Crowe

Smart decisions. Lasting value.™

Becoming a Privacy Resilient Organization

Pam Hrubey, CCEP, CIPP/US, DrPH

Bill Dykstra

September 2018

What is the first word people say when the topic of privacy and data protection is raised?

UGH*

**The other "first word" people say probably isn't polite to say out loud in a meeting.*

Probably the better question is why are people so easily frustrated by the topic of privacy and data protection?

Our goal today is to provide you a framework to use to ‘tackle’ the topic of privacy and data protection in a fashion that allows you to maintain some resiliency as the environment external to your organization continues to evolve.

Discussion Topics

- Global overview of the evolving privacy and data protection landscape and rationale for including related organizational obligations within the role of a senior leadership function, such as the General Counsel.

- Establishing a resilient privacy and data protection program framework

- Tips for considering privacy and data protection in the context of the seven elements of an effective compliance program with the goal of fostering development of a resilient privacy and data protection program

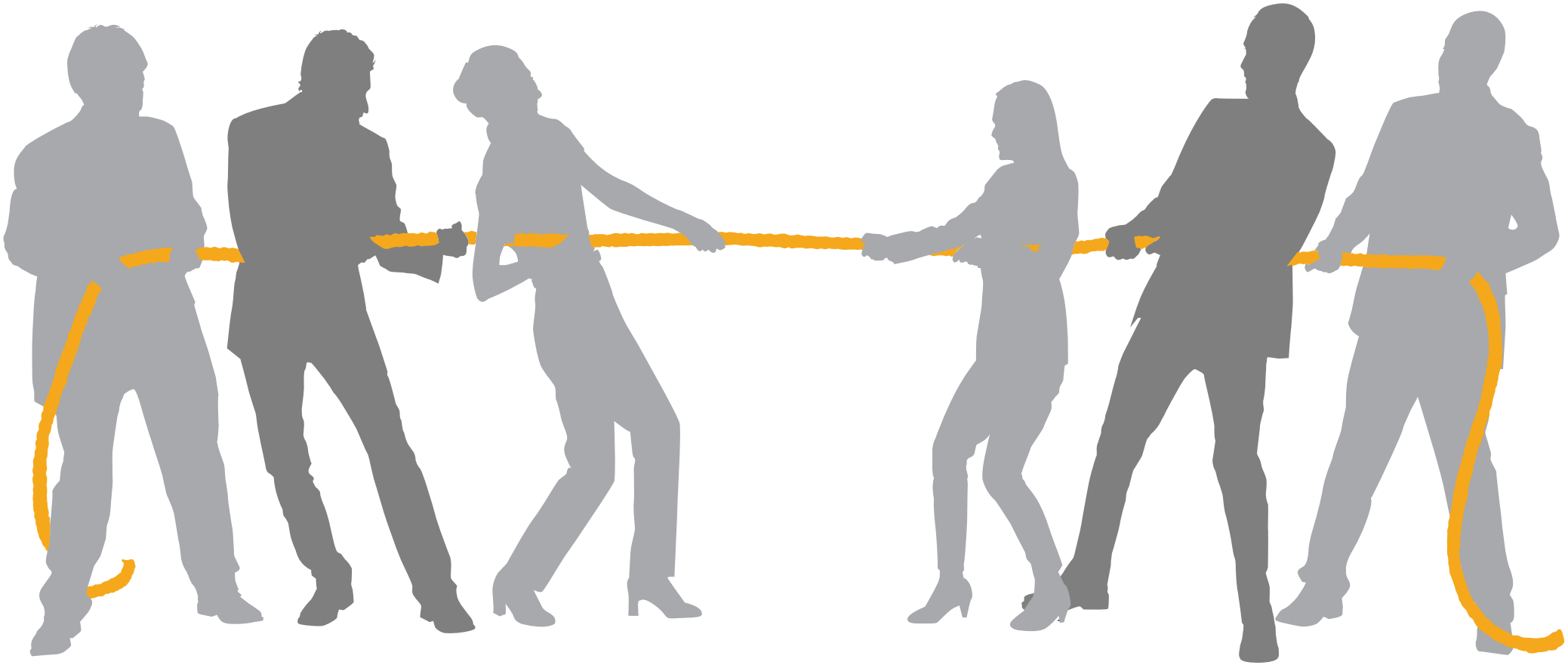
Polling Question Number One

Who at your organization or institution is responsible for implementation and monitoring compliance activities relating to data privacy?

A. Chief Data Privacy Officer
B. Chief Ethics and/or Compliance Officer
C. Head of Information Security
D. Chief Financial Officer
E. Do not know

Global Privacy and Data Protection Landscape

Different Laws, Different Expectations, Difference Approaches = Frustration



Evolution of Privacy and Data Protection Globally

- Sweden, 11 May 1973 – First national-level data protection law designed to address the advent of computers processing personal data
- EU Data Protection Directive (95/46) 24 October 1995 – Expanded on the concepts put forward in Sweden
- Personal Information Protection and Electronic Documents Act (Canada) 1 January 2001 – Addressed commercial operations-related privacy concerns
- Health Information Portability and Accountability Act 14 April 2003 (United States, only addressing personal health data) – Addressed personal health information used for purposes of paying for healthcare
- HIPAA Security Rule 21 April 2005 (United States, only addressing security of health data)
- Global Data Protection Regulation (EU) 25 May 2018 – a brave new world
- California Consumer Privacy Act 1 January 2020 – a braver new world in a portion of the US
- General Data Protection Law (Brazil) Post 1 January 2020 – privacy protections expand in S.A.

Privacy and Data Protection impacting University/Education Sector

- Family Educational Rights and Privacy Act passed in 1974
  - Federal grants students five basic rights
  - Prior to 2013 this was the primary law utilized for privacy regulation
  - School or University remains accountable for students' information even if utilizing a third party
- Federal Policy for the Protection of Human Subjects published 1991 addresses ethical principals in research involving human subjects, including privacy
- Gramm Leach Bliley Act of 1999 imposes privacy provisions on financial institutions designed to protect consumer data
- Securing a Hybrid Environment for Research Preservation (SHERPA) in 2002.
- Fair and Accurate Credit Transaction Act of 2003 requires entities engaged in credit transactions to be aware of warning signs of identity theft and take steps to respond to suspected incidents
- Since 2013 what has happened
  - 40 States have passed 125 laws relating privacy in the education space
  - 35 of these laws supplement the FEPRA regulation

The evolving California Consumer Privacy Act of 2018

- **Who is protected?**
  - Any “natural person who is a California resident.” Applies to “consumers” but also to patients, students, employees, etc.

- **Who must comply?**
  - An organization must comply with the Act if any one of three conditions are present:
    - Annual gross revenues greater than $25 million OR
    - Obtains personal information on 50k or more CA residents annually OR
    - 50% or more of the revenue comes from selling CA resident data
  - Exception: An organization may avoid complying if they have
    - No Physical presence in or an affiliate in California AND
    - they can demonstrate that its “commercial conduct takes place wholly outside of California.”

- **What are the penalties of non-compliance?**
  - Organizations will be fined up to $7,500 per intentional violation.
  - Organizations will be fined up to $2,500 per unintentional act that is not cured within 30 days of notice.
  - Organizations whose data is breached or stolen are subject to fines of $100 to $750 per California resident (or actual damages, whichever is greater) in civil court.

More About the California Consumer Privacy Act of 2018

- **What are the protections?**
  - The Act protects “personal information” which is defined as “any information that relates to a particular consumer or household.” The Act provides California residents the right to:
    - Request a record of what types of data, how it’s used, and who it’s shared with.
    - Full right of erasure
    - Object to the sale
    - Private cause of action for unauthorized access to non-encrypted or non-redacted personal information.

- **What are the requirements?**
  - Organizations must take proactive steps of compliance including (but not necessarily limited to):
    - Establish an ID verification process.
    - Provide data access requests method including a toll-free number.
    - Respond to data access requests within 45 days.
    - Obtain express opt in consent.
    - Avoid discrimination against a consumer based on the exercising of any of the rights granted in the bill.
    - Prepare data maps and inventories of personal information that documenting critical flows/location of data.
    - Update privacy policies and disclosures to inform consumers of their rights.

  - **And what will change before we actually get to 1 January 2020?**

Overview of the General Data Protection Regulation

Accountability & Governance

Determining the organisation's risk appetite in relation to data protection, enhancing accountability and governance through policies and standards that address the requirements of GDPR.

RISK GOVERNANCE
(DP risk appetite and the link to wider Enterprise Risk Management framework)

DATA GOVERNANCE
(ownership, stewardship and control of personal data acquired and processed)

DP POLICY & STANDARDS
(enhanced policies and standards to govern the design of operational changes, in line with risk appetite)

Legal, Processes & Organisation

Establishing the legal basis for use, the Data Protection Officer's role, handling data subjects' requests, managing third parties, responding to data breaches, and implementing the supporting organisation, process and cultural changes.

CONSENT, USE & LAWFULNESS OF PROCESSING

DATA SUBJECT REQUESTS & RIGHTS
(SAR; RTBF; portability; restriction; rectification)

THIRD PARTY MANAGEMENT
(legal docs; DD; oversight)

BREACH MANAGEMENT & NOTIFICATION

DATA PROTECTION OPERATING MODEL
(DPO role; privacy by design; DPIA; line 1 & 2 responsibilities)

TRAINING AND AWARENESS
(delivery of enhanced DP training to meet needs, plus communications and culture change)

Information Security & Data Retention

Understanding and defining the approach to information security and personal data retention.

INFORMATION SECURITY - ELECTRONIC

INFORMATION SECURITY - PHYSICAL

DATA RETENTION
(deletion; obfuscation; pseudonymisation)

Data Definition & Mapping

Understanding, defining and documenting the personal data that the organisation acquires and processes.

DATA DEFINITION AND MAPPING
(documenting and classifying uses, locations and internal/external movements of personal data)

TRANSFERS OF PERSONAL DATA OUTSIDE EEA
(Standard Agreement; Binding Corporate Rules; Privacy Shield)

Polling Question Number Two

Do you believe the Global Data Protection Requirement is applicable to your organization?

A. Yes
B. No
C. Not sure

Questions to consider when assessing if GDPR applies?

- Do you conduct any recruiting or admissions activities either in the EU or with students living in the EU?
- Do you sponsor or administer any study abroad programs in the EU?
- Do you recruit or hire faculty and staff residing in the EU?
- Do you conduct research on human subjects within the EU or on individuals residing in the EU?

If you answer yes to any of the above questions then GDPR applies to your organization and its potential impact should be assessed.

How is this done in a resilient approach?

Establishing a Resilient Privacy and Data Protection Framework

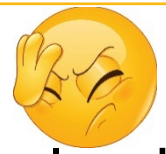
What is privacy resilience?

- In a world where every day brings new events in the privacy and data protection space, “resiliency” is not the word that most organizations think of when they consider their approach to privacy-related compliance with emerging regulations, standards, and consumer and other stakeholder expectations. Resiliency, defined by Merriam-Webster as the capacity to recover quickly from difficulties, or having toughness and elasticity.

- The constantly changing environment of privacy and data protection regulations is an unusual place to highlight a need for toughness, particularly using that term as a positive attribute. Some say toughness is the right approach – implying that an organization must “stand firm” in use of current practices, or even “stay strong” as the legal team prepares a defense against needless or over-reaching regulations.

- We say that “toughness” or “elasticity” can instead be applied to one’s approach to applying essential privacy principles across the enterprise.

So How Does an Organization Tackle the Conundrum of the Global Privacy and Data Protection Regulatory Landscape

- There is a reason why people  when someone mentions privacy and data protection. The global regulatory landscape is complicated.
- Some have proposed that the GDPR offers a solution to the complexity conundrum.
  - Except…that isn't helpful if you are a company focused only in the US.
  - It especially doesn't help if you do business in California – or one of the many states that have special privacy and/or data protection laws – like South Dakota, for example, that has a new breach notification law.
  - And the GDPR doesn't really qualify as "simple"
- And, to be fair, while the GDPR attempts to remove some of the variability across the privacy and data protection landscape in Europe by creating a common regulation, there are application differences in specific EU member states so even the GDPR isn't a uniform framework.

We propose using the Generally Accepted Privacy Principles (GAPP) as a Starting Point Towards a Privacy Resilient Framework

- **Management.** The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.
- **Notice.** The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.
- **Choice and consent.** The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.
- **Collection.** The entity collects personal information only for the purposes identified in the notice.
- **Use, retention, and disposal.** The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information.

Generally Accepted Privacy Principles, Continued

- **Access.** The entity provides individuals with access to their personal information for review and update.
- **Disclosure to third parties.** The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.
- **Security for privacy.** The entity protects personal information against unauthorized access (both physical and logical).
- **Quality.** The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.
- **Monitoring and enforcement.** The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy related complaints and disputes.

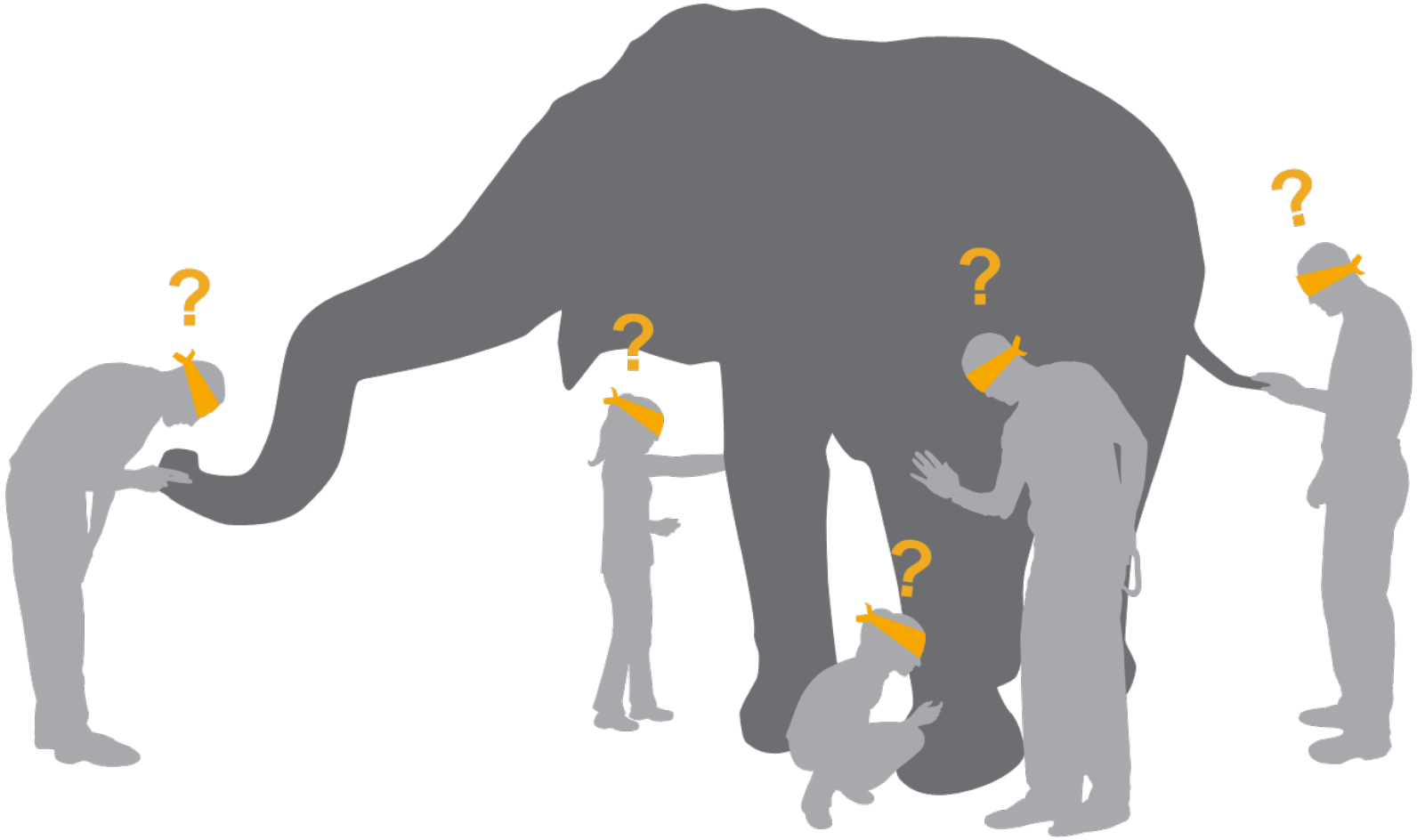
Polling Question Number Three

How does your organization or institution address the varying requirements of current data privacy standards and implementation of new requirements?

A. Separate department for each regulation
B. Separate group within each impacted department/college (admissions, recruiting, and etc.)
C. Centralize department utilizing an organization wide approach
D. Address when an issue arises/occurs
E. Do not know

Establishing a Resilient Privacy and Data Protection Program

We Want to Place Privacy and Data Protection Into a Construct That Leaders Can Identify With…Even Though Individual Perspectives Vary



The Seven Elements of an Effective Ethics and Compliance Program

Equally useable for topics from anti-bribery and anti-corruption to conflict minerals, trade sanctions, and privacy & data protection.

So why don't more organizations leverage this model to help their employees understand how to operate in a way that is consistent with the organization's expectations for effective privacy and data protection?

We Aren’t Sure Why More Organizations Don’t Consistently Apply the Seven Elements to Privacy and Data Protection…But We Have Some Suggestions About How To Start

Governance

- **Elevate the position of Chief Privacy Officer or Data Protection Officer**
  - Avoid burying the role in the legal function or technology function
- **Talk about privacy and data protection at the organization’s senior-most meetings**
  - Make sure the senior most leaders understand why privacy and data protection matters
    - Students, research participants, and faculty expect it
    - Maintaining the organization’s reputation is dependent on it

Policies and Procedures

- **Create policies and procedures that make sense to non-experts**
  - Easily understand doesn’t mean “talk down to

Training

- Not necessary to cover every topic in one sitting – consider telling a story a little bit at a time

Communication

- Short, frequent, and different mediums works well here

Some Additional Suggestions

Auditing, Monitoring, Assessment

- Consider external assessment periodically as this may eventually become an regulatory requirement

Investigations

- It is still possible (and perhaps necessary) to talk about investigations that relate to privacy and data protection matters, protecting the privacy of those involved.

Corrective Action

- Because of the complexities associated with privacy and data protection (and the associated requirements associated with information security) it is critically important to identify the root cause of privacy failures.

Polling Question Number Four

What do you believe would be the most difficult hurdle for your organization to overcome, in order to implement a resilient data privacy program?

A. Buy-in from Senior Leaders across the organization
B. Identifying where ownership should reside
C. Determining where to begin in implementing
D. Establishing effective communication and monitoring
E. We should be able to implement

Questions?

Pam Hrubey
Managing Director
Crowe LLP
317.208.1904
Pam.Hrubey@Crowe.com

Bill Dykstra
Manager
Crowe LLP
303.831.5022
Bill.Dykstra@Crowe.com