Privacy by Design with EA

Casimir Artmann
Enterprise Architect
Sensitive personal information?

- Age
- Sex
- Race
- Income
- E-mail address
- Social security number
- Friends & family
- Length
- Purchase history
- Medical records
- Religious belief
- Political opinion
- Shoe size
- DNA
- GEO tracking
- Facial recognition
- Sexual preferences
Privacy by Design is not a new concept

- 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

Ph.D Ann Cavoukian
Facebook, Cambridge Analytica and others

Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach

Whistleblower describes how firm linked to former Trump adviser Steve Bannon compiled user data to target American voters

- I made Steve Bannon's psychological warfare tool’: meet the data war whistleblower
- Mark Zuckerberg breaks silence on Cambridge Analytica

Carole Cadwalladr and Emma Graham-Harrison
Sat 17 Mar 2018 22.03 GMT
GDPR and privacy regulations
Is consent good enough?
Security breaches are more common
Privacy by design means that the privacy protection rules are taken into account already when IT systems and procedures are designed.

It is a way to ensure that the General Data Protection Regulation’s requirements are complied with and that the data subjects’ rights are protected.
Design business for privacy

Process design requirements

• **Inform** the individual how his/her data is used and for what purpose
• **Give Control** over the personal data for the individual
• **Enforce** documentation how the personal data is protected
• **Demonstrate** how to control and follow up
Inform

Example – Privacy policy

• What information do we have?
• How do we use the information?
• Who do we provide information for?
• Sharing information on social media
• Your privacy rights
• Child protection
Example – Customer self service in Norway

Dine abonnement

Velkommen! Her kan du enkelt administrere ditt eget abonnement og bl.a.:

- Endre leveringsadresse
- Legge inn midlertidig ferieadresse
- Legge inn feriestopp for en gitt periode
- Få gode tilbud på våre andre publikasjoner
- Oppdatere kontaktinformasjon
- Endre passord
- Kjøpe gaveabonnement
- Værk nye abonnenter

For å logge deg inn, begynn med å taste inn *enter

- din e-postadresse
- eller ditt telefonnummer
- eller ditt kundenummer her:

Gå videre >>

Ofte stilte spørsmål

1. Hvor finner jeg kundenummeret mitt?
Enforce

Example – Architecture documentation

- Involved parties
- Business Processes
- Information Models
- Information Classification
- Information Lifecycle

- Used applications
- Used infrastructure
- Location of infrastructure

*Architecture view: Business process and information modelling*
Demonstrate

Example – Checklists for reviews

• Mandatory requirements for management
• Training
• Requirements
• Design
• Coding
• Testing
• Maintenance
Design IT-systems for privacy

Data design requirements

• **Minimize and limit** amount of collected personal data

• **Hide and protect** personal data and their relations

• **Separate** different types of personal data for different purposes

• **Aggregate** personal data and avoid detailed personal data

• **Data protection by default**
Minimize and limit

Example – Call Data Record

A Call Data Record contains data fields describing a particular instance of a telecommunications transaction, but does not include the contents of this transaction.

- the telephone number of the subscriber coming from the call (calling party, A-party)
- the phone number that receives the call (called party, B-party)
- the start time of the call (date and time)
- call duration
Hide and protect

Example – Call Data Record

The availability of call history is limited, as it may contain confidential or secret information

Within EU

• Only handed out by court order
• Only stored for a limited time

*We need security related services as access control, logging, data retention and encryption of data to fulfill business requirements*
Example – Call Data Record

A call data entry does not contain names or social security numbers, but may be associated with a single subscription (Product)
Aggregate

Example – Call Data Record

The data from the call log gathered for billing purposes can also be used for other purposes by the operator and its partners

• Need to aggregate or anonymise personal data for other purposes
Data protection by default

We need to design new systems so that we only handle the data needed for the purpose, and not more.
State sponsored hackers
Zero trust security
Privacy governance
Legal compliance
Damage limitation
Increased brand value
## Credits

<table>
<thead>
<tr>
<th>Writer</th>
<th>Casimir Artmann</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stock footage</td>
<td>Adobe</td>
</tr>
<tr>
<td>Illustrations</td>
<td>TM Forum</td>
</tr>
<tr>
<td>Newspapers</td>
<td>The Guardian</td>
</tr>
<tr>
<td></td>
<td>CNN</td>
</tr>
<tr>
<td></td>
<td>CSO</td>
</tr>
<tr>
<td></td>
<td>Forbes</td>
</tr>
<tr>
<td></td>
<td>Bank Info Security</td>
</tr>
</tbody>
</table>
# Behind the scenes

<table>
<thead>
<tr>
<th>Layer</th>
<th>Business aspect area</th>
<th>Information aspect area</th>
<th>Application aspect area</th>
<th>Infrastructure aspect area</th>
<th>Governance</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Contextual layer</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Ann and her seven principles Facebook, Cambridge Analytica and others Privacy by design and privacy by default State sponsored hackers Damage limitation Value of privacy for individuals Value of privacy for brand</td>
<td></td>
</tr>
<tr>
<td><strong>Conceptual layer</strong></td>
<td>GDPR and privacy regulations Is consent good enough Design business for privacy</td>
<td>GDPR and privacy regulations Sensitive personal information</td>
<td>GDPR and privacy regulations Design IT-systems for privacy</td>
<td>GDPR and privacy regulations</td>
<td>GDPR and privacy regulations Privacy governance</td>
<td>GDPR and privacy regulations Zero trust security</td>
</tr>
<tr>
<td><strong>Logical layer</strong></td>
<td>Design business for privacy</td>
<td>Design IT-systems for privacy</td>
<td></td>
<td>Privacy governance</td>
<td>Zero trust security</td>
<td></td>
</tr>
<tr>
<td><strong>Physical layer</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>