SNIA DPPC | DATA PROTECTION & PRIVACY COMMITTEE

Why data privacy matters

Presentation to the Annual Symposium

Presented by the DPPC

Privacy – A human right

Article 12 – UN Declaration of Human Rights

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

To be free and equal

Source: www.privacyinternational.org

Privacy has become more essential in the age of data exploitation. The way data and technology are now deployed means that our privacy is under increased threat and on a scale that we couldn't possibly have imagined 20 years ago – the ways in which we can be tracked and identified have exploded, alongside the types and scale of information available about us.

Privacy is having the choice – it is the right to decide who we tell what, to establish boundaries, to limit who has access to our bodies, places and things, as well as our communications and our information. It allows us to negotiate who we are and how we want to interact with the world around us, and to define those relationships on our own terms.

Privacy is how we seek to protect ourselves and society against arbitrary and unjustified use of power, by controlling what can be known about us and done to us, while protecting us from those who aim to exert control over our data, and ultimately all aspects of our lives.

Privacy is foundational to who we are as human beings, and every day it helps us define our relationships with the outside world. It gives us space to be ourselves, free of judgement, and allows us to think freely without discrimination. It gives us the freedom of autonomy, and to live in dignity.

In addition to all of the above, privacy is a right that as such also enables our enjoyment of other rights, and interference with our privacy often provides the gateway to the violation of the rest of our rights.

Privacy by design

- What is privacy by design?
  - The term “Privacy by Design” has been generally accepted as meaning “data protection through technology design.” In essence, this means you must proactively integrate or ‘bake in’ data protection into your processing activities and business practices, from the design stage right through the lifecycle.

Source: Regulation (EU) 2016/679 (General Data Protection Regulation)

Source: European Data Protection Board Guidelines 4/2019 on Article 25 Data Protection by Design and by Default

Privacy by design – 7 Foundational Principles

- Proactive not Reactive; Preventative not Remedial
- Privacy as the Default Setting
- Privacy Embedded into Design
- Full Functionality – Positive-Sum, not Zero-Sum
- End-to-End Security – Full Lifecycle Protection
- Visibility and Transparency – Keep it Open
- Respect for User Privacy – Keep it User-Centric

Source: IAPP https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf

Data Protection by design

- What is data protection by design?
  - Data protection by design is ultimately an approach that ensures you consider privacy and data protection issues at the design phase of any system, service, product or process and then throughout the lifecycle.
  - As expressed by the GDPR, it requires you to:
    - Put in place appropriate technical and organisational measures designed to implement the data protection principles effectively; and integrate safeguards into your processing so that you meet the GDPR's requirements and protect individual rights.
    - In essence this means you must integrate or ‘bake in’ data protection into your processing activities and business practices.
    - Data protection by design has broad application. Examples include:
      - developing new IT systems, services, products and processes that involve processing personal data;
      - developing organisational policies, processes, business practices and/or strategies that have privacy implications;
      - physical design;
      - embarking on data sharing initiatives; or
      - using personal data for new purposes.
  - The underlying concepts of data protection by design are not new. Under the name ‘privacy by design’ they have existed for many years.

Source: Regulation (EU) 2016/679 (General Data Protection Regulation)

Source: European Data Protection Board Guidelines 4/2019 on Article 25 Data Protection by Design and by Default

Examples - Penalties for non-compliance

- **Equifax: (At least) $575 Million**
  - 2017 saw Equifax lose the personal and financial information of nearly 150 million people due to an unpatched Apache Struts framework in one of its databases. The company had failed to fix a critical vulnerability months after a patch had been issued and then failed to inform the public of the breach for weeks after it been discovered.
- **Home Depot: ~$200 million**
  - In 2014 Home Depot was involved in one of the largest data breaches to date involving a point-of-sale (POS) system, leading to a number of fines and settlements being paid. Stolen credentials from a third party enabled attackers to enter Home Depot's network, elevate privileges, and eventually compromise the POS system. More than 50 million credit card numbers and 53 million email addresses were stolen over a five-month period between April and September 2014.
- **Uber: $148 million**
  - In 2016 ride-hailing app Uber had 600,000 driver and 57 million user accounts breached. Instead of reporting the incident, the company paid the perpetrator $100,000 to keep the hack under wraps. Those actions, however, cost the company dearly. The company was fined $148 million in 2018 — the biggest data-breach fine in history at the time — for violation of state data breach notification laws.
- **Yahoo: $85 million**
  - In 2013 Yahoo suffered a massive security breach that affected its entire database, about 3 billion accounts — almost the entire population of the web. The company, however, didn't disclose this information for three years.
- **Capital One: $80 million**
  - In 2019 Capital One bank suffered a breach affecting 100 million people in the US and 6 million in Canada. The company said an "outside individual" – later identified as former Amazon Web Services software engineer Paige Thompson – had obtained personal information of Capital One credit card customers and people who had applied for credit card products via a configuration vulnerability in the company's web application firewall.
- **Morgan Stanley: $60 million**
  - While it didn't suffer a breach, failure to conduct robust hardware decommissioning processes cost Morgan Stanley after it failed to adhere to expectations from the regulator. In October 2020 the US Office of the Comptroller of the Currency (OCC) fined the bank $60 million for failing to properly decommission hardware containing wealth management data from two of its US data centers in 2016.

Latest examples – Google and Amazon

- London December 10th 2020
  - France's data protection regulator, the Commission nationale de l'informatique et des libertés, issued Google and Amazon with substantial fines on Thursday for breaking rules on online advertising trackers, known as cookies.
  - The watchdog ordered Google to pay 100 million Euros ($121m) and Amazon 35 million Euros
  - The CNIL said both companies had breached Article 82 of the French Data Protection Act, with Google committing three offences and Amazon committing two.
  - The companies were fined for placing tracking cookies on their user's computers in France "without obtaining prior consent and without providing adequate information."

Case study

- Marriott data breach
  - On November 30, 2018, hospitality giant Marriott International announced that an “unauthorized party” gained access to the personal information of 500 million Starwood customers.
  - Marriott announced that, sometime in early September 2018, they received an alert from an internal security tool indicating that an attempt had been made by an unknown entity to access the Starwood guest reservation database. It was discovered that there had been unauthorized access to the Starwood network as early as 2014. It was then discovered that this party had copied and encrypted customer information and acted towards removing it from the Starwood database.
  - Marriott advised that the data exposed included passwords, email addresses, departure and arrival dates and well as passport information.
  - **Background on Marriott Breach**
  - Marriott should have been able to identify and isolate the intrusion risk in 2014, however it was also around this point that Marriott had announced is acquisition of the Starwood Hotels and Resorts Worldwide, and that’s where the issue may have begun.
  - Two months after the merger, Starwood reported that it had suffered a large-scale credit card hack. Shortly thereafter, the company’s home website was the victim of a SQL injection attack and offers to hack the site were being made across the dark web. It is for this reason that experts are saying Marriott should have known, at that time, that they were taking a considerable risk in acquiring Starwood.
  - **Risk Model Estimates**
  - Estimates that the direct cyber incident losses for the breach will be in the neighborhood of $200 million to $600 million. These estimates are based on both the quantity of consumers affected, as well as the type of information involved.
  - The range loss estimates reflect the relative uncertainty about the data that was stolen, such as duplicate records and additional uncertainty relating to whether or not encryption keys had been stolen along with encrypted credit card data.
  - **Government Regulation**
  - The hospitality industry is under pressure from privacy regulators to comply as the range and nature of personal data held in any guest database poses a particularly high risk if found in the wrong hands.

So what has all this got to do with SNIA?

Responsibility to the storage industry

Challenge

- Increasing volume of privacy legislation that takes no account of the impact on the storage industry.
- International standards being developed that require compliance and are written without expert knowledge or consultation

Response

- SNIA to be the vendor neutral voice of the industry to:
  - Assess the legislation, add context and advise members accordingly
  - Work more effectively with standards bodies to create consistency of understanding
  - Collaborate with other associations

Responsibility to our constituents

Challenge

- Increasing volume of privacy legislation that requires compliance

Response

- External collaboration
- Internal collaboration
- SNIA to be the champion for:
  - Promoting greater awareness and understanding of data protection and privacy issues brought about by increasing legislation.
  - Educating constituents on best practice and establishing common guidance on storage technology/data protection, privacy and security.

Examples (1)

Right to be forgotten

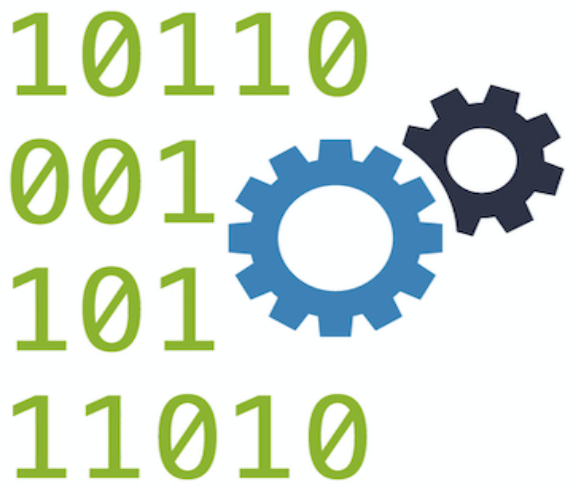
- The right to erasure (Articles 17 & 19 of the GDPR) also known as the **'right to be forgotten'.**
- You have the right to have your data erased, without undue delay, by the data controller, if one of the following grounds applies:
  - Where your personal data are no longer necessary in relation to the purpose for which it was collected or processed.
  - Where you withdraw your consent to the processing and there is no other lawful basis for processing the data.
  - Where you object to the processing and there is no overriding legitimate grounds for continuing the processing.
  - Where you object to the processing and your personal data are being processed for direct marketing purposes.
  - Where your personal data have been unlawfully processed.
  - Where your personal data has to be erased in order to comply with a legal obligation.
- Impact on enterprise storage management disciplines
  - Definition of personal data includes a wide range of information, such as **IP addresses** and **genetic, biometric**, and **location-based data**.
  - Storage has become more distributed than ever as a result of new technologies and the huge amount data that websites and applications gather and create about consumers.
  - However large those data sets have become, storage owners still need to maintain visibility into and control over that data, so they can protect customer privacy and manage storage as cost-effectively as possible. This can be a significant undertaking in a complex enterprise IT environment made up of a diverse mix of cloud and on-premise infrastructures.
  - Adopt a **privacy-by-design** approach at your enterprise.

Examples (2)

Sanitization

IEEE-2883 Standard for Sanitizing Storage

- This standard specifies methods of sanitizing logical storage and physical storage as well as providing technology-specific requirements and guidance for the elimination of recorded data.
- **Need for the Project:** A wide variety of data types are recorded on a range of data storage technologies. When these systems or their media are repurposed or retired from use, the recorded data often must be eliminated (sanitized) to avoid data breaches. Depending on the storage technology, specific methods must be employed to ensure that the data are either eliminated or the logical storage and physical storage associated with the data devices/media are disposed of properly.
- **Stakeholders for the Standard:** The stakeholders for this standard include all consumers of data storage technologies, especially those that store sensitive or high-value data, and the vendors that manufacture, maintain, and support these technologies. Additionally, regulators and other standards development organizations may be able to leverage the contents of this standard.



Examples (3)

Secure data deletion

- On 15th March 2019, the European Union announced a new Regulation referred to as:
- The EU COMMISSION REGULATION 2019/424
- https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0424&from=EN
- It lays down ecodesign requirements for **servers and data storage** products pursuant to Directive 2009/125/EC of the European Parliament and of the Council and amending Commission Regulation (EU) No 617/2013
- The majority of the Directive sets out the ecodesign requirements for energy-related products that present significant potential for improvement in terms of their environmental impact without entailing excessive costs.
- Importantly, the Directive also places special emphasis on non-energy related aspects, including extraction of key components and critical raw materials (CRMs), **availability of functionality for secure data deletion, and provision of latest available version of firmware.**

Why should I join the DPPC?

"Data privacy has become something that is not just for the lawyers anymore. At LinkedIn we call it a culture of privacy because it's not just the lawyers' responsibility, our job is to help interpret the laws, but it's really the responsibility of everybody at the company.

As a data-driven company [LinkedIn], that's an important thing for every employee to understand and get a sense of. So a lot of the work that we do here at LinkedIn is to make sure everyone feels that culture of privacy and that they are aware of the responsibilities we have."

Kalinda Raina, Head of Global Privacy, LinkedIn, during Data Privacy Day, National CyberSecurity Alliance.

44% of CEO respondents rank **data privacy** among top 3 policies most impactful to their business

Source: PwC Election 2020 Poll, November 2019

Value statement

- Welcome to the DPPC, the storage industry forum for data protection and privacy experts
  - The DPPC is the place where data protection and privacy experts from the data storage industry gather to improve standards, spread awareness and understanding, and share knowledge and insights into the future challenges of protecting all forms of data.
- *Benefits of joining include:*
  - *Be at the forefront of legislation announcements – understand what will impact you, your company, and your customers*
  - *Use your expertise to influence and improve standards and education that help others understand how to protect sensitive data and adopt best practice*
  - *Learn from counterparts in other areas of the industry – see a different perspective*
  - *Collaborate with SNIA experts in storage security – influence international data protection and security standards*

Projects for 2021

- Strategic
  - Goal:
    - Monitor and advise on global data privacy legislation changes
  - Deliverables:
    - Issue industry advisories on changes to GDPR and CCPA/CPRA in California.
    - Prepare for possible US federal privacy laws, in addition to bills introduced such as the Consumer Online Privacy Rights Act (COPRA) and the Consumer Data Privacy Act of 2019 (CDPA).
    - Advisory on changes to the EU NIS Directive that came into force in 2016, which will be updated with more stringent supervision measures, new sanctions and fines, streamlined incident reporting and more.
    - Cover legislation directly affecting the storage industry such as secure data deletion, right to be forgotten, and media sanitization

https://iapp.org/resources/article/copra-cdpa-comparison-whitepaper/

Projects for 2021

- Educational
  - Goal:
    - Produce comprehensive reference materials
  - Deliverables:
    - Storage technology concepts reference guide
    - Consolidate terminology definitions to drive consistency
    - Educational content covering the role of the Data Protection Officer, privacy issues related to long term archiving
    - Support all content production with marketing tools such as white papers, blogs, tutorials, webcasts, podcasts, and conferences

Projects for 2021

- Collaborative
  - Goal:
    - Input and influence international standards and formalize alliances with key associations
  - Deliverables:
    - Continue supporting the SNIA Security TWG on updates to ISO international standards and comments on external publications (NIST etc.)
    - Complete the work on formalizing an alliance with the IAPP, and establish representation on key IEEE working groups
  - Goal:
    - Utilize the storage expertise within SNIA to enhance the quality of content
  - Deliverables:
    - Empower all SNIA groups to include aspects of data protection, security and privacy in their content and specifications

Joining the DPPC

- The DPPC is a SNIA Committee – no additional fees associated other than SNIA membership
  - Governing Committee – active participants
  - DPPC Subscribers - observers
- Expectations within the Governing Committee
  - Attend the weekly calls (1 hour)
  - Use some of your time to provide comment, content, expertise
  - Participate in events, webcasts, podcasts
- ROI
  - You will personally benefit from the Committee discussions – viewpoints
  - Opportunities to expand your profile as a subject matter expert
  - Your company will benefit from the extent and quality of the content we produce
    - Early awareness of new standards or legislation is the most obvious one
- To join the DPPC please contact either:
  - Paul Talbut, DPPC Facilitator (paul.talbut@snia.org)
  - DPPC Co-Chairs (dppc-gc@snia.org)

Thank you

Questions/Open discussions

Are we covering all the right areas?
What aspects of data protection and privacy are important to you?
Is there an aspect of this work that you feel is missing?

