Going Mainstream: Privacy by Design

Tomas Sander
Data Protection Officer
Senior Research Scientist

November 2018
DATA PROTECTION BY DESIGN

• Requirement in Art. 25 GDPR

• Basic idea
  Include privacy considerations into the creation of technology and processes personal data from the start

• This talk
  A basic DPbD Process for products and processes

November 2018
Other PbD studies and strategies
• ENISA (2015), Hoepman (2012) etc.

Challenges
• No commonly agreed PbD framework
• Criticisms: vague, not actionable
• Hard to understand for organizations what they actually have to do
• Unclear if GDPR requirements are met
# RECENT PRIVACY BY DESIGN INITIATIVES

<table>
<thead>
<tr>
<th>ISO/np 23485</th>
<th>NIST Privacy Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO®</td>
<td>NIST Privacy Framework</td>
</tr>
<tr>
<td><strong>Consumer protection – Privacy by design for consumer goods and services</strong></td>
<td><strong>An Enterprise Risk Management Tool</strong></td>
</tr>
</tbody>
</table>

ISO/NP 23485: Consumer protection – Privacy by design for consumer goods and services

NIST Privacy Framework: An Enterprise Risk Management Tool
DATA PROTECTION BY DESIGN AND DEFAULT (ART. 25, GDPR)

• Technical and organisational measures [...] to implement
  – GDPR data-protection principles
  – protect rights of individuals

• Taking into account
  – state of the art
  – cost
  – nature and scope of processing
  – risks to rights and freedoms of natural persons
PROPOSAL: BASIC DPbD PROCESS

• Determine privacy risks to individuals adjust safeguards accordingly

• Emphasize privacy engineering

• Privacy goals:
  – Implement GDPR data protection principles (Chapter 2)
  – Implement GDPR Data Subject Rights (Chapter 3)
DATA PROTECTION BY DESIGN AND DEFAULT (ART. 25, GDPR)

• What
  – technical and organisational measures [...] by default, only personal data which are necessary for each specific purpose [...] are processed.

• Applies to
  – amount of personal data collected,
  – extent of their processing,
  – period of their storage,
  – their accessibility
GDPR PRINCIPLES – CHAPTER 2, ARTICLE 5-11

Article 5(a) Lawfulness, fairness and transparency

Article 5(b) Purpose limitation

Article 5(c) Data minimisation

Article 5(d) Accuracy

Article 5(e) Storage limitation

Article 5(f) Integrity and confidentiality

Article 7 Consent conditions

Article 9 Special categories of data
ADVANTAGES OF THIS APPROACH TO DPbD

1. Help products meet a number of GDPR requirements

2. Address high risk privacy risks for organization

3. Implementable with limited resources

4. Blueprint for training your privacy engineers
DATA PROTECTION BY DESIGN PROCESS
A BASIC DPbD PROCESS

DPbD Review Template
- Structured DPbD evaluation
- Tracking of findings and mitigations

DPbD Review Team
- Privacy expert
- Security expert
- Technologist/developer with basic privacy understanding
<table>
<thead>
<tr>
<th>Product overview</th>
<th><img src="image" alt="Diagram" /></th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal data categories</td>
<td><img src="image" alt="Diagram" /></td>
</tr>
<tr>
<td>Dataflow diagram</td>
<td><img src="image" alt="Diagram" /></td>
</tr>
<tr>
<td>Purposes</td>
<td><img src="image" alt="Diagram" /></td>
</tr>
</tbody>
</table>
RISK ASSESSMENT

Criteria indicating potentially high risk processing include (WP 29 guidance):

- Automated decision making with significant effects
- Systematic monitoring
- Combining data sets
- Sensitive data
- Large scale processing
- Innovative uses/New technologies
• If High Risk, then full Data Protection Impact Assessment (DPIA) is needed

• In addition necessary to identify concrete risks to the individual
  – Start with a broad list of possible privacy violations
    e.g. Daniel Solove’s “A Taxonomy of Privacy”
  – Review which might apply. Also identify potential threat actors and their objectives

Carefully thinking through privacy risks will raise red flags that a checklist based approach alone could miss
TRANSPARENCY – DPbD REVIEW

PRIVACY NOTICE
CONTENT – DPbD Review

1. UI
   – Limited set of privacy friendly UX Design Patterns

2. Backend
   – Store specifics about when, how, to what a user consented to
CONSENT – AVOID UX DARK PATTERNS

Turn on face recognition if you want us to use this technology

If you turn this setting on, we’ll use face recognition technology to understand when you might appear in photos, videos and the camera to do things such as help protect you from strangers using your photo, find and show you photos that you’re in but haven’t been tagged in, tell people with visual impairments who’s in a photo or video, and suggest people that you may want to tag. Select Accept and Continue to turn on face recognition or Manage Data Settings to keep it turned off.

What’s collected?

MANAGE DATA SETTINGS

ACCEPT AND CONTINUE

See: Deceived by Design, Norwegian Consumer Council
IMPLEMENTATION OF DATA SUBJECT RIGHTS

- **Article 15**
  Right to access

- **Article 16**
  Right to rectification

- **Article 17**
  Right to erasure

- **Article 18 & 21**
  Right to restrict processing

- **Article 20**
  Right to data portability
DATA SUBJECT ACCESS

- Responding with manual processes to a large volumes of data subject’s request is difficult for organizations to manage

- Where higher volume of DSARs is expected automated solutions highly recommended
DATA SUBJECT ACCESS VIA THIRD PARTY APPS

Source: One.Thing.Less

Empowering digital trust.

Source: One.Thing.Less
DATA PORTABILITY

- Review which data should be made available to customers
- Simple solutions that help meet requirement include use of
  - CSV, XML
  - JSON
• Data Minimization
  – Document that collected data are needed for purpose
  – Explore use of pseudonymization techniques, data aggregation, data masking etc.

• Data accuracy

• Resilience
• Request evidence that findings of DPbD have been properly addressed and that corresponding requirements are included in SDL
### HOW TO DEPLOY WITH AGILE DEVELOPMENT OR DEVOPS?

| One approach |  
| --- | --- |
| – Privacy reviews during design phase |  

| Challenge |  
| --- | --- |
| – Agile development, devops |  

| One solution |  
| --- | --- |
| – Train developers to be privacy engineering champions in their teams |  
| – Perform regular reviews |
ACCOUNTABILITY FOR DPbD

• DPbD documentation
  – Completed evaluation form
  – Document tracking of privacy requirements or mitigations

• Response to customer requests about your DPbD practices
  – Share DPbD templates and process, but not details
SUMMARY AND FUTURE WORK

• Proposed a simple DPbD process that helps organizations meet substantive GDPR requirements for products and processes
  – Works in most standard scenarios

• Blueprint for training basic “privacy engineers”

• Future work
  – Refine methodology
  – Add design patterns, use cases, templates and resources
CONTACT

Tomas Sander
tsander@intertrust.com
1. Evaluation or scoring

2. Automated-decision making with legal or similar significant effect

3. Systematic monitoring

4. Sensitive data or data of a highly personal nature

5. Data processed on a large scale

6. Matching or combining datasets
7. Data concerning vulnerable data subjects

8. Innovative use or applying new technological or organisational solutions

9. Processing in itself “prevents data subjects from exercising a right or using a service or a contract matching or combining datasets