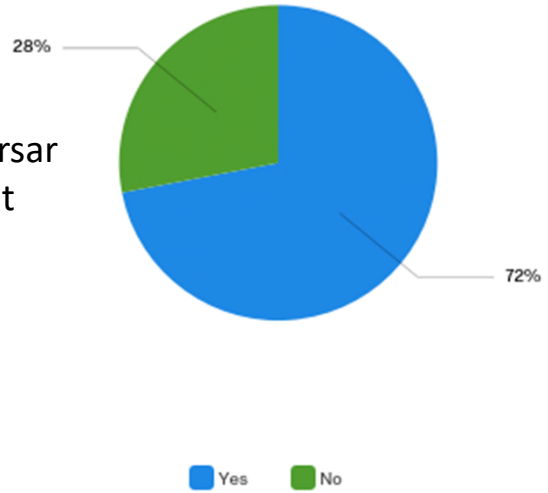
AACRAO Survey: Are You Planning?

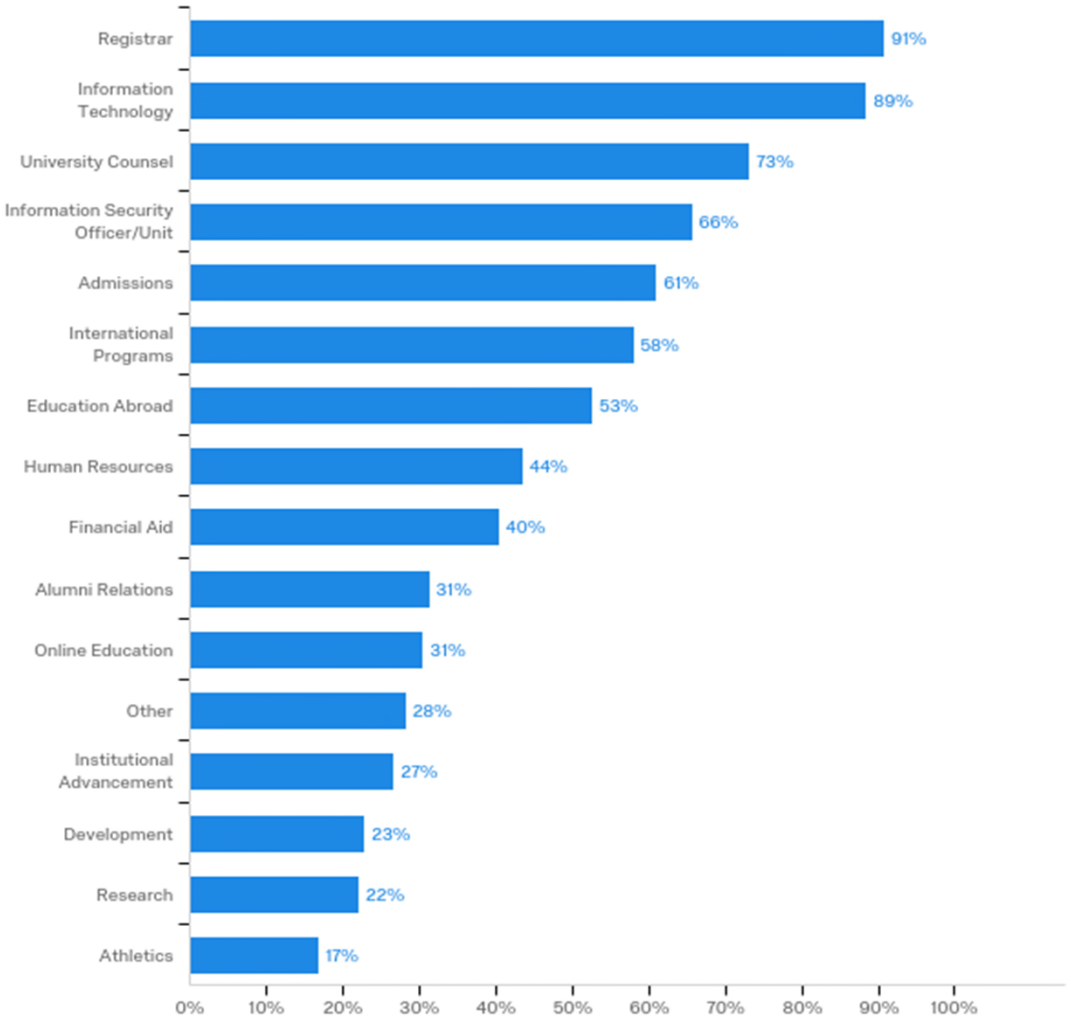




AACRAO Survey: Institutional Planning

Archivist
Academic Affairs/Provost
Compliance Office
Residence Life
Reps from Academic Units
IR/Assessment
Purchasing
Public Safety
Business Office/Bursar
Travel Management
Academic Support
Contacts Office
Procurement





KEY GDPR DEFINITIONS

- **Personal data** – any information related directly or indirectly to a natural person physically in the EU (EU data subject)
  - **Sensitive Personal data** – personal data concerning race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetics or biometrics, health, sex life or sexual orientation, criminal record
- **Controller** – entity that determines the purposes and means of the processing of personal data.
- **Processor** – entity which processes personal data on behalf of and at direction of the controller.
- **Processing** – any operation or set of operations performed on personal data, whether or not by automated means.

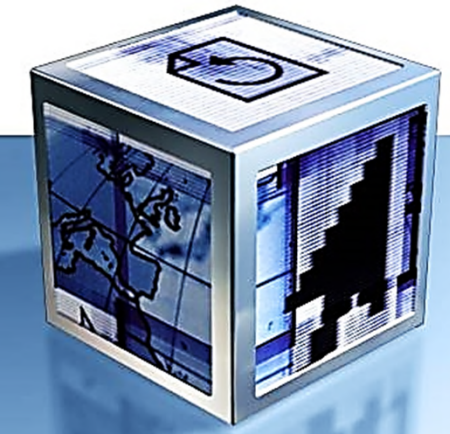
Audience Polling Question 4

Join at Slido.com

Event Code #D210

Extraterritorial Scope of GDPR

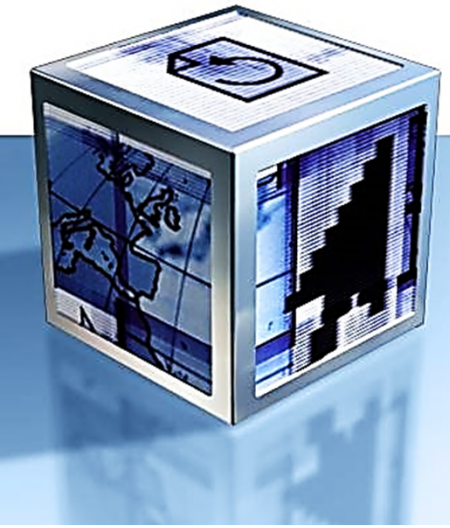
- **Applies to controllers and processors established in the EU even if processing of personal data is outside of the EU**



- **Applies to the processing of personal data by controllers and processors not in the EU where the processing is related to:**
  - Offering good or services to EU data subjects or
  - Monitoring EU data subjects behavior within the EU

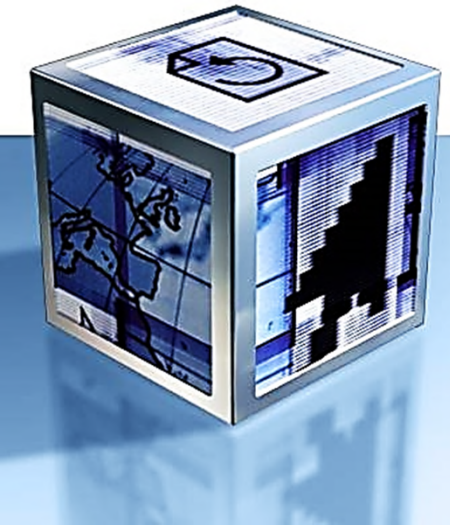
GDPR FUNDAMENTALS

- **Principles Required Under EU Law**
  - Transparency
  - Lawful Basis for Processing
  - Data Minimization
  - Accuracy/right of rectification*
  - Right to be forgotten
  - Data portability*
  - Privacy by design
  - Right to access
  - Security and breach notification*
  - Appointment of Data Protection Officers



GDPR FUNDAMENTALS CONT.

- **Requirement of a Lawful Basis for all data processing**
  - **Consent**
    - Requires clear, affirmative, demonstrable action
    - Right to withdraw consent
    - Cannot be a condition of performance of contract when not necessary
    - Notice requirements attach
  - **When necessary**
    - **To perform or enter into a contract with EU data subject**
    - **For purpose of legitimate interest of the controller**
      - Two part test: ID of legitimate interest and balancing test weighing interest versus fundamental rights and freedoms of data subjects
    - **For compliance with a legal obligation** (EU and Member State law)
    - **To protect "vital interests" of data subject or natural person** (i.e. risk of life or serious harm)
    - **For performance of task carried out in public interest or exercise of official authority**



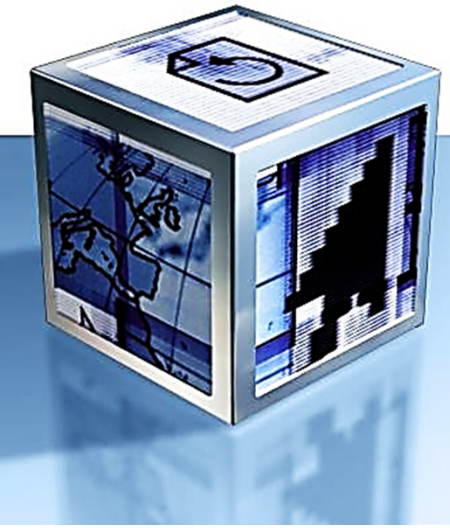
GDPR FUNDAMENTALS CONT.

➢ Controller Obligations

- Implement data protection policies
- Privacy by design and default
- Record keeping of processing activities
- Data security
- Appoint processors by written contract with flow downs

➢ Processor/Service Provider Obligations

- Processor only act on documented instructions of controller
- Confidentiality obligations of all persons who process data
- Security measures
- Implement measures to assist controller in complying with data subject rights
- Deletion or return of data
- Engagement of sub-processors only with written authorization
- Keep records of processing activities

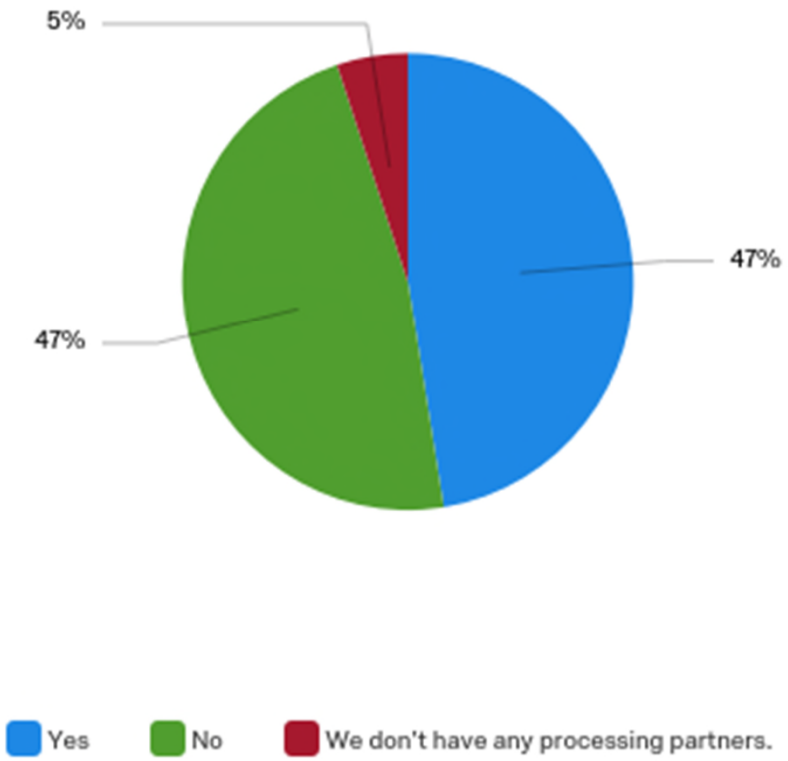


Audience Polling Question 5

Join at Slido.com

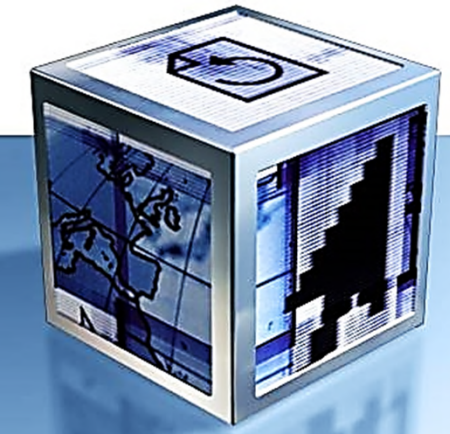
Event Code #D210

AACRAO Survey: Contact with Partners?

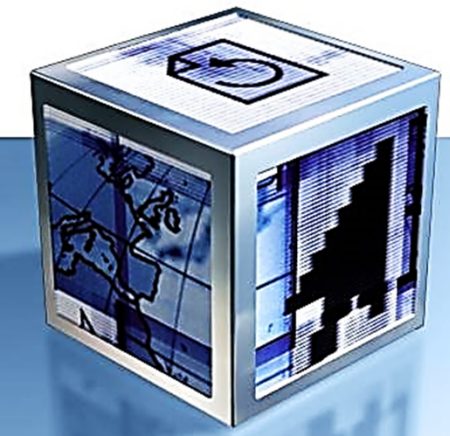


Preparation and Strategies for Compliance

- **Assemble a working group**
  - Counsel
  - Information security and Information technology representatives
  - Representatives from functional units that process personal data
- **Identify impacted offices/departments/units and gather information about activities**
  - Universities with branch campus or study center in the EU
  - Study abroad, exchange, faculty-led, research or internship programs
  - Collaboration with EU institutions
  - Online learning platforms
  - Admissions
  - Recruiting faculty from the EU
  - Alumni relations
  - Development and research
  - Fundraising in the EU
- **Identify what data is collected and where data is collected directly from EU data subjects**



Preparation and Strategies for Compliance Cont.

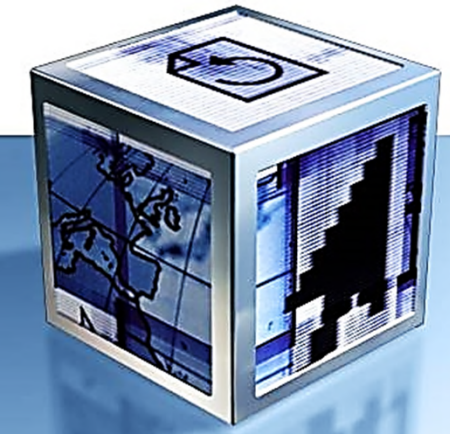


- **Understand business process/scenarios to identify:**
  - Data pathways of the collected data, repositories for data and what processing is taking place
  - Are service provider/vendors processing data
  - Are GDPR compliant contracts governing the processing
- **Determine impact of GDPR on the processing**
  - Determine lawful basis for processing
  - If consent, are notice methods adequate and complete
  - Document lawful basis and analysis
- **Understand existing policies germane to GDPR and revise policies and notices** (FERPA, Institutional policies, state privacy regulations)
- **Prepare for compliance with EU-US cross-border transfers**

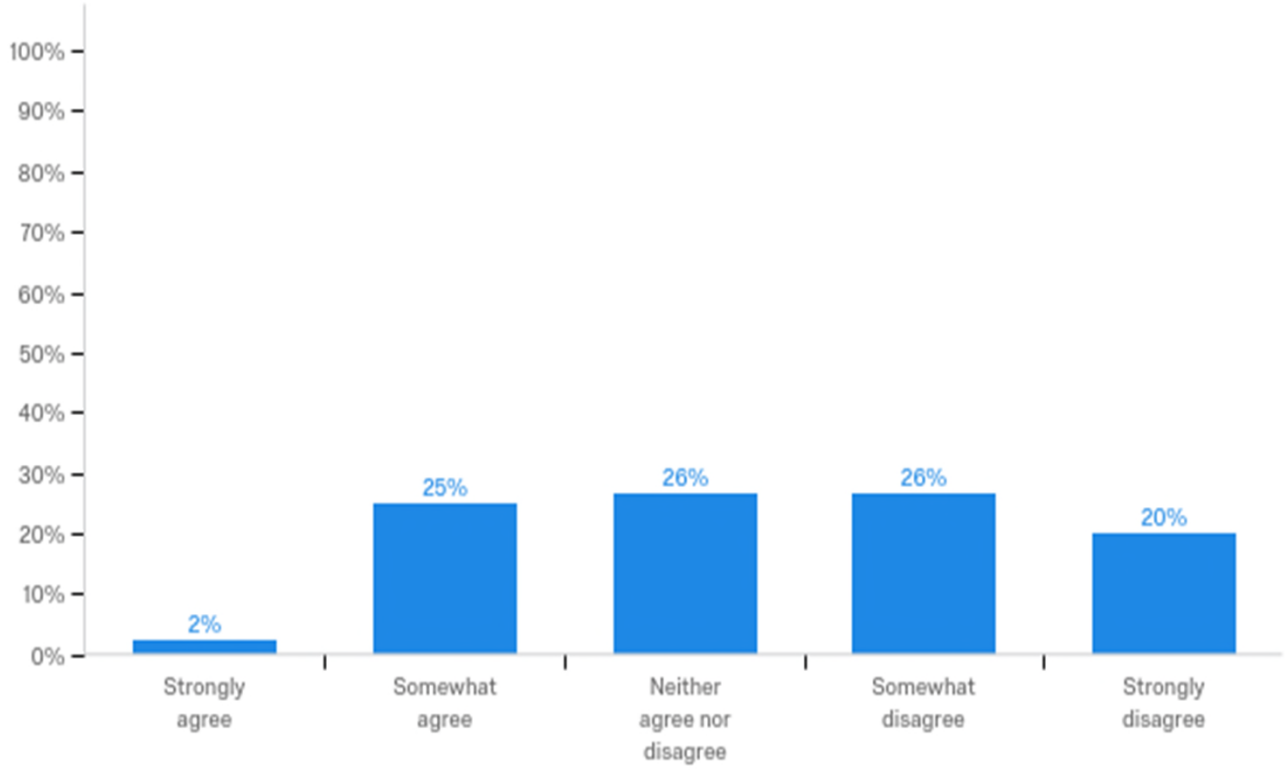
Audience Polling Question 6

Join at Slido.com

Event Code #D210



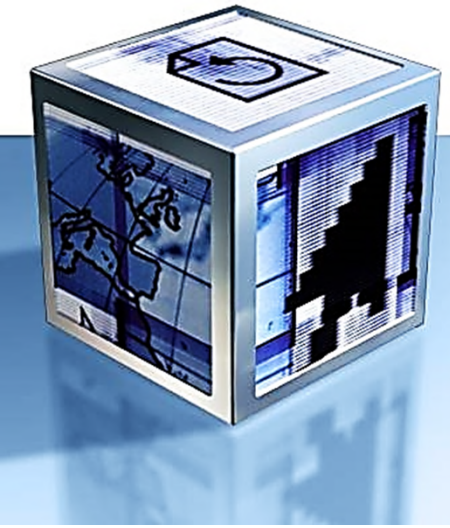
AACRAO Survey: Will you be ready?



Case Study 1– NSC

(Enrollment Reporting Service):

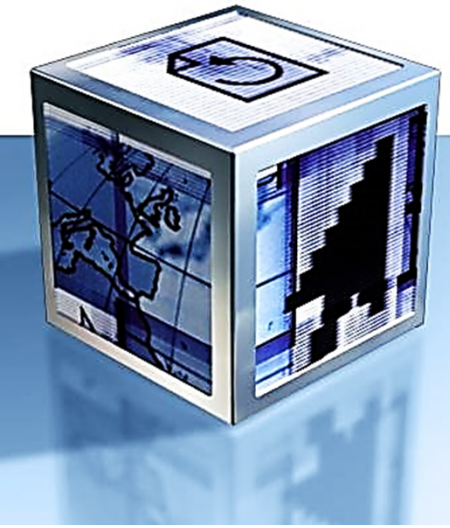
Situation: NSC enters into a contract with individual institutions pursuant to which an institution reports its student enrollment information to NSC and, on the institution's behalf, NSC receives and responds to requests from the National Student Loan Data System (NSLDS), other lenders and servicers in the federal student loan programs, and private lenders seeking to verify the enrollment status of student loan recipients, for purposes of ensuring that such enrolled loan recipients have their loans placed in deferment while they are in school.



Case Study 2– International Enrollment Management

(Recruitment fairs and inquiry cards):

Situation: A university recruitment staff attends a recruitment fair and collects information (inquiry cards) from attendees of the fair who express an interest in attending University X . Upon returning to University X, recruitment staff inputs data into the Customer Resource Management (CRM). This list is used for future outreach campaigns.



THANK YOU!

QUESTIONS & ANSWERS