# IAPP EUROPE
# Data Protection Congress 2017

## Kira Ahveninen-Kuha

Lead, Data Protection and Cybersecurity Law

## Matti Suominen

Lead Security Consultant

#DPC17


“
Integrating data protection requirements with privacy by design
”

# Why requirements?

Requirements are the way to steer development process




“
Show of hands
Have you been involved in drafting development requirements?
”

# Development (in 2 minutes)

## SDL

Secure Development Lifecycle, process for including security in development cycles

## Requirement

Something that needs to be implemented or considered in the development process

## Epic

Group of related requirements that collectively represent a business requirement for the system

## Waterfall

Development models where design is made up-front, followed by a longer development phase

## Agile

Development models where design is created on-demand and development phases are iterative

## Sprint

Smallest interval for development in Agile models, often 2 weeks at a time



# Waterfall v Agile

- Proactive
- Long-term
- Stable

- Reactive
- Short-term
- Volatile

# In-house v procurement

- Flexible
- Recommendations
- Focus on process

- Inflexible
- Requirements
- Focus on results


“
Show of hands
Have you used any common frameworks for requirements?
”

# Privacy requirements

- Purpose, consent
- Accountability
- Data subject rights
- Data breaches
- Security
- Portability
- Anonymisation

# EPIC requirements?

1 Split the requirement into individual tasks

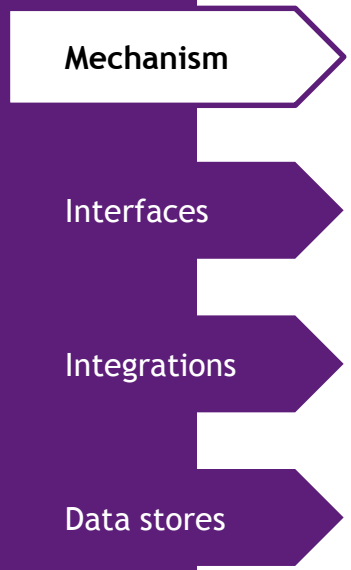
2 Identify relevant technical measures

3 Identify stakeholders for each task

# Example: data erasure

“Implement data erasure into our business application”

# Example: data erasure




- Erasure strategy
- Technical mechanisms
- Data retention
- Immutable systems?
- Legacy and proprietary systems?
- **Stakeholders:**
  - System specialists
  - System owners

# Example: data erasure

Mechanism

Interfaces

Integrations

Data stores

- User interface changes
- Partial erasure
- Cache updates
- Dependencies and relations
- **Stakeholders:**
  - UI Designers
  - Developers



# Example: data erasure

Mechanism

Interfaces

**Integrations**

Data stores

- Identifying integrations
- Signaling and synchronization
- Master v slave
- Third-party systems?
- **Stakeholders:**
  - System owners (many)
  - Third parties, partners (also many)



# Example: data erasure

Mechanism

Interfaces

Integrations

**Data stores**

- Databases, caches, indices
- Log files
- Backups
- **Stakeholders:**
  - Data owners
  - Developers




“
Show of hands
Have you defined privacy activities into an existing SDL?
”

# Know your environment

- Business
- Architecture
- Development process
- Stakeholders
- Selling points



# Privacy in SDL

| | |
|---|---|
| 1 Preparation | PIA, data inventory |
| 2 Requirements | Threat review, privacy requirements |
| 3 Design | Security architecture and controls, privacy strategy |
| 4 Development | Implementation, documentation |
| 5 Testing | Verification, compliance |
| 6 Production | Monitoring, incident response |

Quality gates between phases



# Useful questions

*"Is co-operation between different teams required?"*

*"Are there multiple implementation strategies?"*

*"What are the wider implications?"*

# Useful resources

**OWASP**

www.owasp.org

**OASIS**

www.oasis-open.org

**Microsoft SDL**

microsoft.com/en-us/sdl/

**Kantara Initiative**

kantarainitiative.org

**Privacy Patterns**

privacypatterns.org



# Things to remember

- Join the existing process
- Know your environment
- Get involved
- It can get complex at times




“
Questions?
”

**Don’t forget to vote!**

Open IAPP App

“Integrating data protection requirements with privacy by design”

**Thank you!**


# Kira Ahveninen-Kuha

kira.ahveninen-kuha@nixu.com

/kiraahveninenkuha



# Matti Suominen

matti.suominen@nixu.com

/mattisuominen


#DPC17