LINDDUN privacy engineering

Kim Wuyts

@wuytski

DistriNet

SecAppDev 2018

LINDDUN PRIVACY ENGINEERING

www.linddun.org

@linddun

LINDDUN.privacy

DistriNet

Large team of professionals

- 12 faculty members
- 8 research managers
- 15 postdocs
- 50 PhD Students
- Business office

Project-centric research

- fundamental research at the core
- strategic basic research
- applied research with industry
- contract research

Distributed Software

Secure Software

Software engineering

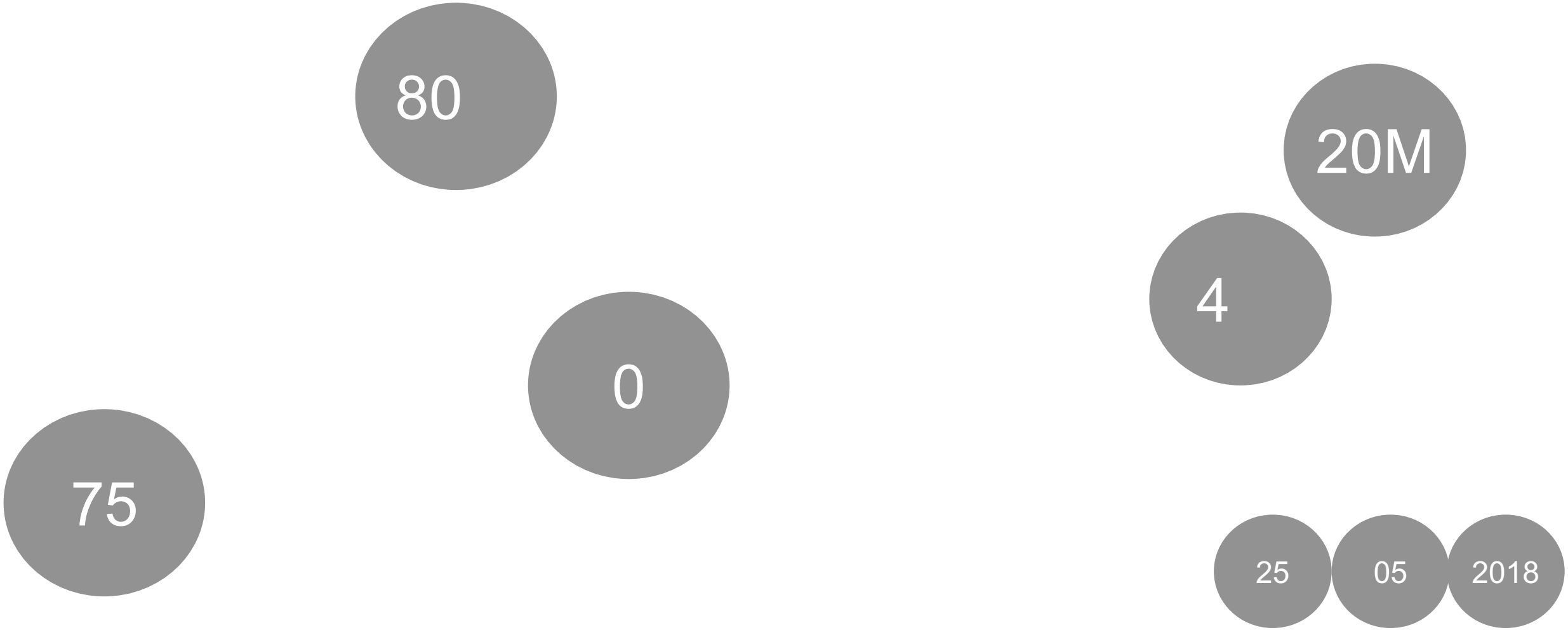
GDPR

is an **evolution**
in data protection

not a burdensome revolution

ICO blog
https://iconewsblog.org.uk/2017/08/25/gdpr-is-an-evolution-in-data-protection-not-a-burdensome-revolution/

GDPR in numbers



Special thanks to our colleagues at CiTiP, KU Leuven

GDPR in numbers

80%

Percentage of GDPR rules already existed in Data Protection Directive

20M

4

0

Companies (that process personal data) can ‘escape’ from the regulation

75

25 05 2018

Date when GDPR will be enforced

LINDDUN PRIVACY ENGINEERING

DistriNet

Processing principles (art. 5)

Clarified – no fundamental changes

Lawfulness
fairness
transparency

- Legitimacy (art. 6)
  - Legal basis needed
    - Consent has stricter conditions!
- Transparency
  - Objective of collection and processing should be clear to data subject

unroll.me

“It was heartbreaking to see that some of our users were upset. Recent customer feedback tells me we weren’t explicit enough.”

- CEO Unroll.me

Processing principles (art. 5)

Clarified – no fundamental changes

- It's all about the **PURPOSE**
  - Proportionality
    - processing reasonable w.r.t. purpose
  - Finality
    - Data cannot be used for other purpose

Lawfulness fairness transparency

Purpose limitation

Data minimization (proportionality)

Storage limitation

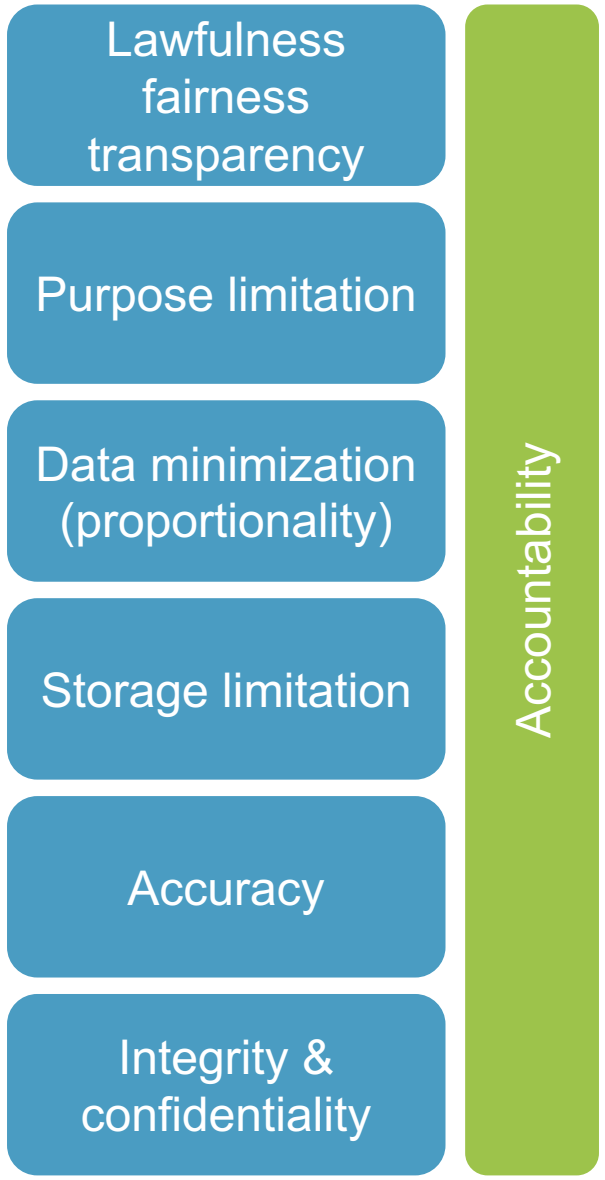
"In the future, with your permission, this information will enable the smart home and the devices within it to work better."

- Roomba

Processing principles (art. 5)

Clarified – no fundamental changes

- Confidentiality
  - Data should be **protected** "***appropriately***"



- **ACCOUNTABILITY** is key
  - Being able to **demonstrate** compliance is as important as actually being compliant

Data subject rights (art. 12-23)

› Enhanced, no fundamental changes

- Right to information
- Right of access
- Right to object
- Right to rectification

NEW TERMINOLOGY

- Right to be forgotten
- Right to object to profiling
  - Automated individual decision making

NEW

- Right to data portability
  - › Data provided by data subject
  - › If reasonably possible between providers

GDPR in numbers

80%

Percentage of GDPR rules already existed in Data Protection Directive

Hefty fines up to

20M

4%

0

Companies (that process personal data) can ‘escape’ from the regulation

75

Date when GDPR will be enforced

25 05 2018

GDPR in numbers

80%

Percentage of GDPR rules already existed in Data Protection Directive

Hefty fines up to

20M

4%

0

Companies (that process personal data) can ‘escape’ from the regulation

75

Number of times ‘**risk**’ is mentioned in GDPR

Date when GDPR will be enforced

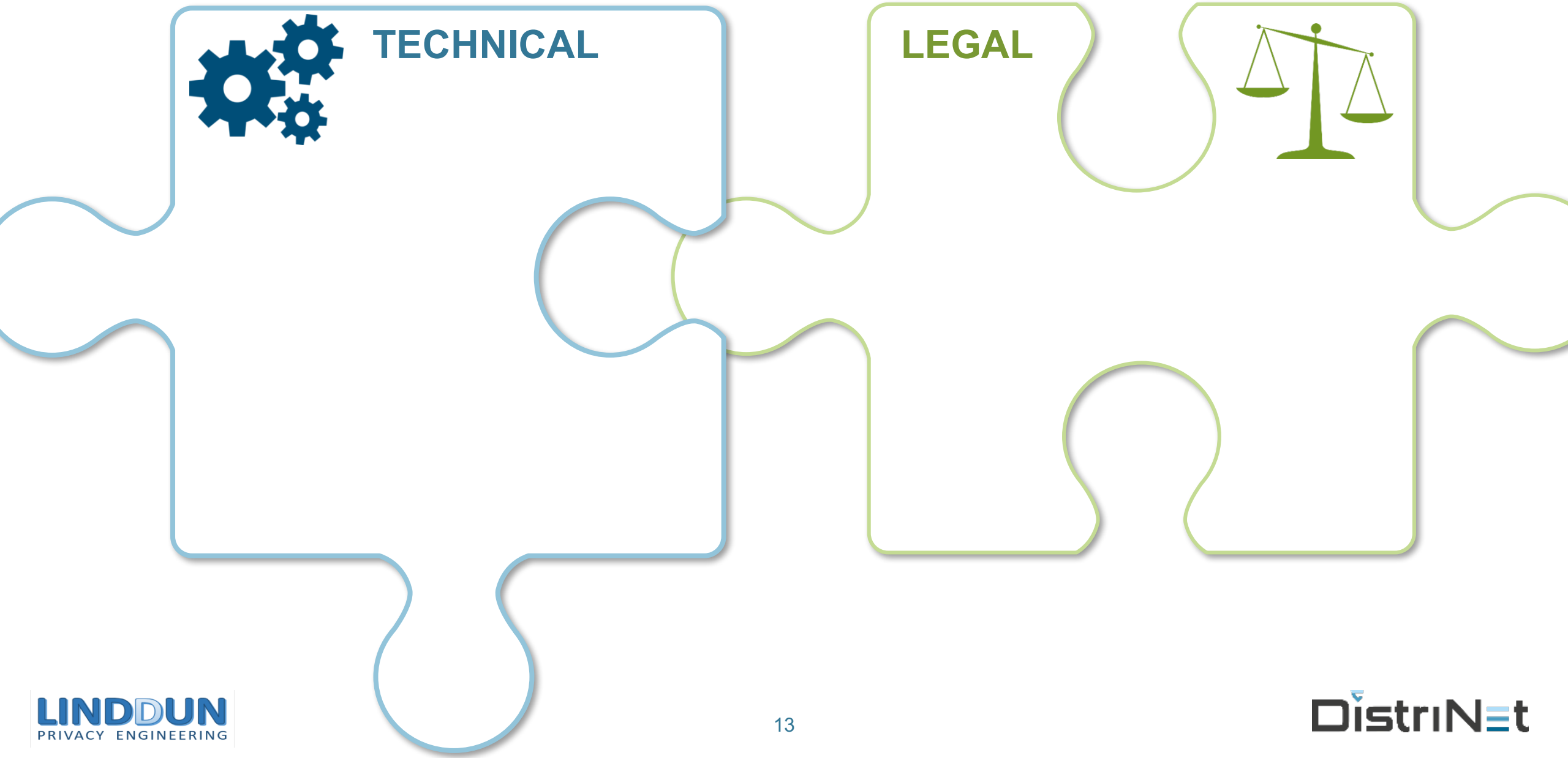
25 05 2018

LINDDUN PRIVACY ENGINEERING

DistriNet

Privacy engineering

GDPR Compliance



GDPR Compliance

GDPR Compliance

TECHNICAL

- **Functional requirements**

Right to be forgotten	✔
Right to information	✔
Right to rectification	✔
…	

- **Appropriate technical measures…”**

LINDDUN
PRIVACY ENGINEERING

LEGAL

LINDDUN privacy by design

- Include privacy early on in the development lifecycle
- Threat modeling framework
  - System description
  - Threat elicitation
  - Threat management / mitigation
- Technical data protection impact assessment methodology

- ☑ Industry acceptance (ISO27550)
- ☑ Scientifically renown

LINDDUN privacy engineering framework

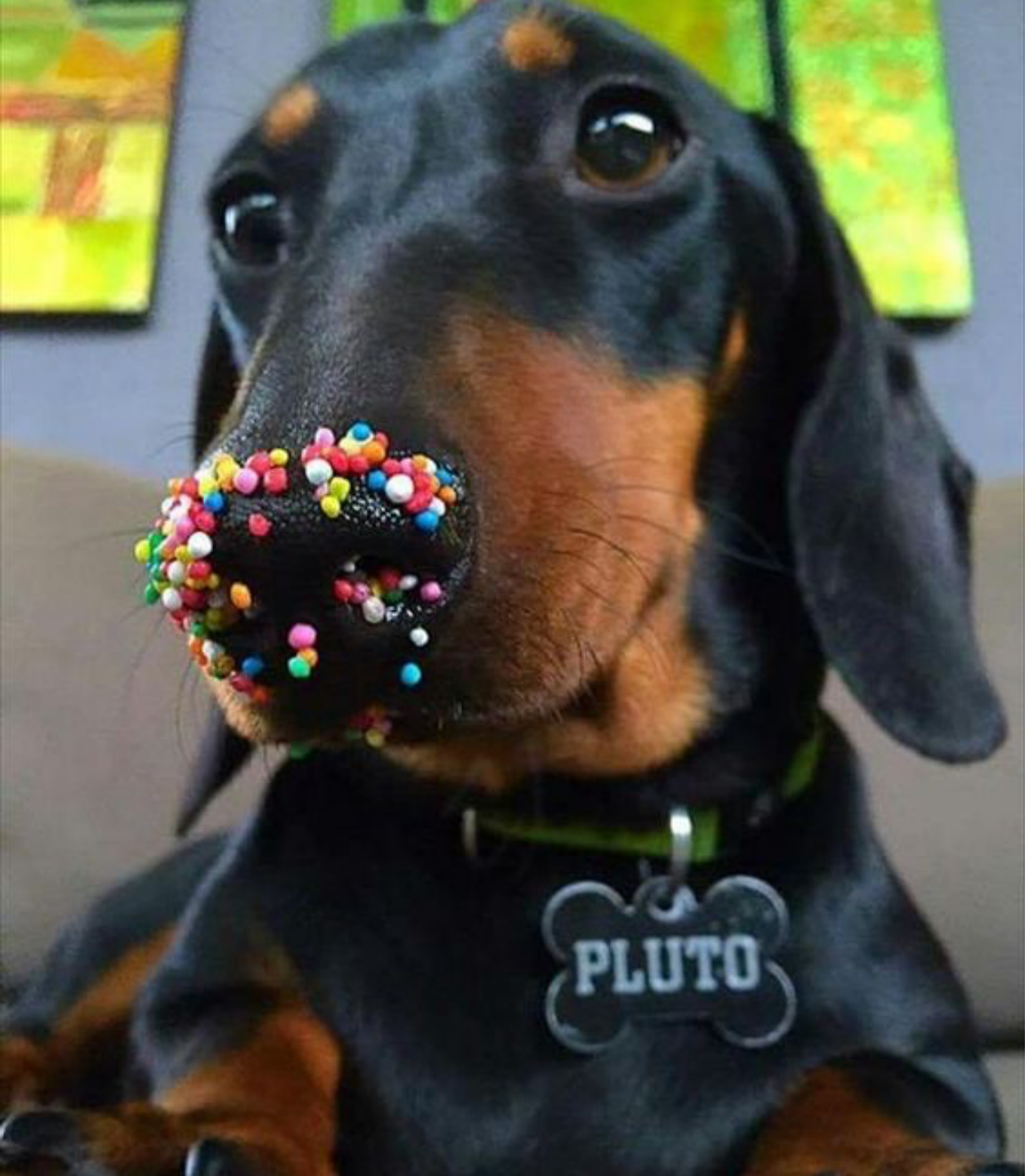
- **Systematic** support for *elicitation* and *mitigation* of privacy threats in software systems

- From high-level model of the system

- Privacy knowledge base
  - Linkability
  - Identifiability
  - Non-repudation
  - Detectability
  - Disclosure of information
  - Unawareness
  - Non-Compliance

Identifiability

LINDDUN
PRIVACY ENGINEERING



Non-Repudiation

Detectability

LINDDUN* privacy engineering framework

METHOD

- **Step 1: describe the system**
  - create a data flow diagram (DFD)
  - describe all data
- **Step 2: elicit threats/risks**
  - map threats to DFD elements
  - identify threats using threat trees
- **Step 3: manage threats/risks**
  - prioritize in dialog with the DPO
  - mitigate using a taxonomy of PETs

KNOWLEDGE BASE

Mapping table

LINDDUN threat taxonomy

Taxonomy of mitigation strategies

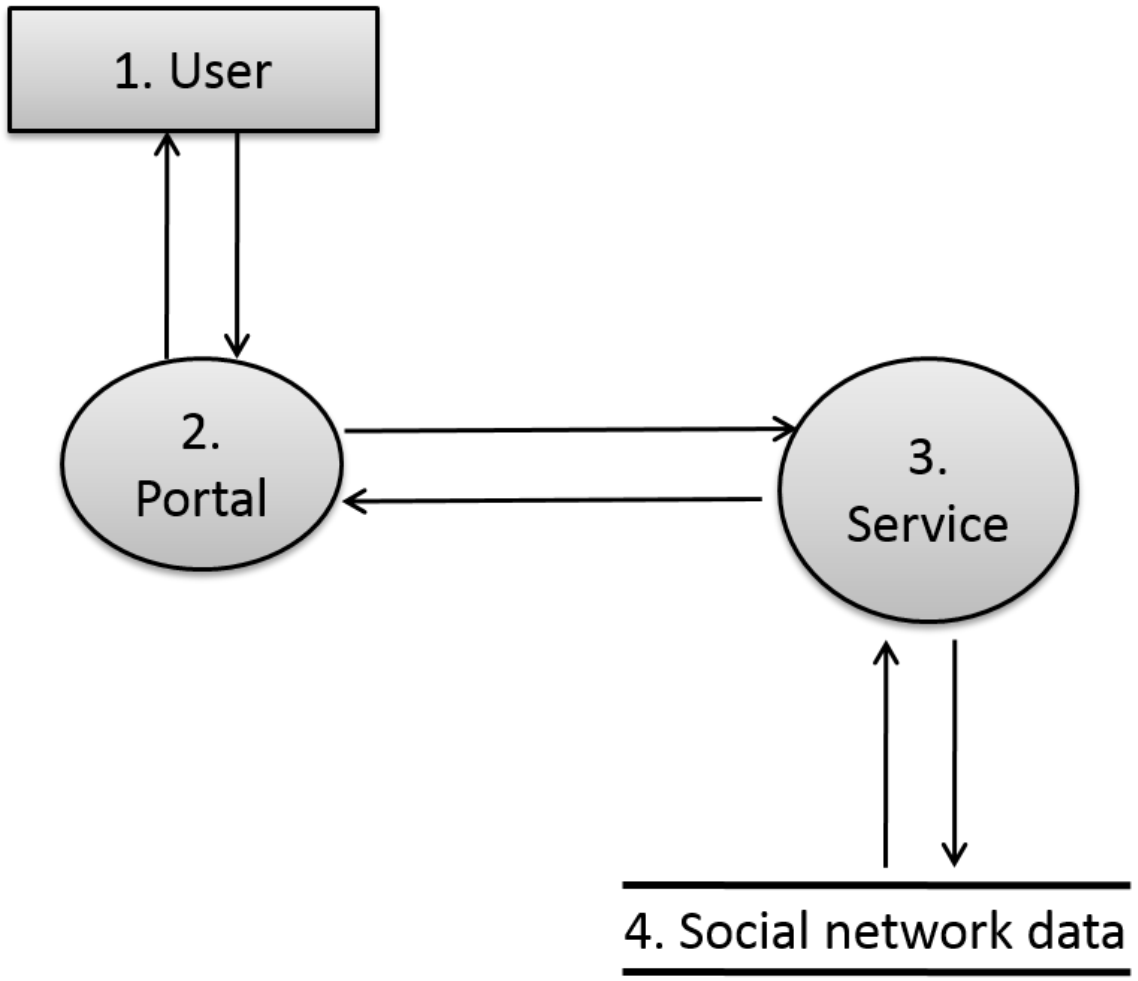
Classification of privacy-enhancing technologies (PETs)

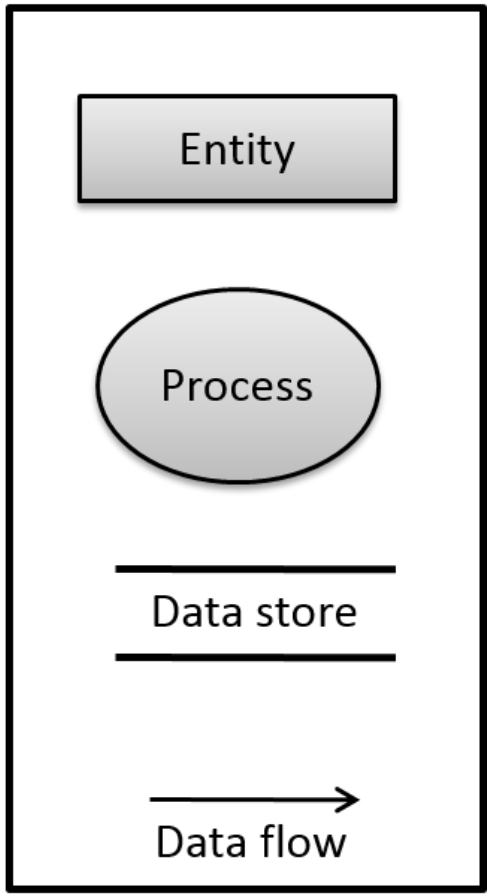
LINDDUN PRIVACY ENGINEERING

* We present a modified version of LINDDUN

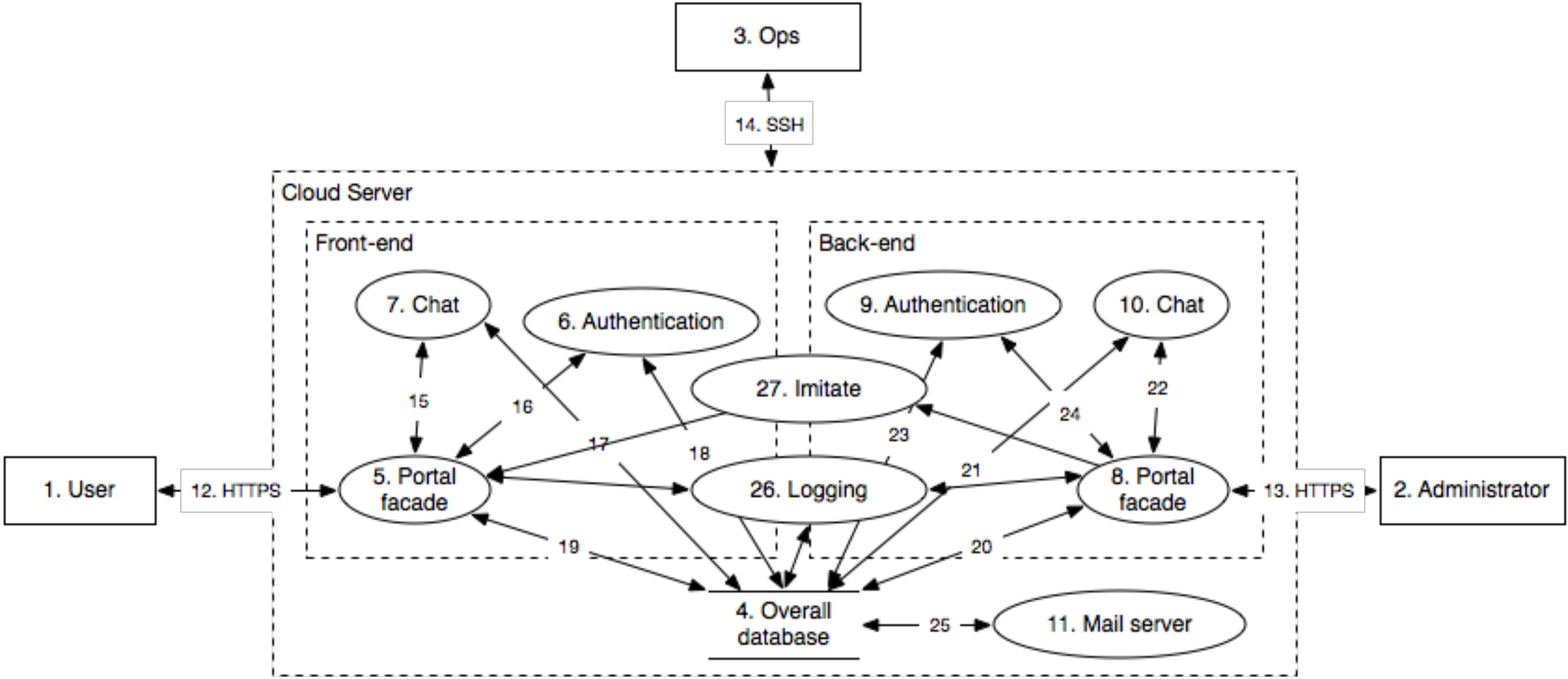
DistriNet

Step 1: Create the DFD



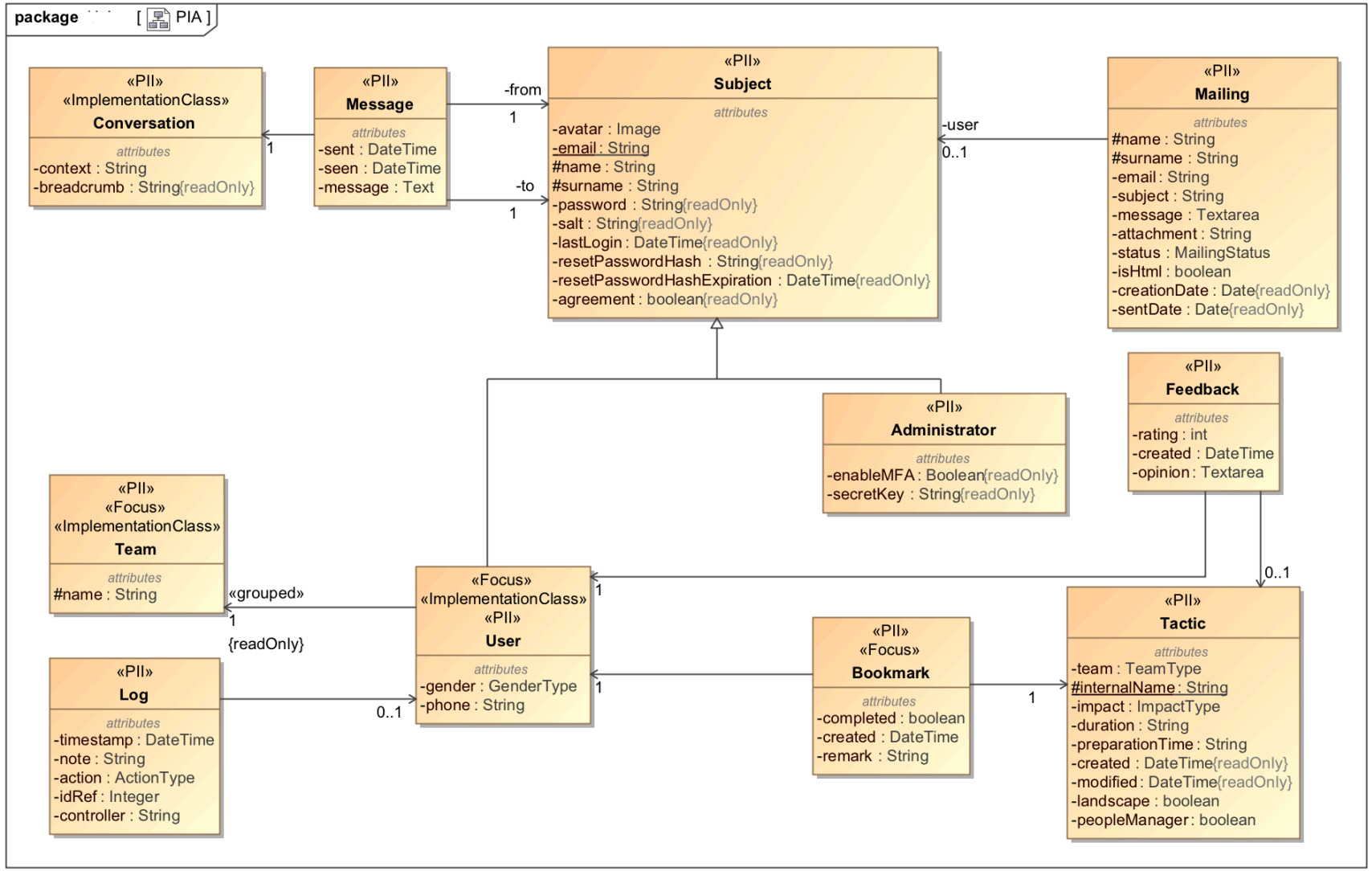


Step 1: Create the DFD



Step 1: Describe all data

- Databases
- Files
- Logs
  - apache logs
- Using
  - UML
  - ER scheme
  - Text



Step 2: Elicit threats

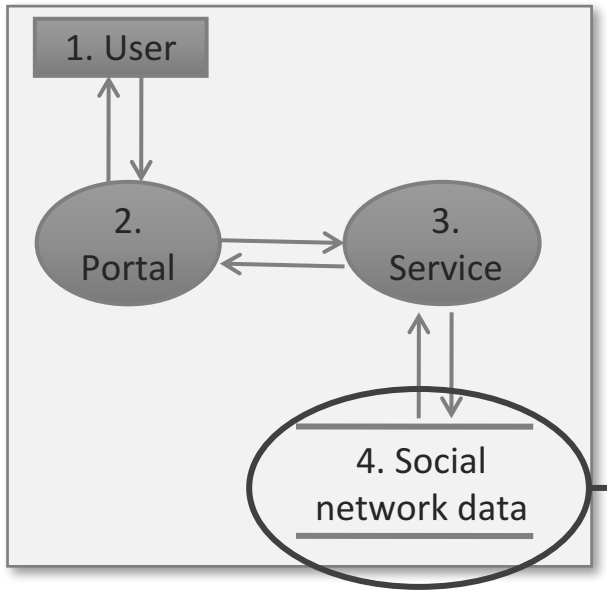
- **Linkability**
  - An adversary is able to link two items of interest without knowing the identity of the data subject(s) involved.
- **Identifiability**
  - An adversary is able to identify a data subject from a set of data subjects through an item of interest.
- **Non-repudiation**
  - The data subject is unable to deny a claim (e.g., having performed an action, or sent a request).
- **Detectability**
  - An adversary is able to distinguish whether an item of interest about a data subject exists or not, regardless of being able to read the contents itself.
- **Disclosure of Information**
  - An adversary is able to learn the content of an item of interest about a data subject.
- **Unawareness**
  - The data subject is unaware of the collection, processing, storage, or sharing activities (and corresponding purposes) of the data subject's personal data.
- **Noncompliance**
- The processing, storage, or handling of personal data is not compliant with legislation, regulation, and/or policy.

Step 2: Map LINDDUN to DFD elements

› Each element in the DFD is susceptible to one or more threat types

MAPPING TEMPLATE	LINDDUN PRIVACY BY DESIGN	Linkability	Identifiability	Non-repudiation	Detectability	Information Disclosure	Content Unawareness	Policy & Consent Non-compliance
	Data store	X	X	X	X	X		X
	Data flow	X	X	X	X	X		X
	Process	X	X	X	X	X		X
	Entity	X	X				X	

1. DFD



2. Map

MAPPING TEMPLATE

LINDDUN PRIVACY THREAT MODELING	L	I	N	D	D	U	N
Data store	X	X	X	X	X		X
Data flow	X	X	X	X	X		X
Process	X	X	X	X	X		X
Entity	X	X				X	

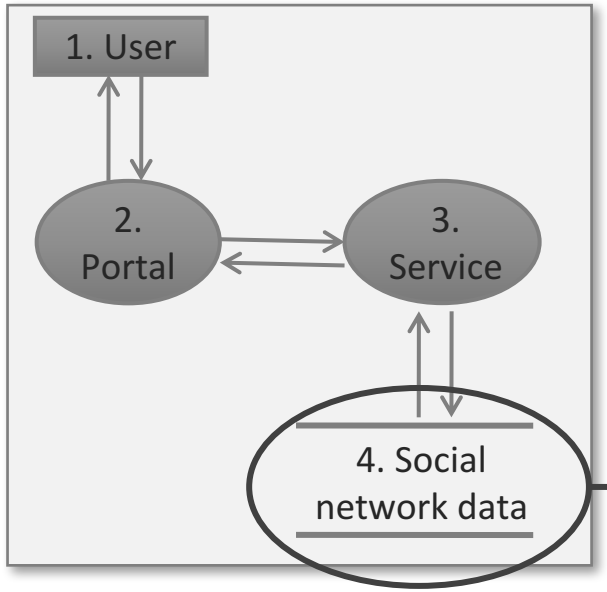
	Threat target	L	I	N	D	D	U	N
Data store	Social network db	X	X	x	x	X		X*
Data flow	User data stream (user-portal)							
	...							

Assumptions

Preconditions / invariants that invalidate threats e.g.:

- non-repudiation threats often not applicable
- secure communication (https A+ grade)
- identifiability and linkability of data flow not be applicable to closed systems

1. DFD



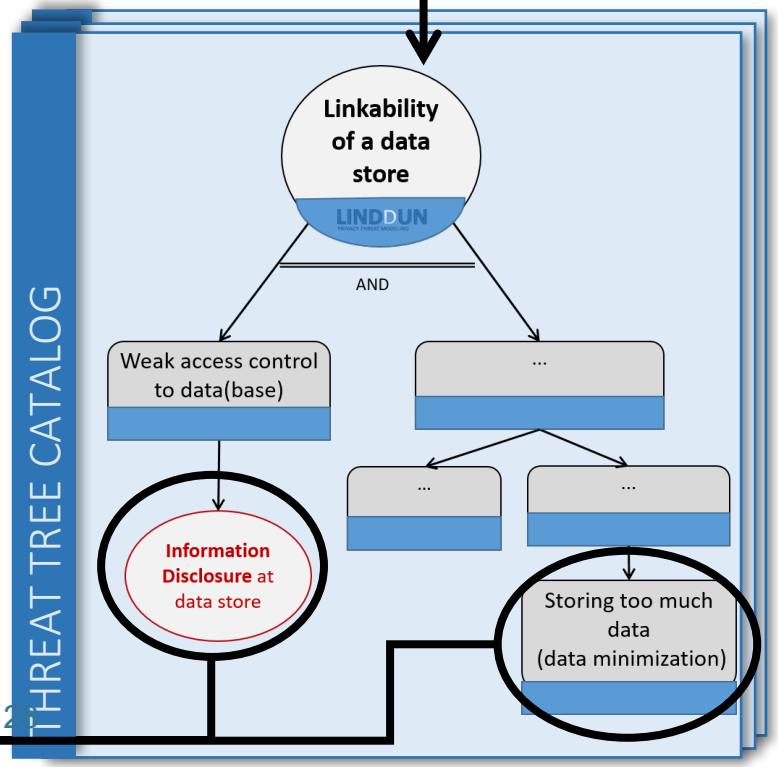
2a. Map

MAPPING TEMPLATE

LINDDUN PRIVACY THREAT MODELING	L	I	N	D	D	U	N
Data store	X	X	X	X	X		X
Data flow	X	X	X	X	X		X
Process	X	X	X	X	X		X
Entity	X	X				X	

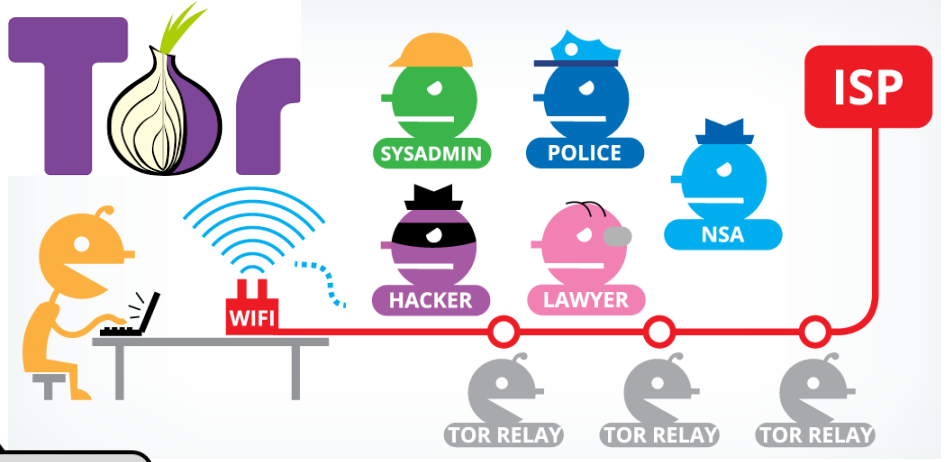
	Threat target	L	I	N	D	D	U	N
Data store	Social network db	X	X	x	x	X		X*
Data flow	User data stream (user-portal)							
	...							

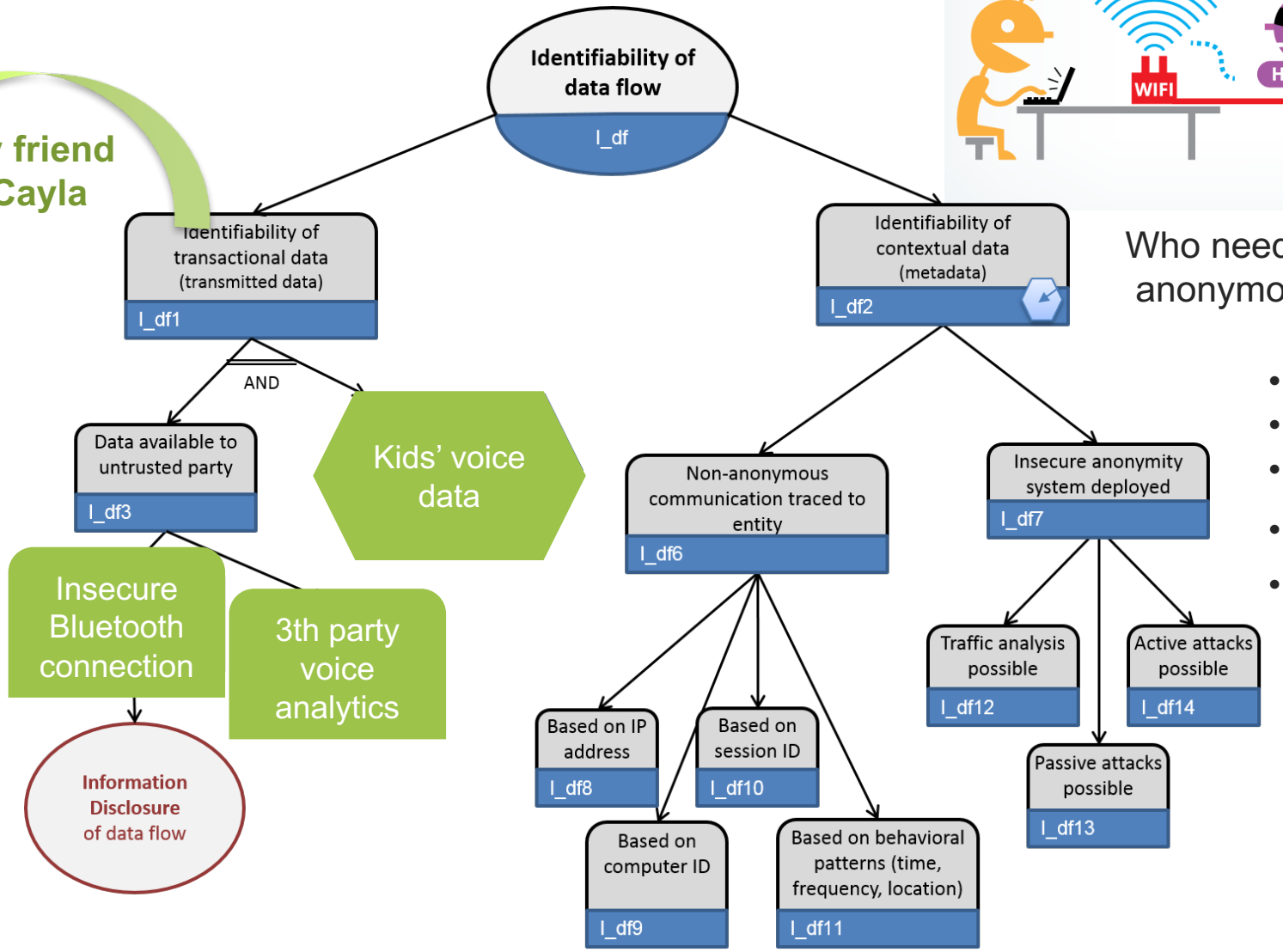
2b. Elicit and document threats



Step 2: Identify threat using threat tree catalog

My friend Cayla





Who needs anonymous communication?

- Whistleblowers
- Activists
- Reporters
- Normal people
- Business executives
  - Security breach information clearinghouses

Step 2: Traceability of threats and assumptions

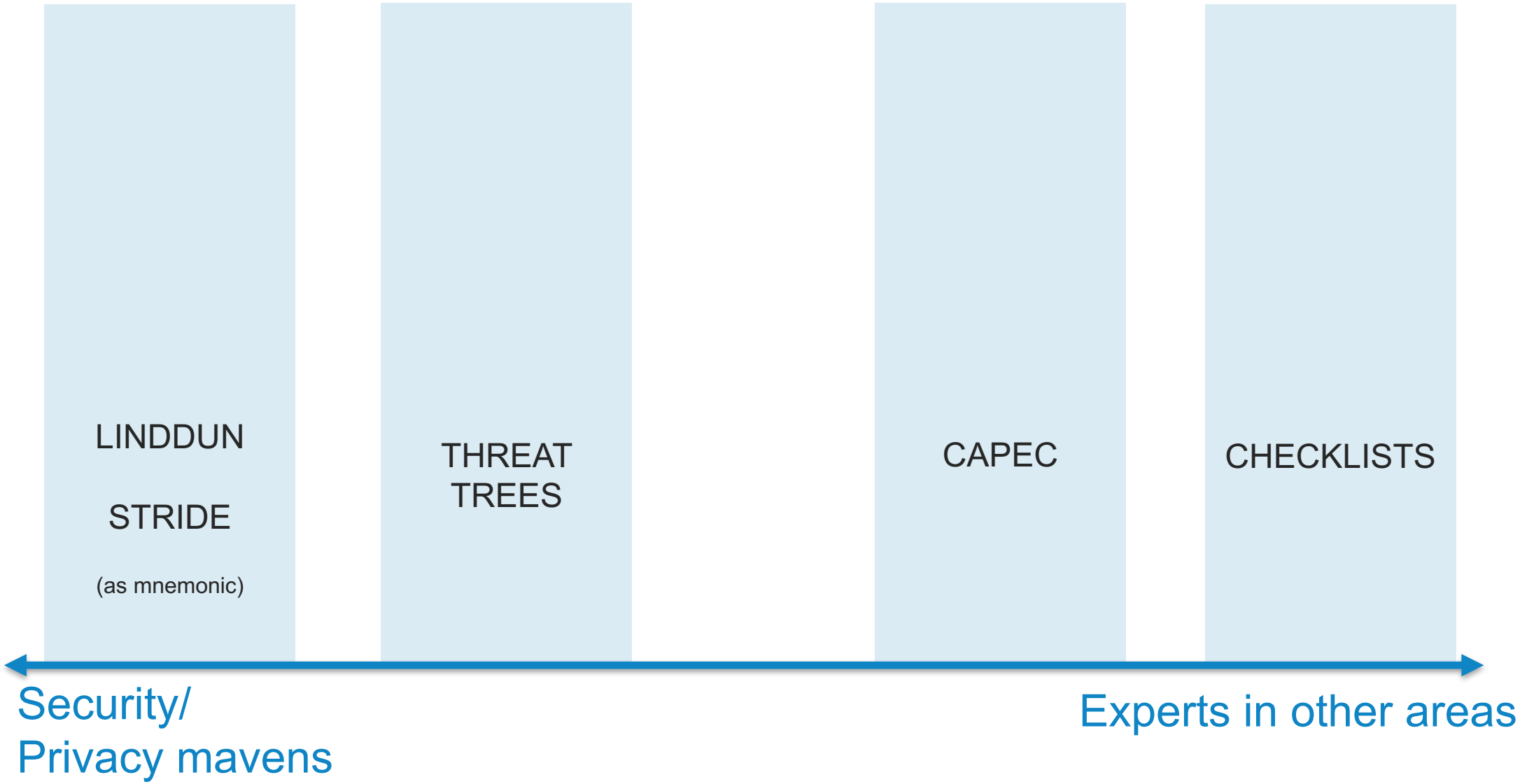
	L	I	Nr	D	iD	U	Nc
E1. Patient	T01	T02				X	
E2. External disease services	X	X				X	
DS1. patient data	X	X	X	X			
P1. patient portal	A05						
P2. consult PHR							
P3. browse diseases							
DF1 (E1. patient -> P1. patient portal)	T07, T08	X	X	X	A03		T05
DF2 (P1. patient portal -> E1. patinet)		X	X	X			
DF3 (E1. patient -> P1. patient portal)		X	X	X			
DF4 (P1. patient portal -> E1. patinet)		X	X	X			
DF5 (E2. disease service -> P3. browse diseases)		X	X	X			
DF6. (P3. browse diseases -> E2. disease service)		X	X	X			
DF7 (P3. browse diseases -> P1. patient portal)		X	X	X			
DF8 (P1. patient portal -> P3. browse diseases)		X	X	X			
DF9 (P1. patient portal -> P2. consult OHR)		X	X	X			
DF10 (P2. consult PHR -> P1. patient portal)	X	X	X	X			
DF11 (P2. consult PHR -> DS1. patient data)	X	X	X	X			
DF12 (DS1. patient data -> P2. consult PHR)	X	X	X	X			

GDPR requires traceability

Step 2: Document identified threats - example

Threat 1	**Using the forgot password feature we can identify a system user. DFD 4 (Detectability).**
Description	Forgot password feature asks the email address of the user and after resetting the password says that a reset password email is successfully sent to the user. This could lead to identifiability problems where an attacker can easily check whether the user has a registration within the platform.
Countermeasure	None
Likelihood	Limited
Impact	Negligible
Action point	Modify the forgot password feature to always produce the same message making it impossible to figure out whether the user with the specified email address exists or not.
Reference	D_p (12)

Step 2: Elicit threats - INTERMEZZO

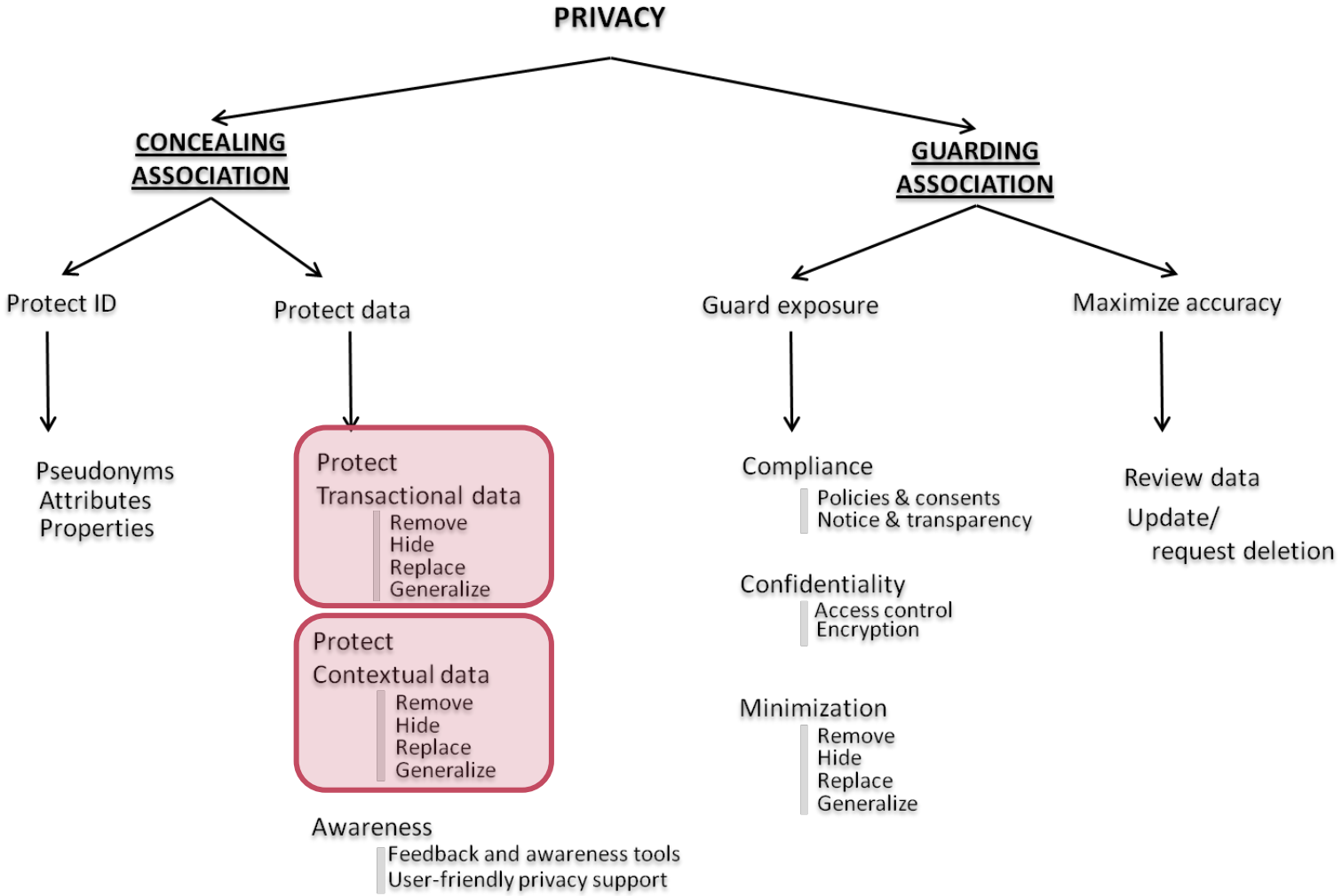


Step 3: Manage threats

- prioritize in dialog with the DPO
  - Risk = impact x likelihood

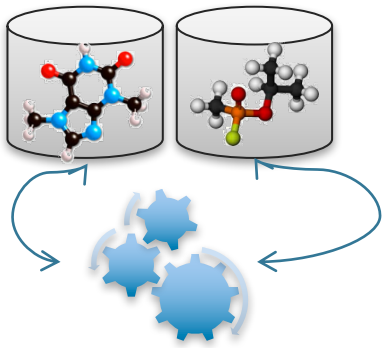
- Accept
- Mitigate
  - Avoid
- Transfer

Step 3: Decision & Trade-off support with mitigation strategies



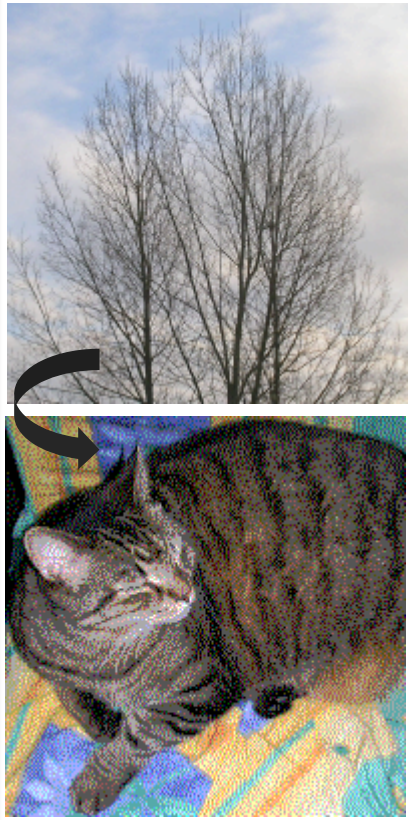
MITIGATION STRATEGY	LINDDUN THREAT TREE
Protect ID	L_e, I_e
Protect data	
Transactional data	L_df1, I_df1
Contextual data	L_df2, I_df2, D_df, NR_df
Awareness	U_1
Guard exposure	
Compliance	NC
Confidentiality	ID_ds, NR_ds, *_p
Minimization	L_ds, I_ds, D_ds
Maximize accuracy	
Review data	U_2
Update/request deletion	NR_ds3

Step 3: Adopt PETs



MPC & FHE:
Collaboration between companies without revealing data

Mitigation Strategy				Privacy Enhancing Techniques (PETs)
Concealing association	Protect ID	Pseudonyms		Privacy enhancing identity management system [HBC+04], User-controlled identity management system [CPHH02]
		Attributes		Privacy preserving biometrics [STP09], Private authentication [AF04, ABB+04]
		Properties		Anonymous credentials (single show [BC93], multishow [CL04])
	Protect data	Transactional data	Remove	(see *awareness* to minimize information sharing)
			Hide	Data-flow specific	**Multi-party computation**) [Yao82, NN01], Anonymous buyer-
				General	see guard exposure - Confidentiality - encryption
			Replace	/
			Generalize	*see guard exposure - minimization - generalize*
		Contextual data	Remove	[PPW91], Onion Routing (1996) [GRS96]
			Hide	General	**Onion Routing – Tor** nication (Freedom Network (1999-2001)
				Undetectability	**Steganography** 2000) [BFK00]
				Non-repudiation	munication [MNCM03], Spread spectrum [KM01]
			Replace	Deniable authentication [Nao02], Off-the-record messaging [BGB04]
			Generalize	Undetectability	Single proxy (90s) (Penet pseudonymous remailer (1993-1996), Anonymizer, SafeWeb), anonymous Remailer (Cipherpunk Type 0, Type 1 [Bac], Mixmaster Type 2 (1994) [Mixa], Mixminion Type 3 (2003) [Mixb])
					dummy traffic, DC-networks (1985) [Cha85, Cha88]
		Awareness	Feedback and awareness tools		Feedback tools for user privacy awareness [LHDL04, PK09, LBW08]
			User-friendly privacy support		Data removal tools (spyware removal, browser cleaning tools, activity traces eraser, harddisk data eraser)
Guarding association	Guard exposure	Compliance	Policies and Consents		Policy communication (P3P [W3C]), Policy enforcement (XACML [oo], EPAL [IBM])
			Notice and Transparency		/
		Confidentiality	Encryption		**Homomorphic encryption** Deniable encryption [Nao02], [CD98]
			Access control		Context-based access control [GMP 101], Privacy-aware access control [CF08, ACK+09]
		Minimization	Remove		/
			Hide	Receiver privacy	Private information retrieval [CGKS98], Oblivious transfer [Rab81, Cac98])
				Database privacy	Privacy preserving data mining [VBF+04, Pin02], Searchable encryption [ABC+05], Private search [OS05]
				General	*see guard exposure - confidentiality - encryption*
			Replace		/
			Generalize		K-anonymity model [Swe02b, Swe02a], l-Diversity [MGKV06]
	Maximize accuracy	Review data			/
		Update/ request deletion			/



Hidden in least significant bits

Towards agile privacy engineering with LINDDUN

- **Incremental** analysis
- **Reusable** privacy **knowledge**
- Support for **automation**

Validated through **pilot projects** with industry

LINDDUN PRIVACY ENGINEERING

In a nutshell

GDPR

- **Risk**-based assessment
- Requires "***appropriate technical measures***"
- **Accountability** is key
  - Being able to demonstrate compliance

LINDDUN privacy engineering

- **Systematic** technical privacy impact assessment framework
- Solid **scientific foundation**
  - Security and privacy expertise
  - Collaboration with research and industry partners
- Extensively **validated** through empirical studies and pilot projects
- **Industry acceptance**
  - ISO27550

LINDDUN privacy engineering

Kim Wuyts

@wuytski

DistriNet

SecAppDev 2018

LINDDUN PRIVACY ENGINEERING

www.linddun.org

@linddun

LINDDUN.privacy