The relationship between Privacy and RIM

- Overview
- Perspectives
- Partnerships
- Programs
- Future Issues
- Conclusion
- References
- Questions
Overview

Privacy seen from a RIM viewpoint

- Perspectives
- Partnerships
- Programs
The first anniversary of the EU’s General Data Protection Regulation (GDPR) is this month (May, 2019)

- Highlights of the first year
  - *The Future of Data Protection: Adapting to the Privacy Imperative* (RSA Conference, Mar 4-8, 2019, San Francisco)

Source: [https://www.youtube.com/watch?v=E2f50z04dI&feature=youtu.be](https://www.youtube.com/watch?v=E2f50z04dI&feature=youtu.be)
GDPR ONE YEAR ANNIVERSARY
Hundreds of thousands of cases — and the DPOs to handle them

Complaint topics included:
- access requests
- right to erasure
- unfair processing
disclosure
- unsolicited marketing
- employee privacy

200,000+
CASES RECEIVED by DPAs

375,000+
ORGANIZATIONS
are DOCUMENTED
to have registered DPOs

182,000+ Germany
51,000+ France
48,000+ Italy
32,000+ U.K.
36,000+ Spain

94,000+
individual
COMPLAINTS

500,000
ORGANIZATIONS
are ESTIMATED
to have registered DPOs

64,000+
data breach
NOTIFICATIONS

280+
cross border
CASES

GDPR enforcement actions have RESULTED in
€56,000,000+
FINES

AND THE WORK CONTINUES.
European Data Protection Board Guidance
Expected in 2019/2020

- Deletion
- PSE2
- Public body international transfers
- Certification and codes of conduct
- Connected vehicles
- Video surveillance
- Data protection by design/default
- Targeting social media users
- Children's data
- Concepts of controller and processor
- Legitimate interest
- Art. 47 of the Law Enforcement Directive
- Rights of access, erasure, objection, and restriction

iapp.org
Perspectives

- Privacy – treat as a Business Asset
- Good data protection practices provide a competitive advantage
- Be proactive – not reactive
- The role of privacy has evolved from strictly compliance to GRC
Perspectives

Establishing an effective privacy structure

- Build a consensus among members of your organization that a business imperative exists
- Set up a privacy workshop with stakeholders
- Data Protection includes training and awareness
Perspectives

Training and Awareness Tips

- Don’t confuse awareness with training
- Use more than one communication channel
- Do not overlook metrics
- Do not eliminate training due to budget concerns
Perspectives

Privacy legislation, regardless of jurisdiction, assigns many of the same rights to individuals. Common inclusions are:

- Notice
- Choice
- Consent
- Rights to access
Partnerships

Information Security

- Uses the principles of CIA (Confidentiality, Integrity, Availability) to ensure privacy.
- Applies technological controls such as complex passwords, encryption, role based access, etc.
Partnerships

Information Technology

- Privacy by Design
  - Approach attributed to Ann Cavoukian is the gold standard of system design
  - implementing privacy principles into technological development

Ann Cavoukian,
3rd Information and Privacy Commissioner of Ontario, Canada
Partnerships

Information Technology

- GDPR requirement for stored data

Anonymization or Pseudonymization

**Anonymization**

*The process in which individually identifiable data is altered in such a way that it no longer can be related back to a given individual.*

**Pseudonymization**

*The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information....*
Partnerships

• Procurement
  • Insert privacy language into contracts with third party service providers

• Business Continuity / Disaster Recovery
  • Establish a crisis plan to safeguard personal information
    • Before, during, after events
  • Does the current BC/DR plan align with the organization’s privacy policies and procedures

• Marketing
  • Collected customer information must not violate privacy regulations
Programs

The Ongoing Journey

- Building out a Privacy Program is similar to building out a RIM Program
Programs

Governance

- Develop a vision, mission and strategy statement
- Create a Privacy Team and Oversight Committee
  - assign responsibility and accountability
- Develop or adopt a framework (master plan)
  - numerous examples exist online
    - select a model and then modify as needed
    - establish a current baseline (IT designation of ‘As Is’)
    - determine where personal information resides (e.g. Customer Relationship Management [CRM] systems)
- expand, extend policies and procedures as necessary
Programs

Operational Lifecycle

- Continual monitoring, refining, improving
Programs

- A published Maturity Model exists
  - *Generally Accepted Privacy Principles (GAPP)*
    - Created by the American Institute of CPAs and the Canadian Institute of Accountants

- Metrics
  - initially, limit to 3-5 metrics
  - standardize reporting format
Future Issues

Privacy Challenges
- data breaches
- policy debates
- legislative proposals
- technological shifts
Future Issues

Monitor privacy threatening technologies

- Data dissemination by the tech giants
  - selling of private data for profit
  - inappropriate sharing of data

- Technologies to monitor:
  - artificial intelligence
  - 5G
  - quantum computing
  - robotics
  - facial recognition
Conclusion

Mindset necessary for a successful Privacy Program

- maintain flexibility
- strive for continuous improvement
- establish and maintain partnerships
- communicate benefits (e.g. compliance, protect marketplace reputation, safeguard data, etc.)
References

Numerous resources are available including:

- **IAPP resources**

- Website

- Extensive networking opportunities exist (membership now exceeds 50,000)
Questions
PRIVACY – Terms

(from IAPP’s Glossary unless otherwise noted)

CIA Triad

Also known as information security triad; three common information security principles from the 1960s: Confidentiality, Integrity, Availability.

**Confidentiality:**

Data is "confidential" if it is protected against unauthorised or unlawful processing. The General Data Protection Regulation requires that an organization be able to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services as part of its requirements for appropriate security. In addition, the GDPR requires that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

**Integrity:**

The General Data Protection Regulation requires that controllers and processors implement measures to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services. Integrity refers to the consistency, accuracy and trustworthiness of the data (see Accuracy).

**Availability:**

Data is "available" if it is accessible when needed by the organization or data subject. The General Data Protection Regulation requires that a business be able to ensure the availability of personal data and have the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
DATA CONTROLLER

The natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. Where the purposes and means of such processing are determined by EU or member state law, the controller or the specific criteria for its nomination may be provided for by EU or member state law.

DATA PROCESSOR

A natural or legal person (other than an employee of the controller), public authority, agency or other body which processes personal data on behalf of the controller. An organization can be both a controller and a processor at the same time, depending on the function the organization is performing.

GDPR

The General Data Protection Regulation (GDPR) replaced the Data Protection Directive in 2018. The aim of the GDPR is to provide one set of data protection rules for all EU member states and the European Economic Area (EEA). The document comprises 173 recitals and 99 articles.

INFORMATION LIFECYCLE MANAGEMENT

Also known as data life cycle management (DLM) or data governance, ILM is a policy-based approach to managing the flow of information through a life cycle from creation to final disposition. ILM provides a holistic approach to the processes, roles, controls and measures necessary to organize and maintain data, and has 11 elements: Enterprise objectives; minimalism; simplicity of procedure and effective training; adequacy of infrastructure; information security; authenticity and accuracy of one’s own records; retrievability; distribution controls; auditability; consistency of policies; and enforcement.

Minimalism - ...The overall goal is to comply with law and to achieve business objectives, but not to save data that is not required by law or for business purposes.* (Privacy Program Management, Tools for Managing Privacy Within Your Organization, R. Densmore, 2013, p. 107)
INFORMATION PRIVACY

One of the four classes of privacy, along with territorial privacy, bodily privacy, and communications privacy. The claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others.

Territorial Privacy

One of the four classes of privacy, along with information privacy, bodily privacy and communications privacy. It is concerned with placing limitations on the ability of one to intrude into another individual's environment. Environment is not limited to the home; it may be defined as the workplace or public space and environmental considerations can be extended to an international level. Invasion into an individual's territorial privacy typically comes in the form of video surveillance, ID checks and use of similar technology and procedures.

Bodily Privacy

One of the four classes of privacy, along with information privacy, territorial privacy and communications privacy. It focuses on a person's physical being and any invasion thereof. Such an invasion can take the form of genetic testing, drug testing or body cavity searches.

Communications Privacy

One of the four classes of privacy, along with information privacy, bodily privacy and territorial privacy. It encompasses protection of the means of correspondence, including postal mail, telephone conversations, electronic e-mail and other forms of communicative behavior and apparatus.

PRIVACY BY DESIGN

Generally regarded as a synonym for Data Protection by Design (see Data Protection by Design). However, Privacy by Design as a specific term was first outlined in a framework in the mid-1990s by then-Information and Privacy Commissioner of Ontario, Canada, Ann Cavoukian, with seven foundational principles.

This framework dictates that privacy and data protection are embedded throughout the entire life cycle of technologies, from the early design stage to their deployment, use and ultimate disposal. (source: Privacy Program Management, Tools for Managing Privacy Within Your Organization, R. Densmore, 2013, p. 88)