Privacy Considerations for Project Managers & Incorporating Privacy into Agile Methodology

IT Project Management Community of Practice
Katy Ruckle, State Chief Privacy Officer
May 23, 2022
Background – path to privacy

- Admitted to WSBA 2005
- Started with state in 2006
- Contracts/procurement
- Healthcare & DSHS
Overview of Today’s Presentation

I. What is privacy?
II. How do we implement privacy?
III. When does privacy need to be at the table?
IV. What will privacy do?
What is privacy?
What is Privacy?

- Communications Privacy
- Territorial Privacy
- Bodily Privacy
- Information Privacy
What is Privacy?

- Communications Privacy
- Territorial Privacy
- Bodily Privacy
- Information Privacy
Effective Privacy and Data Protection

- Maturity Models
- Privacy Frameworks
- Privacy Principles
- Laws & Regulations
Office of Privacy and Data Protection (OPDP)

- Executive Order 16-01
- RCW 43.105.369
- Statutory creation of the Office of Privacy and Data Protection
- Position of State Chief Privacy Officer created in RCW
OPDP Duties in Law

- Serve as a central point-of-contact for state agencies on policy matters involving data privacy and data protection
- Serve as a resource to local governments and the public on data privacy and protection concerns
- Conduct an annual state privacy review
- Conduct an annual privacy training for state agencies and employees
- Articulate privacy principles and best practices
- Coordinate data protection in cooperation with state agencies
- Review of major state agency projects involving PII
- Promote best practices for the collection and storage of PII
- Educate consumers about the use of PII on mobile and digital networks
- Legislative Reports on Metrics
OPDP Duties in Law

- Serve as a central point-of-contact for state agencies on policy matters involving data privacy and data protection
- Serve as a resource to local governments and the public on data privacy and protection concerns
- Conduct an annual state privacy review
- Conduct an annual privacy training for state agencies and employees
- Articulate privacy principles and best practices
- Coordinate data protection in cooperation with state agencies
  - Review of major state agency projects involving PII
  - Promote best practices for the collection and storage of PII
- Educate consumers about the use of PII on mobile and digital networks
- Legislative Reports on Metrics
Washington State Agency Privacy Principles

- Lawful, fair, & responsible use
- Data minimization
- Purpose Limitation
- Transparency & accountability
- Due diligence
- Individual participation
- Security
Washington State Agency Privacy Principles

- Lawful, fair, & responsible use
- Data minimization
- Purpose Limitation
- Transparency & accountability
- Due diligence
- Individual participation
- Security
Laws and Regulations

Gaps may exist where laws:

• Do not establish strong enough protections to meet people’s expectations
• Do not keep pace with changes in technology and business practices
• Do not account for an organization’s specific mission or cultural context
How do we implement privacy?
Threshold Question

Does the project “process” personal data?
Does the project “process” personal data?

Process means:

- any operation or set of operations which are performed on personal data or on sets of personal data, whether or not by automated means, such as the:
  - collection
  - use
  - storage
  - disclosure
  - analysis
  - deletion
  - modification of personal data
Incorporating Privacy
Incorporating Privacy
To deal with these challenges – you need to classify* the data

<table>
<thead>
<tr>
<th>Data Classification:</th>
<th>Example Category:</th>
<th>Example Data Set:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Category 4 - Confidential Information requiring special handling</td>
<td>• Healthcare data protected by HIPAA</td>
<td>• Medical diagnosis</td>
</tr>
<tr>
<td>• Category 3 - Confidential</td>
<td>• Government identifier</td>
<td>• Driver’s License</td>
</tr>
<tr>
<td>• Category 2 – Sensitive</td>
<td>• Operational information</td>
<td>• Internal emails</td>
</tr>
<tr>
<td>• Category 1 – Public</td>
<td>• Public information</td>
<td>• Agency websites</td>
</tr>
</tbody>
</table>

* OCIO 141.10 4.1
Privacy-by-Design Principles
Privacy-by-Design Principles
Privacy-by-Design Principles

- Full functionality: positive sum
- Transparency
- End-to-end security
- Privacy as the default setting
- Proactive, not reactive
- Privacy embedded into design
- User-centric
Privacy by Design Principles

- Full functionality: positive sum
- End-to-end security
- Privacy as the default setting
- Proactive, not reactive
- Privacy embedded into design
- User-centric
- Transparency
Privacy-by-Design Principles
When does privacy need to be at the table?
Potential triggers for Privacy involvement

- At project conception if PII is going to be used.
  - Privacy can help determine whether the information should be collected.
  - Being involved early also helps establish the level of our involvement throughout the project.
- When confidential data is involved … internally and with third parties.
- Where data sharing agreements or contracts are being executed.
- Sometimes at more than one point in the project – agile method is iterative.
- Systems and processes established with security design review.
Privacy stakeholders for Agile Methodology

- Privacy
- Engineering & Development
- Other Stakeholders
- Security

Data Classification and handling
Agile process challenge

➢ Challenge: Determining privacy risk for a system that will exist later

➢ Fix: Quick assessment (mini privacy review)
Agile Methodology – Quickly Assess Each Sprint

### A Quick Assessment Overview Result

<table>
<thead>
<tr>
<th>List of Personal Data Item Processes</th>
<th>List of Processing Purposes</th>
<th>Indicate Use of Data per Purpose and Include Retention Periods</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Describe Retention Period Trigger**

Source: Gartner
Quick assessment - ties directly to Privacy Principles

Determine:
✓ What personal data are you collecting?
✓ Where are you going to get it from?
✓ Where will it be stored?
✓ Who will have access?
✓ Purpose for collection? Why do you actually need it?
✓ How long does it need to be retained?
What is the anticipated outcome and benefits from this process?

➢ Outcomes:
  • Flag privacy review and detect privacy issues
  • Technical privacy requirements for specific part of the project
  • Prioritization of mitigation efforts
  • Consult with privacy and legal based on assessment

➢ Benefits:
  • Further analysis of project based on discovered knowledge
  • Embed privacy into project for further iterations
  • Improved data classification and data handling standards
What will privacy do?
Privacy Impact Assessment Tool and Privacy Threshold Analysis Process

**The PIA Process**

- **Privacy Threshold Analysis (PTA)**: A PTA is a brief, high-level assessment used to determine whether the subject of the review may have privacy implications and require a PIA.

- **Continuous Review Cycle**: A PIA is a tool used to describe how projects interact with information assets. A PIA should document the risks identified by through the process and the privacy solutions or mitigations strategies adopted as a result.

- **Review and Update, as Appropriate**
Coordinate data protection with WaTech’s Office of Cybersecurity

- Collaboration on data security initiatives that overlap with data governance
- Security is one of the WA state agency privacy principles
- Initiative to perform privacy impact assessments as a part of the security design review process
- OCS Operational Plan coordination
Privacy in Action

M365 Implementation

- Webinar on Privacy Considerations for M365
- Attend M365 Meetings with eDiscovery and records community
- Data management issues
- MyAnalytics questions
- Privacy concerns
- Waivers

OneWa Project

https://one.wa.gov/

- SME support and guidance to the OneWa Project
- Privacy Subcommittee under the OneWa Data Governance Advisory Committee
- Design and review the Privacy Impact Assessment
Key takeaways to incorporate privacy

First ask: Does the project or sprint process personal data?

If so:

Determine:

✓ What personal data are you collecting?
✓ Where are you going to get it from?
✓ Where will it be stored?
✓ Who will have access?
✓ Purpose for collection? Why do you actually need it?
✓ How long does it need to be retained?
Privacy is a Right
Privacy Training and Communications

Privacy Points – Monthly blog on events, initiatives, legislative updates, and other current privacy topics

Privacy.wa.gov

Subscription Topics

- [ ] WaTech Products and Solutions
- [ ] Communications
- [ ] Hosting
- [ ] Internet & Web
- [ ] Networks
- [ ] Security
- [ ] WaTech Support Center
- [ ] Office of Privacy & Data Protection
- [ ] Privacy Community
- [ ] Office of the Chief Information Officer (OCIO)
- [ ] WaTech Customers
Thank you!

privacy@watech.wa.gov