Privacy by Design and Privacy by Default

Suk Kim, VP, General Counsel, Urban Airship, Inc.

Amanda Gratchner, Principal, IdeaLegal, LLC

Alex Wall, Privacy Counsel, Marketo, Inc.

The General Data Protection Regulation

- It's a Regulation versus a Directive
- Implementation by May 25, 2018
- Extra-jurisdictional reach
- Privacy by Design/Privacy by Default
- Privacy Impact Assessments
- Fines: 2%-4% of *global* annual turnover

GDPR Article 25

Taking into account the **state of the art**, the **cost of implementation** and the **nature, scope, context and purposes** of processing as well as the **risks of varying likelihood and severity** for rights and freedoms of natural persons posed by the processing, the **controller** shall, both at the time of the determination of the means for processing and at the time of the processing itself, **implement appropriate technical and organisational measures, such as pseudonymisation,** which are designed to implement data-protection **principles**, such as data minimisation, in an effective manner and to **integrate the necessary safeguards** into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

GDPR Article 25

The controller shall implement appropriate technical and organisational measures for ensuring that, **by default**, **only personal data which are necessary for each specific purpose of the processing are processed**. That obligation applies to the **amount of personal data collected**, the **extent of their processing**, the **period of their storage** and their **accessibility**. In particular, such measures shall ensure that **by default personal data are not made accessible without the individual's intervention** to an indefinite number of natural persons.

GDPR Recital 78

The protection of the rights and freedoms of natural persons with regard to the processing of personal data **require** that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to **demonstrate compliance** with this Regulation, the controller should adopt **internal policies and implement measures** which meet in particular the principles of **data protection by design and data protection by default**. Such measures could consist, inter alia, of **minimising the processing of personal data**, **pseudonymising personal data** as soon as possible, **transparency** with regard to the functions and processing of personal data, enabling the data subject to **monitor** the data processing, enabling the controller to **create and improve security features**.

GDPR Recital 78

When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, **producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing** such products, services and applications and, with due regard to the **state of the art**, to make sure that controllers and processors are **able to fulfil their data protection obligations**. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders.

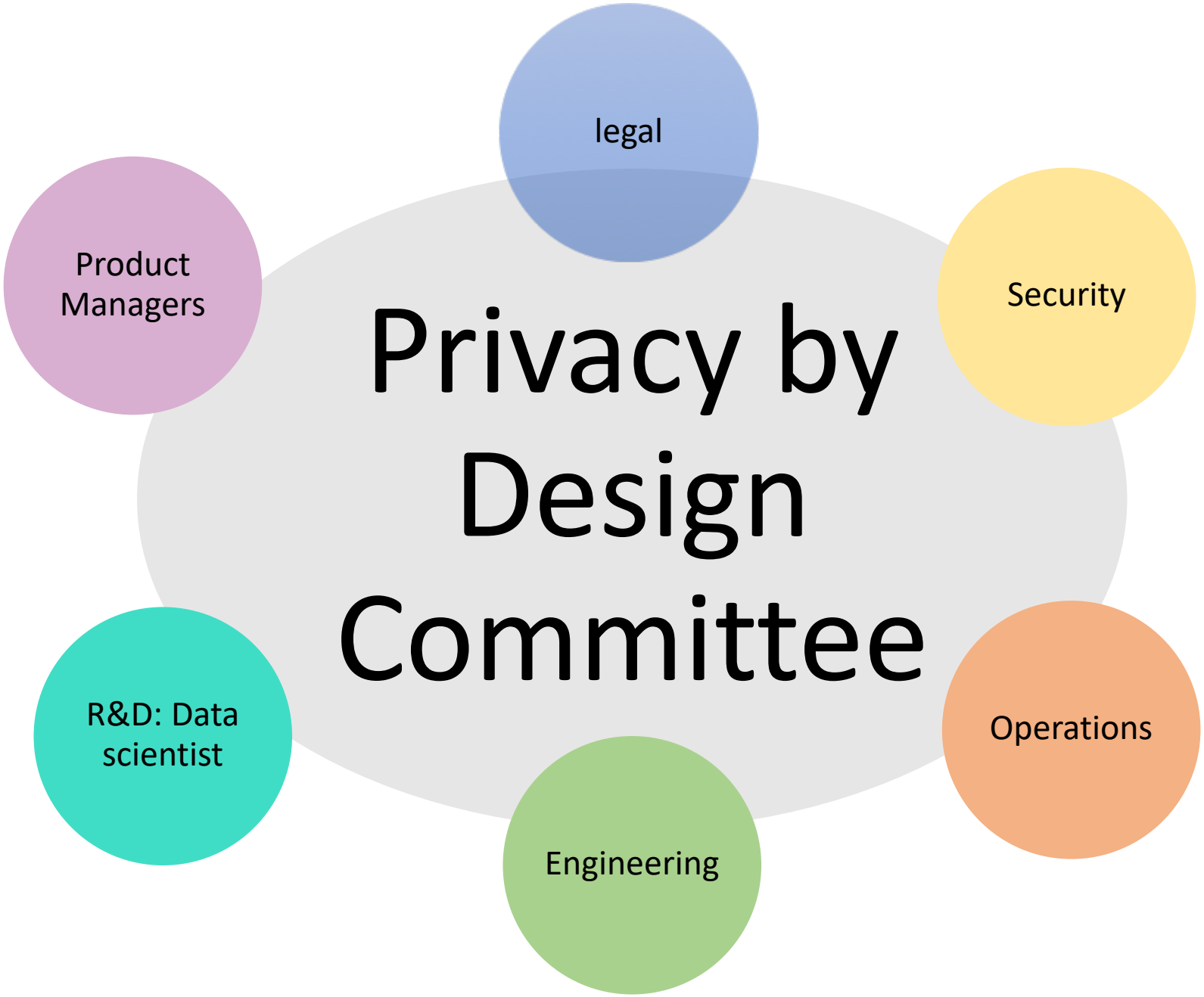
Privacy by Design/Privacy by Default

- Privacy by Default: no collection, display or sharing of personal data without explicit consent
- Privacy by Design: build privacy into the development and design process
- Document compliance
- Security
  - Encryption
  - Logging
- Not just for software development

URBAN AIRSHIP

Privacy by Design and Privacy by Default in practice at Urban Airship: Data Processor Example

* Technology company with global enterprise customers
* Agile design and development
* Collaborative
* Problem Solvers
* Millenial Workforce


legal
Product Managers
Security
Privacy by Design Committee
R&D: Data scientist
Operations
Engineering

Seven Foundational Principles of PbD

1. Proactive not Reactive; Preventative not Remedial
2. Privacy as the Default Setting
    - Purpose Specification
    - Collection Limitation
    - Data Minimization
    - Use, Retention, and Disclosure Limitation
3. Privacy Embedded into Design
4. Full Functionality—Positive-Sum, not Zero-Sum
5. End-to-End Security: Lifecycle Protection
6. Maintain Visibility and Transparency
7. Respect for User Privacy
    - Notice and Consent
    - Accuracy
    - Access

Privacy by Design Committee Sample Agenda

- Default data retention.
  - Different retention periods for different types of data?
  - Should customers be able to override?
- Encryption
  - Encryption during transmission
  - Encryption at storage
  - Encryption at database level
  - Encryption at field/data level
  - Performance impact and system architecture design
- Consent for in-app notifications
  - Opt-in?
  - Opt-out?
  - What does it mean to opt-out?
  - Required or customer to implement?

Resources

EU Commission: https://ec.europa.eu/info/strategy/justice-and-fundamental-rights/data-protection_en

GDPR: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

Information Commissioner's Office (UK): https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/

Privacy by Design Centre of Excellence at Ryerson University. Dr. Ann Cavoukian

https://www.ryerson.ca/pbdce/certification/seven-foundational-principles-of-privacy-by-design/