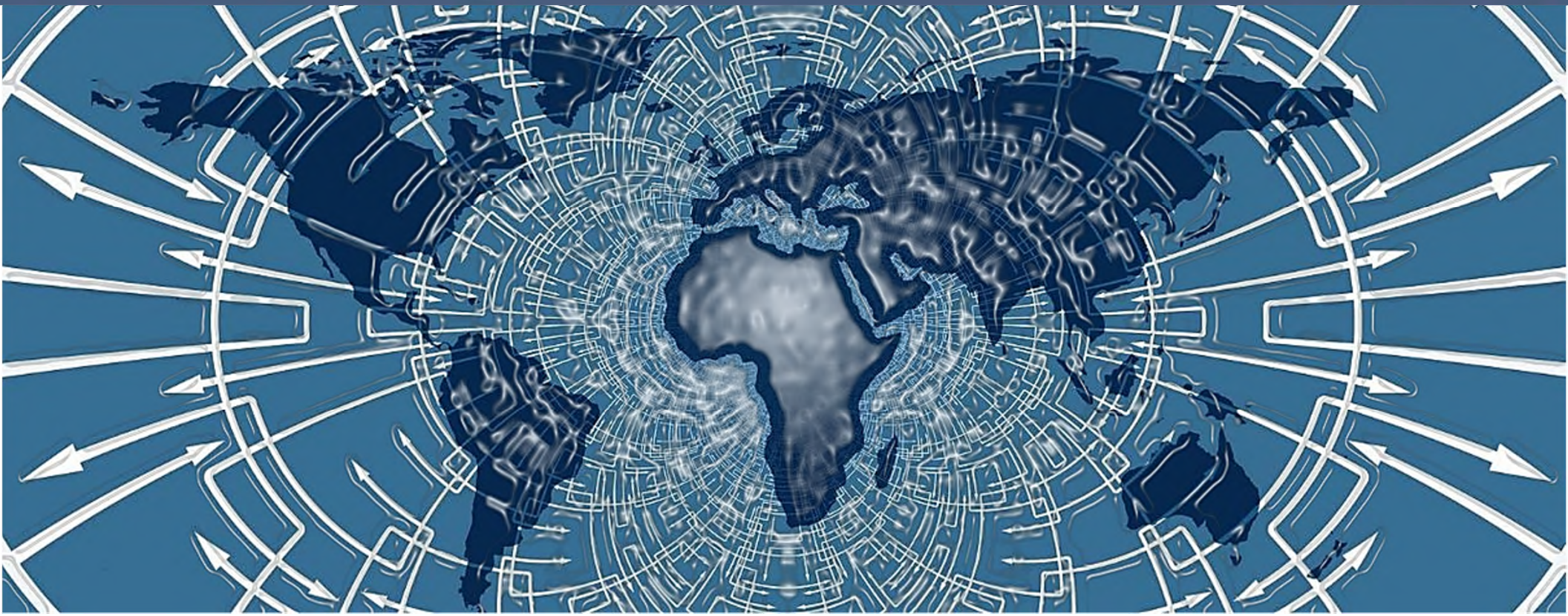
FALL 2019 DATA SUMMIT



PESC CANADIAN USER GROUP

ARUCC 50 COMMITMENT DEDICATION

Groningen Declaration

PESC

FALL 2019 DATA SUMMIT

Data Privacy & Protection

Mary Chapin,
Chief Legal Officer, VP & Corporate Secretary, National Student Clearinghouse

Doug Falk,
CIO & VP, National Student Clearinghouse

Melanie Gottlieb,
Deputy Executive Director, AACRAO

October 23, 2019

FALL 2019 DATA SUMMIT

AGENDA

1. **DATA PRIVACY AND PROTECTION TASK FORCE**
   - Goals/Focus of Task Force
   - Status of efforts

2. **COMPARISON OF GDPR, CCPA, FERPA AND PIPEDA**

3. **CHALLENGES OF ADDRESSING DIFFERENT PRIVACY LAWS**

4. **HOW ARE INSTITUTIONS APPROACHING THEIR PRIVACY COMPLIANCE OBLIGATIONS**
   - Survey information about how institutions are managing their obligations
   - Administering a real-time survey of attendees

5. **WHAT'S NEXT?**

6. **QUESTIONS?**

OCTOBER 23, 2019

PESC

FALL 2019 DATA SUMMIT

DATA PRIVACY & PROTECTION TASK FORCE

- ***TASK FORCE LAUNCHED AT FALL 2018 DATA SUMMIT SAN FRANCISCO***
  - **Ensure uniform, technical implementation of GDPR**
  - **Prepare for additional rules (GDPR, CCPA, etc.)**
  - **Harmonize with policy leaders & practitioners**
  - **Serve as a free, open & transparent information clearinghouse**
  - **Propose technology-neutral solutions**

OCTOBER 23, 2019

PESC

FALL 2019 DATA SUMMIT

Data Privacy & Protection Task Force

- ***Monthly Meetings Since October 2018***
- ***Participants from:***
  - AACRAO Membership
  - PESC Membership (International)
  - SIS Vendors
  - Education Finance Industry
  - Third-Party Data Processors
  - Admissions Services
  - Testing Agencies

October 23, 2019

PESC

CONCLUSIONS/RECOMMENDATIONS

- Institutions are “data controllers” and will interpret privacy regulations to determine whether a person’s record is subject to specific privacy regulations.
  - Therefore, student information system (SIS) providers must provide a mechanism for institutions to flag a person’s record to indicate which privacy regulations the person is subject to.
- Institutions transmit education records to vendors, partners, and other institutions (“data processors”) for subsequent processing of data and for specific services provided under contract. The privacy flags attached to the education record in the SIS must be included in the transmitted records for processors to process the records according to contractual obligations.
  - Therefore, SIS providers need to update their systems to add privacy flags to the output files in accordance with the new standards and any proprietary vendor formats they support. This will also apply to any institutions with homegrown SIS systems.

CONCLUSIONS/RECOMMENDATIONS

- A contract between the controller and processor will specify how the processor shall handle data that has been flagged as being subject to a privacy regulation(s).
  - Therefore, data handling instructions will occur outside of the transmission of data.
- When records are transmitted from the controller to the processor, the controller shall use the then-current value of the privacy flags, even though the value may be different than previously reported flags. Processors will apply their business rules to the current flag values as it pertains the current record being transmitted. Processors are not required to update previously received records with the current flag values. This prevents over-designation of records.
  - However, it should be noted that some privacy regulations pertain to ***records***, while other may pertain to ***individuals***.

CONCLUSIONS/RECOMMENDATIONS

- Standards setting organizations who set education data exchange standards need to update their standards to include the privacy flags.
  - PESC is proposing XML and EDI privacy flags for data exchange standards.
- SIS providers may implement the storage of privacy flags and methods for updating the flags using any mechanisms they choose.
  - Those details are not in scope of this workgroup's work.

DATA PRIVACY & PROTECTION TASK FORCE

- ***PRESENTED AT AACRAO ANNUAL CONFERENCE APRIL 2, 2019***
  - INTRODUCED SAMPLE TAGGING STRUCTURE IN XML AND EDI
- ***CONDUCTED PRE-CONFERENCE WORKSHOP AT PESC SUMMIT MAY 7, 2019***
  - DEEPER CONVERSATIONS REGARDING TAGGING STRUCTURE
  - INTRODUCTION TO GLOBAL EDUCATION PRIVACY STANDARD (GEPS) – A4L.ORG

OCTOBER 23, 2019

PESC

CURRENT STATUS

- ***PESC STANDARDS FORUM CREATED FINAL DRAFT OF XML TAGS***
  - ***PREPARATIONS FOR 30-DAY PUBLIC COMMENT PERIOD***
- ***RECEIVED ADDITIONAL FEEDBACK ON NAMING CONVENTION***
  - ***RECOMMENDATION TO USE ISO COUNTRY/REGION CODES INSTEAD OF CREATING VARIED NAMES***
  - ***RECOMMENDATION FOR TASK FORCE TO LEARN MORE ABOUT GEPS***
- ***30-DAY PUBLIC COMMENT PERIOD ON HOLD***
- ***TASK FORCE IS CONSIDERING FEEDBACK AND LEARNING ABOUT GEPS***

Scope of GDPR & CCPA—Personal & Territorial Scope

GDPR

- **Protects "Data Subjects" who are natural persons**
  - located in the EU while data collected
- **Applies to Controllers** – natural or legal persons, private or public law entities that determine the means and purposes of processing
- **Applies to Processors**—entity which processes PI on behalf of a Controller
- **Applies to Non-profit Entities**
- **Applies to Entities or Organizations**
  - established in the EU
  - established outside the EU if they offer goods or services to EU Data Subjects or monitor their behavior

CCPA

- **Protects natural persons**
  - who are California residents
- **Applies to Businesses**
  - Collects consumer personal information
  - Determines the means and purposes of processing
  - For-profit business
  - Does business in CA and meets one of the thresholds:
    - Annual gross revenue in excess of $25M
    - Annually purchases, receives for business purposes, sells, shares PI of 50,000 or more consumers, households or devices
    - Derives 50% or more of annual revenue from selling PI
- **Applies to Service Providers**
  - For-profit entity that processes PI on behalf of a Business

Scope of GDPR & CCPA—Material Scope

GDPR

- **Personal Data**—any information that directly or indirectly relates to an identified or identifiable individual
  - Anonymized data is specifically excluded
- **Applies to the Processing of PI**
  - Any operation performed on personal data such as "collecting, organization, structuring, storage, retrieval, use, disclosure, transmission or otherwise making available…"

CCPA

- **Personal Information**—comprises information that directly or indirectly relates to or could reasonably be linked to a particular consumer or household
  - Aggregate consumer info and deidentified info is excluded
- **Applies to the Collecting, Selling & Processing**
  - Collecting—buying, renting, gathering, obtaining, receiving, or accessing PI pertaining to a consumer
  - Selling*—renting, disclosing, releasing, disseminating, making available or otherwise communicating PI for monetary or valuable consideration
  - Processing—any operation/set of operations that are performed on personal data by either automated or non-automated means or sharing of PI

Scope of GDPR & CCPA—Rights of EU Data Subject & CA Resident

GDPR

- **Legal Basis Required for Processing of PI**
  - E.g., consent, processing necessary for performance of contract, compliance with legal obligations
- **Right to Erasure/Deletion or "Right to be Forgotten"**
  - Impacts third parties such as Processors and Sub-Processors
  - Data subjects must be informed they are entitled to ask for erasure
  - Exceptions: for defense of legal claims or complying with legal obligation

CCPA

- **Legal Basis Not Required to Collect, Sell and Disclose PI**
- **Right to Deletion from PI Collected From CA Resident**
  - Impacts third parties to whom data has been sold
  - Privacy notice must inform Consumers they are entitled to ask for deletion of their PI
  - Exceptions:
    - processing necessary to comply with legal obligation
    - To perform a contract between the Business and Consumer
    - Use the Consumer PI internally in a lawful manner compatible with the context in which the consumer provided the information

Scope of GDPR & CCPA—Rights of EU Data Subject & CA Resident

GDPR

- **Right to be Informed**
  - Categories of PI processed
  - Purpose of processing
  - Existence of the Data Subject's rights
  - Controllers cannot collect and process PI for purposes other than those informed
  - GDPR enumerates other notice obligations different from CCPA, e.g., identity of the controller and recipients or categories of PI, right to withdraw consent
- **Right to Object to "Processing"**
  - Data Subjects can withdraw consent or object to processing based on legitimate interests
  - Not an absolute right where Controller can demonstrate compelling legitimate grounds for processing that override the rights and interests of the data subject

CCPA

- **Right to be Informed**
  - Categories of PI to be collected
  - Purposes for which the PI is collected
  - Right to Opt-out via a link to "Do Not Sell My Personal Info"
  - Businesses cannot collect additional PI without advising what info is collected and purpose for processing
  - CCPA enumerates other information must be provided to the CA Resident, e.g., categories of PI collected/sold/disclosed for business purposes in the previous 12 months
- **Right to Opt-out of "Selling"**
  - Absolute right to opt-out of selling
  - Requires a link to "Do Not Sell "My Personal Information" on homepage of the Business
  - Third parties that receive CA Resident PI can only sell the PI if consumers provided explicit notice and opportunity to Opt-out

Scope of GDPR & CCPA—Rights of EU Data Subject & CA Resident

GDPR

- **Right of Access**
  - Permits full visibility of data an organization holds and a right to a "copy" of the data free of charge
  - Includes all personal data collected and processed
  - Must indicate the purposes of the processing, categories of personal data, recipients or categories of recipients to whom the personal data was disclosed
- **No Non-discrimination Right but Consent Must Be Freely Given**
  - Where processing based on consent, it is not freely given if data subject has no genuine choice or is unable to withdraw consent without detriment
- **Right to Data Portability**
  - Applies only to PI provided by the Data Subject and processed on basis of consent or contract and processing carried out by automated means
  - Right permits having PI transmitted from Controller to another Controller

CCPA

- **Right of Access**
  - Permits full visibility of the data an organization holds
  - Only includes PI collected 12 months prior to the request
  - Must indicate purposes of collecting/selling PI, categories of PI collected, recipients or categories of recipients to whom the PI was disclosed
- **Right Not to be Subject to Discrimination in Exercise of Rights**
  - Cannot be denied goods or services
  - Charged different prices or rates for goods or services
  - Provided different level or quality of goods or services
- **Right to Data Portability**
  - Extension of Right to Access and limited to data collected in prior 12 months
  - Does not permit transfer of PI from Business to Business

Scope of GDPR & CCPA—Cross Border Transfers & Breach Notification Reqs

GDPR

- **Restrictions on Cross-Border Transfers** without a valid transfer mechanism:
  - Between EU member states without restriction
  - European Commission Adequacy Determination:
    - Canada (only covers data subject to PIPEDA)
    - US via certification under EU-US Privacy Shield
  - **Binding Corporate Rules**—internal codes of conduct adopted by multinational companies to allow transfers between branches of the organization; approval required
  - **Model Contract Clauses**—legal terms in a DPA for each new purpose for processing
  - **Derogations:**
    - Consent after disclosure of risks
    - Transfer necessary for performance of the contract between the data subject and the Controller
    - Transfer necessary for reasons of public interest or protect the vital interest of data subject
- **Breach Notification Requirement**—72 hours after becoming aware notify supervisory authority/data subject without undue delay

CCPA

- **No Restrictions on Cross-Border Transfers**
- **No Breach Notification Requirement under CCPA**
  - But CA Data Breach Notification Law requires notification:
    - Doing business in CA
    - Owns or licenses computerized data
    - Data include PI of CA residents
    - Unauthorized acquisition of electronic PI belonging to CA residents
    - PI was not encrypted or if encrypted the key was compromised

Scope of PIPEDA & FERPA

PIPEDA

- **Applies to Private-Sector Organizations**—that collect, use or disclose PI in the course of a commercial activity
  - Alberta, British Columbia and Quebec have their own private sector privacy laws for the collection, use or disclosure of PI and PIPEDA would not apply
- **Applies to Cross-Provincial and Cross-Border transfers** for businesses operating in Canada
- **Applies to Private Universities**
- **Public Universities Subject to Public Sector Provincial Laws** because they are public bodies—PIPEDA does not apply to core activities of universities, which are central to their mandate
- **Public Sector Provincial Laws** require:
  - Consent and Security
  - Cross-border Restrictions

FERPA

- **Applies to all Educational Agencies, K-12 schools and postsecondary public/private institutions**—that receive funds under applicable programs of the Department of Education
- **Applies to Access and Disclosure of Education Records**
  - Education Records—defined as records that are:
    - Directly related to a student
    - Maintained by an educational agency or institution or by a party acting for the agency or institution
- **Pre-empts any Conflicting State Law**
- **No Cross-Border Restrictions**

PESC

Scope of PIPEDA & FERPA

PIPEDA

- **Protects Personal Information**—includes any factual or subjective information, recorded or not, about an identifiable individual. This includes information in any form, such as:
  - age, name, ID numbers, income, ethnic origin, or blood type;
  - opinions, evaluations, comments, social status, or disciplinary actions; and
  - employee files, credit records, loan records, medical records, existence of a dispute between a consumer and a merchant, intentions (for example, to acquire goods or services, or change jobs).
- No analogous concept as Directory Information

FERPA

- **Personally identifiable information** —includes name, address, personal identifiers like SSN or date of birth or other information that could be used alone or in combination to identify a student
- **Protects disclosure of PII in a student's education record—**without the consent of a parent or eligible student unless an "exception" to the consent requirement applies
- Schools must tell parents or eligible students about directory information and allow reasonable time to request school not to disclose Directory Information
- Directory information considered info not usually considered harmful or invasion of privacy: includes e.g., student's name, address, telephone number, date of birth, honors, awards, dates of attendance
- Directory information cannot include: grades, GPA, race, gender, religion, national origin, SSN

Requirements Under PIPEDA & FERPA

PIPEDA

- Ten Principles must be met:
  - Accountability
  - Identifying Purpose
  - Consent
  - Limiting Collection
  - Limiting Use, Disclosure and Retention
  - Accuracy
  - Safeguards (Security)
  - Openness
  - Individual Access
  - Challenging Compliance

FERPA

- Permissible Uses of Student PII:
  - Consent
  - School Officials
  - Audit and Evaluation
  - Studies
  - Other schools to which student seeks to or is enrolled
  - Judicial Order
  - Directory Information

Scope and Requirements of PIPEDA & FERPA

PIPEDA

- Transparency and Consent Obligations
- Data Minimization
- Data Retention
- Data Security
- Data Quality and Access Rights
- Outsourcing and Service Provider Exception
  - Must be transparent about info handling to extent Service Provider outside of Canada
  - Must notify when PI may be sent outside of Canada for storage and processing
  - Agreement with Service Provider must include contractual safeguards
- Cross Border Restrictions
- Breach Notification Requirement

FERPA

- Rights of Eligible Students/Parents*
  - Right to be notified of FERPA rights annually
  - Right to inspect and review
  - Right to request amendment
  - Right to limit disclosure of PI info that would directly identify the student or make the student's identity easily traceable-–known as "Directory Information"
  - Right to file complaint with Department of Ed if rights violated
- No Cross Border Restrictions
- No Breach Notification Requirement

Challenges to Compliance

GDPR v. CCPA

- GDPR applies to for-profit and nonprofit
- CCPA applies to for-profit only
- GDPR requires a legal basis for processing in contrast to the CCPA
- CCPA has absolute right of "Do Not Sell My Personal Information" and GDPR does not

FERPA v. PIPEDA

- PIPEDA applies to all PI handled by private sector versus FERPA applying to education records
- No cross-border restrictions for FERPA; PIPEDA subject to cross-border restrictions
- Directory Information for FERPA with no analogous provision in PIPEDA
- No breach notification requirements for FERPA but required for PIPEDA

FALL 2019 DATA SUMMIT

AACRAO.ORG ON GDPR

PESC

FALL 2019 DATA SUMMIT

INSTITUTIONAL RESPONSES TO PRIVACY REGULATIONS

- INFORMAL SURVEY CONDUCTED THIS MONTH

LIVE POLL USING SLIDO

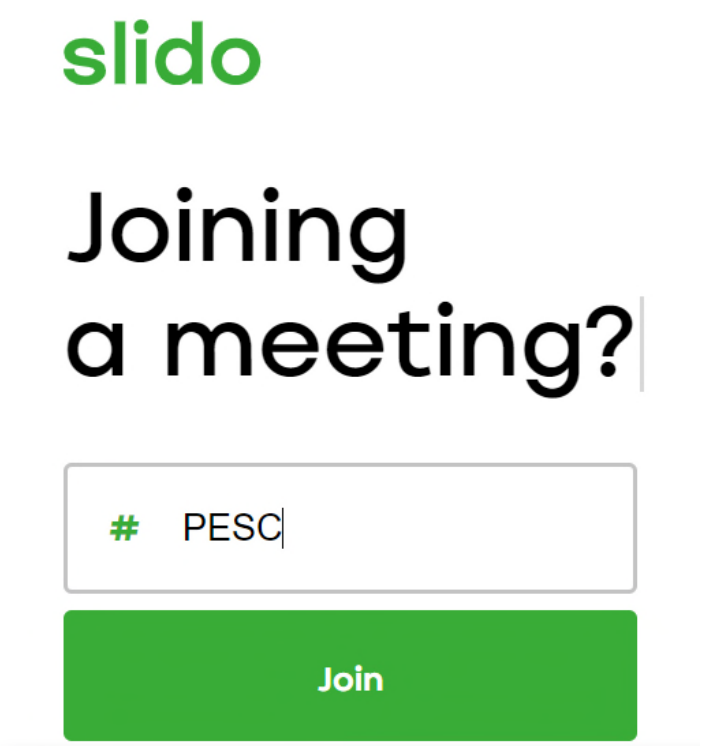
OCTOBER 23, 2019

PESC

FALL 2019 DATA SUMMIT

LIVE POLLING

NAVIGATE TO SLI.DO
MEETING CODE PESC

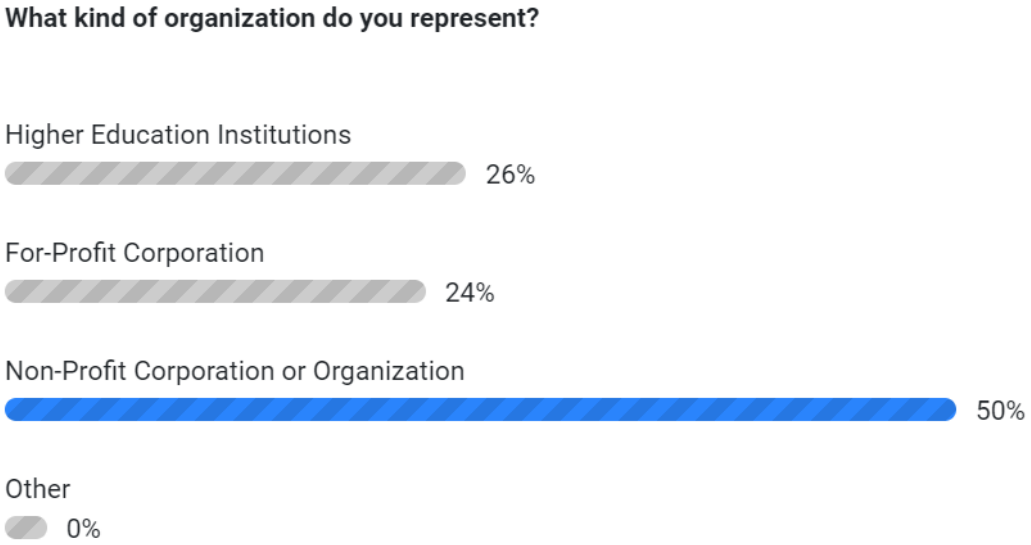


OCTOBER 23, 2019

PESC

FALL 2019 DATA SUMMIT

WHAT KIND OF ORGANIZATION DO YOU REPRESENT?



OCTOBER 23, 2019

PESC

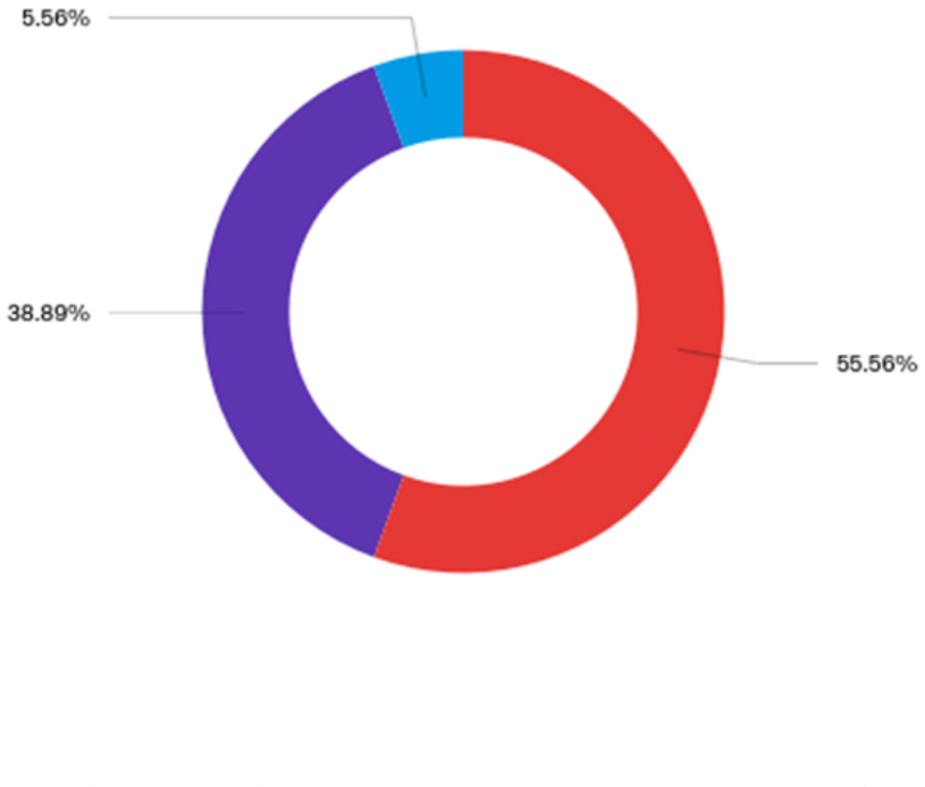
FALL 2019 DATA SUMMIT

IN A WORD OR TWO, HOW ARE YOU FEELING ABOUT THE PRIVACY REGULATION LANDSCAPE?

OCTOBER 23, 2019

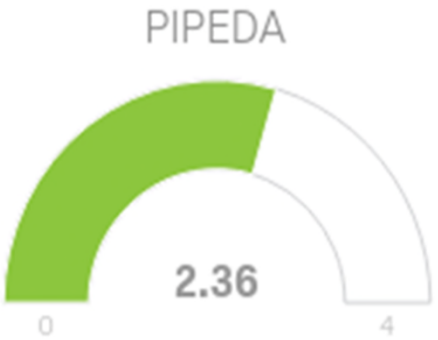
WHO DID WE POLL?

- 21 RESPONDENTS
- MAINLY 5000+ STUDENTS



FALL 2019 DATA SUMMIT

WHAT LEVEL OF CONCERN DOES YOUR INSTITUTION HAVE WITH THE FOLLOWING PRIVACY REGULATIONS?

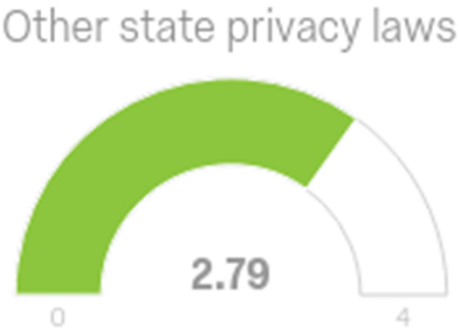


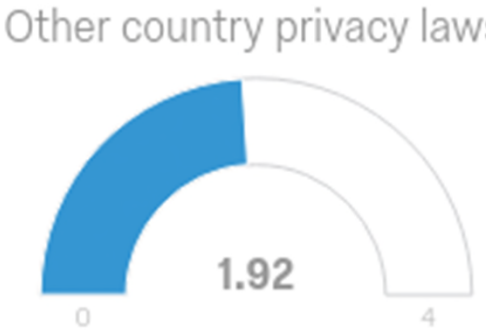
OCTOBER 23, 2019

PESC

FALL 2019 DATA SUMMIT

WHAT LEVEL OF CONCERN DOES YOUR INSTITUTION HAVE WITH THE FOLLOWING PRIVACY REGULATIONS?



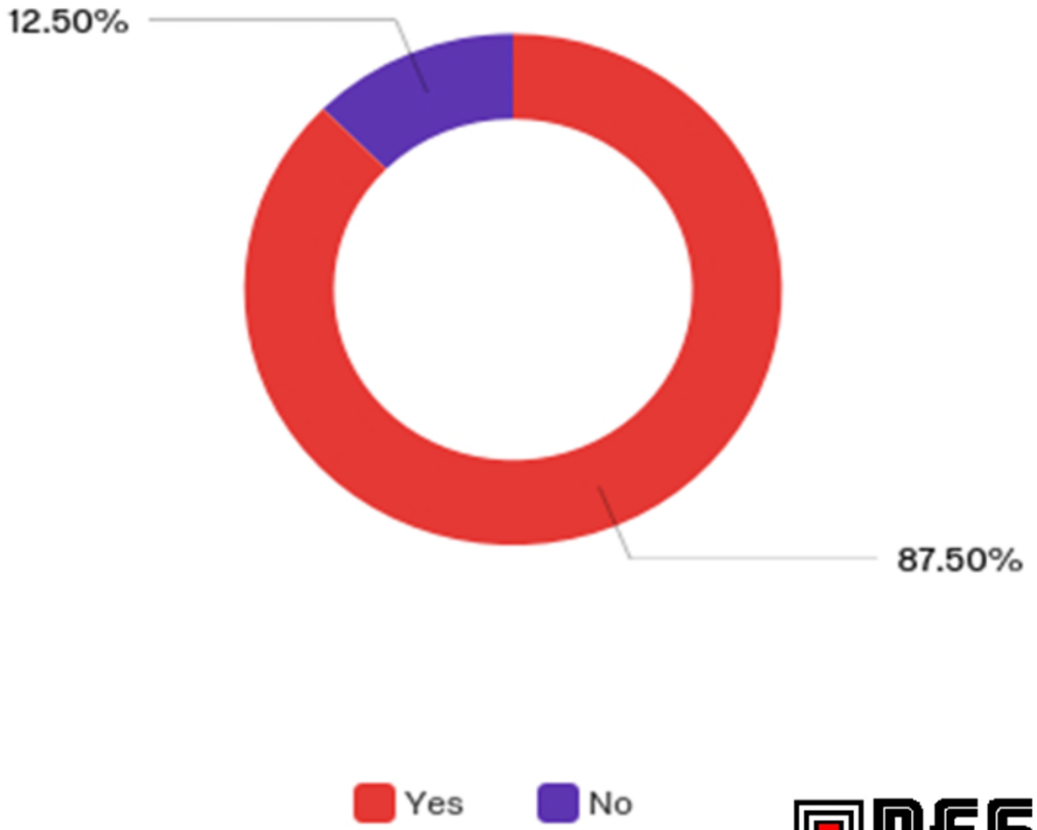


OCTOBER 23, 2019

PESC

FALL 2019 DATA SUMMIT

HAS YOUR INSTITUTION DETERMINED IF CURRENT AND FORTHCOMING PRIVACY LAWS AND REGULATIONS AFFECT YOUR CAMPUS AND WOULD THUS REQUIRE COMPLIANCE WITH THEIR PROVISIONS?



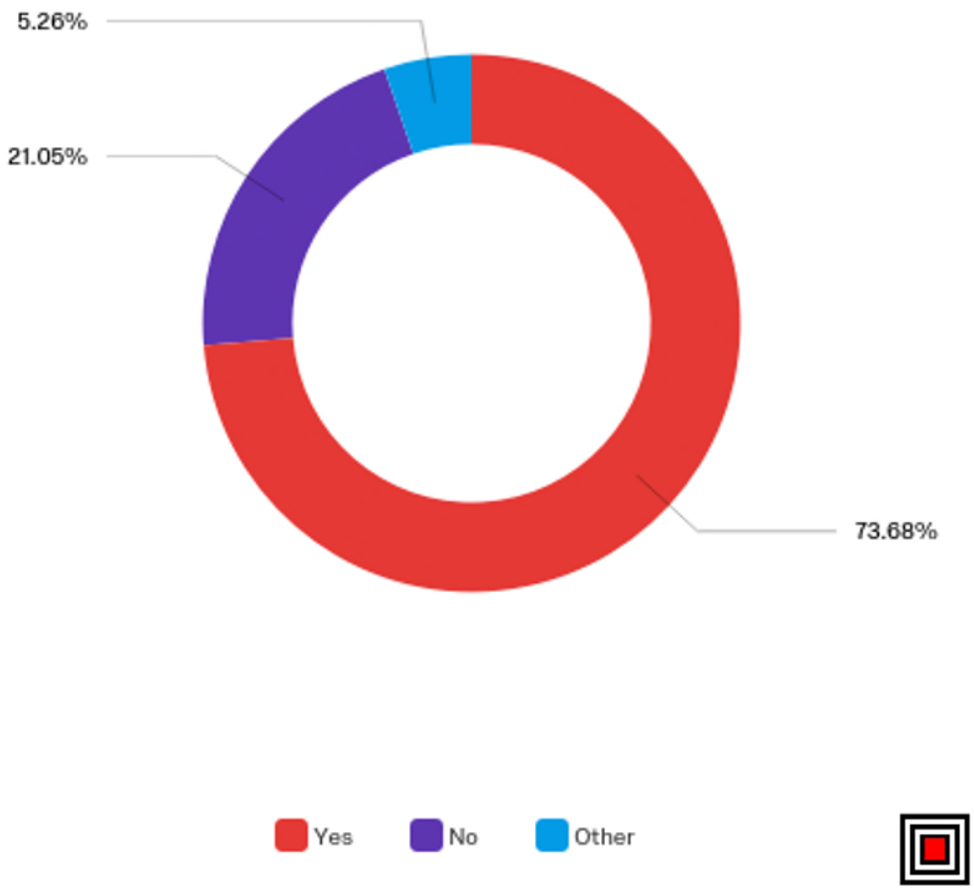
OCTOBER 23, 2019

HAS YOUR INSTITUTION OR ORGANIZATION FORMED A DATA PRIVACY AND PROTECTION COMPLIANCE WORKGROUP?

PESC

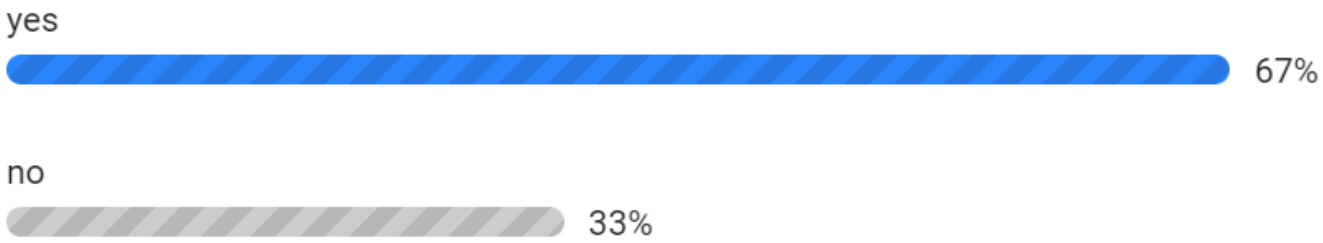
FALL 2019 DATA SUMMIT

HAS YOUR INSTITUTION FORMED AN INTERNAL DATA PRIVACY AND PROTECTION WORKGROUP? (E.G., GDPR COMPLIANCE WORKGROUP, CCPA COMPLIANCE WORKGROUP, ETC.)



OCTOBER 23, 2019

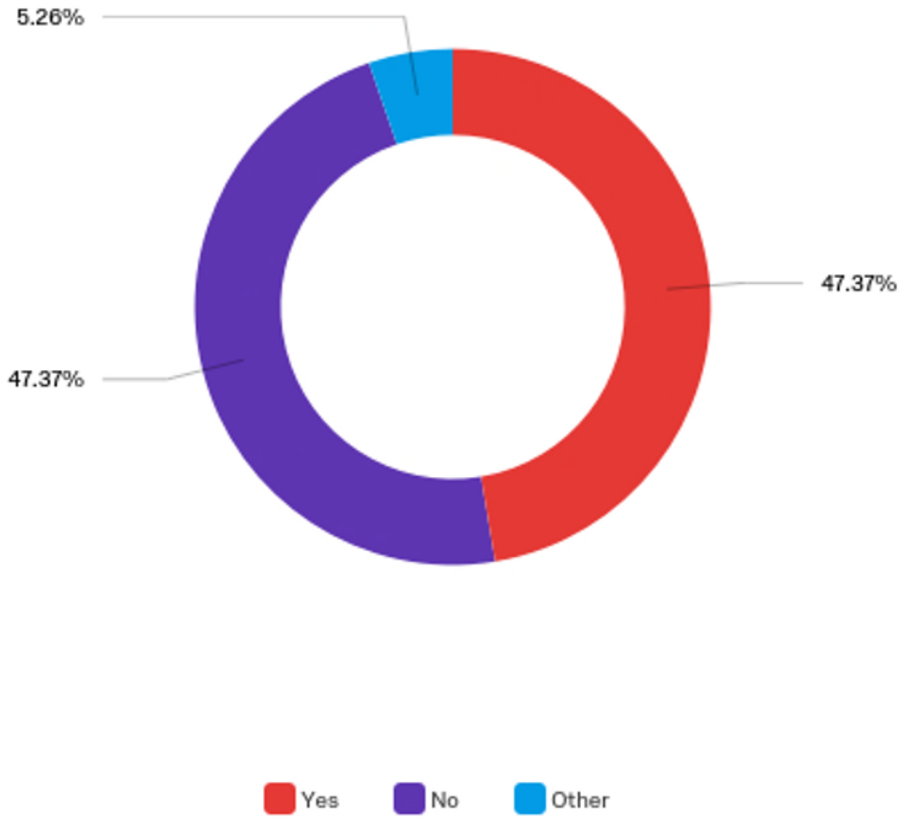
HAS YOUR INSTITUTION OR ORGANIZATION UPDATED ITS INSTITUTIONAL PRIVACY POLICY TO ACHIEVE COMPLIANCE WITH CURRENT PRIVACY REGULATIONS?



PESC

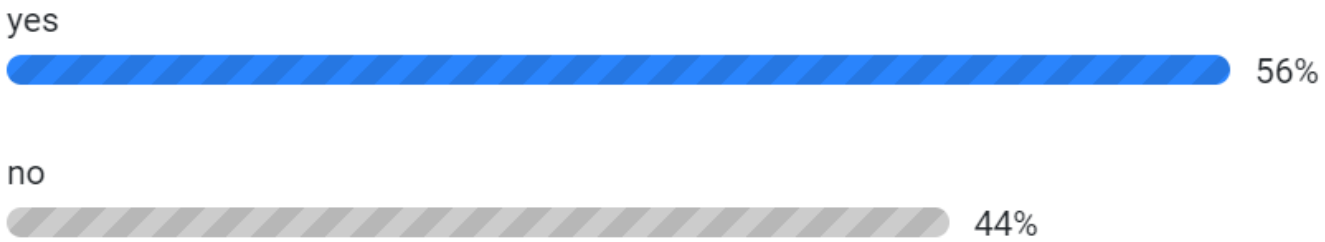
FALL 2019 DATA SUMMIT

HAS YOUR INSTITUTION UPDATED ITS INSTITUTIONAL PRIVACY POLICY TO ACHIEVE COMPLIANCE WITH CURRENT PRIVACY REGULATIONS?



OCTOBER 23, 2019

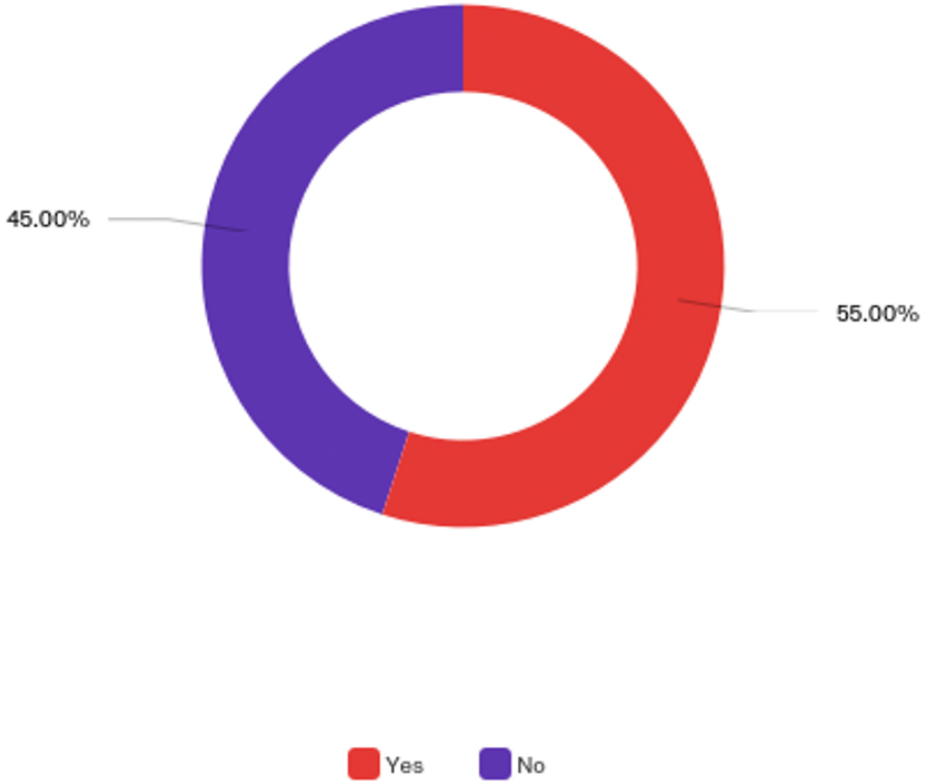
HAS YOUR INSTITUTION OR ORGANIZATION CONDUCTED A DATA INVENTORY TO ASSESS THE IMPACT OF COMPLIANCE WITH PRIVACY REGULATIONS?



PEGC

FALL 2019 DATA SUMMIT

HAS YOUR INSTITUTION CONDUCTED A DATA INVENTORY TO ASSESS THE IMPACT OF COMPLIANCE WITH PRIVACY REGULATIONS?

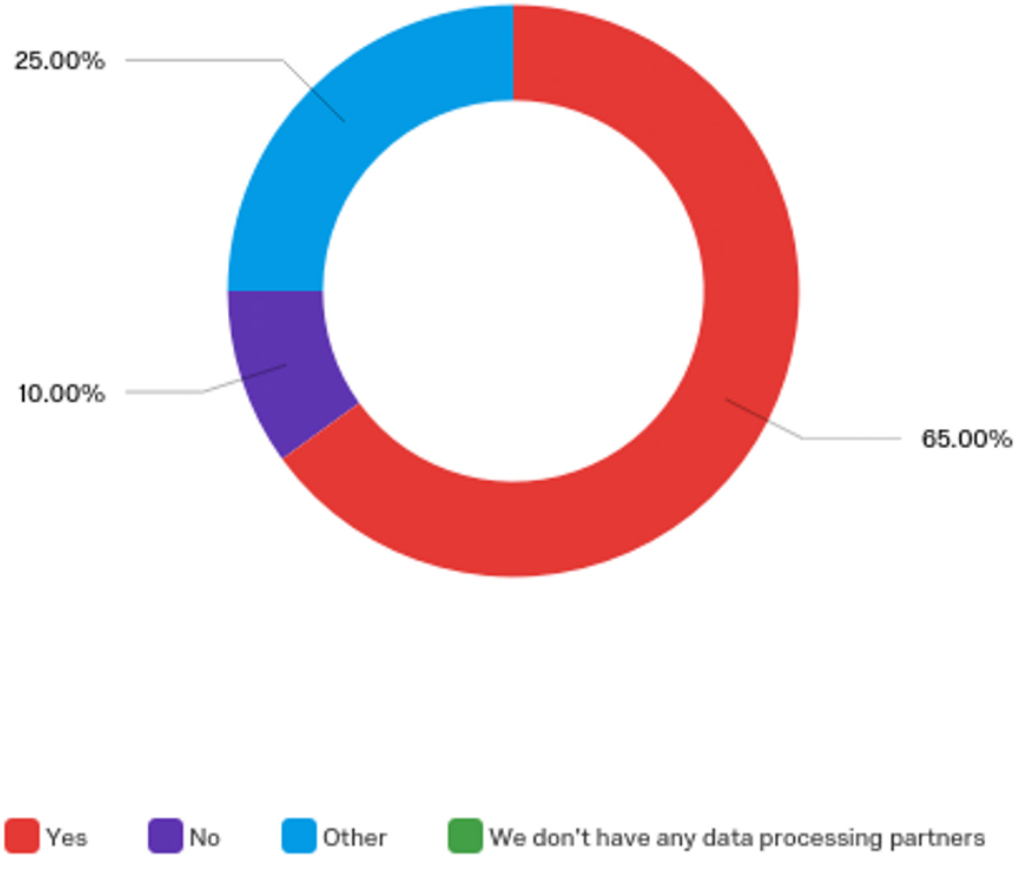


OCTOBER 23, 2019

PESC

FALL 2019 DATA SUMMIT

HAS YOUR INSTITUTION HAD DISCUSSIONS WITH YOUR VENDORS ABOUT THEIR COMPLIANCE PRIVACY REGULATIONS?

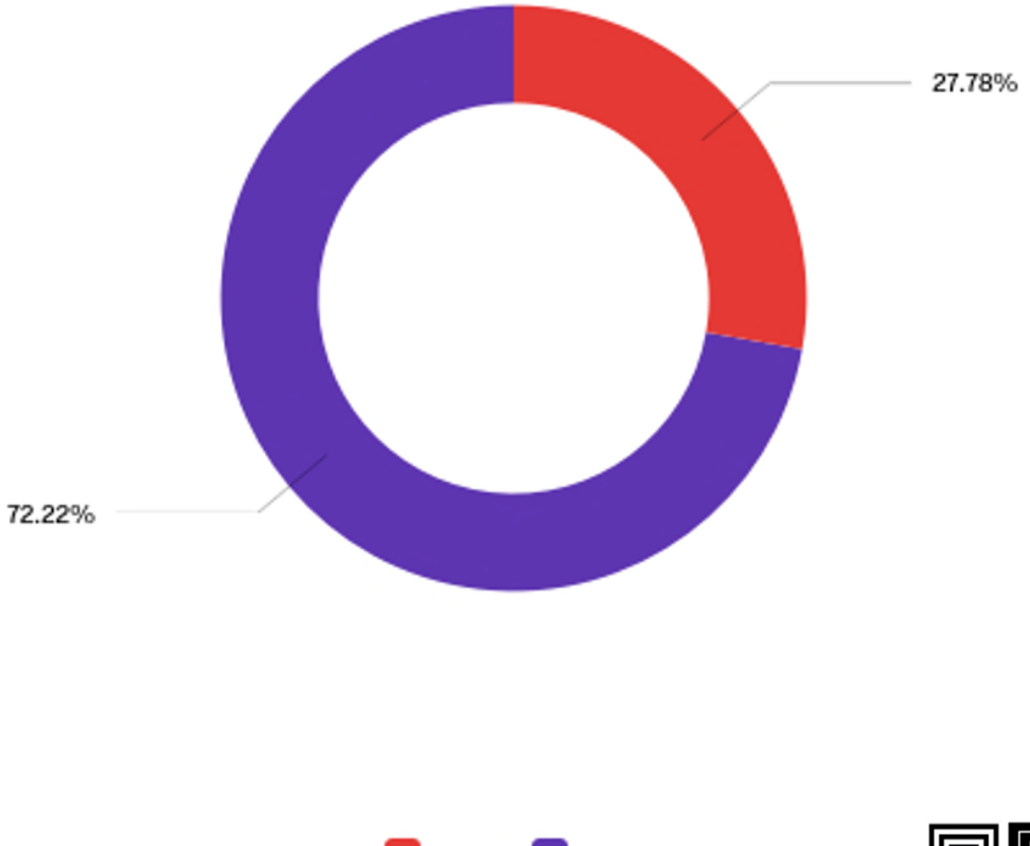


OCTOBER 23, 2019

PESC

FALL 2019 DATA SUMMIT

HAS YOUR INSTITUTION GIVEN ITS VENDORS INSTRUCTIONS THAT DIRECT HOW THEY PROCESS THEIR DATA?



OCTOBER 23, 2019

PESC

What's Next?

- **Monthly Task Force Meetings**
  https://www.pesc.org/data-privacy---protection.html

- **Continued discussions, learning and monitoring of emerging privacy regulations**

- **Recommend standards for flagging records and exchanging data**

PESC

Thank You!

Q & A

Mary Chapin: chapin@studentclearinghouse.org
Doug Falk: falk@studentclearinghouse.org
Melanie Gottlieb: gottliebm@aacrao.org

October 23, 2019

PESC