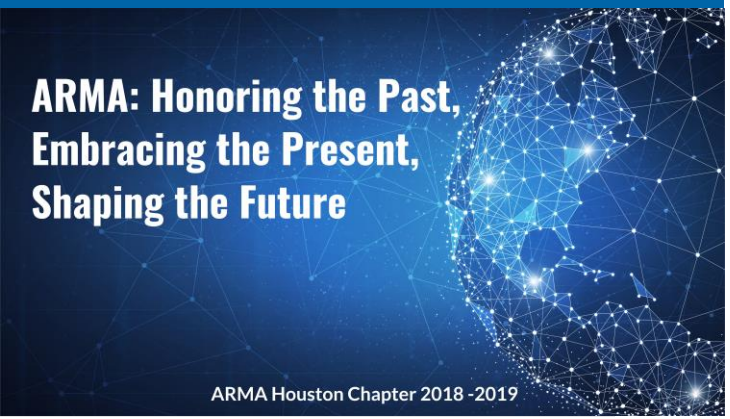
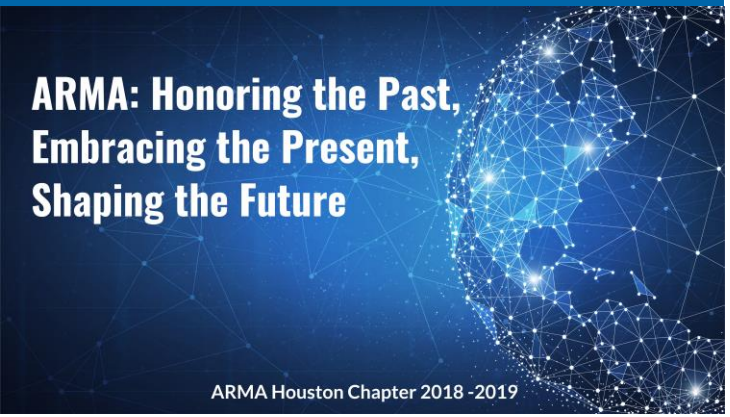


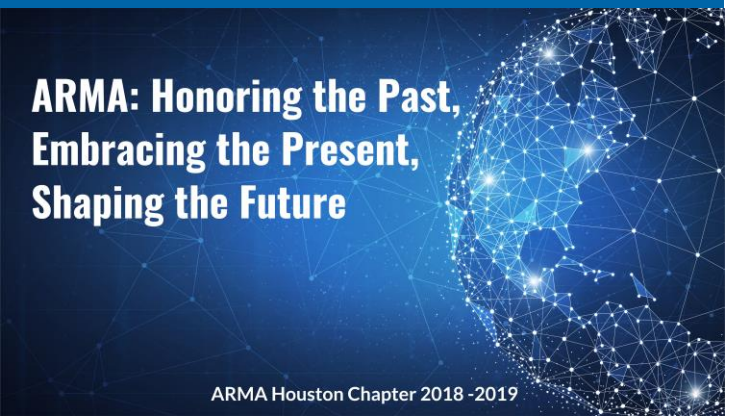
Using Your Organization's Data Privacy Initiative to Breathe New Life into Your RIM Program

Agenda



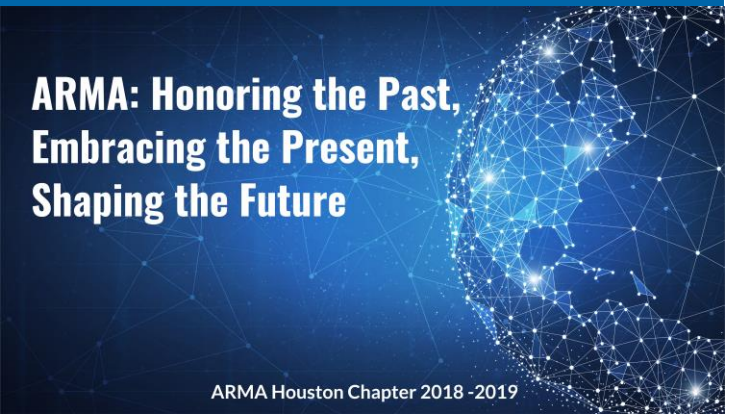
1. Privacy Background
2. Privacy as a Driver for RIM
3. Privacy Initiative Details
4. RIM Next Steps

Privacy Background



- Privacy is coming!
- Your organization is subject to GDPR if you collect **personal data** via online services from consumers in the EEA/EU or via an establishment located in the EEA/EU
- Data Privacy Law is designed to protect individuals' rights to control their data
- Privacy Law is driven by behavioral or targeted advertising. Companies are building profiles with extensive details on the interests and activities of individuals, browser tracking history, cookies, etc…

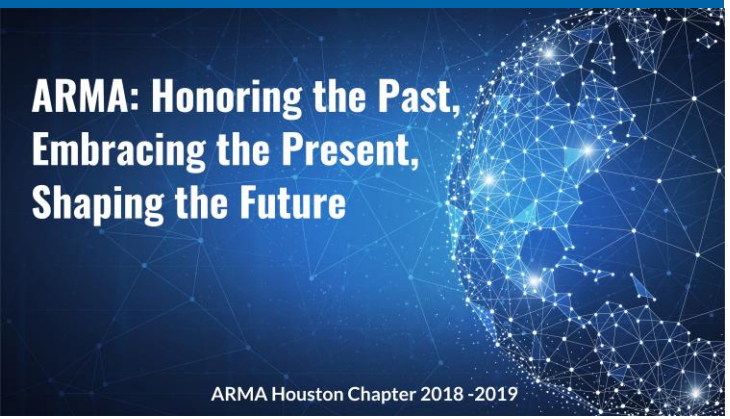
Privacy Background



- Guiding Principle - Personal data must be processed lawfully, fairly and transparently
- Data subjects have rights and need to be informed
- Data minimization – refrain from storing any personal data that is not required for legitimate business purposes
- **Retention** – personal data is retained only as long as required

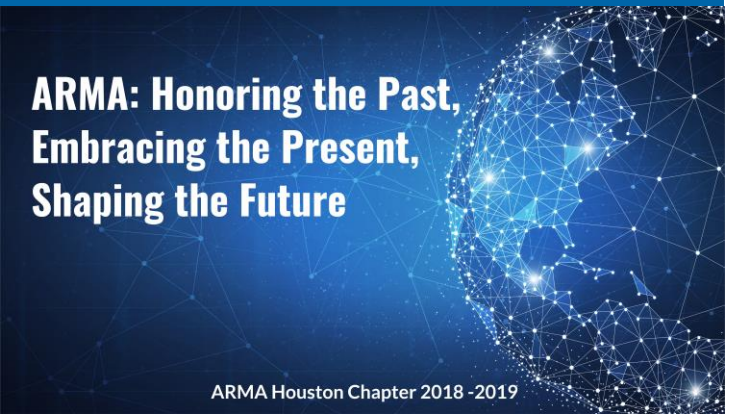
- The wild west days of collecting and exploiting personal data are coming to an end
- Need to take a holistic approach

Does GDPR Apply?



- All individuals who are currently residing in the EEA/EU – Includes citizens and residents?
- Non-EU individuals whose data is collected while in an EEA/EU country – (i.e., foreign students, ambassadors, immigrants, asylum seekers, refugees, vacationers and migrant workers)?
- EU citizens on vacation in a non-EU country (USA, Australia)?

Does GDPR Apply?

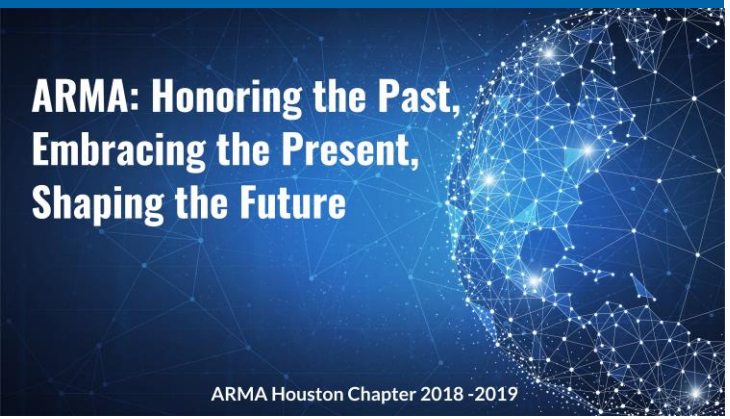


- **Applies** - Applies to Data Subjects as Natural Individuals who are in the EEA/EU – Includes citizens and residents
- **Applies** - non-EU individuals whose data is collected while in an EEA/EU Country – (i.e., foreign students, ambassadors, immigrants, asylum seekers, refugees, vacationers and migrant workers)
- **Does Not Apply** – EU Citizens on vacation in a non-EU country

---

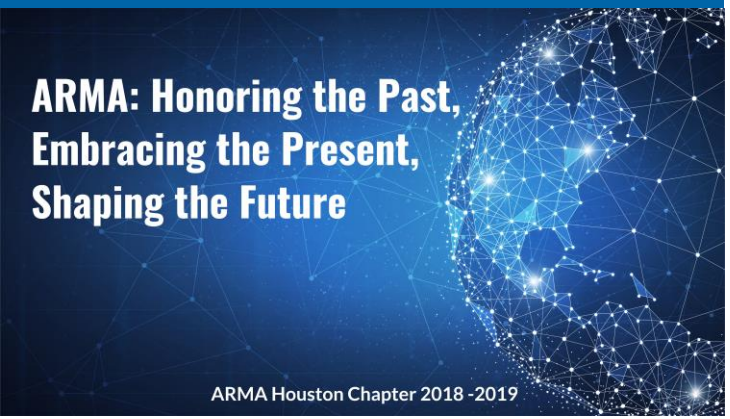
- GDPR covers any individual whose personal data is collected while in the EEA/EU, even if their Personal Data is processed elsewhere
- Only applies when personal data is collected from an individual person who is located in an EU country at the time data is collected.

Personal Data under GDPR



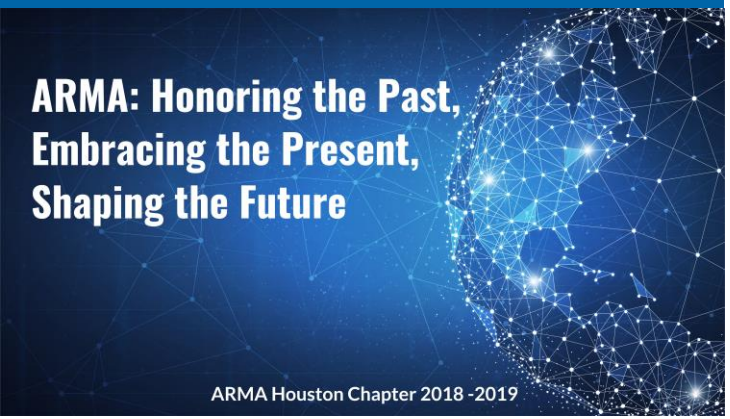
- Any information that relates to an identifiable human individual
  - Test – Can you use the information to identify an individual?
- It is not necessary that the data by itself can identify a person
- It is sufficient that the data relates, in a meaningful way, to an individual who could be identified

Is this Personal Data?



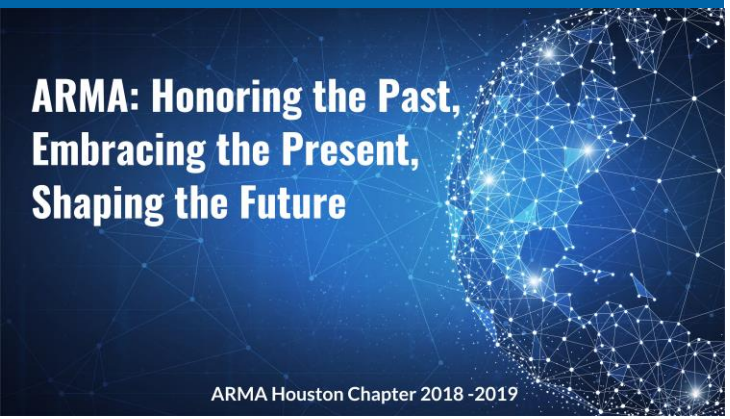
- A person's full name?
- General corporate phone number?
- Phone extension?
- A company phone number, combined with the time of the call?
- Email address?
- Physical address?
- IP address ?
- IP address range used by an organization?

Is this Personal Data?



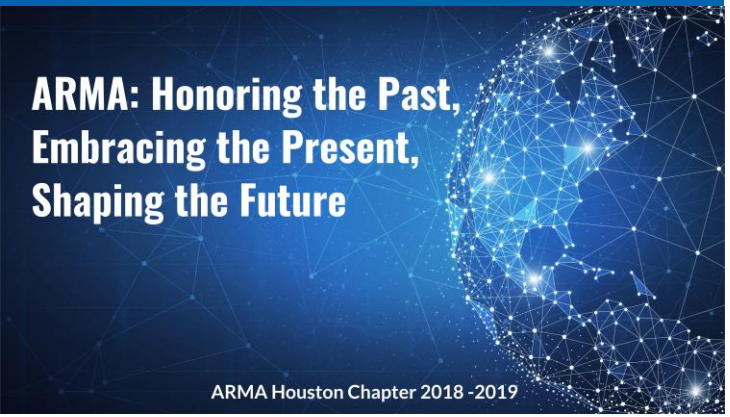
- A person's full name? **Yes**
- General corporate phone number? **No**
- Phone extension? **Yes**, if combined with main number.
- A company phone number, combined with the time of the call? Yes
- Email address? **Yes**
- Physical address? **Yes**
- IP address ? **Yes**, if tied to an individual's device
- IP address range used by an organization? **No**

Is this Personal Data?



- Encrypted data?
- Redacted data?
- Anonymized data?

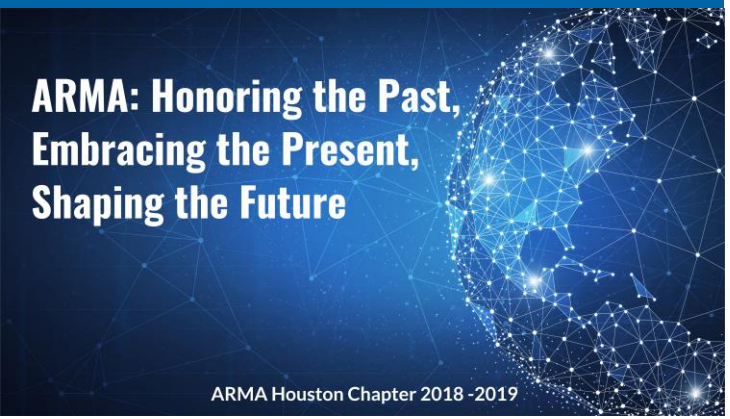
Is this Personal Data?



- Encrypted data? **Yes** (if encrypted data is lost, with no key, then normally not)
- Redacted data? It depends. **Yes**, if the redacted data retains any information that allows the reversal of the redaction process.
- Anonymized data? **Normally No**. Can the anonymization be reversed? If so, it is personal data (a.k.a. pseudonymization)

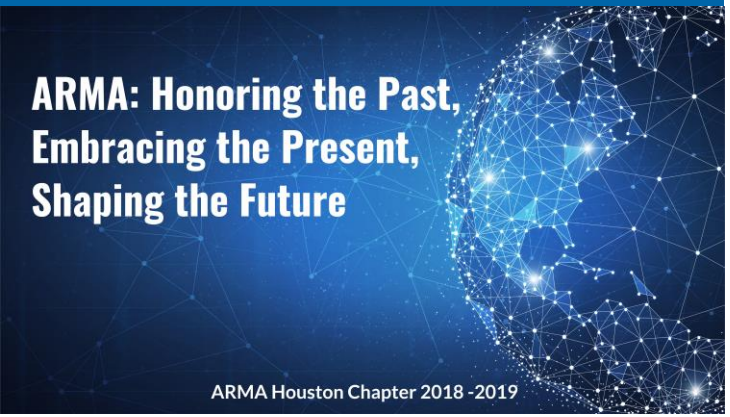
- Data will cease to qualify as personal data if it has been redacted or aggregated in a manner that destroys the connection to an individual

Processing of Personal Data - Defined



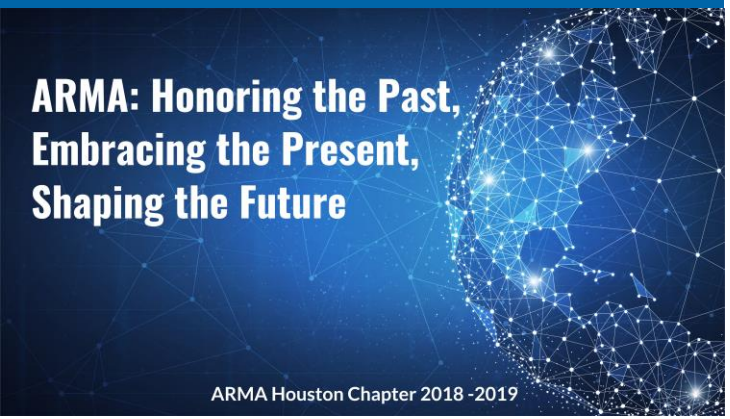
- Collection
- Storing / retaining
- Retrieval / online access
- Alteration / combining
- Transferring
- Redacting / anonymizing / Encrypting
- Destruction

Legal Basis for Processing Data



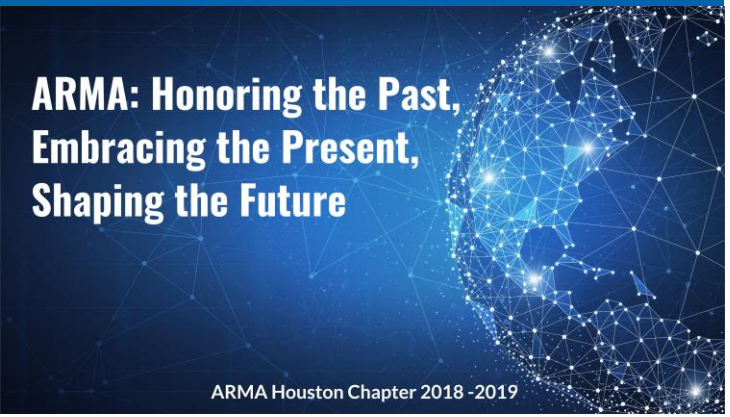
- Under GDPR:
  - Businesses are generally prohibited from processing personal data unless they obtain consent from the data subject or find acceptable statutory exceptions **(need to have a compelling reason, Legal Basis, to process personal data)**
  - This will minimize the amount of personal data that is collected, processed, retained and transferred
- Legal Basis: (most common)
  - Legitimate Interests - needed to provide a service
  - Contractual – fulfill obligations
  - Consent – need explicit consent

Legitimate Interests - Considerations



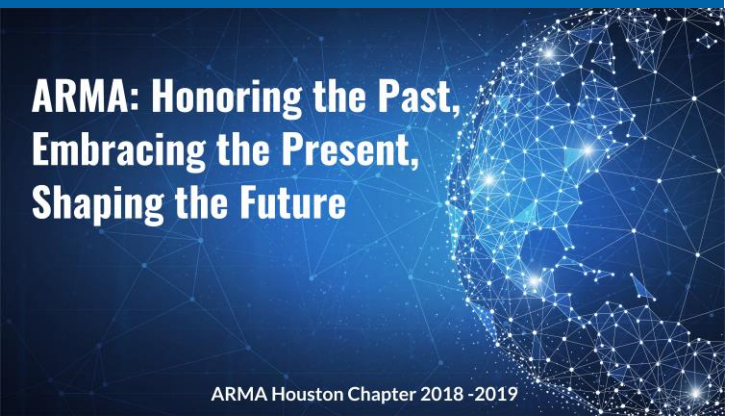
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject. Necessary may mean:
  - In order to provide the requested services for the data subject
  - Employment purposes
  - Vital interests
- Processing on the basis of legitimate interest requires a balancing of the needs of an organization to provide services and the fundamental rights of the data subject

Consent - Considerations



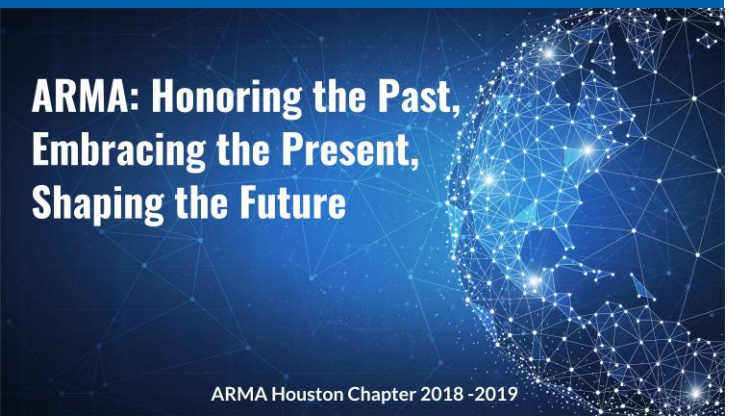
- Need consent specific for each processing activity (cannot have one global consent)
- Consent cannot be coerced and can be withdrawn at any time
- What can and will you do if data subjects deny their consent?
- What can and will you do if data subjects grant their consent and later revoke it?
- Are you prepared to go back to the data subjects and seek consent to changes when you need to expand or modify the processing or use of their data?
- Is there a risk of disrupting an existing business relationship by seeking consent?
- Do any laws restrict the validity of consent or discourage seeking consent?
- How easy is it to obtain and track consent? (click-through during purchase is easy)

PII and Special Categories of Data



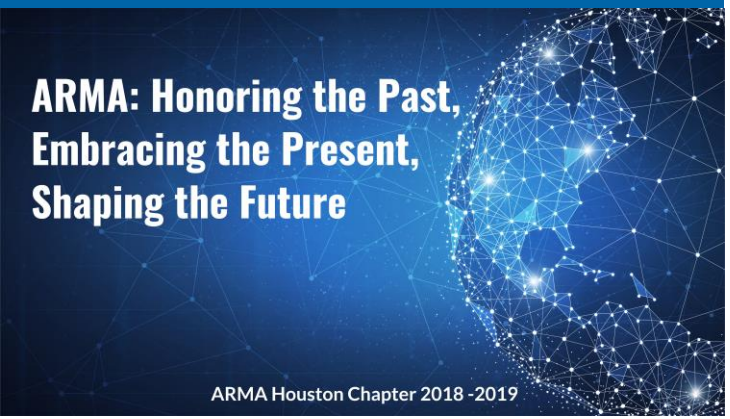
- USA – Laws focus on PHI & PII (SSN, Credit Card Info, etc.)
- GDPR has Special Categories of Personal (Sensitive) Data
  - Political opinions
  - Trade union memberships
  - Medical or health conditions (e.g., employee sick days, prescriptions, clinical trial data)
  - Racial or ethnic origin (place of birth, photos showing skin color)
  - Religious or philosophical beliefs
  - Information relating to sexual orientation (marital status in jurisdictions that do not recognize same sex marriages)
  - Certain types of criminal records (OK to do background checks on employees)

Special Categories of Data



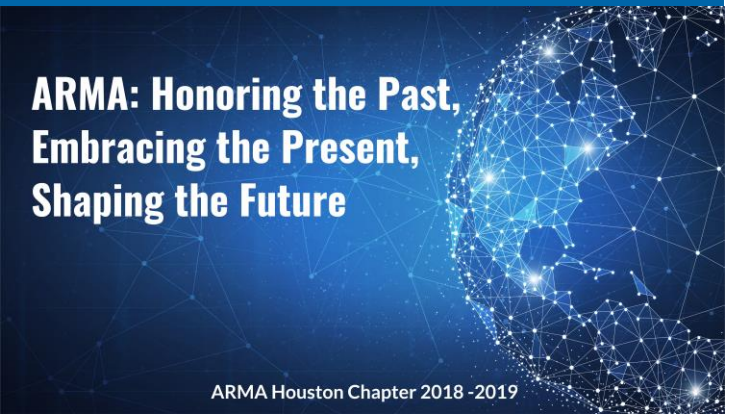
- OK to collect and process locally (inside EEA), sensitive data by employers that are required by law
- Companies need to obtain express consent before transferring any sensitive data outside the EEA
- Exceptions may apply:
  - US export control may require the collection of citizenship
  - Legitimate Interests example - A religious institution may require "religious affiliation" as part of the personal data collected

Data Controllers and Data Processors



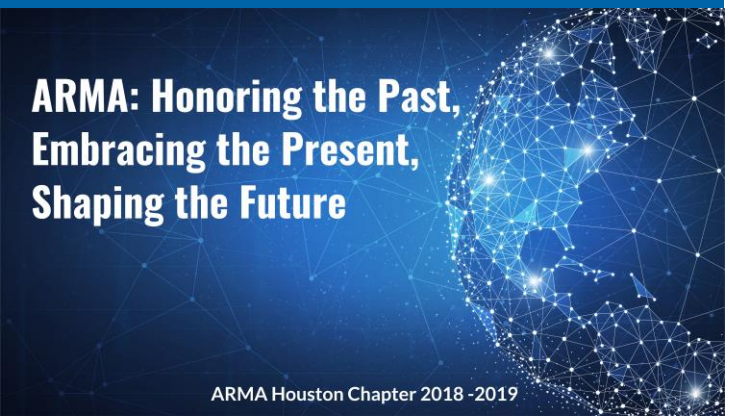
- Data **controllers** will be required to maintain **records of processing activities** and will be subject to greater liability if responsible for a breach
- Data **controllers** cannot push liability onto **data processors**
- Data **controllers** must have contracts that require data **processors** to comply with GDPR. This is normally done by adding data processing agreement language to vendor agreements and data sharing agreements
- Data **processors** – Only process data in the interest and on behalf of data controller (not necessary to disclose to data subject)

Transfers



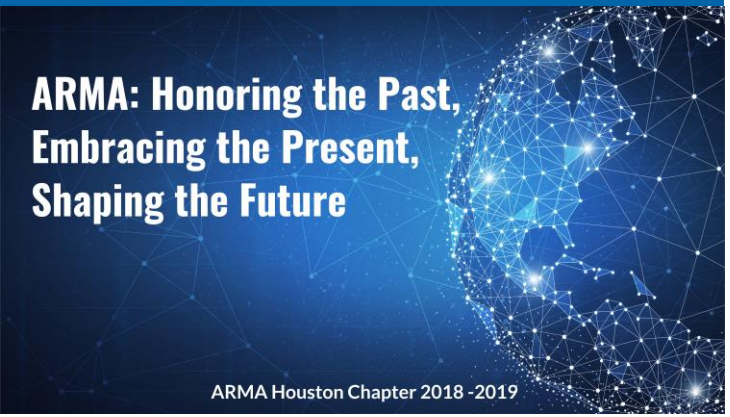
- Provide notice to data subject (Privacy Notice)
- Justify the disclosure (sharing) to another data controller or contractually limit the recipient company to act as a mere data processor
  - EEA companies are generally permitted to engage service providers for data processing purposes – payroll services
  - EEA companies are generally prohibited from disclosing personal data to data controllers, even within the EEA unless they can claim a legally valid justification
- Restrictions of data transfers outside the EEA
  - Requires the recipient company to provide adequate levels of data protection. U.S. companies need to comply with the EU-U.S. Privacy Shield Program. This replaced the U.S. Safe Harbor Program

Some Additional GDPR Requirements for Controllers



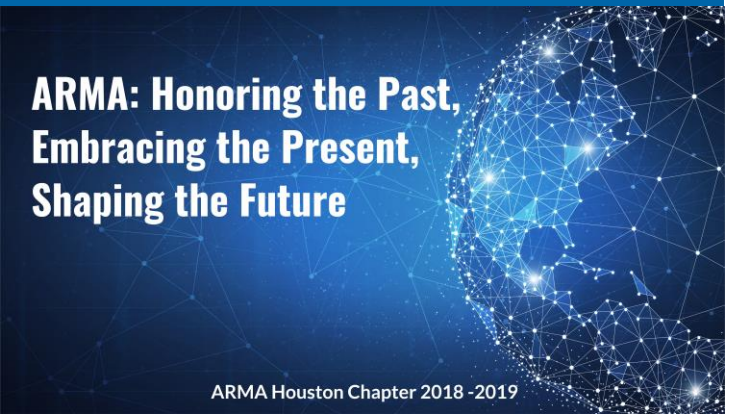
- Document all data processing activities and compliance efforts
- Need Data Processing Agreements with all data processors
- Complete Data Protection Impact assessments for high risk areas
- Privacy Notices and Cookie Banners
- Privacy by Design (Privacy standards for information systems)
- Robust Data **Retention and Deletion** program

Common RIM Program Progression



- Governance Structure
- Policy Development
- Retention Schedule
- Develop a Network of Records Coordinators
- Training and Communications
- Address Physical Records
- Address Electronic, Unstructured Records
- Address Electronic Communications (Email, IM, Social Media)
- **Address Structured Information Systems – Personal Data**

RIM and Structured Information Systems

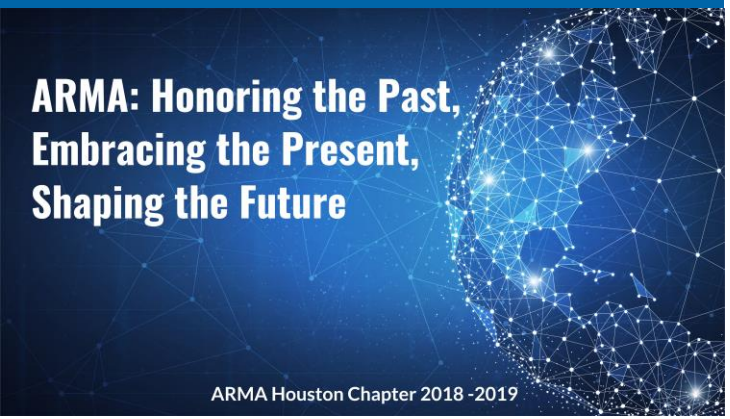


- Address Structured Information Systems – Personal Data

Privacy initiatives require the personal data maintained in structured information systems to be managed:

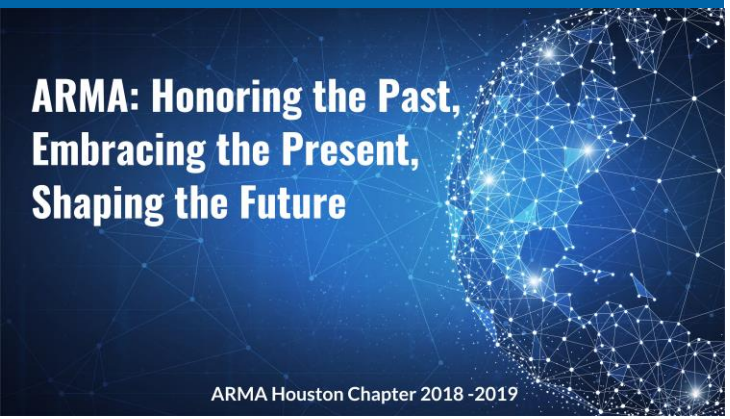
- **Security** – safeguard personal data
- **Privacy** – transparency to data subject. Disclose what is being processed, why and for how long
- **Data Governance** – data integrity, accuracy, access, definitions
- **Retention** – retained long enough to meet legal requirements, but not longer than disclosed purposes of processing

How does Privacy Impact RIM?



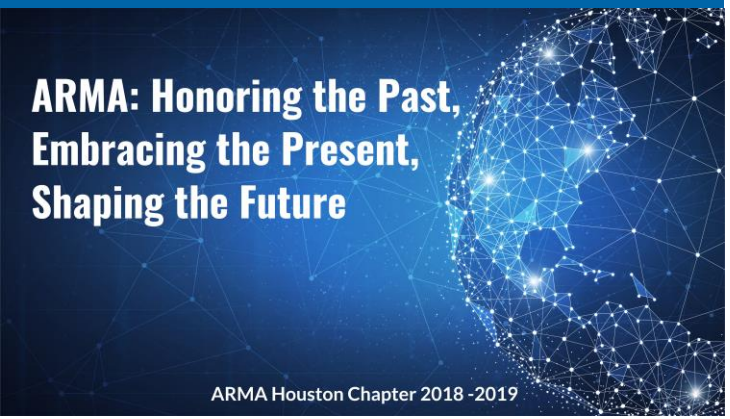
- Privacy notices – need to identify the organization's purpose for collecting, processing, sharing and **retaining** personal data
  - Privacy notices can reference the **retention schedule**
  - Business purpose for collecting data can be added to retention categories
  - **Retention** language can be added directly to privacy notices
- Address personal data stored and processed in structured information systems – align **retention** of system with privacy notices and retention schedule
- Data Map / System Inventory – need to know where impacted records and personal data reside

How does Privacy Impact RIM?

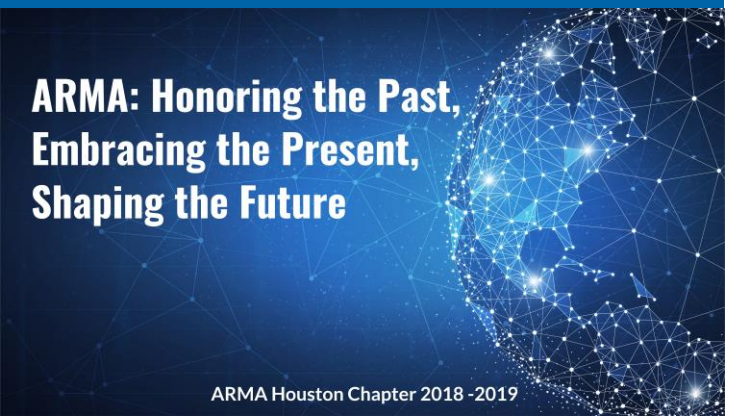


- Data sharing agreements to third parties should define how long shared data must be **retained**, then destroyed
- The retention schedule is the authority for how long data is to be **retained**:
  - Review **retention periods**, from a privacy perspective – do we really need to retain the data for that long?
  - Consider adding **MAX periods** to retention schedule, when driven by privacy requirements
  - Consider updating the retention category description to include the business purpose for retaining the records
- New records will be created to document compliance to the privacy initiative

Privacy Initiative



Privacy Changed Our Reporting Structure



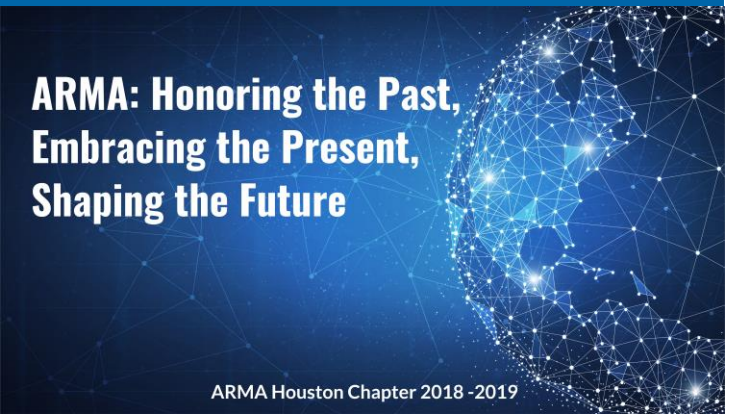
From

- Academic Vice President
- Assoc. Academic VP
- Library Administration
- University Archives
- **RIM**

To

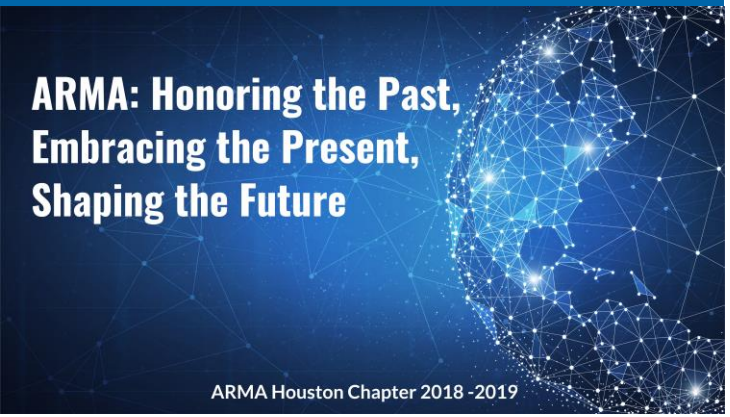
- President
  - Chief Information Officer (CIO)
  - Chief Info Sec Officer (CISO)
    - **IG/RIM**
    - Info Sec
    - Privacy

Foundational / Decisions



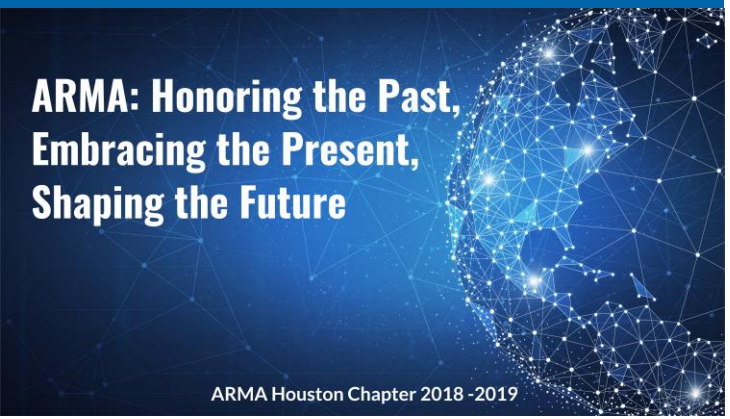
- Data Protection Officer (DPO)
- Authorized GDPR Representative
- Establish Legal Basis – Legitimate Interest or Consent?
- Privacy Policy
- Privacy Notices – Broad or Specific? How to refer to **retention**?
- Cookie Notice Template
- Data Processing Agreement Language
- Develop Privacy Standards for Developers, Vendors, and Websites (Security, Privacy and **Retention**)

Operational Tasks



- Data Privacy Survey – identify high risk processes – departments processing personal data of EU residents
- Data Map/System Inventory – identify systems that store personal data
- Data **Retention** and **Deletion** – review against privacy needs
  - Align **retention** categories with major business processes
  - Add Maximum **retention** periods in relevant areas
  - Add business purpose to **retention** category descriptions
- Develop and roll out Privacy Training Program

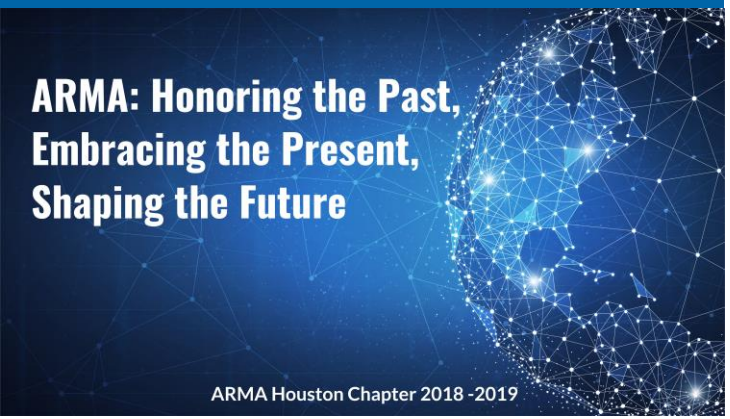
Example Retention Category



STU03	Admissions, Enrolled	Any recorded information associated with the application process for undergraduate and international applicants who applied, were accepted, and enrolled. Records may include CES applications, high school transcripts, academic transcripts from other institutions, entrance exam reports, test results (ACT, SAT, LSAT, MCAT, GRE scores and placement test exception forms), letters of recommendation, letters of recommendation, deferment forms, appeals, acceptance letters, letters offering financial aid or scholarships, student waivers, and related documentation and correspondence.	Permant
STU04	Admissions, Not Enrolled	Any recorded information associated with the application process for undergraduate and international applicants who applied, but were not accepted, or who were accepted, but did not enroll. Records may include CES applications, high school transcripts, academic transcripts from other institutions, entrance exam reports, test scores, letters of recommendation, student waivers, letters of admittance, deferment forms, appeals, and related documentation and correspondence.	Retain 3 year after application semester, then destroy.

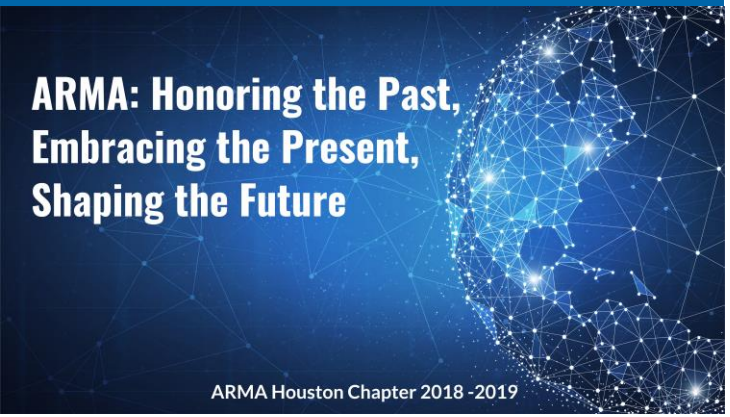
During the student's application process, the privacy notice discloses to the applying student (data subject) that their personal data will be retained permanently, if enrolled or three years, if not enrolled/admitted.

Data Transfers



- Add Privacy Language to Data Sharing Agreements with affiliated entities:
  - Joint Controllers – Process data for their own purposes (must disclose to data subject in privacy notice)
- Add Privacy Language to Vendor Contracts
  - Data Processors – Service Providers
  - Data Handlers – SaaS with no access to data (cloud providers)
- Update Vendor Management Policy

Privacy Notice / Cookie Banner



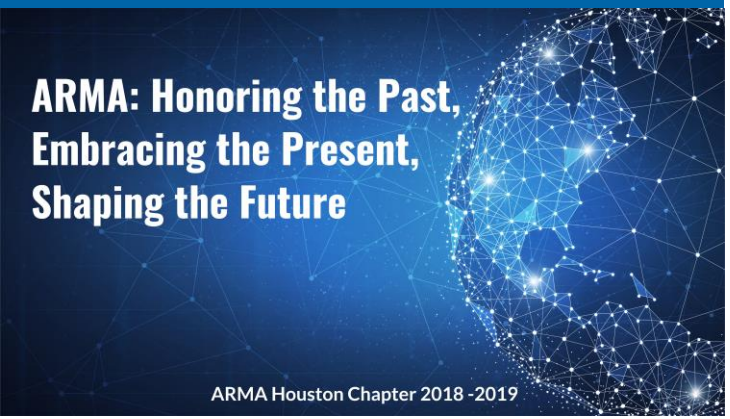
- A single Global Privacy Notice

or

- Student Online Privacy Notice – for Student Data
  - Application process
  - Registration process
- Specific Privacy Notices – for special categories of data
- Privacy Notice to EEA Employees

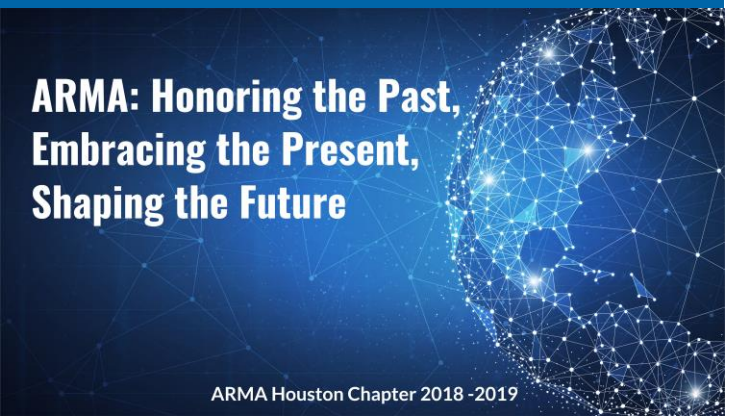
- Cookie Banner template for websites

What is on a Privacy Notice?



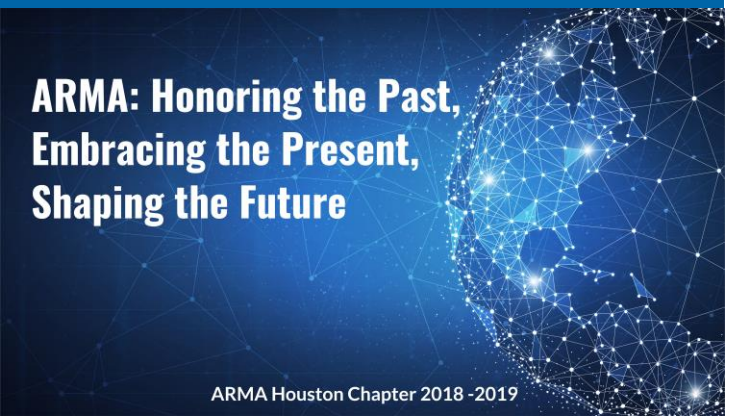
- Legal basis for collecting personal data
- Purpose for processing personal data
- Disclose if the data will be shared with other organizations (data controllers)
- How long the data will be **retained**
- Rights of the data subject
- Contact details of data controller, DPO and EEA representative

Standards and Documentation



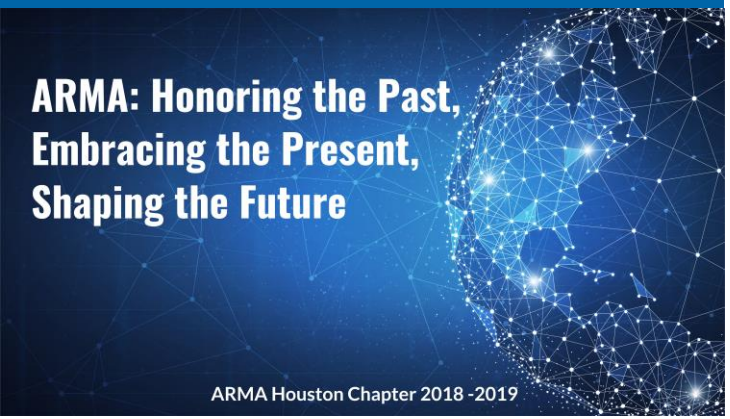
- Records of Processing Activity
- Development of Privacy Standards for Developers, Vendors, and Websites (Privacy by Design)
- Data Protection Impact Assessments (DPIA) – high risk areas
- Lawful Access Request Policy and Protocol (subpoenas)
- Data Subject Request Policies and Protocols
- Technical and Operational Measures (TOMS) - Security
- Data Breach Incident Reporting and Protocols

Data Breach Notification



- "A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data…"
- Notify **supervisory authority**
  - If likely to result in a risk to individual rights and freedoms
  - Within 72 hours (unless law enforcement requests delay)

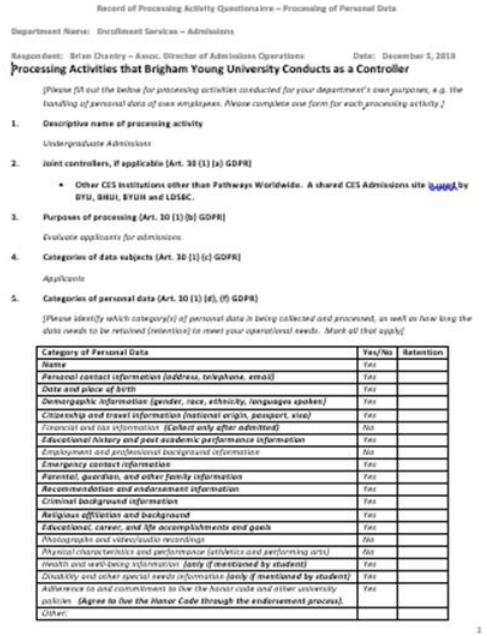
Data Breach Notification



- Notify **individual** (data subject)
  - If likely to result in high risk to individual rights and freedoms
  - Without undue delay
  - Supervisory authority may instruct controller to notify individuals. Exceptions:
    - Unlikely to result in high risk
    - Appropriate technical and organizational protection was in place (e.g., encryption)
    - Would involve disproportionate efforts

Data **Retention** and Data Minimization will reduce the impact of a Data Breach!

Records of Processing Activity



Record of Processing Activity Questionnaire – Processing of Personal Data

Department Name: Enrollment Services – Admissions

Respondent: Brian Chantry – Assoc. Director of Admissions Operations Date: December 3, 2019

Processing Activities that Brigham Young University Conducts as a Controller

[Please fill out the below for processing activities conducted for your department's own purposes, e.g. the handling of personal data of own employees. Please complete one form for each processing activity.]

1. **Descriptive name of processing activity**

   Undergraduate Admissions

2. **Joint controllers, if applicable (Art. 30 (1) (a) GDPR)**

   - **Other CES institutions other than Pathways Worldwide. A shared CES Admissions site is used by BYU, BHUI, BYUH and LDSBC.**

3. **Purposes of processing (Art. 30 (1) (b) GDPR)**

   Evaluate applicants for admissions.

4. **Categories of data subjects (Art. 30 (1) (c) GDPR)**

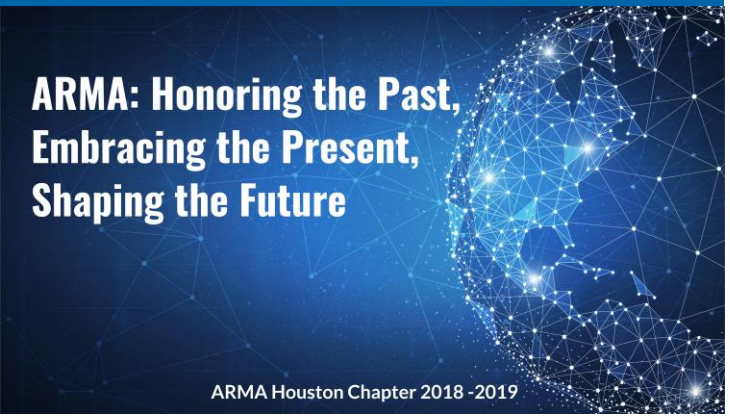
   Applicants

5. **Categories of personal data (Art. 30 (1) (d), (f) GDPR)**

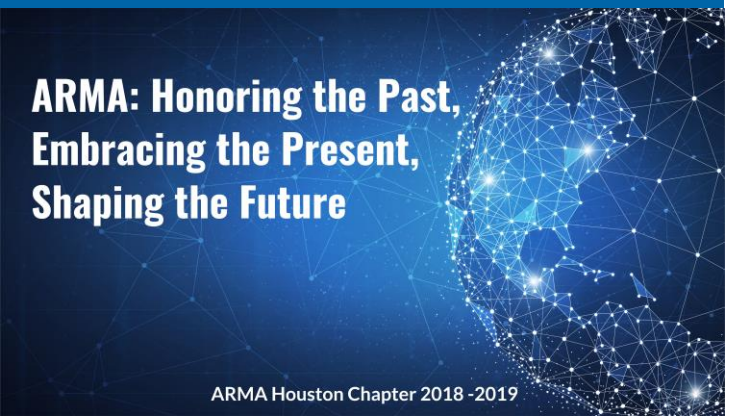
   [Please identify which category(ies) of personal data is being collected and processed, as well as how long the data needs to be retained (retention) to meet your operational needs. Mark all that apply]

Category of Personal Data	Yes/No	Retention
Name	*Yes*	
Personal contact information (address, telephone, email)	*Yes*	
Date and place of birth	*Yes*	
Demographic information (gender, race, ethnicity, languages spoken)	*Yes*	
Citizenship and travel information (national origin, passport, visa)	*Yes*	
Financial and tax information (Collect only after admitted)	*No*	
Educational history and past academic performance information	*Yes*	
Employment and professional background information	*No*	
Emergency contact information	*Yes*	
Parental, guardian, and other family information	*Yes*	
Recommendation and endorsement information	*Yes*	
Criminal background information	*Yes*	
Religious affiliation and background	*Yes*	
Educational, career, and life accomplishments and goals	*Yes*	
Photographs and video/audio recordings	*No*	
Physical characteristics and performance (athletics and performing arts)	*No*	
Health and well-being information (only if mentioned by student)	*Yes*	
Disability and other special needs information (only if mentioned by student)	*Yes*	
Adherence to and commitment to live the honor code and other university policies (Agree to live the Honor Code through the endorsement process).	*Yes*	
Other:		

- Purpose of processing personal data
- Identify joint controllers
- Categories of data subjects
- Categories of personal data being collected
- Data shared within the EU/EEA
- Data shared outside the EU/EEA
- Description of security measures

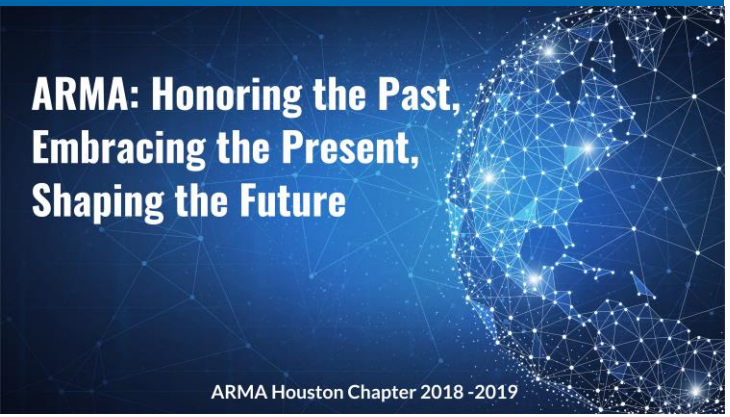


Priority - Highest Risk Areas



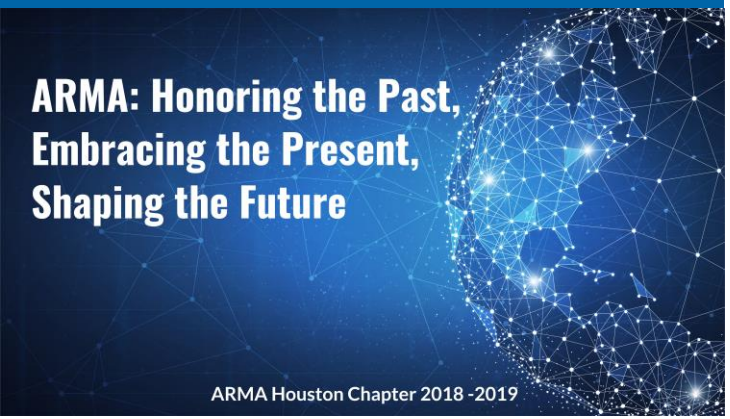
- Student applications from EU residents located in the EU
- Branch campus located in the EU
- Sending students to counterparts in the EU (exchange, research, internship, study abroad)
- Collaboration with EU institutions
- Research incorporating EU data sets
- Recruiting students and faculty from the EU
- Receiving donations from the EU
- Alumni data of EU citizens

RIM – Next Steps



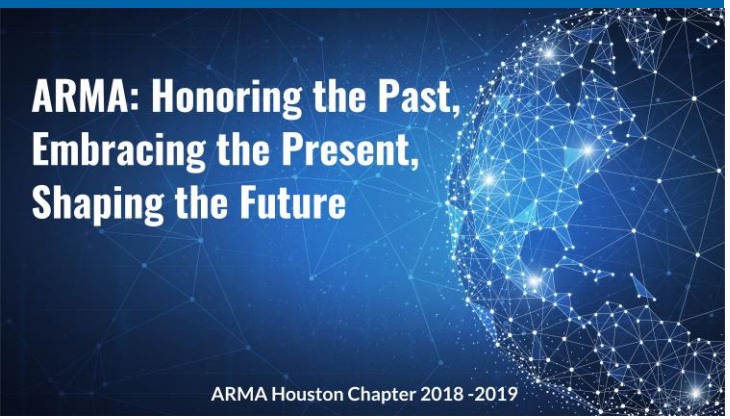
- Align **Retention** Schedule with Privacy requirements
  - Align **retention** categories with major processing activities
  - Consider adding a Max **Retention** period to each retention category
  - Expand description to include purpose for each **retention** category
  - Ensure new compliance records are coved by an appropriate **retention** category
- Work with Privacy to determine how **retention** will be referenced in Privacy Notices and Privacy Policy
- Work with IT to develop a Data Map (System Inventory). Identify **retention** requirements for each system or major processing activity that stores or processes personal data
- Leverage the IT "Privacy by Design" initiative by adding **retention** requirements to the mix
- Work with Purchasing and Contracts to determine how **retention** will be referenced in Data Processing Agreement language added to vendor contracts

Some RIM/Privacy Challenges

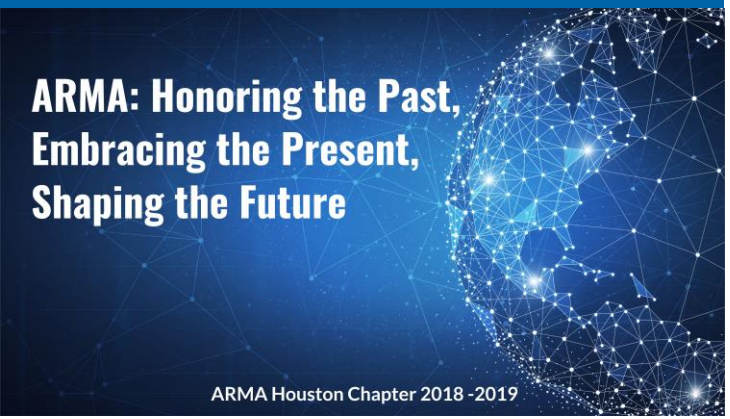


- How to address "mixed" datasets, containing both EU and non-EU data
- If using consent, what records can be "forgotten" and what must be retained
- Addressing legacy records
  - No notifications or disclosures
  - No consent was given
  - How do we respond to requests to view/correct data?
  - Do we have a legitimate reason to keep it?

Some Privacy Solutions/Vendors



- Some Privacy Software Features
  - Surveys and assessments to identify compliance gaps and remediation
  - Manage privacy notices and cookie notices
  - Awareness and remediation training
  - Data breach management
- Some Privacy Vendors
  - **Trustarc**
  - OneTrust
  - IBM Security Guardium
  - DataGrail Privacy Portal
  - Integris



Presenter Name: Howard Loos, CRM, IGP

Director of Records and Information Management

Brigham Young University

Howard.Loos@BYU.edu

801-422-2161

RecordsManagement.byu.edu