Data Privacy & Protection 101

Collaborative Efforts to Address & Exchange Privacy & Protection Statuses

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

Julia Funaki
Associate Director
AACRAO

Rick Skeel
Director of Product Management
Ellucian

Doug Falk
VP & CIO
National Student Clearinghouse

Michael Sessa
President & CEO
PESC

PESC

SPRING 2019 DATA SUMMIT
MAY 7 – 10, 2019 | WASHINGTON, D.C.

SPRING 2019 DATA SUMMIT

MAY 7 – 10, 2019 | WASHINGTON, D.C.

AGENDA

- Introduce PESC Data Privacy & Protection Task Force
- Highlight AACRAO & PESC Resources & Efforts
- Review Key Components of GDPR Rules & Regulations
- Review Upcoming CA Consumer Privacy Act (CCPA)
- Discuss Relationships & Scenarios
- Discuss Proposed Solution | Phase 1 Implementation
- Next Steps & How To Participate

Outcomes of this Workshop:

- Learn about AACRAO & PESC resources on privacy
- Learn about GDPR and CCPA
- Understand how major service providers & partners are digitally communicating privacy data
- Encourage active discussions within institutions & with service providers and vendors
- Promote access to the Data Privacy & Protection Task Force

Postsecondary Electronic Standards Council

- Standards-development & standards-setting body
- Voluntary consensus-based model (not authoritative)
- Founded 1997*
- AACRAO & PESC History and Partnership
- Vision of global connectivity & data integrity

How PESC Operates

- **Free & Open Groups (Admissions, CanPESC, Data Privacy, JSON)**
- **Member-Based Groups (Competencies & Credentials, EdExchange)**
- **Goals of PESC Mission (501c3 non-profit):**
  - **Standardization & PESC Approved Standards (EDI, JSON, PDF, JSON)**
  - **Identify common industry-shared problems & foster open, transparent collaboration**
  - **Optimize institution's digital performance**
  - **Enable sustainable solutions across disparate technologies**

Data Privacy & Protection Task Force

- ***From PESC Board Retreat June 2018, Task Force launched at Fall 2018 Data Summit San Francisco***
  - **Ensure uniform, technical implementation of GDPR**
  - **Prepare for additional rules (FERPA, CCPA, etc.)**
  - **Harmonize with policy leaders & practitioners**
  - **Serve as a free, open & transparent information clearinghouse**
  - **Propose technology-neutral solutions**

AACRAO & PESC Resources

- **AACRAO:** https://www.aacrao.org/resources/compliance
- **PESC:** https://www.pesc.org/groups-and-initiatives.html
- **Implications of the General Data Protection Regulation: An Interassociational Guide:**

  https://www.aacrao.org/signature-initiatives/trending-topics/gdpr/gdpr-interassociational-guide
- **GDPR:** https://gdpr-info.eu
- **Great Guidance by topic from the UK ICO (UK Data Protection Authority):**

  https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr
- **International Association of Privacy Professionals:** https://iapp.org

General Data Protection Regulation

- Implemented on May 25, 2018

- Significantly expands personal privacy rights for processing of and free movement of personal data

What is Privacy?

- *A person's right to control access to his or her personal information*.

GDPR Overview

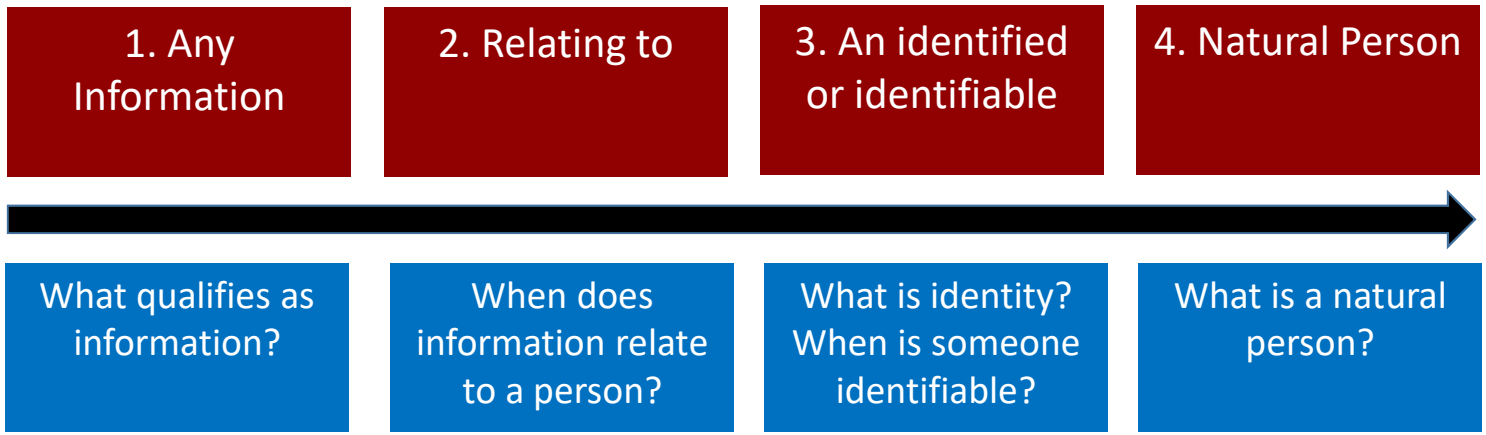
- Privacy as Fundamental Human Right
  - The basis for the EU Data Protection Directive (1995) and the GDPR can be found in the Organization for Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and the Council of Europe's Convention 108
- Applies to **personal data**: any information relating to an identified or identifiable natural person physically in the EU (*EU data subject*) when the data is collected (e.g., name, ID, location data, online ID such as IP addresses, images)

GDPR Overview

- Applies to processing of personal data by Controllers & Processors not in the EU where the processing is related to:
  - Offering goods or services to EU data subjects or
  - Monitoring EU data subject behavior within the EU
- Applies to **Controllers** and **Processors** established in the EU even if processing of personal data is outside of the EU

  There must be a lawful basis for all data processing (e.g., consent, necessary to perform a contract, required by law, "legitimate interests" balanced against impact on individuals)

Definition of Personal Data



Four Step Test*

(Article 4, Recitals 26-27, 30)

*IAPP

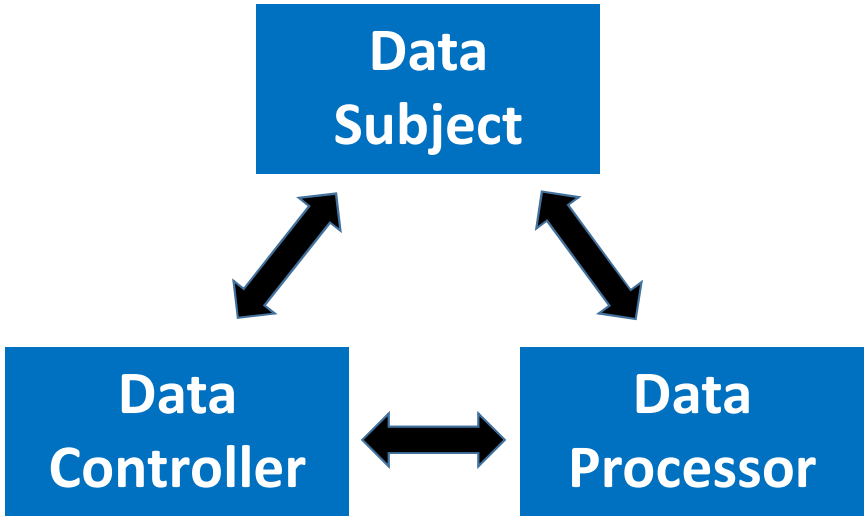
PESC

GDPR: Applies to Processing of Personal Data

Definition of ***Processing***:

- any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (Art. 4)

GDPR Roles, Relationships & Responsibilities



Articles 24-43

- Address responsibilities of **Controller** and **Processor**.
- It is important to understand who is a Controller and who is Processor as each has significant obligations

Who is Subject to GDPR?

Controller:

- an entity that, alone or jointly with others, determines the purposes and means of the processing of personal data (Art. 4)

Processor:

- an entity that processes personal data only on behalf of and on the instructions of the controller (e.g., service providers) (Art. 4)

Who is Subject to GDPR?

Controller Obligations:

- Comply with all data protection principles
- Processing only if lawful/legal basis
- Appoint Processors by written contract
- Ensure Processor's processing complies with the law

Processor Obligations:

- Processing only on documented instructions of Controller
- Security measures
- Implement measures to assist Controller with complying with GDPR
- Keep records of processing activities

PESC

Lawful Processing

Requirement of a Lawful/Legal Basis for All Data Processing:

- Consent
- Performance of a Contract
- Comply with Legal Obligations
- Legitimate Interests
- Protect Vital Interests
- Performance of Task Carried Out in Public Interest

Controllers Processing with Processors

Data Processing Agreements (DPAs):

- Processing instructions from **Controller** to **Processor**
- Subject matter and duration of the processing
- Nature and purpose of the processing
- Confidentiality obligations of all persons who process data
- Security requirements

Controllers Processing with Processors (cont'd)

Data Processing Agreements (DPAs):

- Assist Controller in complying with data subject rights of access and other rights under GDPR
- Deletion or return of data as requested or end of contract
- Processor to keep records of processing activities
- Submit information to Controller to ensure both Controller and Processor meeting their Art. 28 obligations

Recurring Considerations for Compliance

- Territoriality
- Careful consideration of lawful/legal basis for data processing
- Categorize GDPR roles
- Identify Processing Partner
- Identify students who are EU data subjects & subject to GDPR and record it on the student record for period of time student is an EU data subject.

CALIFORNIA CONSUMER PRIVACY ACT

- Enacted September 23, 2018
- Statutory amendments in progress
- Effective January 1, 2020
- Enforcement and statutory regulations by July 1, 2020
- Expansive scope, broad definition of PI, increased disclosure obligations, enhanced consumer rights of access, deletion, and porting of PI
- Penalties
- Private right of action for data security breaches

Who is Protected?

California residents, as defined in tax regulations

What Data is Protected?

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.
- Includes “education information” defined as information that is not publicly available personally identifiable information as defined in FERPA

Who Must Comply?

Businesses

- Any for-profit business doing business in CA exceeding thresholds of:
  - Annual gross revenues of $25M;
  - Receives/buys/sells/shares PI of 50,000 or more CA residents, households or devices annually; or
  - 50% or more of revenue from selling CA residents' PI.
- Obtaining, by any means, PI on CA residents
- Alone or with others determines the purposes and means for processing CA residents' PI

Who Must Comply?

- **Service Provider:** Any for-profit entity providing service to **businesses** for defined purposes.

- **Third Party:** almost all entities not businesses or service providers receiving PI from a **business**, unless meets very strict criteria.

What Activity is Regulated?

Sale, Sell, Selling or Sold Personally Identifiable Information
The terms “sale” “sell” “selling” or “sold” with respect to PI are defined to mean “selling, renting, **releasing, disclosing**, **disseminating, making available, transferring**, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by the business to another business or a third party ***for monetary or other valuable consideration***

What Rights Do California Residents Have?

- Right to request information
- Right of data portability
- Right to request data deletion
- Right to be informed of rights
- Right to opt out of sale of personally identifiable information unless exemption applies because sale of PI is necessary for legal compliance

Cases and Scenarios

When do you need/care about transmitting a students privacy status?

Implications of the

General Data Protection Regulation

AN INTERASSOCIATION GUIDE May 2018

Scenario Review

- Case 1.3: *Prospect data from applications in progress from Common Application*
  - A student located in the EU begins an application on a third party platform
  - Student has selected our institution as one to which they intend to submit an application

By selecting our campus, the student has given permission to the vendor to share their information with colleges and universities for the purpose of receiving recruitment information.

Scenario Review (Case 1.3 cont'd)

Admissions loads the information to Customer Resource Management (CRM) and Student Information System (SIS)

- We use the student information to drive the recruitment communication stream, with special messages encouraging them to complete and submit their application
- All recruitment e-mails provide the opportunity for opt-out

Questions:

- Is the opt-out option in the recruitment messages sufficient to be the GDPR compliant?
- Does an opt-out require that we delete the student record?
- Does admissions office become the controller upon receipt?
- Do our application vendors need to identify EU students?

Scenario Review

➢ Case 2.1: *Enrollment Reporting Services*

- NSC enters into a contract with institution to report your student enrollment to the NSC and, on your behalf, NSC receives and responds to requests from the NSLDS, other lenders and servicers in the federal loan programs, and private lenders seeking to verify enrollment status of participating students, for purposes of ensuring that such enrolled loan recipients have their loans placed in deferment while in school.
- Role:
  - Institution is a Controller as personal information is collected by the institution
  - NSC is a processor and should comply with processing instructions the institution (Controller) provides to the NSC regarding how to process the personal data submitted to NSC for its services. Institution must identify to NSC which information for processing is personal data on an EU data subject (student subject to GDPR) and when it provides to NSC a request under the GDPR (e.g., opt out)

Scenario Review (Case 2.1 cont'd)

➢ Institutional Responsibility

- Controllers must contractually obligate Processors to adhere to certain standards under GDPR
- The Controller is responsible for adhering to data privacy principles including providing notice consistent with the GDPR requirements, such as
- Description of the purposes of processing
- Description of the entities or categories of entities to which it discloses personal data covered by GDPR
- Institution should identify to NSC which personal information is subject to GDPR

➢ Institutional Action

- Should you record students who are EU data subjects governed by GDPR? Or even bigger than that…do you even want to enroll students who are in the EU?
- Institution could consider the work performed by NSC as "necessary for the purposes of legitimate interest" (or lawful processing)
- Institution could consider the processing necessary for the performance of a contract, but the institution needs to provide a rationale for the processing; thus, an institution would need to conclude that the relationship with the student could not exist without the processing of the data at issue. Could mandatory state reporting fall under that?

Proposed Solution

- Education records need to have a set of flags to indicate which privacy regulations the education record is subject to.
- SIS providers will have to update their systems to provide school administrators the ability to apply privacy flags to education records and/or individuals (some privacy regulations apply to the education record, such as GDPR, and some apply to the individual, such as CCPA).
- 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.
- SIS providers will have to update their systems to add the 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.

Proposed Solution

- PESC proposes an XML tag structure for XML data standards:

```
<xs:element name="DataPrivacy" type="DataPrivacyType" />
- <xs:complexType name="DataPrivacyType">
  - <xs:sequence>
      <xs:element name="PrivacyRequirement" type="PrivacyRequirementType" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>
- <xs:complexType name="PrivacyRequirementType">
  - <xs:sequence>
      <xs:element name="PrivacyRegulationCode" type="PrivacyRegulationCodeType" />
    - <xs:element name="PrivacyRegulationName" type="xs:string" minOccurs="0">
      - <xs:annotation>
          <xs:documentation>The text name of the privacy regulation if the PrivacyRegulationCode is "Other"</xs:documentation>
        </xs:annotation>
      </xs:element>
      <xs:element name="PrivacyIndicator" type="xs:boolean" />
    </xs:sequence>
  </xs:complexType>
- <xs:simpleType name="PrivacyRegulationCodeType">
  - <xs:restriction base="xs:string">
      <xs:enumeration value="California" />
      <xs:enumeration value="FERPA" />
      <xs:enumeration value="GDPR" />
      <xs:enumeration value="Other" />
    </xs:restriction>
  </xs:simpleType>
```

Proposed Solution

- PESC Sample XML:

```
- <DataPrivacy>
  - <PrivacyRequirement>
      <PrivacyRegulationCode>GDPR</PrivacyRegulationCode>
      <PrivacyRegulationName>EU General Data Privacy Regulation</PrivacyRegulationName>
      <PrivacyIndicator>true</PrivacyIndicator>
    </PrivacyRequirement>
  - <PrivacyRequirement>
      <PrivacyRegulationCode>California</PrivacyRegulationCode>
      <PrivacyRegulationName>California Consumer Privacy Act</PrivacyRegulationName>
      <PrivacyIndicator>true</PrivacyIndicator>
    </PrivacyRequirement>
  - <PrivacyRequirement>
      <PrivacyRegulationCode>FERPA</PrivacyRegulationCode>
      <PrivacyRegulationName>Family Education Rights and Privacy Act</PrivacyRegulationName>
      <PrivacyIndicator>true</PrivacyIndicator>
    </PrivacyRequirement>
  </DataPrivacy>
```

Proposed Solution

- PESC Proposes Using the NTE Segment for EDI Transactions:

NTE Note/Special Instruction

To transmit information in a free-form format, if necessary, for comment or special instruction

01	363	Note Reference Code	O	ID 3/3
02	352	Description	M	AN 1/80

- Where:
  - Element 363 Note Reference Code = “OTH” (Other Instructions)
  - Element 352 Description contains the privacy flags

Proposed Solution

- Processors who have their own file proprietary file formats will have to evaluate the best method to accommodate current privacy policy flags, as well as allow the expansion of new privacy policy flags into the future.

Next Steps

- Task Force Meeting on Friday, May 10 at PESC Summit
- 30-Day Comment Period for Proposed Solution
- Approval of XML and EDI Tagging Scheme
- Monitoring of Emerging Privacy Regulations

THANK YOU!

QUESTIONS & ANSWERS