Processing Cyber Threat Data Through the GDPR Regulatory Lens:

for Operational Compliance with GDPR and ... Improved Privacy Risk Management

John Sabo, CISSP
Chair OASIS IDTrust Member Section
Chair, OASIS PMRM Technical Committee
john.sabo711@yahoo.com

Special Thanks to Mike Small
GDPR/Privacy Engineering Tutorial

• Eight-part online workshop tutorial recorded at the KuppingerCole European Identity and Cloud Conference 2017 in Munich

• Online on the OASIS YouTube Channel:
  • OASIS Open Standards
  • https://www.youtube.com/user/OASISopen/playlists
Privacy Principles – GDPR Article 5

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Security – confidentiality, integrity, availability and resilience

Consent - GDPR Article 7

- Controller shall be able to demonstrate that the data subject has consented to processing of personal data.
- The request for consent shall be presented in a manner which is clearly distinguishable from … other matters … intelligible … easily accessible … clearly and plain language.
- Data subject shall have the right to withdraw … consent at any time. … It shall be as easy to withdraw as to give consent.
GDPR - Personal Data

- Any information relating to an identified or identifiable natural person. Specific references to:
  - identification number; location data; online identifier
- One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

GDPR – New Regulatory Concepts ...

- Large administrative penalties - up to 4% of annual turnover
- Global Scope (directly impacts non-EU organizations)
- Both Controller and Processor Responsibilities (cloud implications)
- Processors must have documented processing instructions
- Rights of Rectification, Erasure, and Restricted Processing
- Pseudonymisation (separately maintained additional information)
- Data Protection by Design and Default (design + implementation)
- Granular Consent and Withdrawal of Consent
## GDPR as Catalyst

<table>
<thead>
<tr>
<th>Pre-GDPR?</th>
<th>Post-GDPR?</th>
</tr>
</thead>
<tbody>
<tr>
<td>① Primary focus on policy – regulators lawyers</td>
<td>① Multi-stakeholder focus</td>
</tr>
<tr>
<td>② Security-centric</td>
<td>② Holistic “data protection” approach</td>
</tr>
<tr>
<td>③ Limited understanding of technical implementations and inter-dependencies</td>
<td>③ Deep understanding of technical implementation and inter-dependencies</td>
</tr>
<tr>
<td>④ Traditional privacy risk management – “PIAs”</td>
<td>④ Proactive risk management – data protection by design and default</td>
</tr>
</tbody>
</table>
How Can the OASIS PMRM Help You Meet the Letter and Spirit of the GDPR in Cyber Security Systems?

- **PMRM V1.0 CS02** – Privacy Management Reference Model and Methodology
- **An analytic tool:**
  - Enables the **structured analysis of “use cases”** in which Personal Data (or PII) are used, generated, communicated, processed, stored and erased
  - Shows the **linkages** among PII, data flows, data protection [including security] policies, privacy controls, privacy-enabling Services/Functionality/Technical Mechanisms] and Risk Management
  - **Supports any set of privacy standards and policies**
  - **Supports Data Protection by Design requirements and compliance** across policy and system boundaries
  - **Supports all stakeholders**

http://docs.oasis-open.org/pmrm/PMRM/v1.0/cs02/PMRM-v1.0-cs02.html
Privacy Management Analysis is complicated
- Multiple Stakeholders
- and Roles
- Policies, Procedures
- Technical Implementation
- Risk Management
- SDLC Management
- Iterative risk analysis
Privacy Management Analysis

PMRM Methodology

High Level Privacy Use Case Analysis

<table>
<thead>
<tr>
<th>Services/Applications</th>
<th>Privacy Requirements</th>
<th>Impact/Other Assessments</th>
</tr>
</thead>
</table>

Detailed Privacy Use Case Analysis

<table>
<thead>
<tr>
<th>Domains and Owners</th>
<th>Risks - Responsibilities</th>
<th>Data Flows and Touch Points</th>
<th>Systems and Subsystems</th>
<th>Actors</th>
</tr>
</thead>
</table>

PI in Use Case Systems

System 1
- Incoming/Internally Generated/Outgoing

System ...n
Incoming/Internally Generated/Outgoing
Risk Assessment

Technical and Process Functionality and Mechanisms

Services Required for Operationalized Controls

Operational Privacy Control Requirements

Privacy Management Analysis

Operational Privacy Control Requirements

Inherited  | Internal  | Exported

Services Required for Operationalized Controls

Agreement  | Usage  | Validation  | Certification  | Enforcement  | Security  | Interaction  | Access

Technical and Process Functionality and Mechanisms

Risk Assessment

Iterative Process
Key Actions for GDPR Compliance
Mike Small, Senior Analyst
GDPR – Key Actions

**Discovery**

Discover and document all the PII you hold.
- Check that it is necessary and minimum.
- Check it is correct and up to date.
- Models for consent and control

**Control**

Access Control at data field level
- Control of aggregation
- Data Subject access requests
- “Right to be forgotten” and return of data
- Proof that data only used for consented purposes

**Consent**

Processes for freely given, informed, unambiguous, clear statements of affirmative actions
- Per purpose and may be revoked at any point of time
GDPR – Key Actions

Cloud

Assure Compliance when data held in cloud services.
• Control over PII in cloud
• Certification of Cloud Service Providers

Data Protection

Data Protection Officers are required
• DPIAs (Data Protection Impact Assessment) under certain circumstances
• Privacy by default and design

Data Breach

Make sure you have the right procedures to detect, report and investigate a breach.
• Communicate to data subjects in clear and plain language.
# PMRM Services

<table>
<thead>
<tr>
<th>Core Policy Services</th>
<th>Privacy Assurance Services</th>
<th>Presentation &amp; Lifecycle Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agreement</td>
<td>Validation</td>
<td>Interaction</td>
</tr>
<tr>
<td>Usage</td>
<td>Security</td>
<td>Enforcement</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Access</td>
</tr>
</tbody>
</table>
Additional Resources

OASIS PMRM Technical Committee
https://www.oasis-open.org/committees/tc_home.php?
wg_abbrev=pmrm

Privacy Engineering – GDPR OASIS Workshop Presentation Slides and PMRM Technical Committee Documents
https://www.oasis-open.org/committees/documents.php?
wg_abbrev=pmrm&show_descriptions=yes

OASIS Privacy Management Reference Model and Methodology (PMRM)
https://docs.oasis-open.org/pmm/ref/toolkit/PMRM/v1.0/cs02/PMRM-
v1.0-cs02.pdf

OASIS Privacy by Design Documentation for Software Engineers (PbD—SE)
http://docs.oasis-open.org/pbd-se/pbd-se/v1.0/csd01/pbd-
se-v1.0-csd01.pdf
Overview of Use Case

- Use Case: ImproveTheNeighbourhood
PMRM PMA Analysis

PMRM tasks 1 to 18

- Task #1 - Use Case Description
- Task #2 - Use Case Inventory
- Task #3 - Privacy Policy Conformance Criteria
- Task #4 - Assessment Preparation
- Task #5 - Identify Participants
- Task #6 - Identify Systems and Business Processes
- Task #7 - Identify Domains and Owners
- Task #8 - Identify Roles and Responsibilities within a Domain
- Task #9 - Identify Touch Points
- Task #10 - Identify Data Flows
- Task #11 - Identify Incoming PI
- Task #12 - Identify Internally Generated PI
- Task #13 - Identify Outgoing PI
- Task #14 - Specify Inherited Privacy Controls
- Task #15 - Specify Internal Privacy Controls
- Task #16 - Specify Exported Privacy Controls
- Task #17 - Identify the Services and Functions necessary to support operation of identified Privacy Controls
- Task #18 - Identify the Mechanisms that Implement the Identified Services and Functions
## PMRM PMA Analysis

### “Responsibilities” Table

<table>
<thead>
<tr>
<th>Stake-holders/Lead</th>
<th>Use Case Description</th>
<th>Systems</th>
<th>Participants</th>
<th>PI/PII</th>
<th>Domains</th>
<th>Legal/Regs/ Policies</th>
<th>Data Flows/Touch points</th>
<th>Systems</th>
<th>Privacy Controls</th>
<th>Services - Technical Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPO</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT Architect</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business Analyst</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Team Privacy Champion</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Senior Developer</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Line of Business Owner</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Legal Department</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Center Director</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
PMRM PMA Analysis

Iterative steps with stakeholders

Product Owner  Architect  Developer  Business Analyst
<table>
<thead>
<tr>
<th>Task #5 - Identify Participants</th>
<th>Task #6 - Identify Systems</th>
<th>Task #7 - Identify Domains</th>
<th>Task #9 - Identify Touch Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citizen</td>
<td>VBDB Web App</td>
<td>Citizen</td>
<td>VBDB Mobile App - VBDB System</td>
</tr>
<tr>
<td>Fieldworker</td>
<td>VBDB Fieldworker App</td>
<td>VBDB Platform</td>
<td>VBDB Fieldworker App - VBDB System</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Task #10 - Identify Data Flows</th>
<th>Task #11 - Identify Incoming PI</th>
<th>Task #12 - Internally Gen. PI</th>
<th>Task #13 - Identify Outgoing PI</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Picture</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Email address</td>
</tr>
</tbody>
</table>

PMA Interview with Product Owner
<table>
<thead>
<tr>
<th>Task #5 - Identify Participants</th>
<th>Task #6 - Identify Systems</th>
<th>Task #7 - Identify Domains</th>
<th>Task #9 - Identify Touch Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citizen</td>
<td>VBDB Web App</td>
<td>Citizen</td>
<td>VBDB Mobile App - VBDB System</td>
</tr>
<tr>
<td>Fieldworker</td>
<td>VBDB Fieldworker App</td>
<td>VBDB Platform</td>
<td>VBDB Fieldworker App - VBDB System</td>
</tr>
<tr>
<td>Backoffice Employee</td>
<td>VBDB Web App</td>
<td>Councils:</td>
<td>VBDB Web App - VBDB System</td>
</tr>
<tr>
<td>Customer Support Employee</td>
<td>VBDB Mail</td>
<td>Council Type 1</td>
<td>VBDB System - Case Management System</td>
</tr>
<tr>
<td></td>
<td>VBDB System</td>
<td>Council Type 2</td>
<td>VBDB System - CRMOnline</td>
</tr>
<tr>
<td></td>
<td>CRMOnline</td>
<td>Council Type 3</td>
<td>VBDB System - Mail system</td>
</tr>
<tr>
<td></td>
<td>Case Management System</td>
<td>Council Type 4</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Task #10 - Identify Data Flows</th>
<th>Task #11 - Identify Incoming PI</th>
<th>Task #12 - Internally Gen. PI</th>
<th>Task #13 - Identify Outgoing PI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citizen - VBDB Platform</td>
<td></td>
<td>Personalized interests</td>
<td>Picture</td>
</tr>
<tr>
<td>Council Type 2 - VBDB Platform</td>
<td></td>
<td></td>
<td>Email address</td>
</tr>
<tr>
<td>Task #5 - Identify Participants</td>
<td>Task #6 - Identify Systems</td>
<td>Task #7 - Identify Domains</td>
<td>Task #9 - Identify Touch Points</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------------</td>
<td>---------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>Citizen</td>
<td>VBDB Web App</td>
<td>Citizen</td>
<td>VBDB Mobile App - VBDB System</td>
</tr>
<tr>
<td>Fieldworker</td>
<td>VBDB Fieldworker App</td>
<td>VBDB Platform</td>
<td>VBDB Fieldworker App - VBDB System</td>
</tr>
<tr>
<td>Backoffice Employee</td>
<td>VBDB Web App</td>
<td>Councils:</td>
<td>VBDB Web App - VBDB System</td>
</tr>
<tr>
<td>Customer Support Employee</td>
<td>VBDB Mail</td>
<td>- Council Type 1</td>
<td>VBDB System - Case Management System</td>
</tr>
<tr>
<td></td>
<td>VBDB System</td>
<td>- Council Type 2</td>
<td>VBDB System - CRMOnline</td>
</tr>
<tr>
<td></td>
<td>Case Management System</td>
<td>- Council Type 3</td>
<td>VBDB System - Mail system</td>
</tr>
<tr>
<td></td>
<td>MailChimp</td>
<td>- Council Type 4</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ActiveMQ</td>
<td>Rocket Science Group</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mule</td>
<td>ESRI</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Postfix</td>
<td>Wildbit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Postmark</td>
<td>LeaseWeb</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ArgisOnline</td>
<td>OVH</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ArgisPro</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Task #10 - Identify Data Flows</th>
<th>Task #11 - Identify Incoming PI</th>
<th>Task #12 - Internally Gen. PI</th>
<th>Task #13 - Identify Outgoing PI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citizen - VBDB Platform</td>
<td>Personalized interests</td>
<td>Picture</td>
<td>Picture</td>
</tr>
<tr>
<td>Council Type 2 - VBDB Platform</td>
<td></td>
<td>Email address</td>
<td>Email address</td>
</tr>
</tbody>
</table>

PMA Interview with Developer
Architecture of PMRM PMA tool
Architecture of PMRM PMA tool
Small example: outgoing PI

- Thinking about the CTI infrastructure & GDPR
  - Using the visual representations
  - Outgoing PI example in shared thread information
Basic TAXII setup
Value of tool