WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

Incorporating Privacy into the System Development Process

June 15, 2022

Overview of Today's Presentation

I. What is privacy?

II. When do we consider privacy impacts?

III. What privacy concepts do we apply?

IV. Incorporating privacy into project management.

V. Other considerations.

What is privacy?

What is Privacy?

Communications Privacy

Territorial Privacy

Bodily Privacy

Information Privacy

OPDP

What is Privacy?

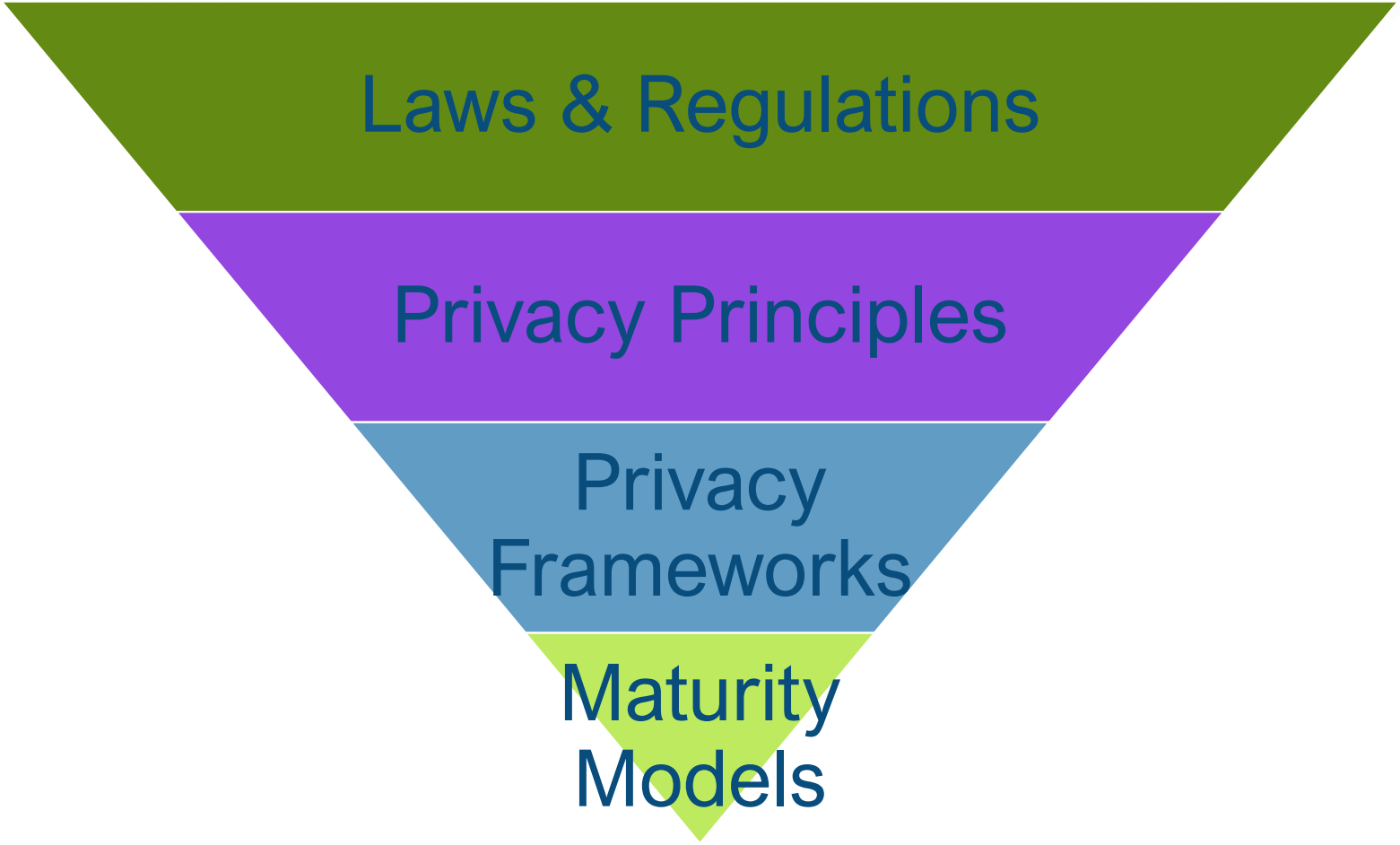
Communications Privacy

Territorial Privacy

Bodily Privacy

Information Privacy

OPDP

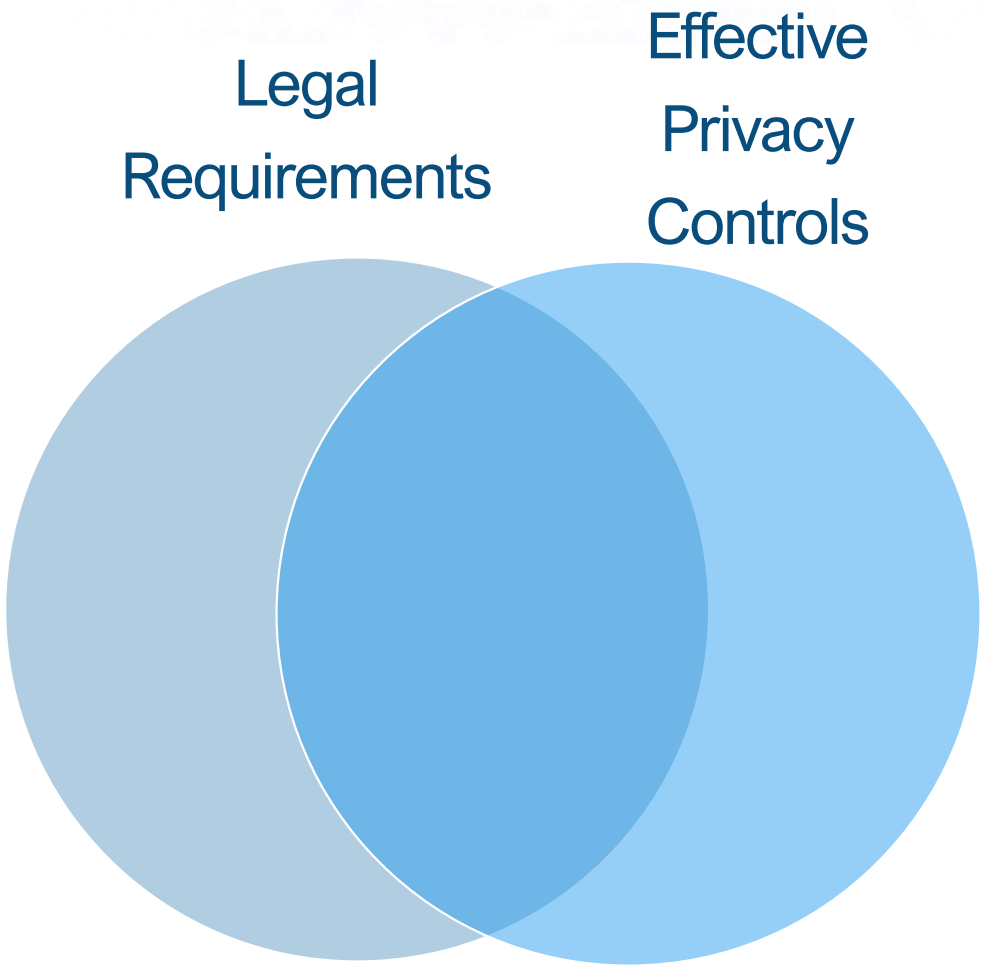


Effective Privacy and Data Protection

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



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

O P D P

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

O P D P

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

When do we consider privacy impacts?

Threshold Question

Does the system "process" personal data?

OPDP

Does the system “process” personal data?

WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

“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, including:

- ✓ Collection
- ✓ Use
- ✓ Access
- ✓ Storage
- ✓ Disclosure
- ✓ Analysis
- ✓ Deletion
- ✓ Modification

OPDP

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.

Identify personal information during classification*

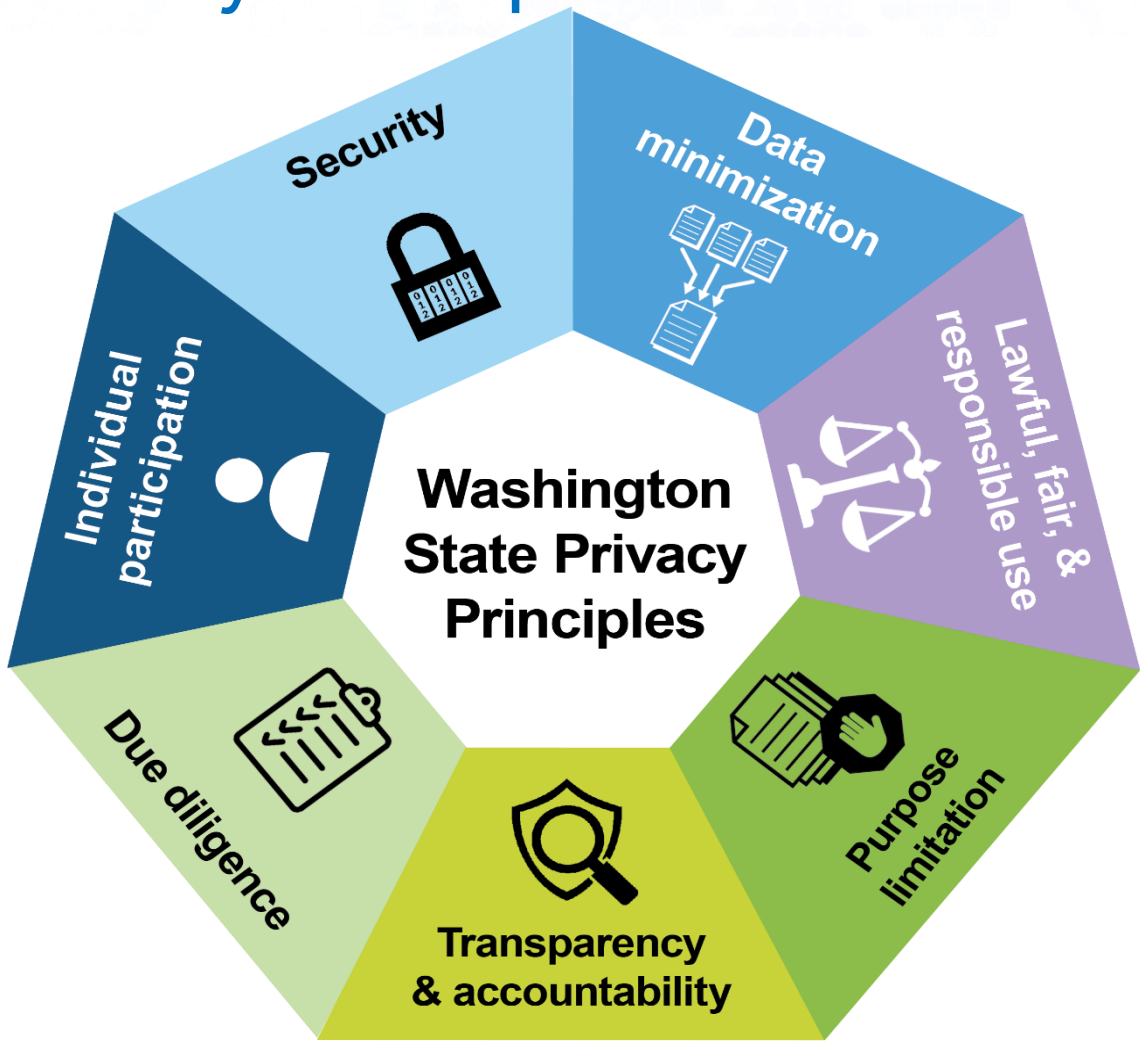
Data Classification:	Example Category:	Example Data Set:
• Category 1- Public	• Public information	• Agency websites
• Category 2 - Sensitive	• Operational information	• Internal emails
• Category 3 - Confidential	• Government identifier	• Driver's license numbers
• Category 4 - Confidential Information requiring special handling	• Healthcare data protected by HIPAA	• Medical records

* OCIO 141.10 4.1

What privacy concepts do we apply?

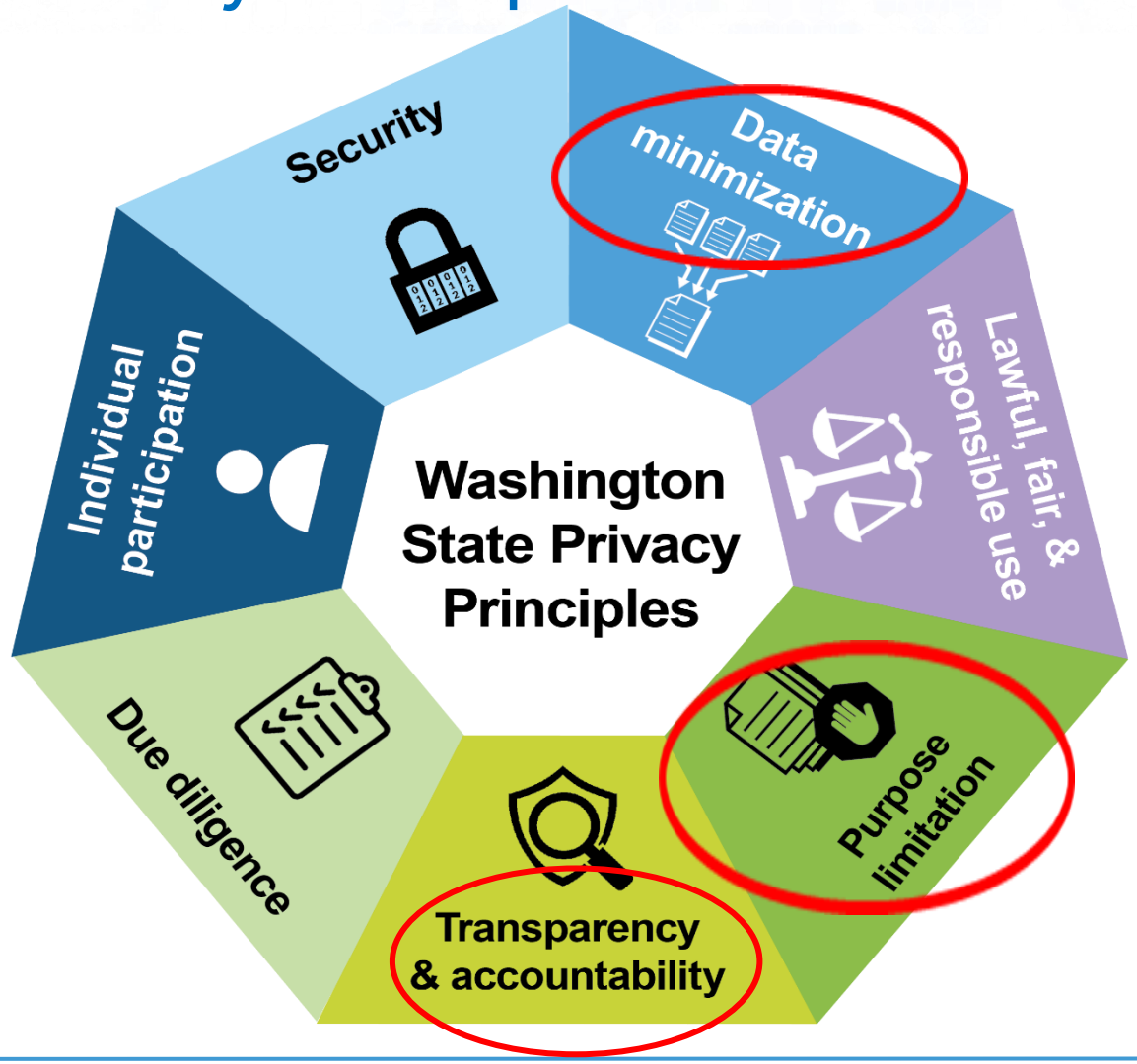
Washington State Agency Privacy Principles

- 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



Privacy-by-Design Principles

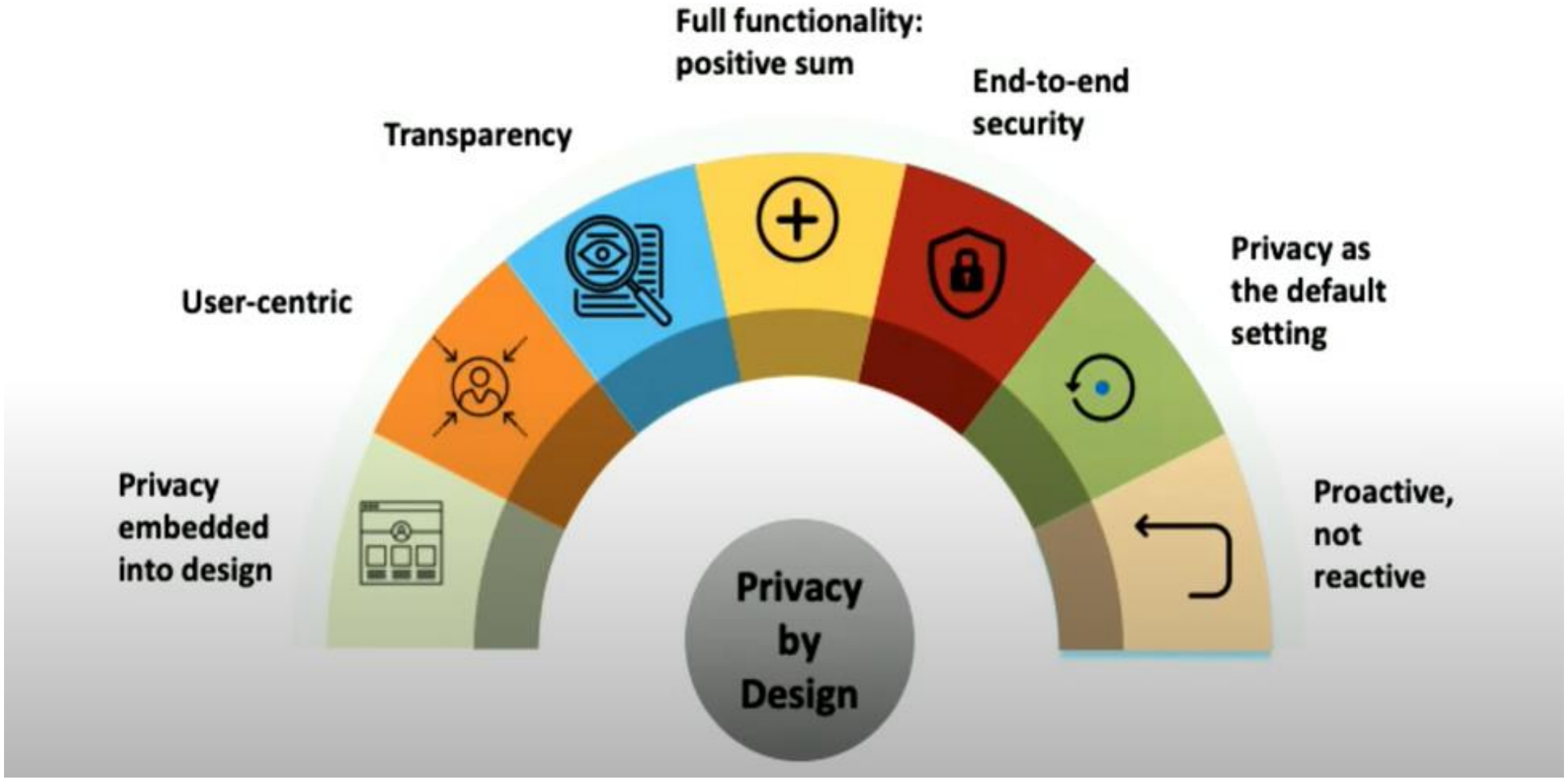
Attributes:

- Operational principles to build privacy into systems and software
- Goes beyond Fair Information Practice Principles and legal requirements
- Consider privacy throughout development lifecycle

Goals:

- Privacy issues mitigated before they arise
- Privacy becomes integral to functionality instead of competition to functionality
- “It takes the pressure off individuals . . . from remembering to ask for privacy.”

Privacy-by-Design Principles



Privacy-by-Design Principles

Proactive not Reactive; Preventative not Remedial

- ✓ Take a proactive approach to data protection and anticipate privacy issues and risks before they happen, instead of waiting until after the fact.

Privacy as the Default Setting

- ✓ Design any system, service, product, and/or business practice to protect personal data automatically. With privacy built into the system, the individual does not have to take any steps to protect their data — their privacy remains intact without them having to do anything. Example – Opt-in vs. Opt-out.

Privacy-by-Design Principles

Privacy Embedded into Design

✓ Data protection forms part of the core functions of any system or service — essentially, it becomes integral to these systems and services.

Full Functionality - Positive-Sum, not Zero-Sum

✓ 'Win-win.' This principle is essentially about avoiding trade-offs, such as the belief that in any system or service it is only possible to have privacy or security, not privacy and security.

Privacy-by-Design Principles

End-to-End Security - Full Lifecycle Protection

✓ Process the data securely and then destroy it securely when you no longer need it. Or aggregate/de-identity/anonymize.

Visibility and Transparency

✓ Keep it open - Ensure that whatever business practice or technology you use operates according to its premises and objectives and is independently verifiable.

✓ Ensure visibility and transparency to individuals, such as making sure they know what data you process and for what purpose(s) you process it.

Privacy-by-Design Principles

Respect for User Privacy - Keep it User-Centric

✓ Make individuals paramount in the design and implementation of any system or service

✓Ensure strong privacy defaults, providing individuals with controls, and ensuring appropriate notice is given.

Challenge – involvement at the right time

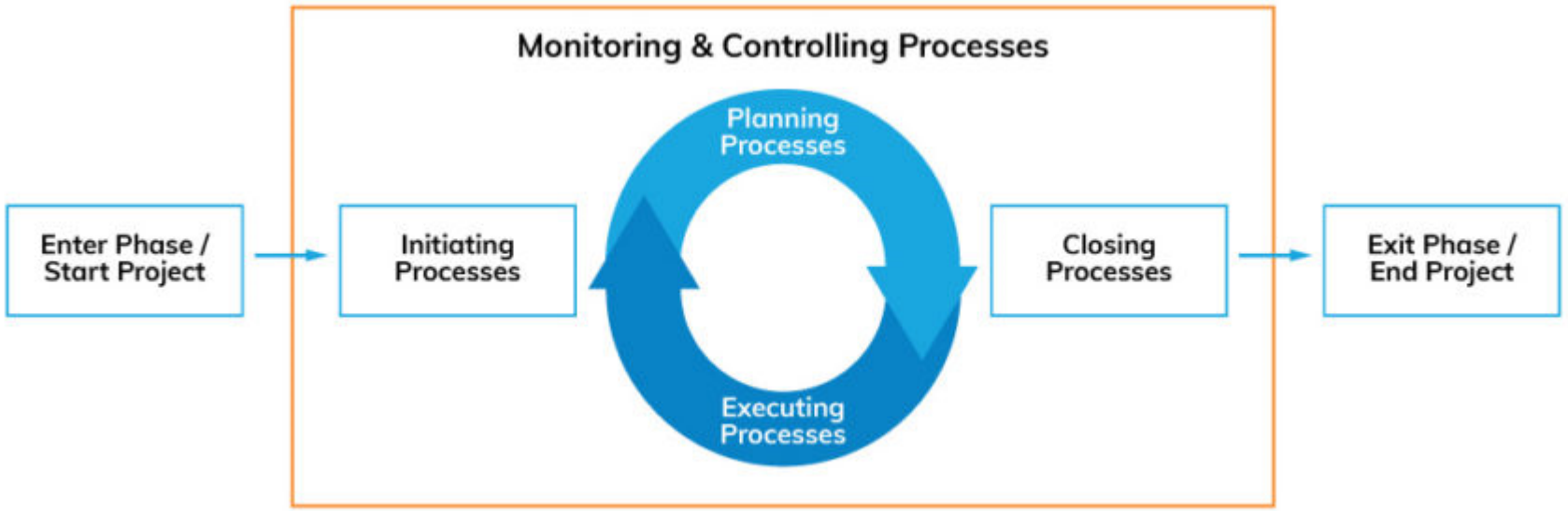
Privacy is interdisciplinary - identify roles within your agency that are central to data management

- Legal
- Risk
- Contracts
- Records (retention, management, public)
- IT
- Security
- Project management
- Other

Privacy-by-Design Principles

Incorporating privacy into project management

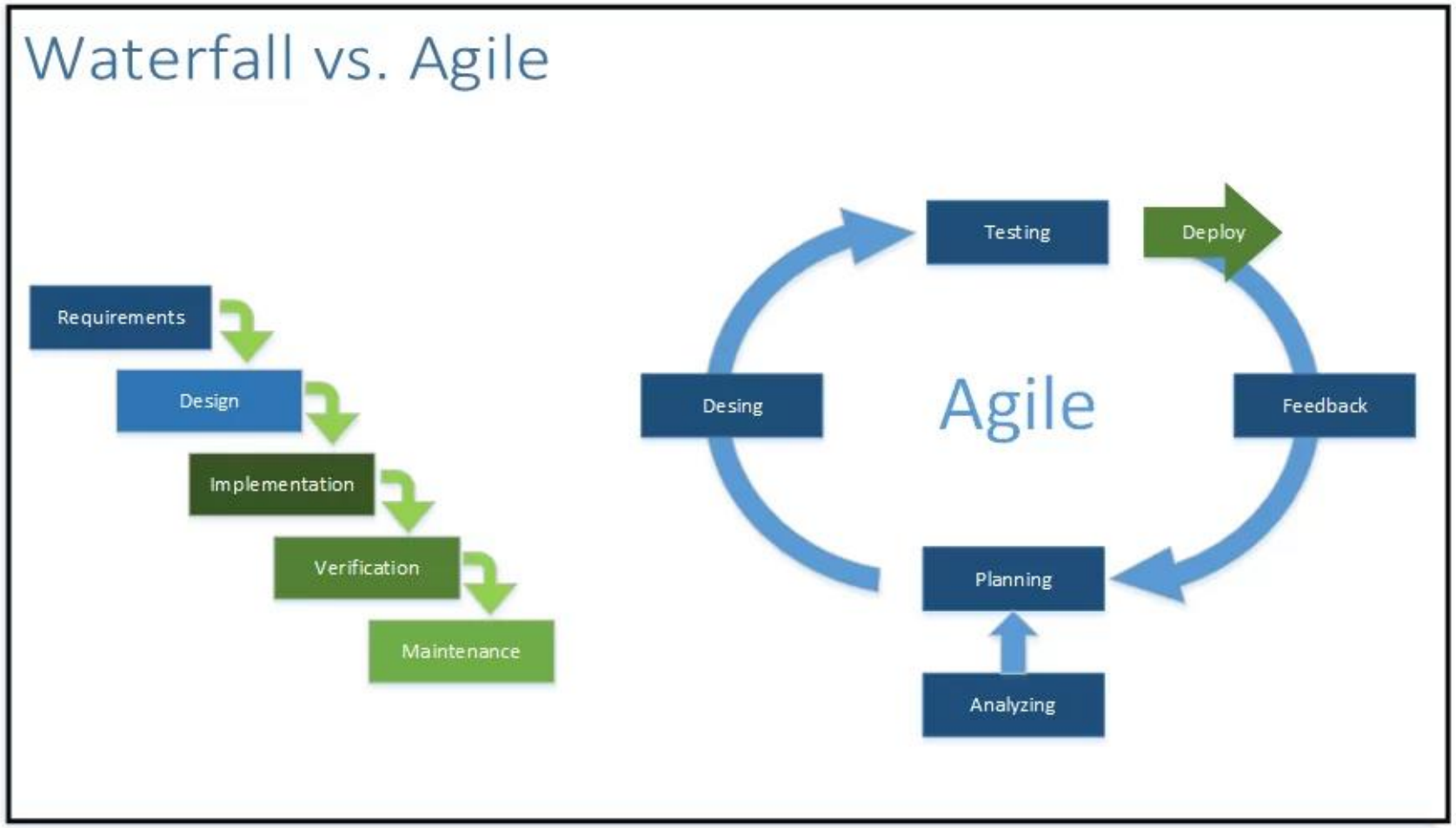
Project Management and Privacy



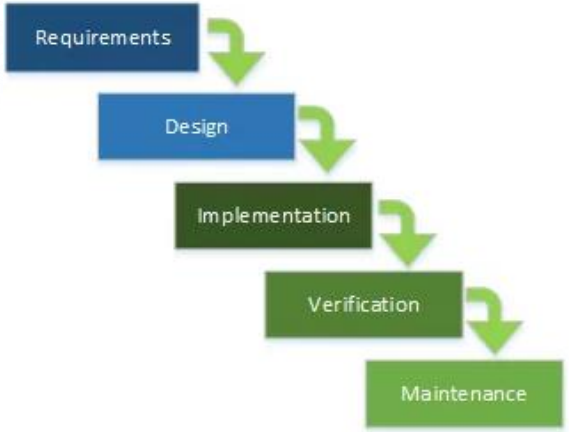
Privacy can and should be part of the conversation at all phases of the project.

Two common approaches to IT Project management are Waterfall and Agile.

Incorporating Privacy



In a Waterfall project



Design

Data Elements – Just because you can capture a data element, should you?
Permissions – Who will need access to what data and why? Do they need it to do their job?
Data Flow – what data elements are coming into your system and leaving your system?

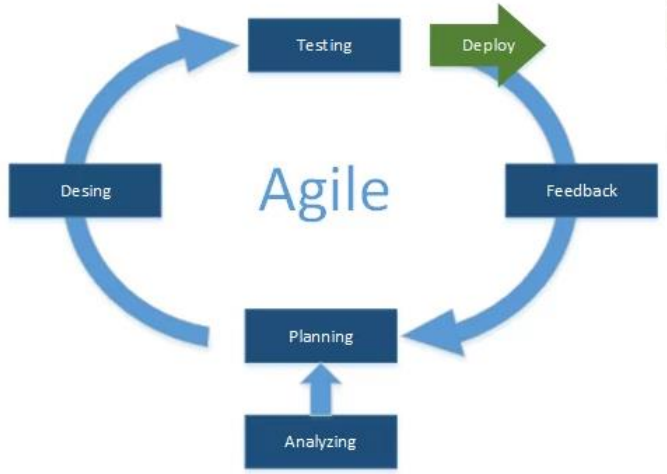
Build

Testing – Involve usability testers from outside the development and testing teams.
Exposure – Is any data visible for a screen shot regardless of where it is stored?

Release

Prior to release – Privacy staff should have a final review
Involve privacy staff early in the Design and Build process to avoid costly re-work.

In an Agile project



User Story and Backlog Management

Include user stories for data privacy reviews in each iteration and prior to each release – prioritize.

Iterations

Provide opportunities for review of small incremental code changes by the privacy team.

Include manual reviews for sensitive data exposure when you use automated regression testing.

Release

Prior to each release privacy staff should have a final review

Include regression testing with production releases.

Retrospectives

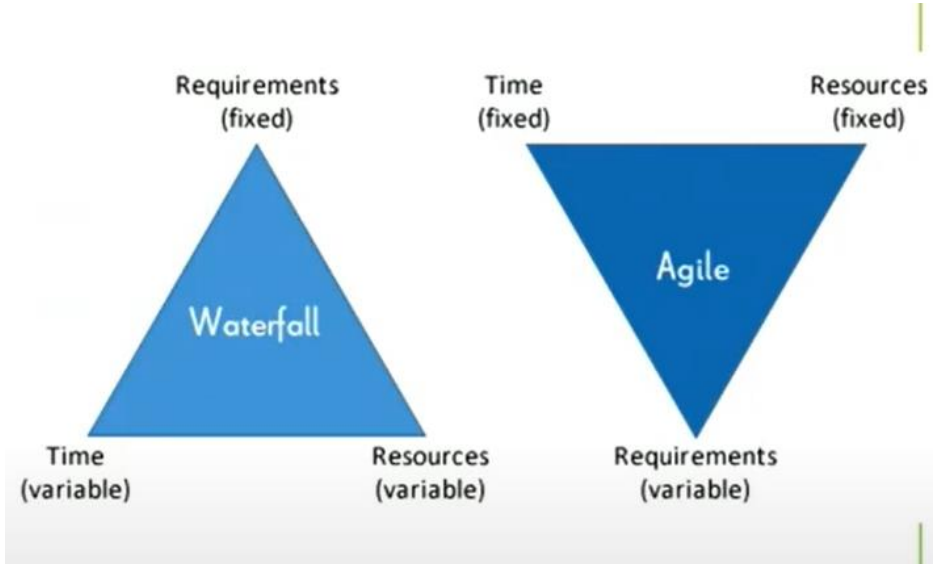
Backlog and Scope Management

In Agile projects, time and resources are fixed, and scope is varied.

Don’t sacrifice quality or privacy over features and functions.

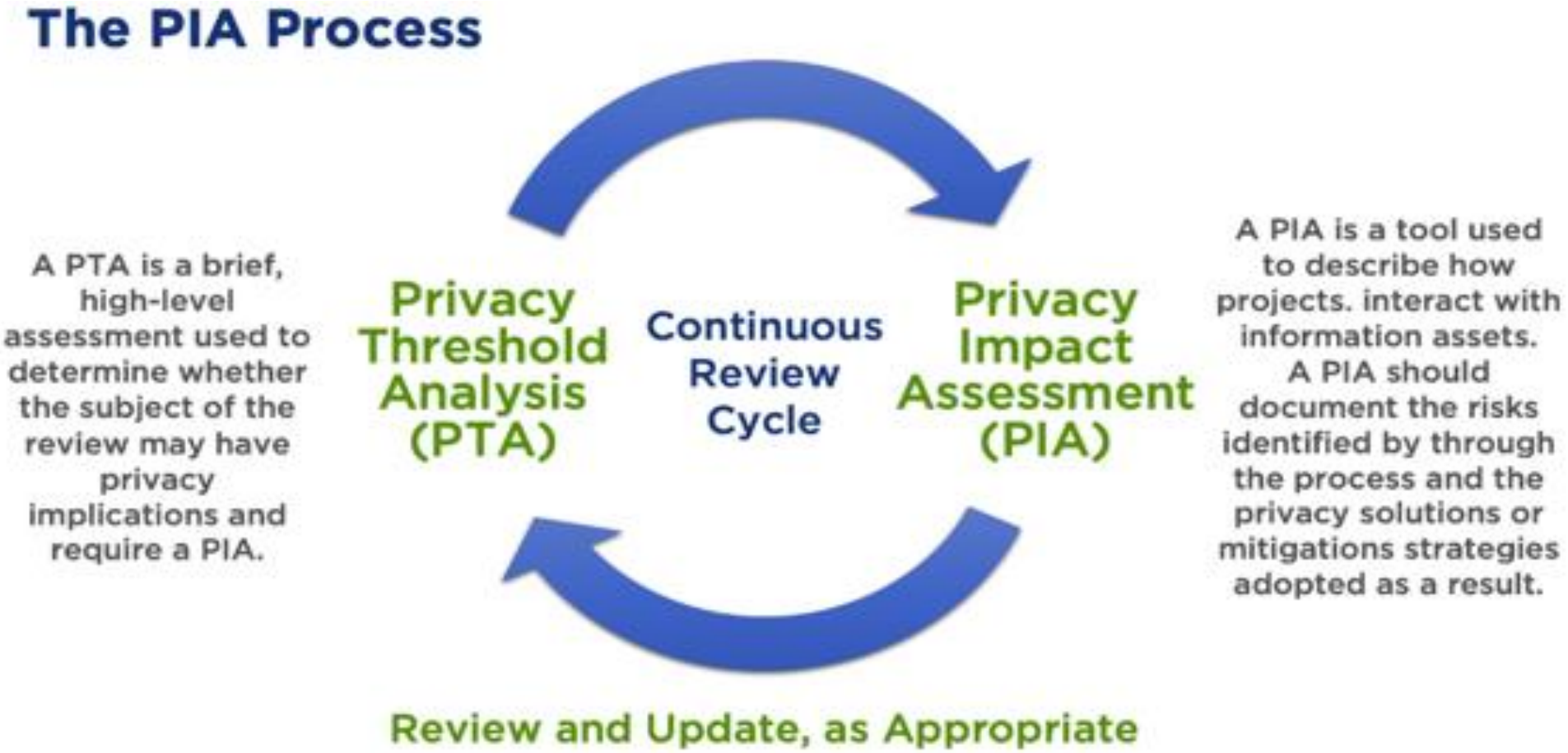
Include privacy reviews, privacy design user stories and continuous regression testing throughout each iteration.

Privacy is not a one and done validation.



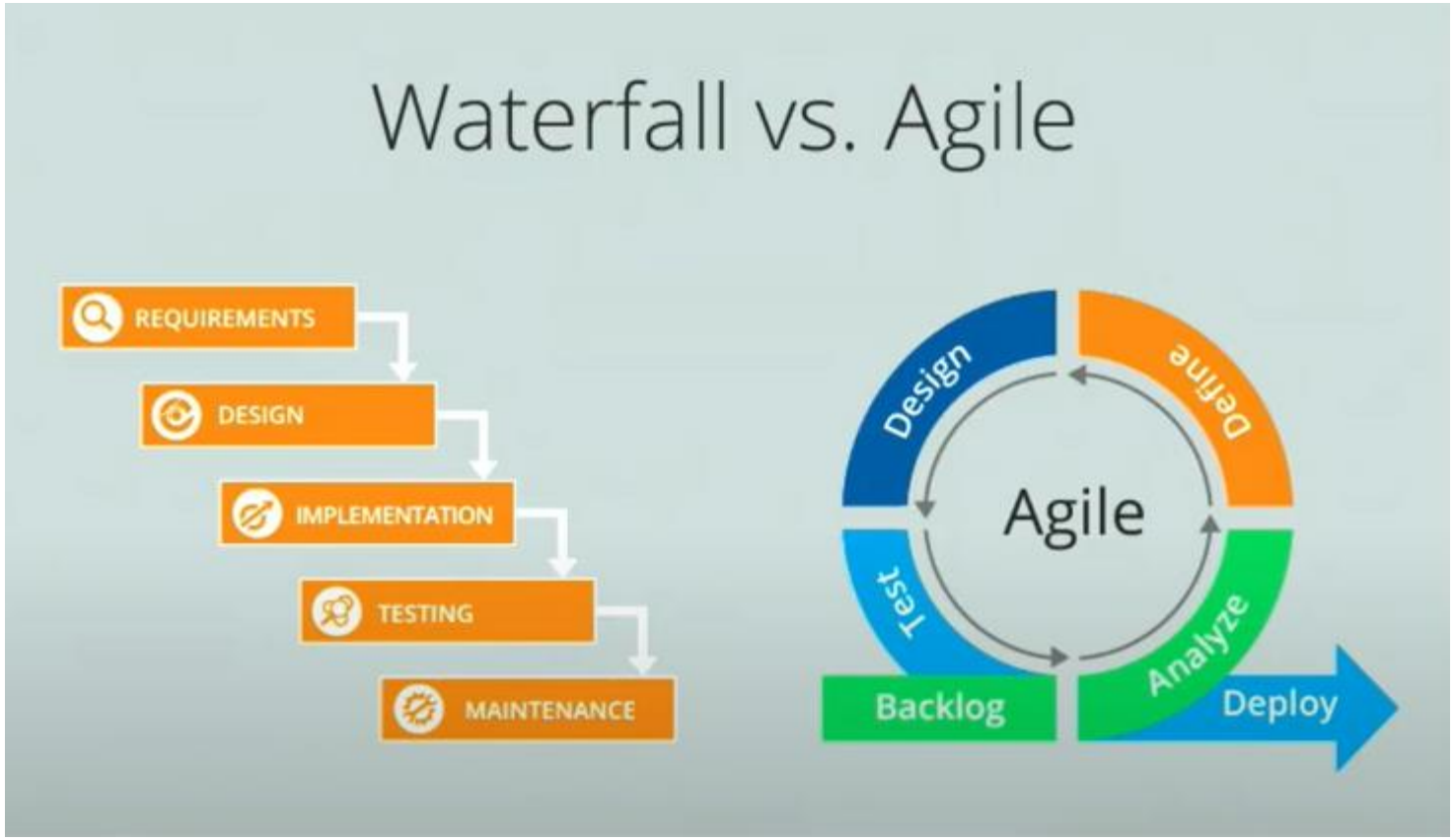
Other considerations

Privacy Impact Assessment Tool and Privacy Threshold Analysis Process



Challenge: when to conduct PIAs

- As soon as possible when developing new system or modifying existing system
- PIAs should be in advance or in parallel with development
  - Not retrospective documentation



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

- Strategy: Quick, iterative assessment

Quick assessment - ties directly to Privacy Principles

WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

Determine:

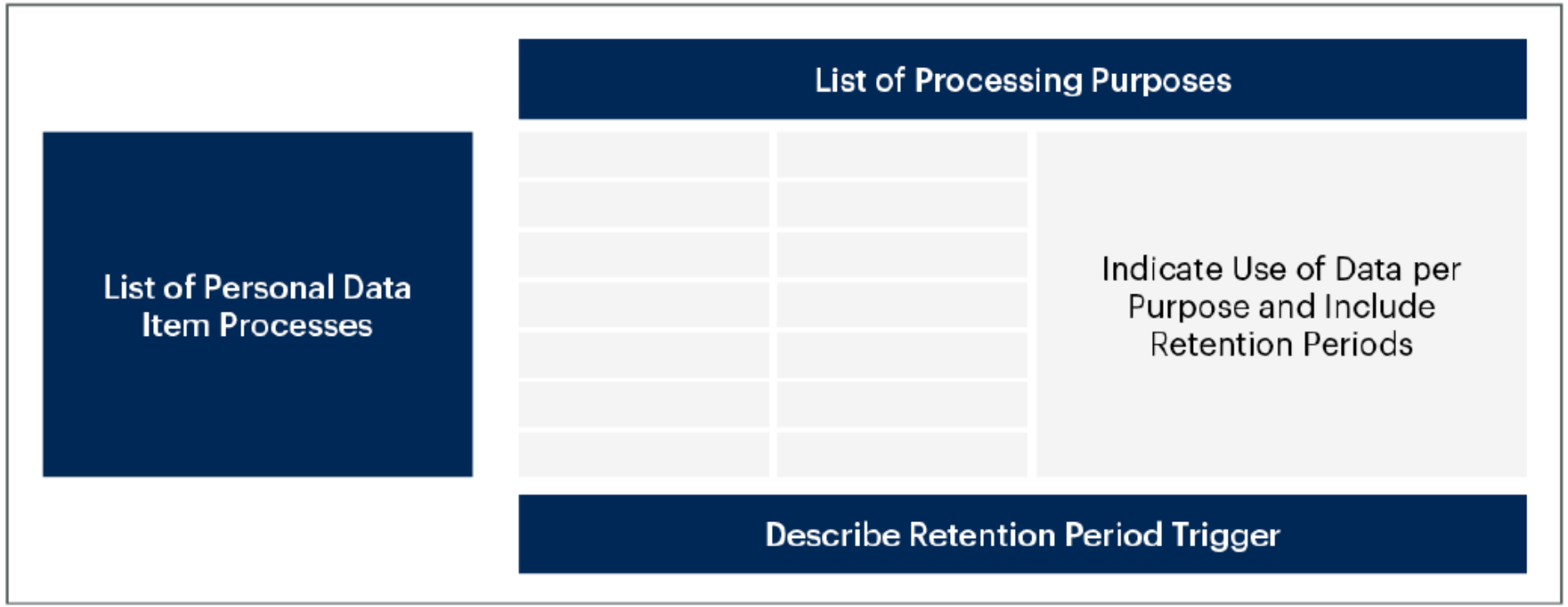
- ✓ What personal data are you collecting?
- ✓ Where are you going to get it from?
- ✓ Where will it be stored?
- ✓ Who will have access?
- ✓ Purpose for collection? Why do you actually need it?
- ✓ How long does it need to be retained?

OPDP

Agile Methodology – Quickly Assess Each Sprint (if new feature processing personal data)

WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

A Quick Assessment Overview Result



Source: Gartner

OPDP

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

Thank you!

privacy@watech.wa.gov

www.watech.wa.gov/privacy