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

New question…what is the first word people say out loud when the topic of privacy and data protection is raised?

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 is it that people are 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 the ethics and compliance officer
- 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

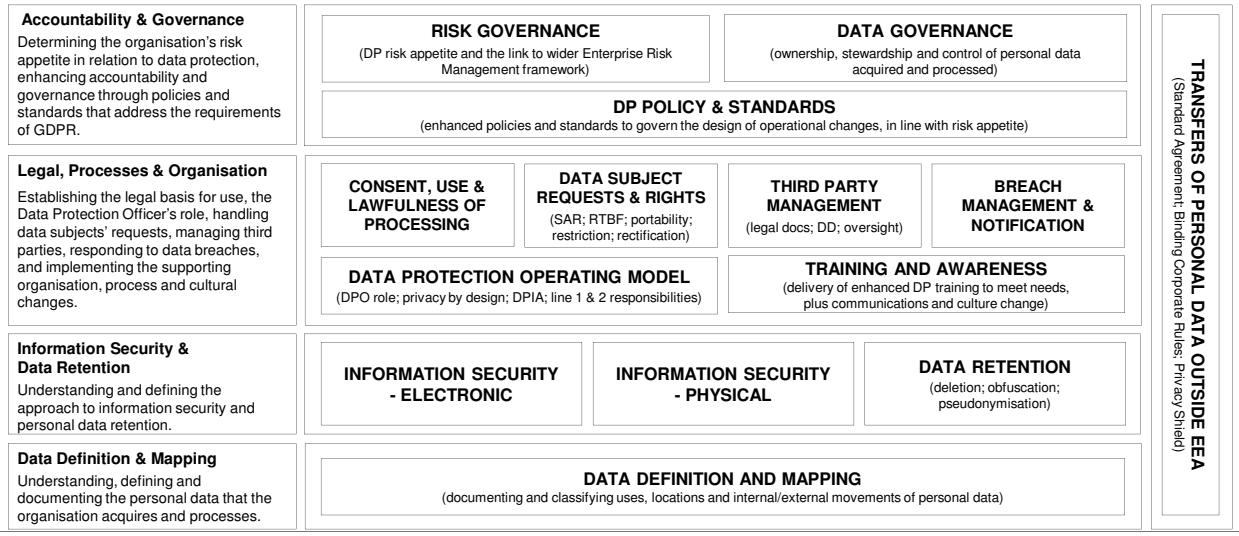
Global Privacy and Data Protection Landscape

Privacy and Data Protection – Different Meanings, Different Locations

Evolution of Privacy and Data Protection

- 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.

Overview of the General Data Protection Regulation



And Now We Have the 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.
  - Does not apply to an individual who is in the state for a transitory purpose.
- **Which companies must comply?**
  - A company 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: A company may avoid complying if they do not have a
    - No Physical presence in or an affiliate in California AND
    - they can demonstrate that its "commercial conduct takes place wholly outside of California."

More About the California Consumer Privacy Act of 2018

- **What are the penalties of non-compliance?**
  - Companies will be fined up to $7,500 per intentional violation.
  - Companies will be fined up to $2,500 per unintentional act that is not cured within 30 days of notice.
  - Companies 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.

- **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.

California Consumer Privacy Act of 2018

- **What are the requirements?**
  - Companies 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.
    - Disclose to whom they sell personal data and have in place a "Do Not Sell My Personal Information" button on their website home page. If an person opts out, do not contact for 1 year.
    - Obtain express opt in consent.
    - Avoid discrimination against a consumer based on the exercising of any of the rights granted in the bill.
    - Be able to offer higher tiers of services or products in exchange for more personal data if the exchange is not unjust or "usurious."
    - Prepare data maps and inventories of personal information that document: locations of personal information, usage, and transfers.
    - Update privacy policies and disclosures to inform consumers of their rights.

General Data Protection Law (Brazil)

- Replaces current sectoral legal framework which has been conflicting (and not widely enforced)
- Any practice that processes personal data will be subject to the law, subject to a few exceptions (areas like national and public security, pure research, artistic and journalistic purposes)
- Any foreign company that has at least an office in Brazil, or offers services to the Brazilian market and collects and treats personal data of data subjects located in the country, regardless of the nationality, will be subject to the new law.
- Very broad definition of personal data (includes data that when aggregated with other information might identify someone as "identifiable")
- Includes a principle of accountability, which makes it mandatory for the data controller and data processor to demonstrate the adoption of effective measures capable of proving compliance with the rules for the protection of personal data (accomplished through a data protection assessment, may need to be transparent about the results)
- Must record all data processing activities
- Must take appropriate technical, security and administrative measures to protect personal data

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 say UGH! 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

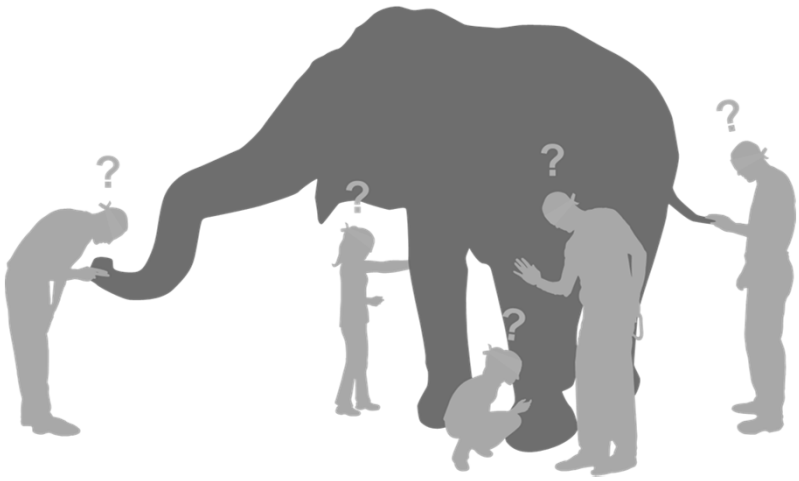
- **Management.** The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.
- **Notice.** The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, 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.

Establishing a Resilient Privacy and Data Protection Program

We Want to Place Privacy and Data Protection Into a Construct That Ethics and Compliance 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 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
  - CPO or DPO isn't just a spot on the org chart
- **Talk about privacy and data protection at the organization's senior-most meetings**
  - If the organization has a board of directors, leverage that
  - Make sure the senior most leaders understand why privacy and data protection matters
    - Customers expect it
    - Maintaining the organization's reputation is dependent on it

Policies and Procedures

- **Create policies and procedures that make sense to non-experts**
  - Members of the workforce need to be able to easily understand what is expected of them
  - Easily understand doesn't mean "talk down to"

Some Additional Suggestions

Training
- Not a one time event
- Short and frequent is better than long and once a year
- Not necessary to cover every topic in one sitting – consider telling a story a little bit at a time

Communication
- Short and frequent works well here also
- Communicate using a variety of media
- Consider – if possible – leveraging awareness contests or other similar techniques

Auditing, Monitoring, Assessment
- Consider deputizing individuals around the organization to help with assessment
- Consider external assessment periodically as this may eventually become an regulatory requirement

Some Final Thoughts

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
- Regulators have signaled that they expect organizations to have an approach to sharing lessons learned. It is yet to be seen if such an approach will reduce fines or penalties associated with violating regulations like the GDPR.

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.

Thank You

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

Mike Varney
Partner
Crowe LLP
440.506.9112
Mike.Varney@Crowe.com