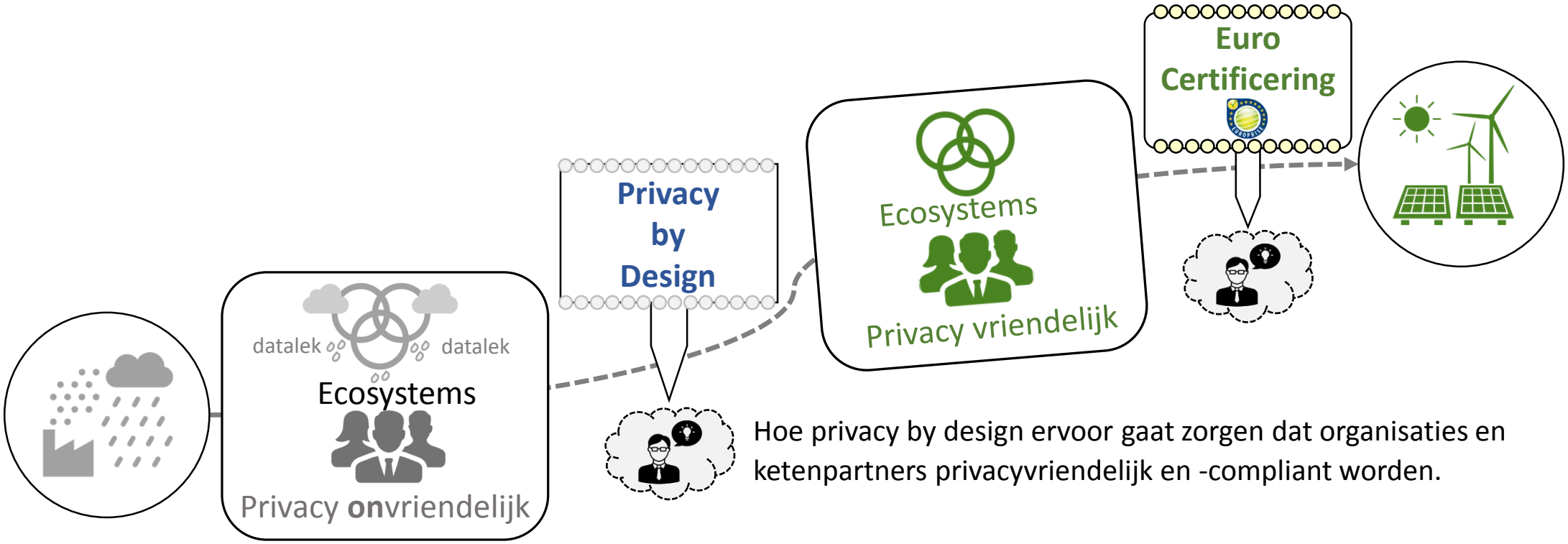
Privacy | het nieuwe groen

Privacy | in complexe ecosystemen beheersbaar maken



Hoe privacy by design ervoor gaat zorgen dat organisaties en ketenpartners privacyvriendelijk en -compliant worden.

Lezing van : Richard Claassens
Tijdstip : vrijdag 29 september 2017
- 14.30 uur Ontvangst
- 15.00 uur Lezing
- 17.00 uur Borrel

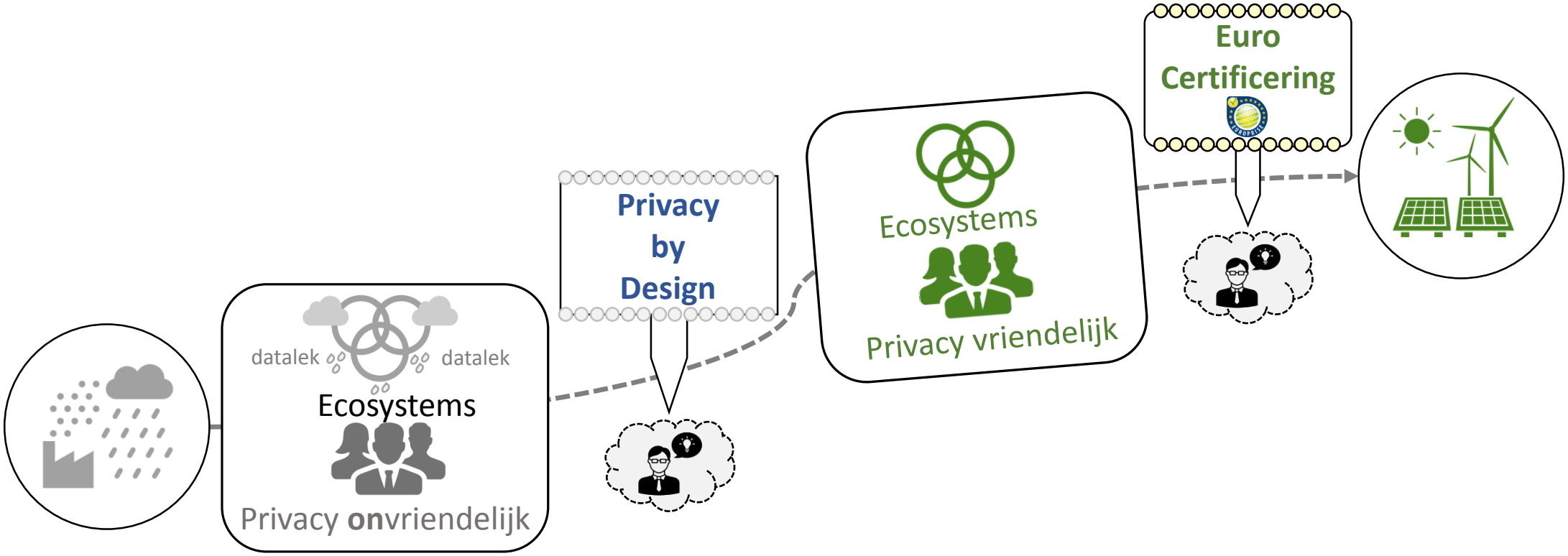
Locatie : Hogeschool Utrecht, Koningsbergerstraat 9 in Utrecht
https://www.hu.nl/overdehu/evenementen/De-Master-spreekt-over-de-privacywet-2018

KNVI-bijeenkomst
Afdeling: IT-Auditing

De Master spreekt...
privacywet 2018 (AVG)

Privacy | het nieuwe groen

Privacy | in complexe ecosystemen beheersbaar maken



Auteur : Richard Claassens
Datum : 29-07-2017
Variant : De Master spreekt... privacywet 2018 (AVG)
Versie : 1.0 | Definitief

| Richard.Claassens@ygdra.com
| https://nl.linkedin.com/in/richardclaassens
| +31(0)626965796

Privacy

Richard Claassens + Privacy opleiding, certificeringen en ervaring

Architectuuropdracht vanaf 1-10-2002 bij:

2002

UWV werken aan perspectief

Technische Architectuur Polisadministratie

2003

→Amalia krijgt een Sofinummer

→Belastingdienst eist afscherming van haar (inkomens)gegevens

2004

Verkenning naar Privacy-Enhancing Technologies (PET)

→*zoals Oracle Label Security*

2005

Privacy opleiding en certificering:

EuroPriSe European Privacy Seal TECHNICAL EXPERT

Privacy opleiding:

PRIVACY ANALYTICS NOW PART OF IMS HEALTH

The Anonymization of Clinical Trial Data: Methodology Course by Khaled El Emam

Security certificeringen:

CCSP Certified Cloud Security Professional

CISSP Certified Information Systems Security Professional

Privacy certificering:

CIPP E iapp Certified Information Privacy Professional/Europe

Werkzaam vanaf 1-1-2006 bij:

2014

SNS BANK N.V.

Privacy Impact Assessment rapport

2015

Blauwdruk programma privacy

PSA Project Start Architectuur | Toestemming Administratie Systeem

PSA Project Start Architectuur | Schoning van persoonsgegevens

2016

Verkenning Privacy by Design met behulp van PRIPARE

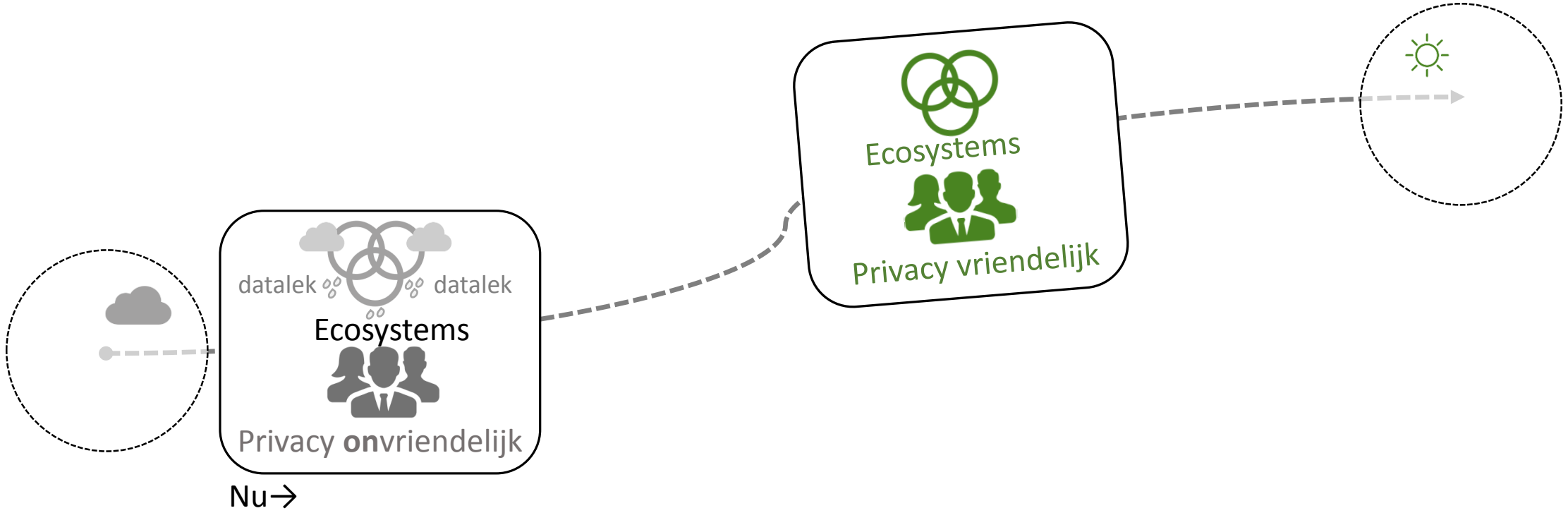
Verkenning data masking

PSA Project Start Architectuur | De-indentificatie van testdata

2017

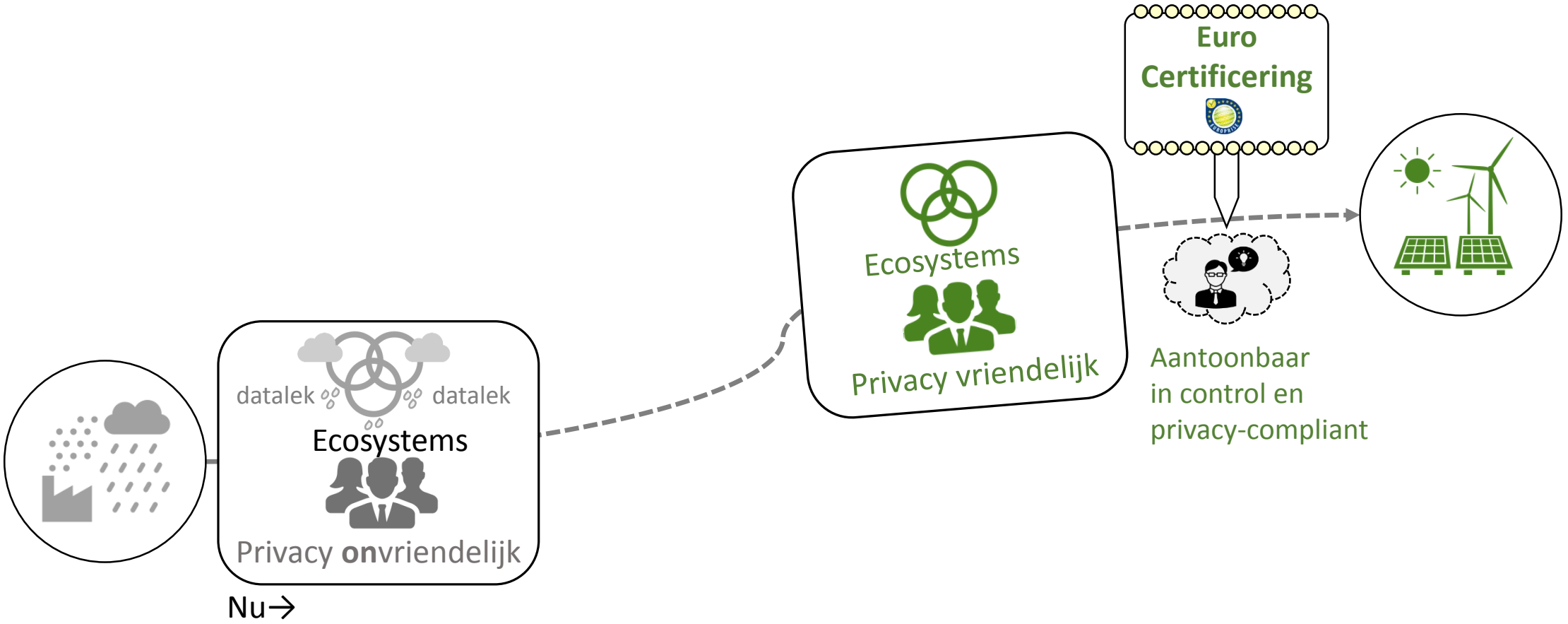
Privacy in complexe ecosystemen | opvattingen

1) Elke organisatie moet van een privacy onvriendelijke *in een* privacy vriendelijke organisatie veranderen



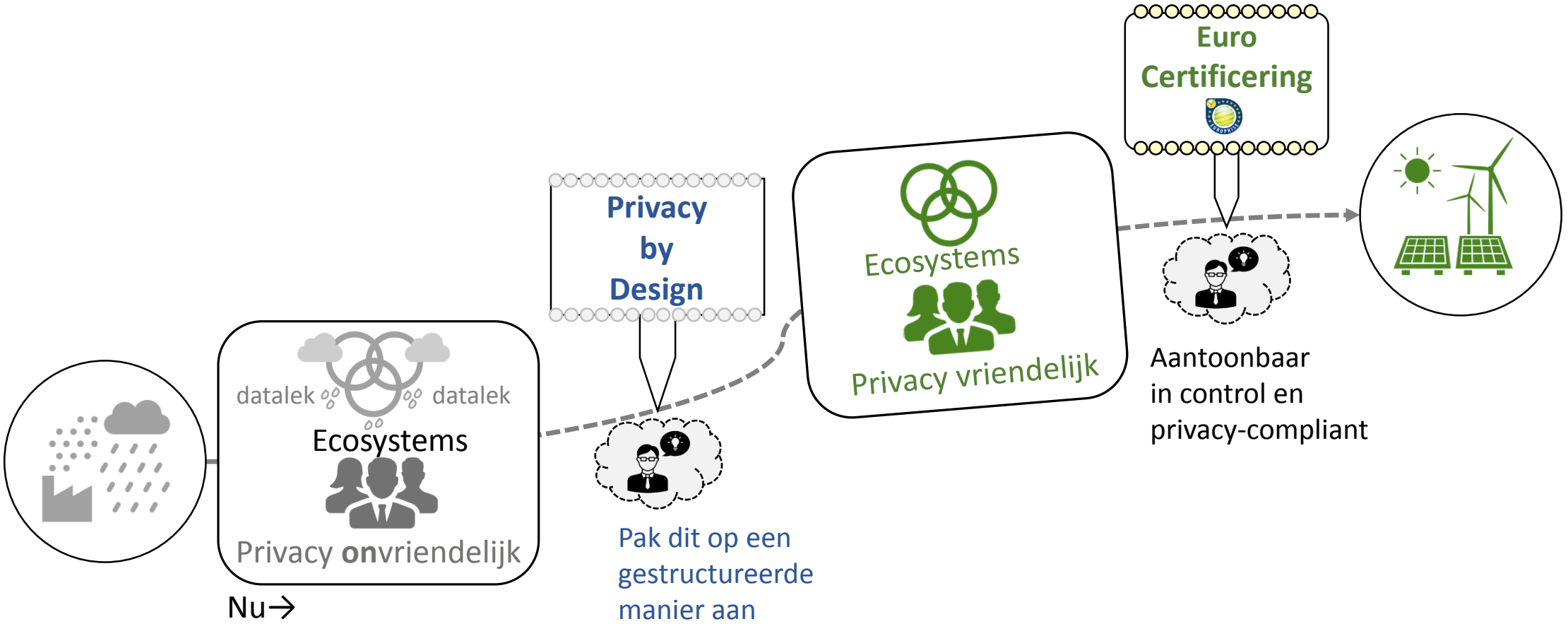
Privacy in complexe ecosystemen | opvattingen

1) Elke organisatie moet van een privacy onvriendelijke in een privacy vriendelijke organisatie veranderen
2) Certificering wordt noodzakelijk



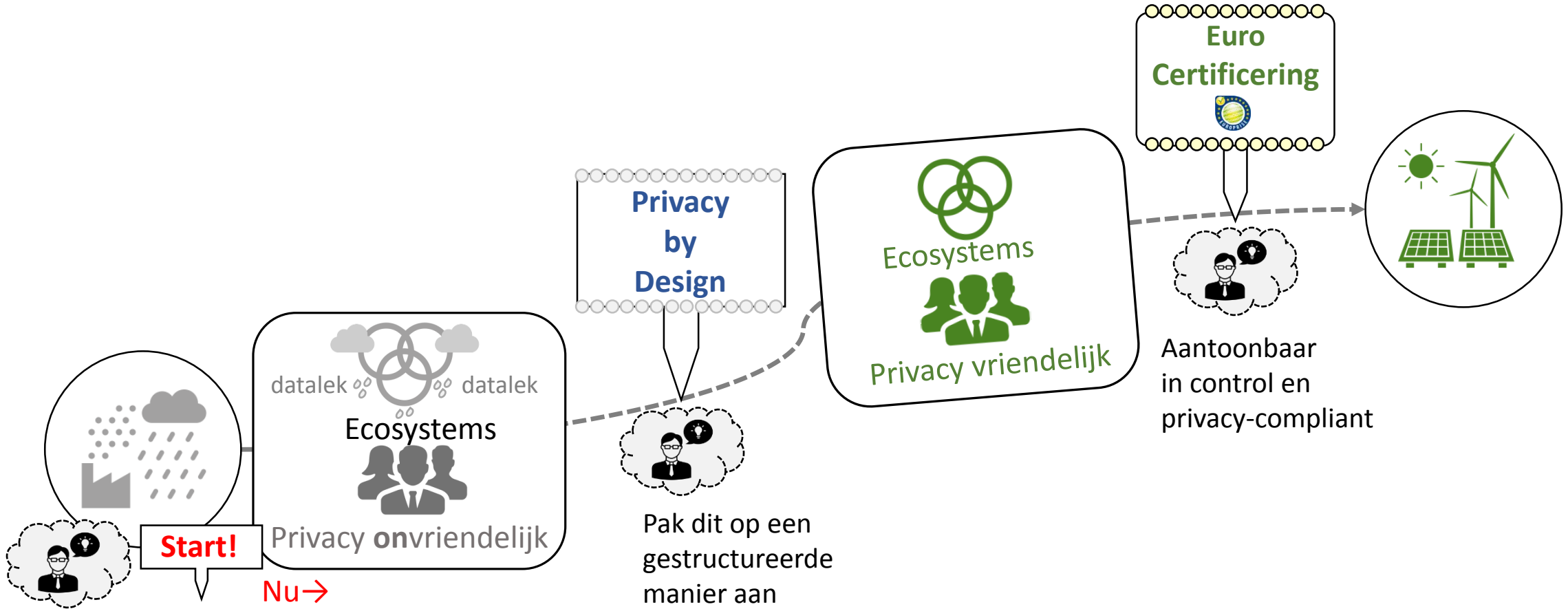
Privacy in complexe ecosystemen | opvattingen

1) Elke organisatie moet van een privacy onvriendelijke in een privacy vriendelijke organisatie veranderen
2) Certificering wordt noodzakelijk
3) Zonder Privacy by Design gaat dit niet lukken



Privacy in complexe ecosystemen | opvattingen

1) Elke organisatie moet van een privacy onvriendelijke in een privacy vriendelijke organisatie veranderen
2) Certificering wordt noodzakelijk
3) Zonder Privacy by Design gaat dit niet lukken
4) Start nu!



Privacy in complexe ecosystemen

De reden om nu te starten! | De Europese Algemene Verordening Gegevensbescherming (AVG)

= General Dataprotection Regulation (GDPR)

Gepubliceerd op 4 mei 2016 | Inwerkingtreding 24 mei 2016 | **Handhaving op 25 mei 2018**

De GDPR vereist onder anderen:

- Functionaris gegevensbescherming
- Privacy Impact Assessment (PIA)
- Privacy-by-design (PbD) *en* by-default

Sancties bij een datalek

- tot 20 000 000 Euro
- tot 4% van de wereldwijde jaaromzet van een concern

Definities

- Privacy Impact Assessment: PIA
  - Een proces dat de impact op privacy evalueert
- Privacy-by-design: PbD
  - Institutionalisering van privacy management
  - Integratie van privacy concerns in het ontwerp en de realisatie van systemen
- Privacy-by-default
  - Het hoogste niveau van privacy is de standaardinstelling (by default)

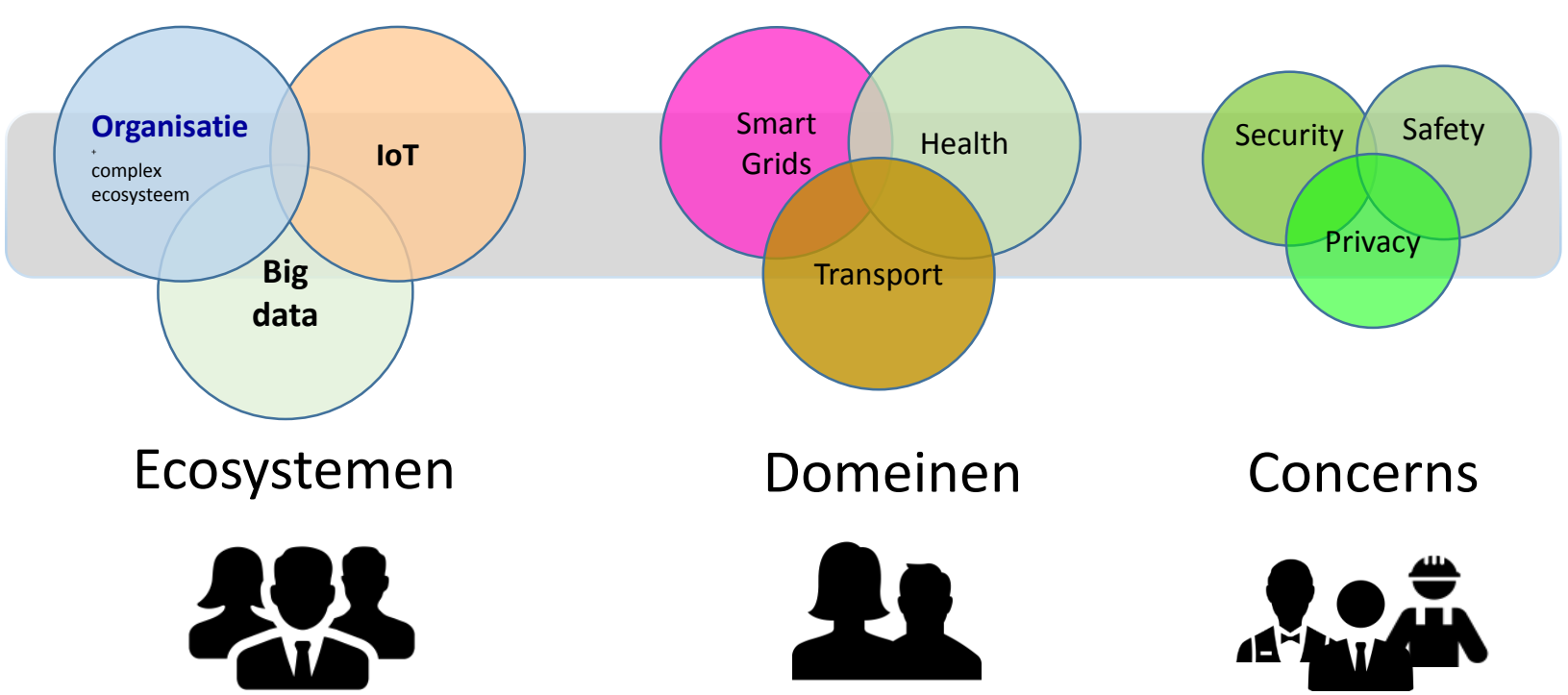
Voer een initiële Privacy impact assessment uit

Verdiep je in wat Privacy by design en Privacy by default inhoudt

Hint: GDPR gebruikt "gegevensbescherming" in plaats van "privacy"

Privacy in complexe ecosystemen

Een organisatie met een complex ecosysteem:
- Integreert business domeinen, zoals smart grid, gezondheid, transport
- Integreert concerns, privacy, security en meer, bijvoorbeeld safety



Voorbeelden van dergelijke organisaties:
- *(Smart) cities*
- *Ziekenhuizen*
- *Luchthavens*
- *Zeehavens*
- *Winkelcentra*
- *Banken*
- *Verzekeraars*
- *Retailbedrijven*
- *Treinstations*

Privacy in complexe ecosystemen

Voorbeeld: camera's die zijn verwerkt in reclamezuilen op treinstations.

Nederlandse Spoorwegen

Exploiteert, ontwikkelt en beheert treinstations

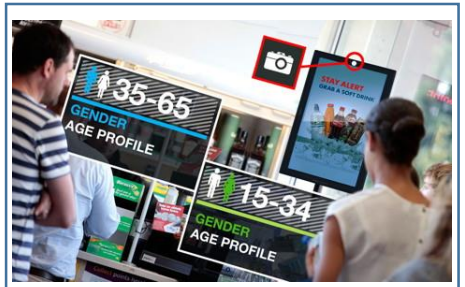
Heeft een exclusieve samenwerking met..

Exterion Media

Plaatst reclamezuilen die zijn uitgerust met camera's die analyseren wie een reclamezuil bekijkt

Neemt camera's en software af van..

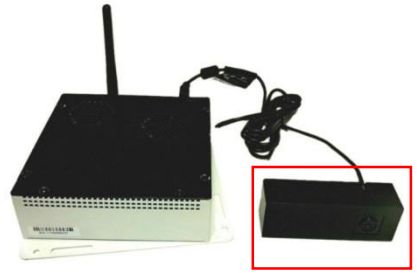
Quividi



Levert camera's en de bijbehorende software om te kunnen bijhouden hoeveel mensen naar de boodschap op een bord hebben gekeken en hoe lang.
Op grond van de kenmerken van de gezichten kan het systeem statistieken aanleggen waarin ook het geslacht en de leeftijd van de kijkers een rol spelen. Ook het ras kan worden vastgesteld.

Laat camerasystemen produceren bij..

Assemblagebedrijf



Assembleert camerasystemen, inclusief de software

Neemt componenten af van..

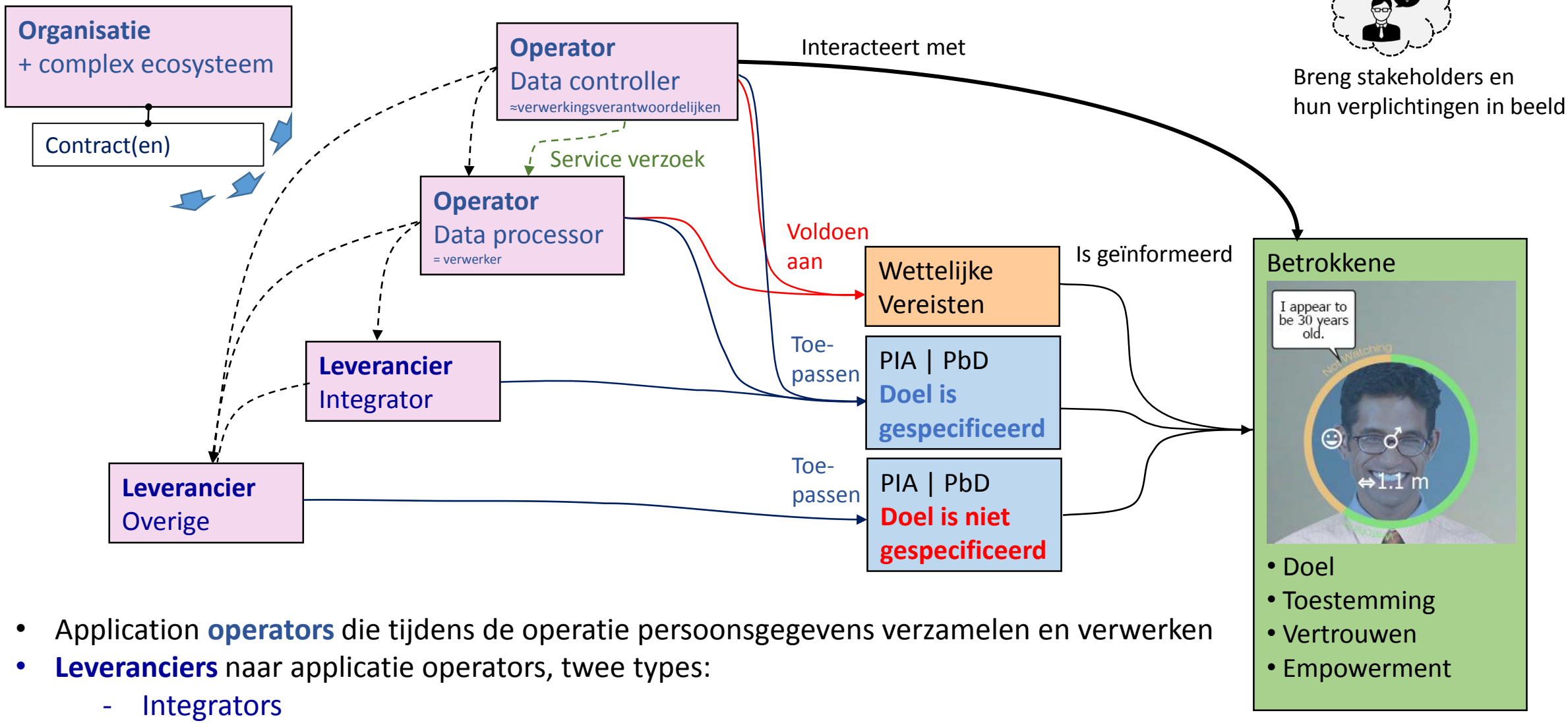
Leverancier

Levert componenten voor de dataopslag, inclusief software voor dataversleuteling

Neemt componenten af van..

Stakeholders in een complex ecosystem

Verplichtingen van de stakeholders moeten bekend zijn



Breng stakeholders en hun verplichtingen in beeld

- Application **operators** die tijdens de operatie persoonsgegevens verzamelen en verwerken
- **Leveranciers** naar applicatie operators, twee types:
  - Integrators
  - Leveranciers aan de integrators (overige)

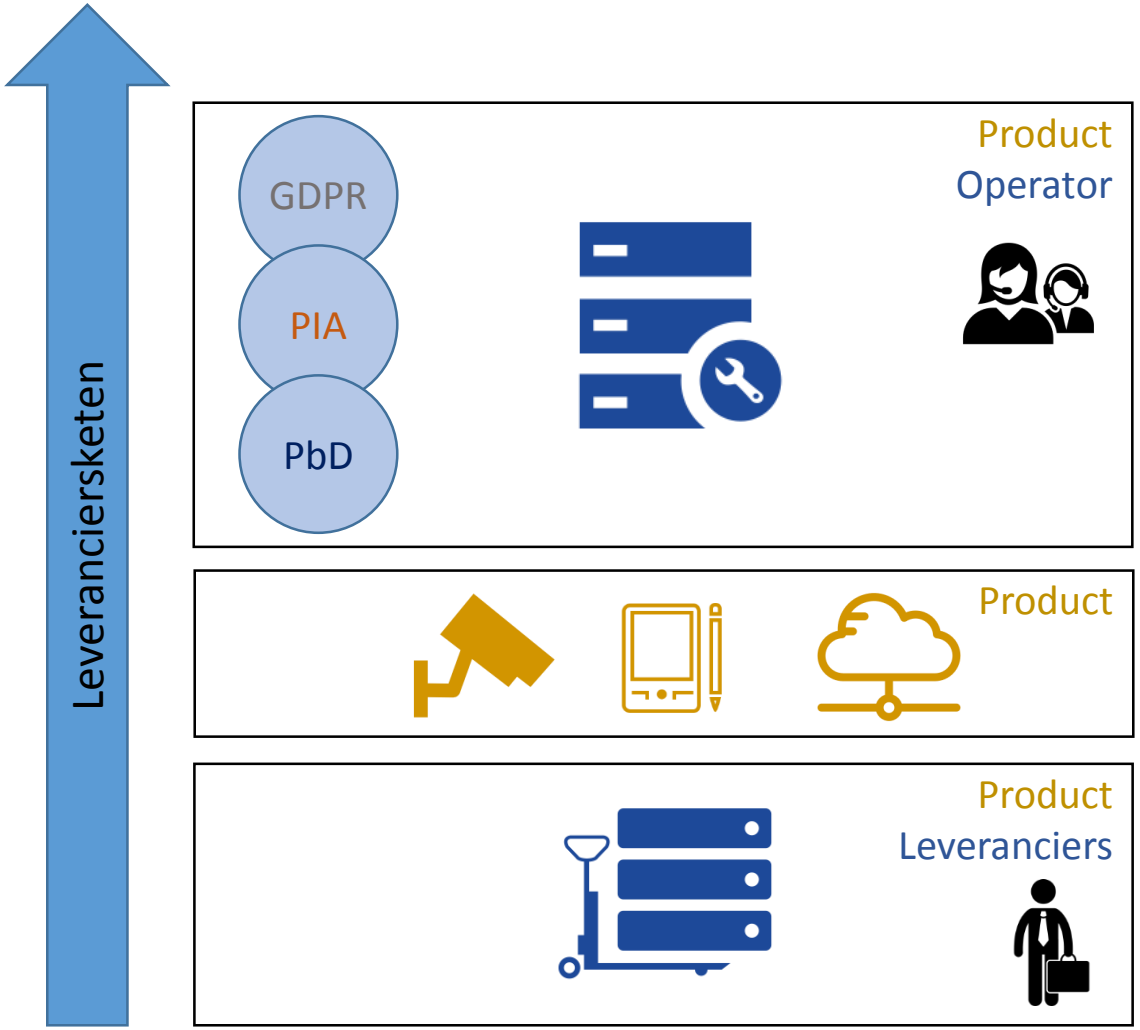
Privacy concerns van stakeholders

Stakeholder		Legal Compliance niveau	Management niveau	System Lifecycle niveau
Vraag zijde	Beleids-maker	Compliance		+ Compliance Check
	Operator Data Controller	Compliance requirements Regels	Compliance Requirements Privacy Impact Assessment	Compliance Requirements Privacy-by-Design
	Operator Data Processor	GDPR	PIA	PbD
Aanbod zijde	Leverancier	Operators requirements		

Breng stakeholders en hun concerns in beeld

- Het concern van de beleidsmaker is om overall compliant te zijn
- De concerns van de operators zijn
  (1) voldoen aan regels,
  (2) het juist uitvoeren van een PIA proces vanuit management perspectief, en
  (3) het juist uitvoeren PbD proces vanuit een systeem lifecycle perspectief.
- Het concern van de leverancier is het voldoen aan de operators requirements

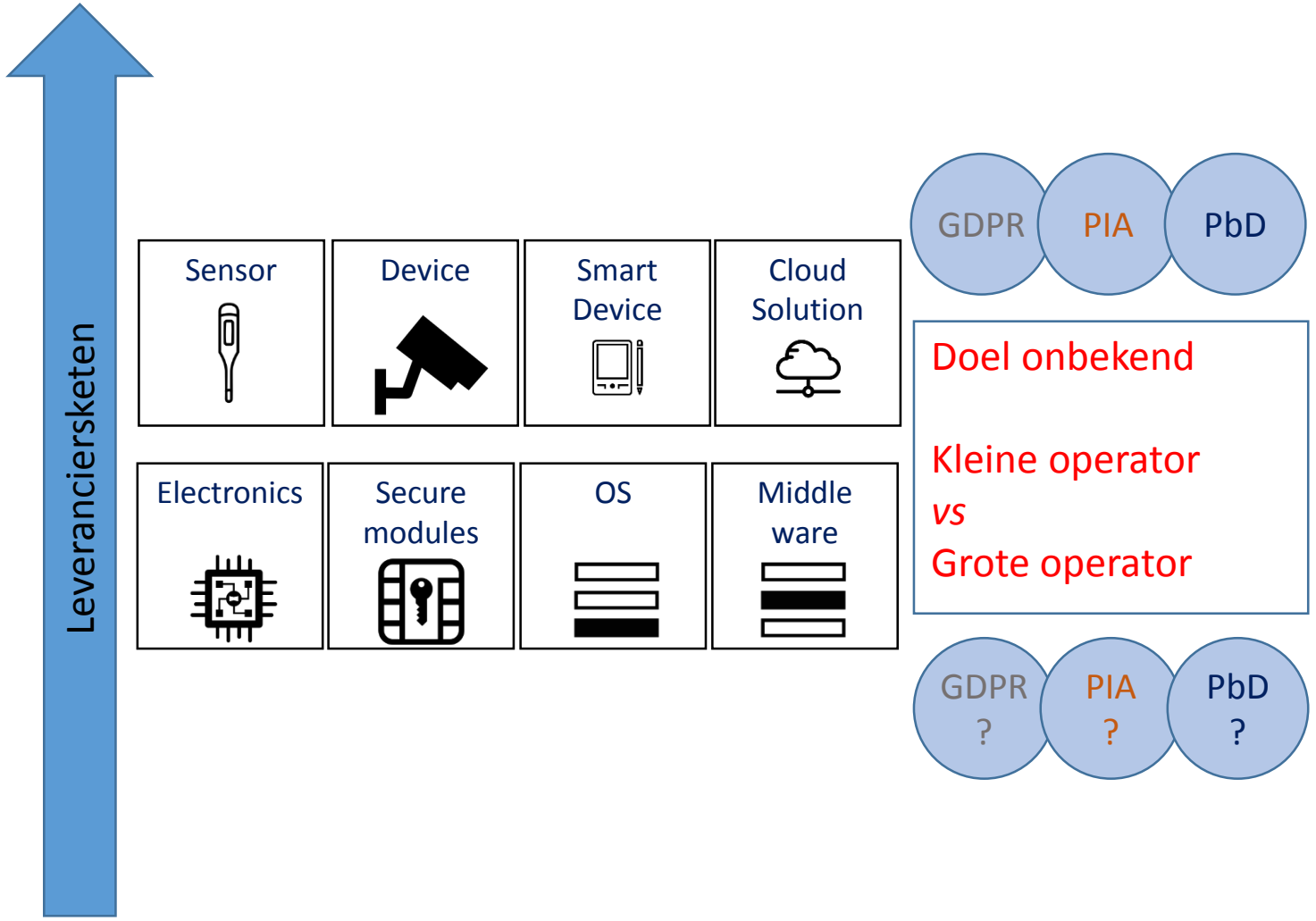
Operators versus leveranciers



Concerns van de operator
–Data controller en data processor verplichtingen in gegevensverwerkingsketen

Concerns van een leverancier?
–Voldoen aan de eisen in markt

Concerns van de leverancier

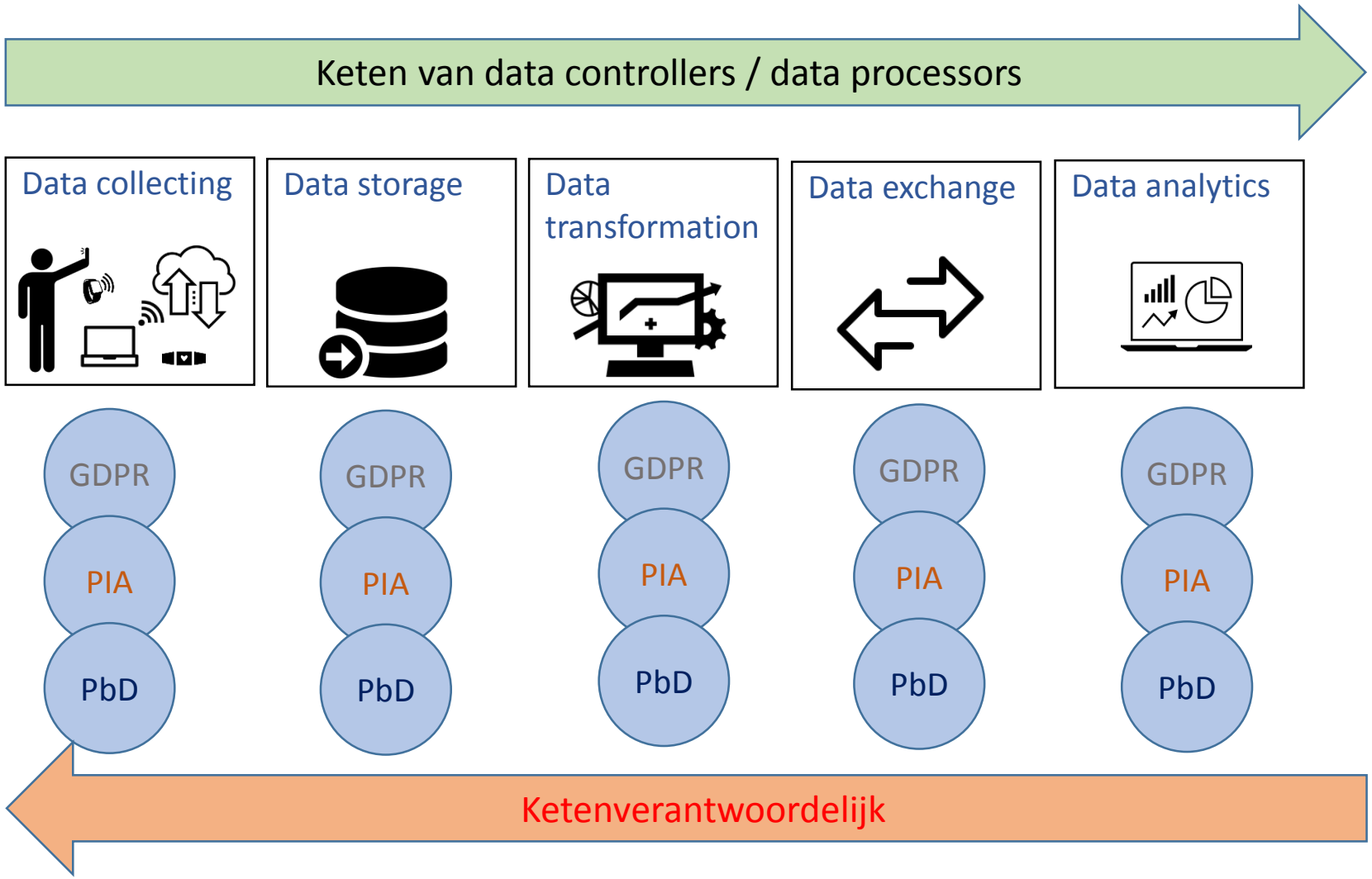


- Er is een breed spectrum van leveranciers
  - Eindproducten als sensoren, devices, smart devices, cloud oplossingen
  - Componenten als electronica, security modules, operating systems, middleware
- Het doel om gegevens te verzamelen en te verwerken is niet bij de leverancier bekend, tenzij het een maatsysteem wordt geleverd.
- In potentie is er onbalans tussen Grote leveranciers en kleine leveranciers.

Privacy in gegevensverwerking keten

Concerns aan de vraagzijde

Breng ketens in beeld



Een organisatie zal een keten van verantwoordelijkheden moeten beheren, van individuele operator naar zichzelf, als de uiteindelijk verantwoordelijke stakeholder

Normen, standaarden en referentiemodellen

- Principes
  - Ann Cavoukian seven's principles
  - ISO 29100 privacy framework
  - PRIPARE Principles
- Impact assessment
  - ISO 29134 privacy impact assessment (in ontwikkeling)
  - Data Protection Authority richtlijnen (Verenigd Koninkrijk., Frankrijk, Spanje, …)
  - Domein specifieke richtlijnen (Smart grid, Biometrics, Rfid, Cloud…)
- Engineering
  - De hele lifecycle
    - PRIPARE methodology handbook — Input voor
    - ISO 27550 Privacy Engineering (een nieuw ISO work item) ←
  - Risk management
    - CNIL PIA methodology
    - NISTIR 8062 Privacy Risk Management Framework for Federal Information Systems
  - Van requirements naar privacy maatregelen
    - ISO 29151 personally identifiable information privacy control (in progress)
    - OASIS Privacy management reference model

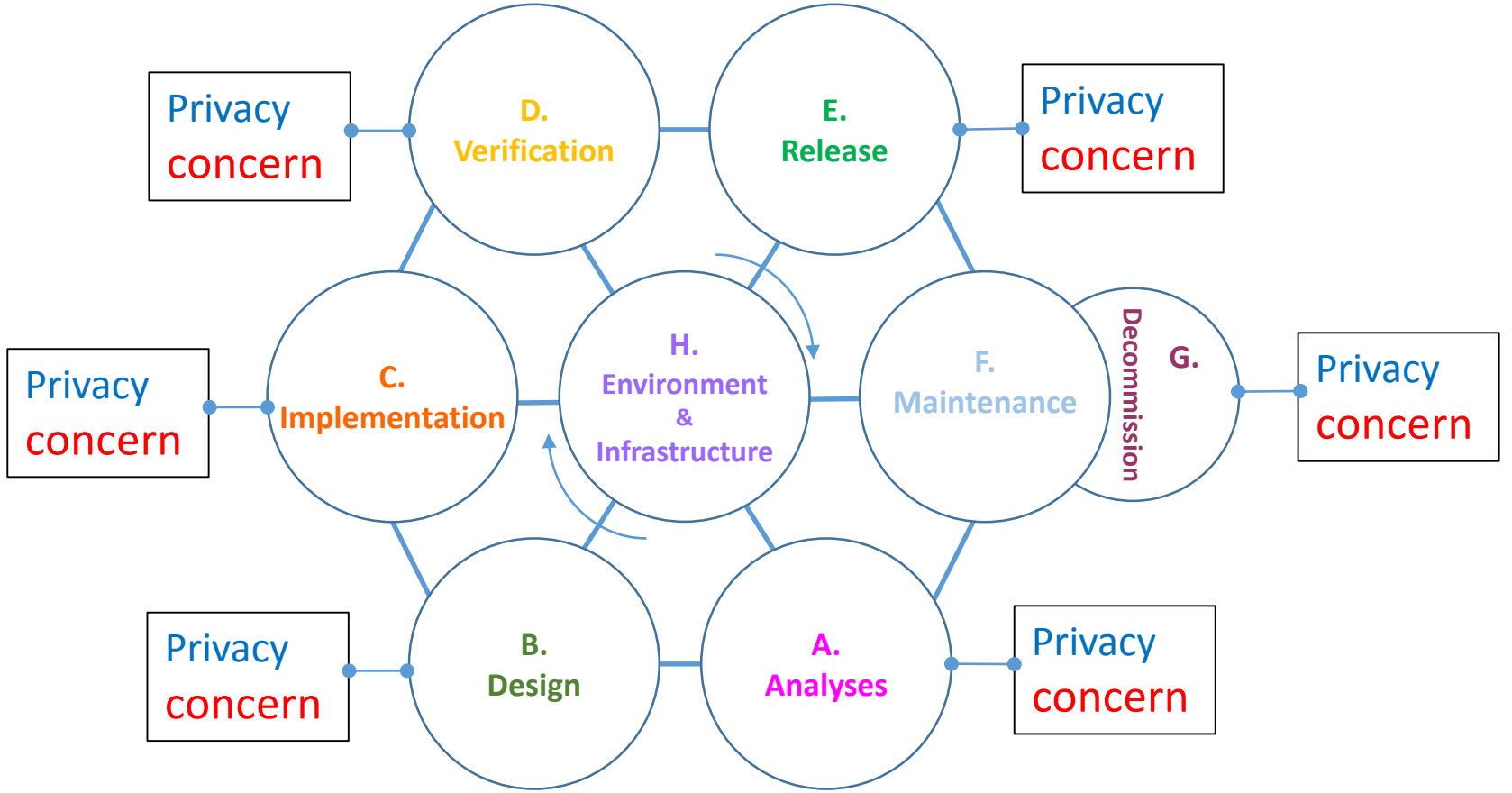
Verdiep je in de beschikbare normen standaarden en referentiemodellen

Bepaal wat relevant en bruikbaar is voor jouw organisatie

De PRIPARE methodologie helpt een organisatie bij de inrichting van een Privacy by design practice

PRIPARE | Privacy and security by design Methodology

Het PRIPARE Handbook harmoniseert en integreert de bestaande normen, praktijken en onderzoeksvoorstellen ten aanzien privacy-engineering

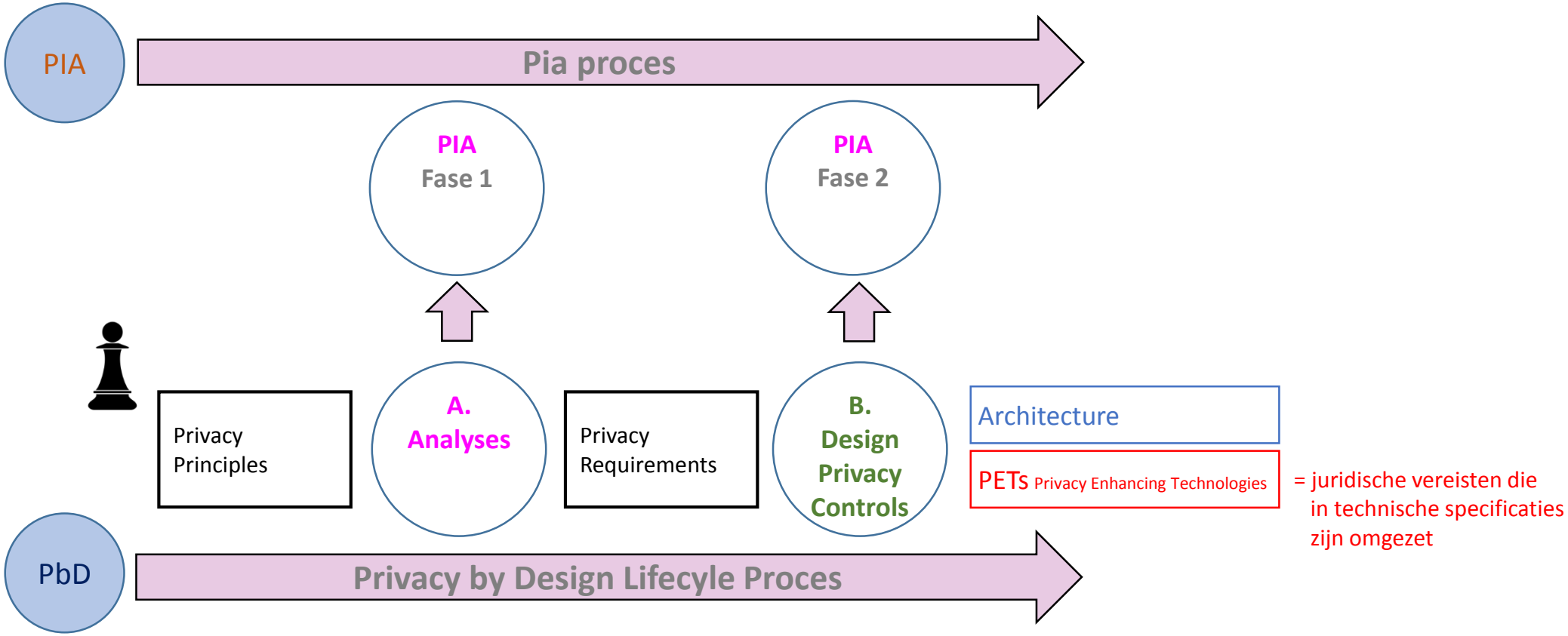


≈

Het kan worden vergeleken met een bedelarmband Per schakel kan voor een eigen invulling worden gekozen.

PRIPARE is gestructureerd in zeven verschillende fasen die overeenkomen met veel toegepaste en ook klassieke systeemontwikkelfaseringen, waardoor eenvoudig te combineren is met de meest toegepaste systeemontwikkelaanpakken of aan normen zoals ISO 15288

PRIPARE | Privacy and security by design Methodology | toelichting



Integratie van het Privacy Impact Assessment proces in het Privacy by Design proces

PRIPARE | Privacy and security by design Methodology | toelichting

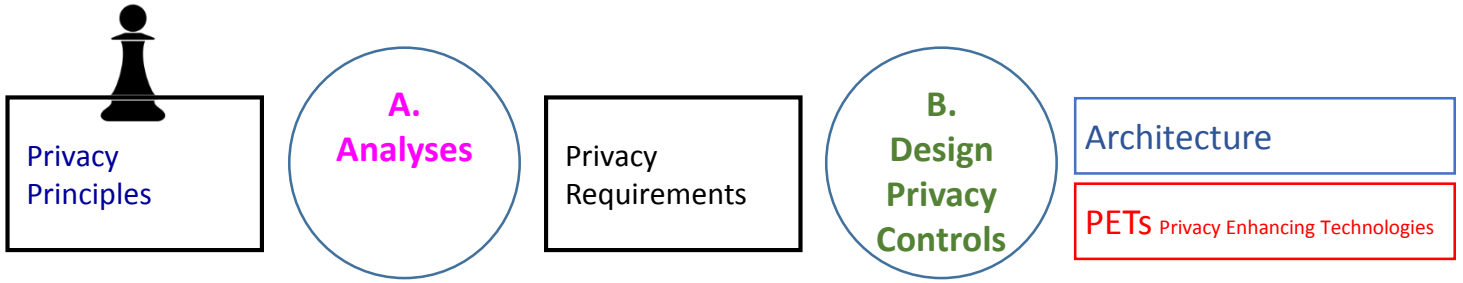
Kies voor een standaard principeverzameling

Seven principles from Ann Cavoukian
1. Proactive not reactive
2. Privacy as default setting
3. Privacy-by-design
4. Positive sum
5. Security
6. Transparency
7. User-centric

ISO 29100 – privacy framework
1. Consent and choice
2. Purpose
3. Collection limitation
4. Data minimization
5. Use limitation
6. Accuracy and quality
7. Openness/transparency/notice
8. Individual participation and access
9. Accountability
10. Security

PRIPARE Principles
1. Data quality
2. Data minimisation / proportionality
3. Purpose specification and limitation
4. Purpose specification and limitation for sensitive data
5. Transparency principle / openness principle
6. Right of access
7. Right to object
8. Safeguarding confidentiality and security of processing
9. Compliance with notification requirements
10. Conservation or retention principle
11. Accountability
12. Right to erasure
13. Privacy by default / data protection by default
14. Privacy by design / Data protection by design

→Afgeleid uit de GDPR

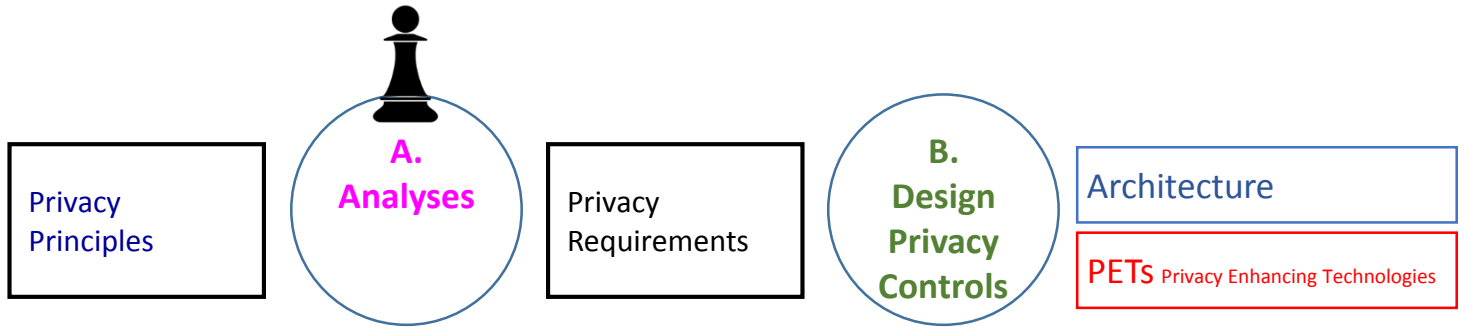


PRIPARE | Privacy and security by design Methodology | toelichting

Identificeer privacyregels en privacy management requirements

OASIS

PMRM	Service	Purpose
Privacy Management Reference Model and Methodology	Agreement	Management of permissions and rules
	Usage	Controlling personal data usage
	Validation	Checking personal data
	Certification	Checking stakeholders credentials
	Enforcement	Monitor operations and react to exceptions / accountability
	Security	Safeguard privacy information and operations
	Interaction	Information presentation and communication
	Access	Data subject access to their personal data



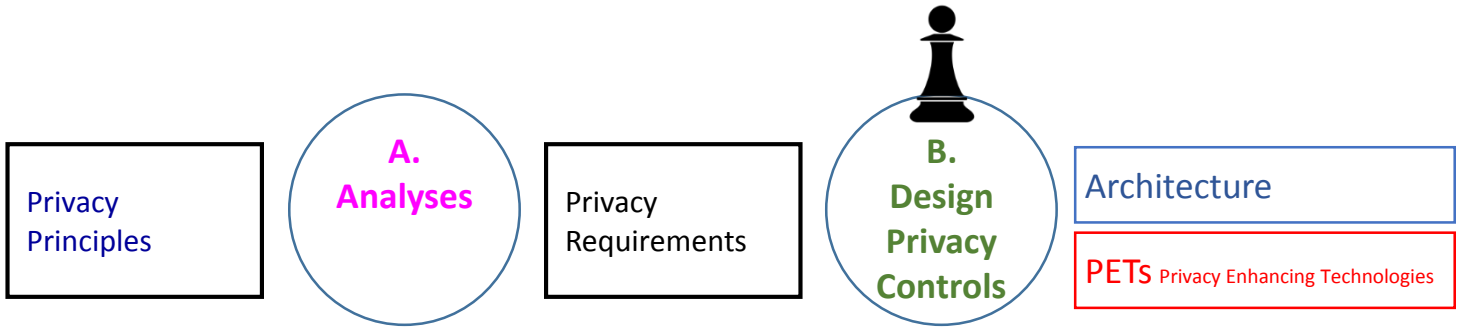
PRIPARE | Privacy and security by design Methodology | toelichting

Design Strategies

PI.lab

Jaap Henk Hoepman Design strategies	
1 Minimization	Select collecting, anonymisation / pseudonyms
2 Hide	Encryption of data, mix networks, hide traffic patterns, attribute based credentials , anonymisation / pseudonyms
3 Separate	Partitioning
4 Aggregate	Aggregation over time, dynamic location granularity, k-anonymity, differential privacy
5 Inform	Platform for privacy preferences, Data breach notification
6 Control	User centric identity management, end-to-end encryption support control
7 Enforce	Access control, Sticky policies and privacy rights management
8 Demonstrate	Privacy management systems, use of logging and auditing

attribute based credentials | uitgewerkt in voorbeeld →



PRIPARE | Privacy and security by design Methodology | toelichting

Design strategieën kunnen aanpassingen op requirements tot gevolg hebben

PI.lab

Principe = Dataminimalisatie

Oorspronkelijke requirement

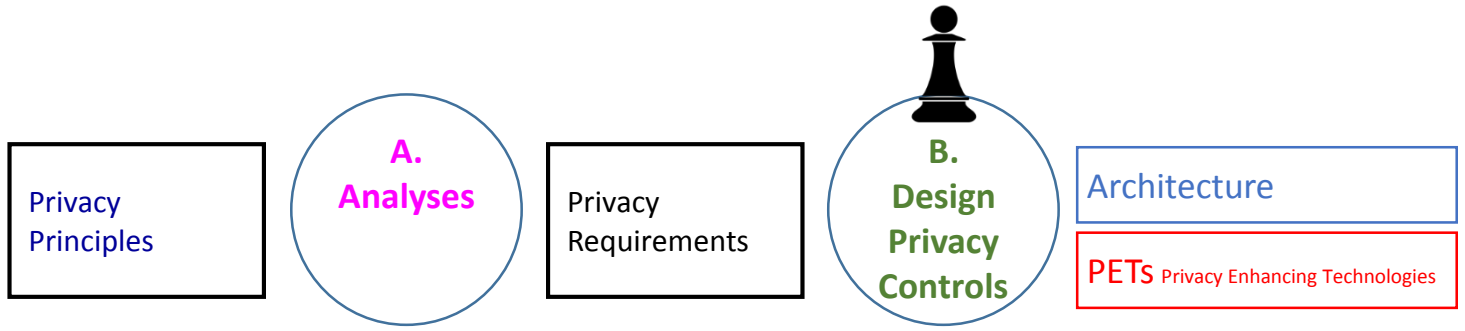
→Verzamel geboortedatum

B. Design Privacy Controls

Attribute-based credentials

→Verzamel geen geboortedatum

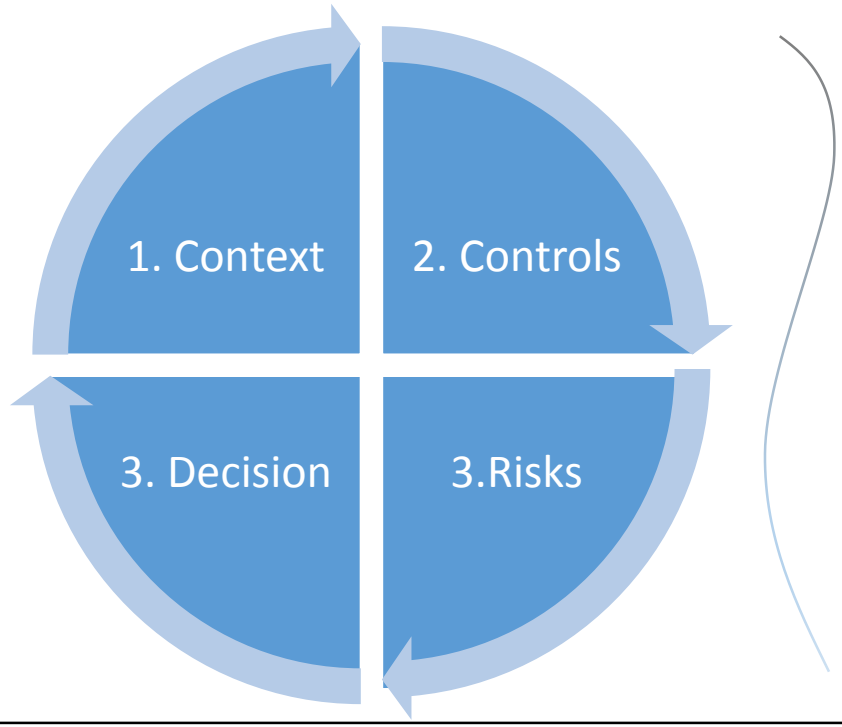
→Voer een toets : > 18 jaar oud



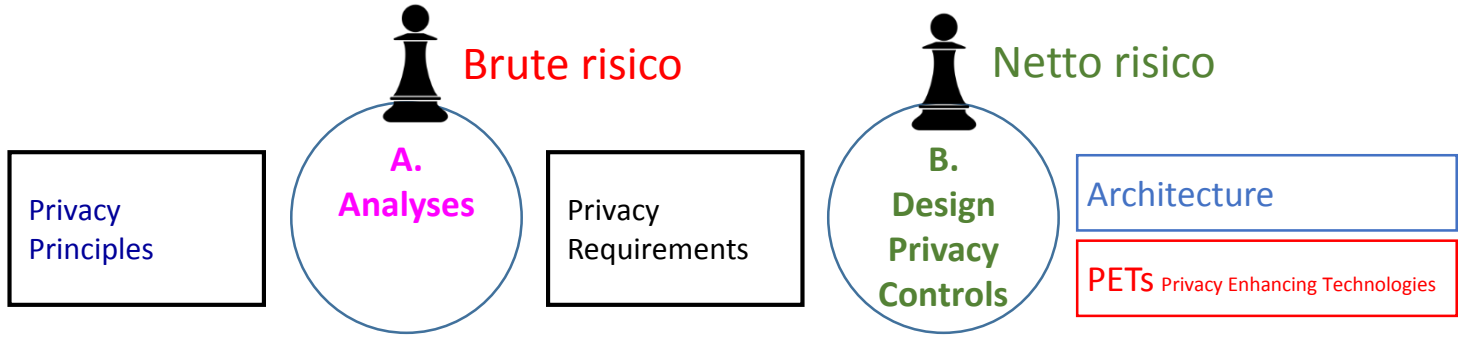
PRIPARE | Privacy and security by design Methodology | toelichting

Risk analysis (voorbeeld : CNIL risk analysis)

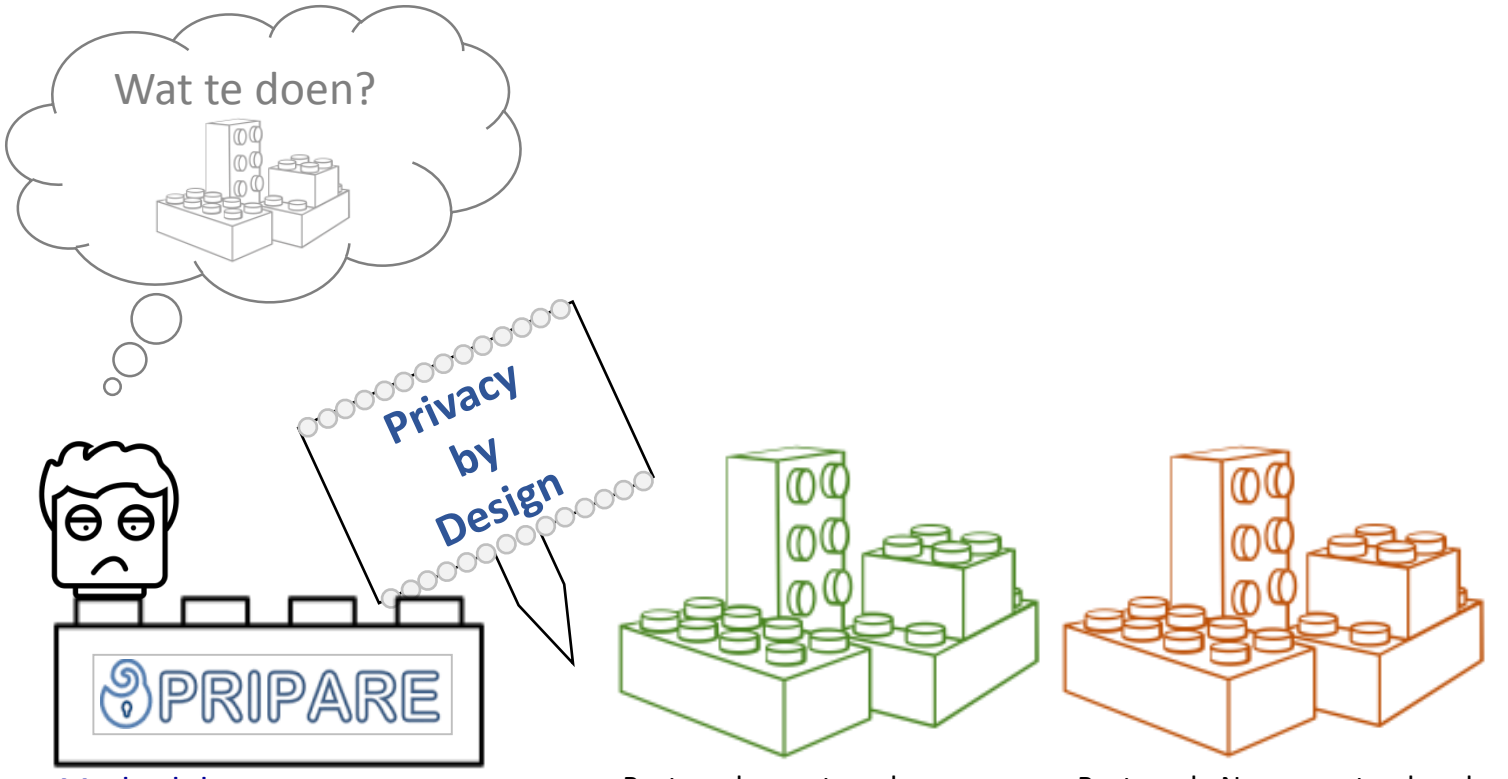
CNIL.



Maximum Severity	Must be Avoided or reduces		Absolutely Avoided or reduces
Significant Severity			
Limited Severity	These risks may be taken		Must Be reduced
Negligible Severity			
	Negligible Likelihood	Limited Likelihood	Significant Likelihood	Maximum Likelihood



PRIPARE | Privacy and security by design Methodology | wat te doen

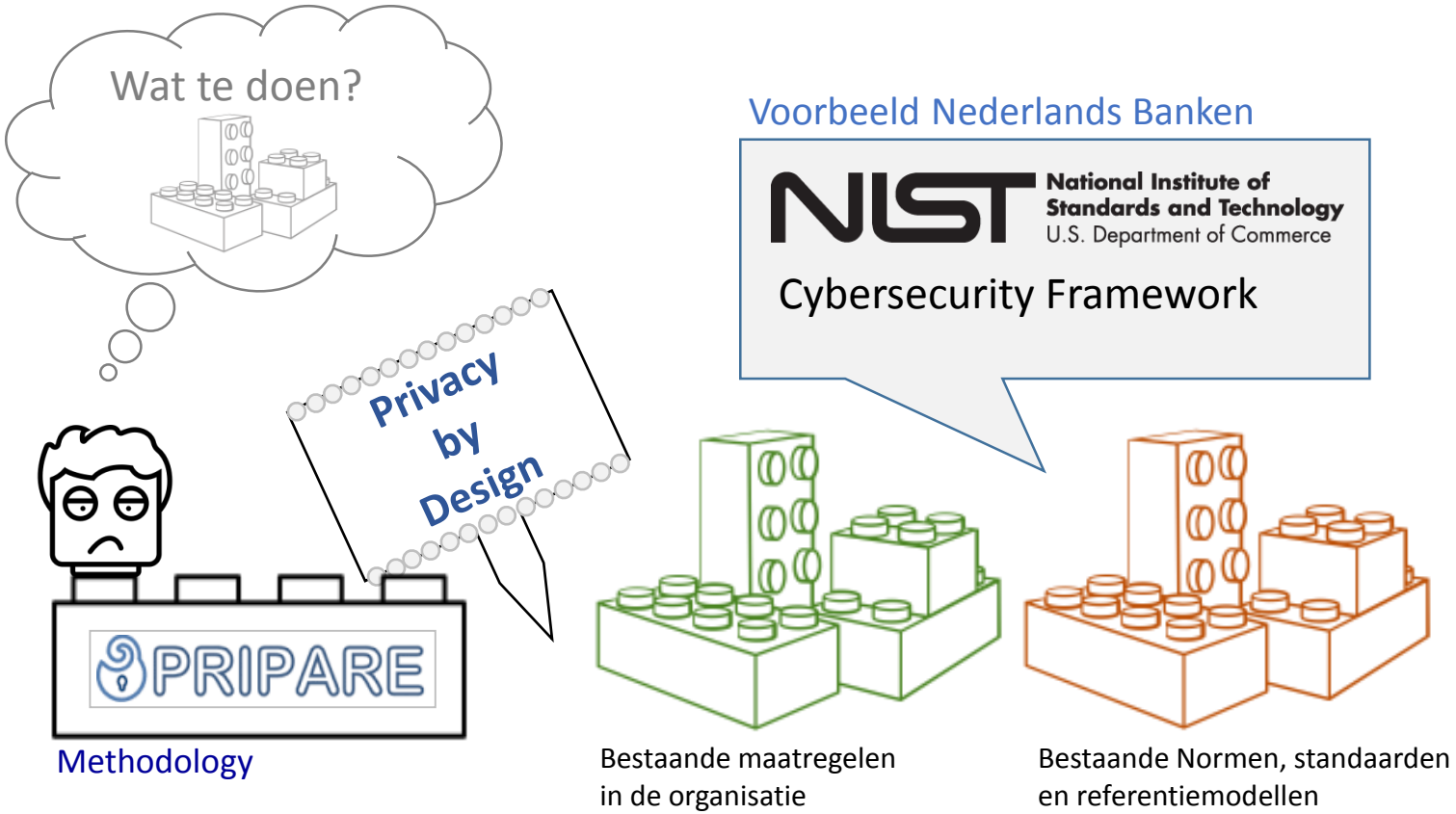


Methodology

Bestaande maatregelen
in de organisatie

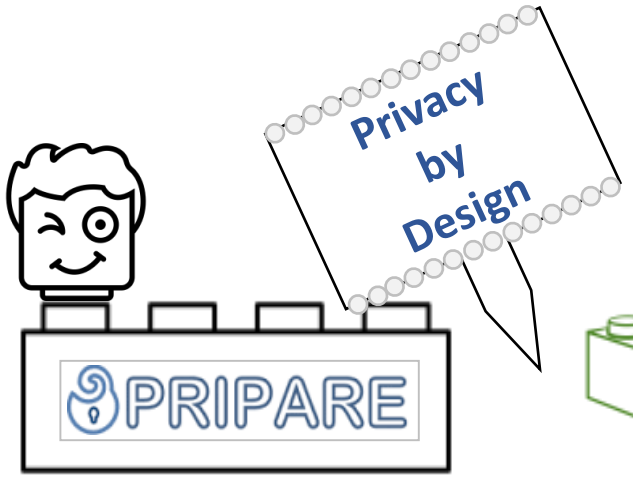
Bestaande Normen, standaarden
en referentiemodellen

PRIPARE | Privacy and security by design Methodology | wat te doen

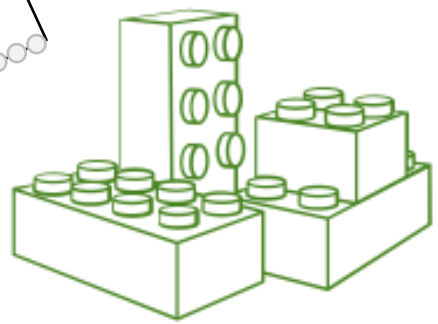


PRIPARE | Privacy and security by design Methodology | wat te doen

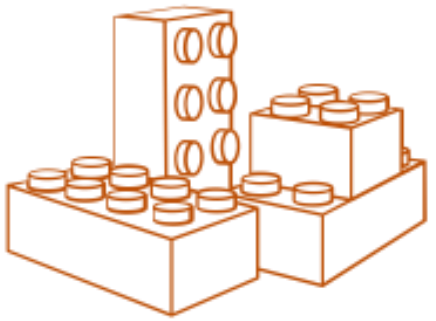
Volg de methode en kies bouwstenen die reeds bij de organisatie in gebruik zijn en vul deze aan met die standaarden en best practices, die het beste bij de organisatie passen.



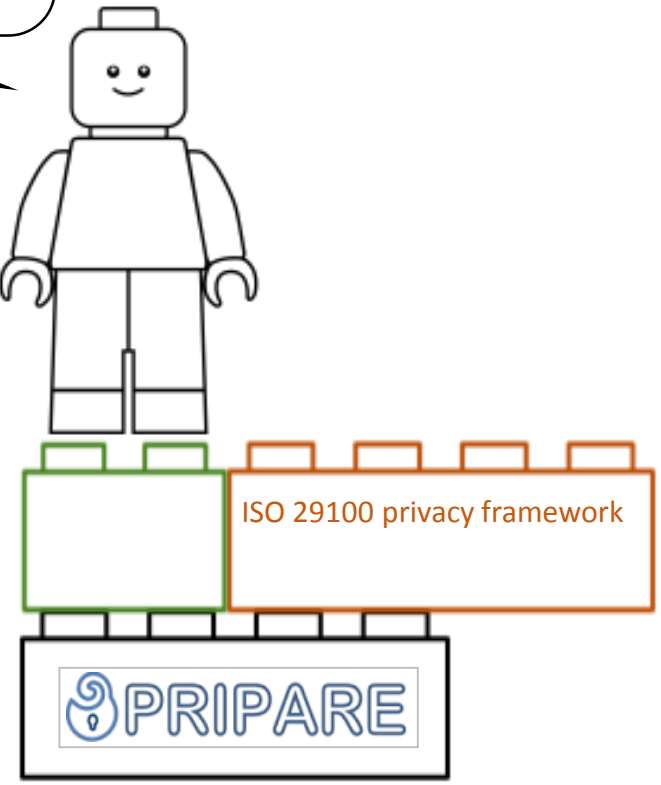
Methodology | raamwerk



Bestaande maatregelen
Binnen de organisatie

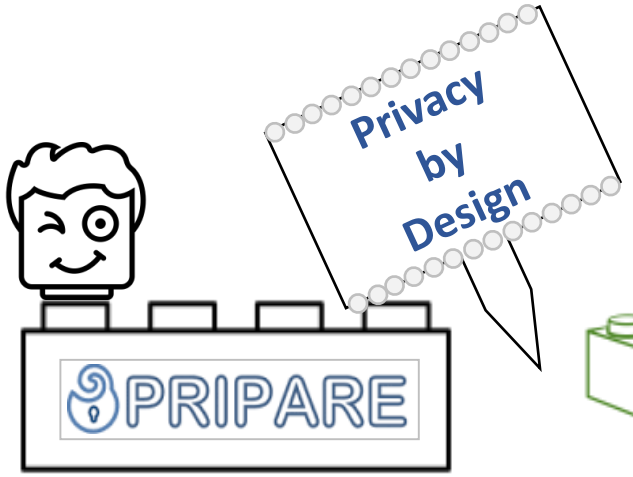


Bestaande Normen, standaarden
en referentiemodellen

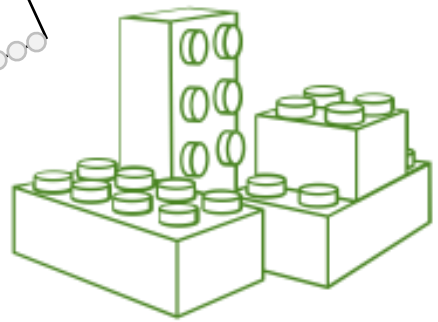


Methodology | bouwen

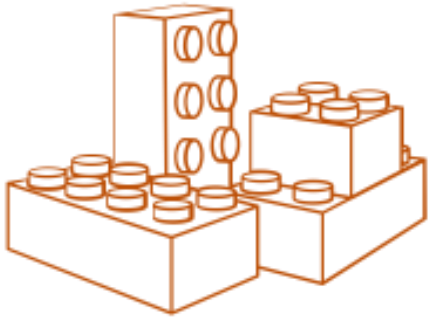
PRIPARE | Privacy and security by design Methodology | wat te doen



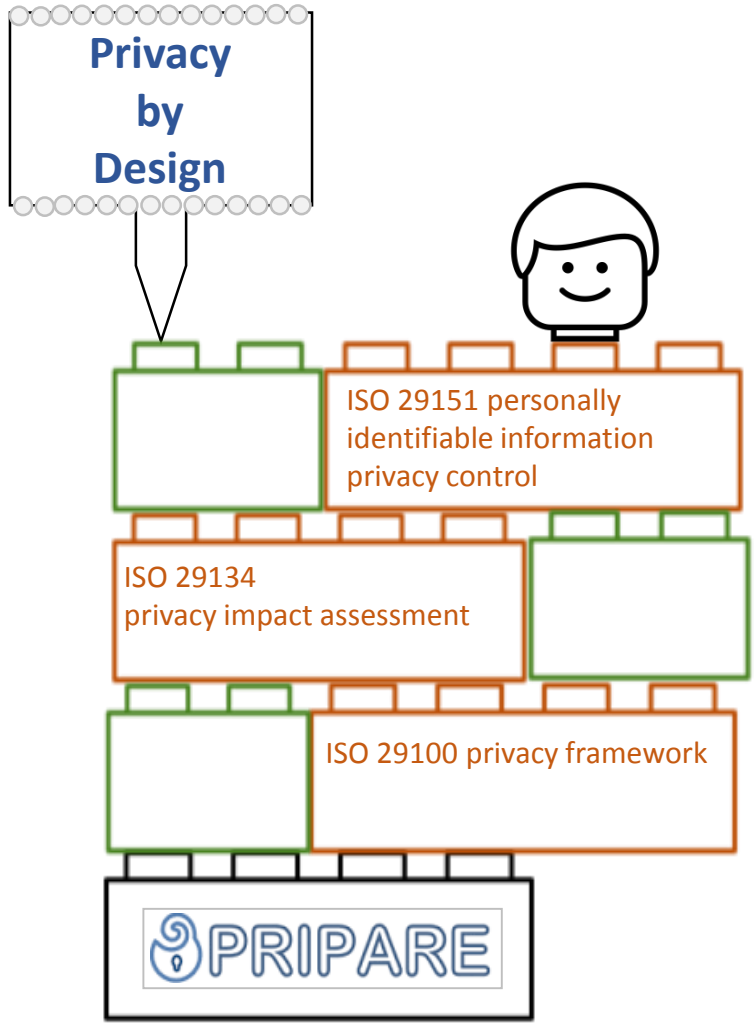
Methodology | raamwerk



Bestaande maatregelen
Binnen de organisatie

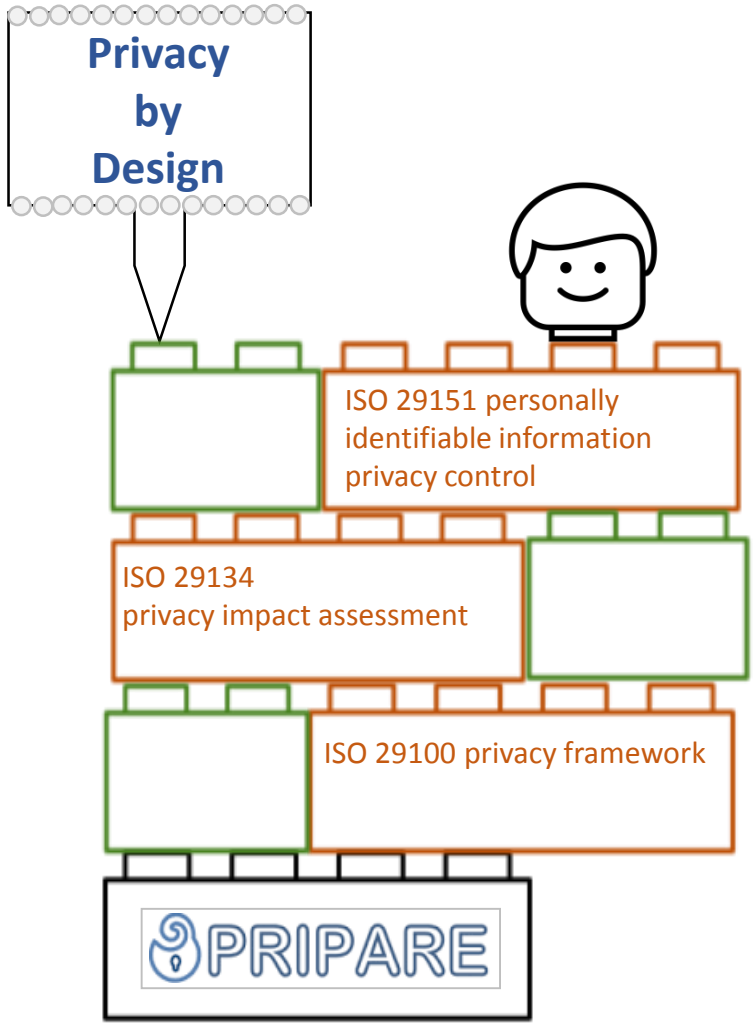


Bestaande Normen, standaarden
en referentiemodellen

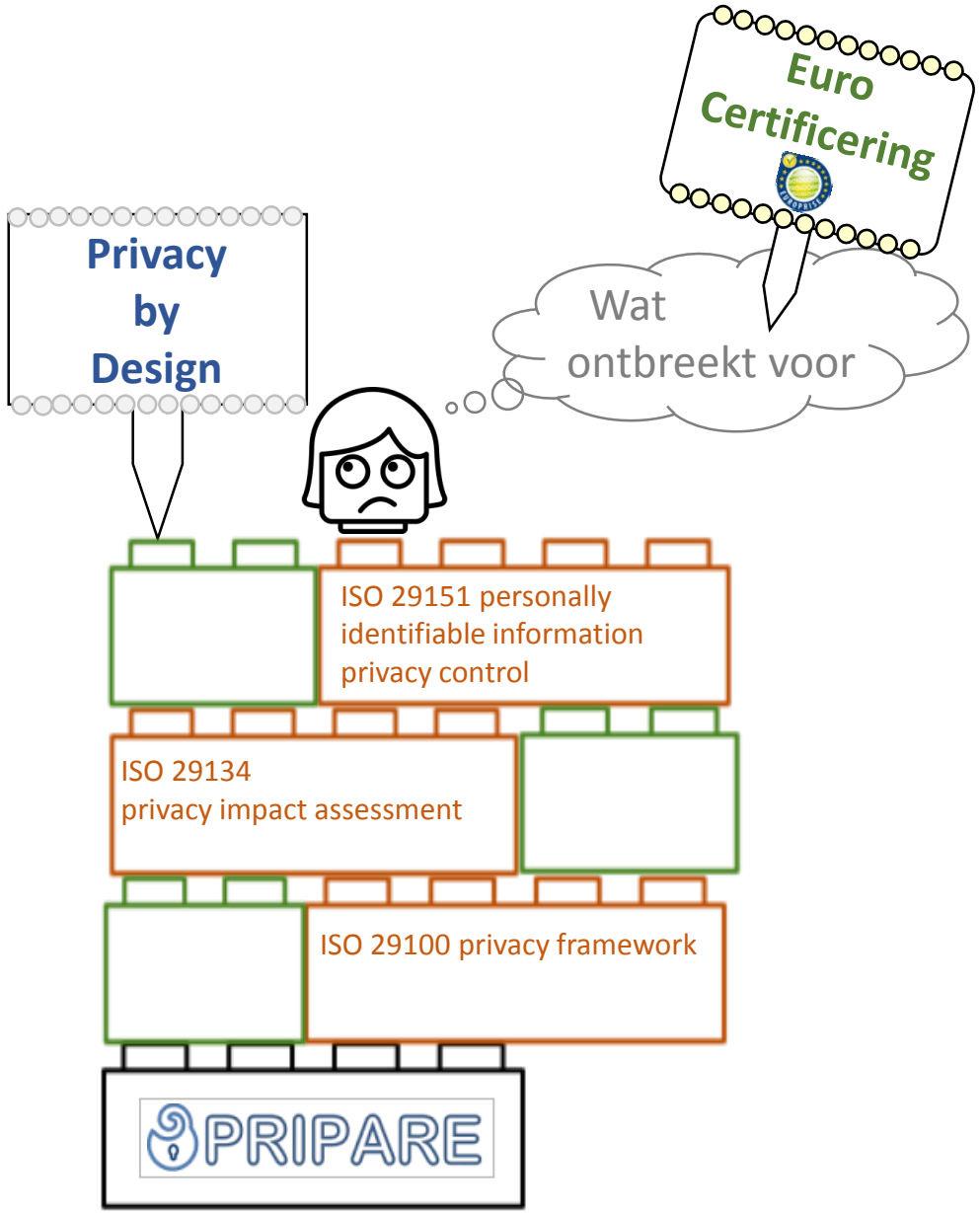


Methodology | gebouwd

PRIPARE ≠ Euro Certificering

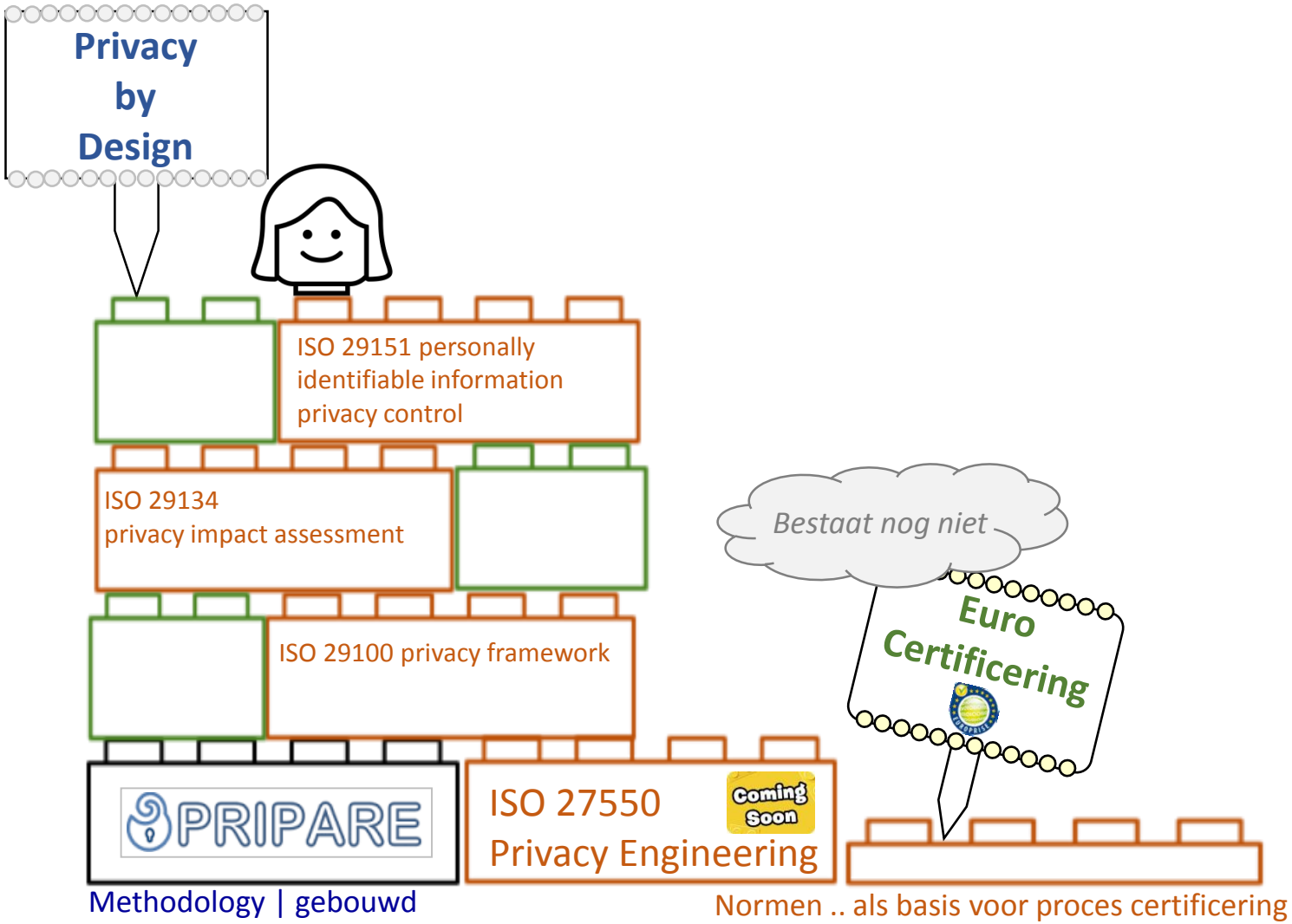


Methodology | gebouwd



Methodology | gebouwd

PRIPARE ≈ Euro Certificering van privacy processen



Euro Certificering van IT producten of IT gebaseerde services

Product of service certificering

EuroPriSe European Privacy Seal

The European Privacy Seal
By the EuroPriSe Certification Authority

Als voorbeeld wordt de werkwijze van de European Privacy Seal toegelicht

Euro Certificering van IT producten of IT gebaseerde services

Product of service certificering

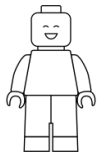
Erkende experts evalueren
Product of service

Een onpartijdige autoriteit
controleert de evaluatie

Toekenning
van de European Privacy Seal

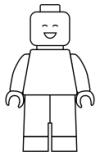
2 jaar geldig

Legal expert



EuroPriSe European Privacy Seal LEGAL EXPERT

Technical expert



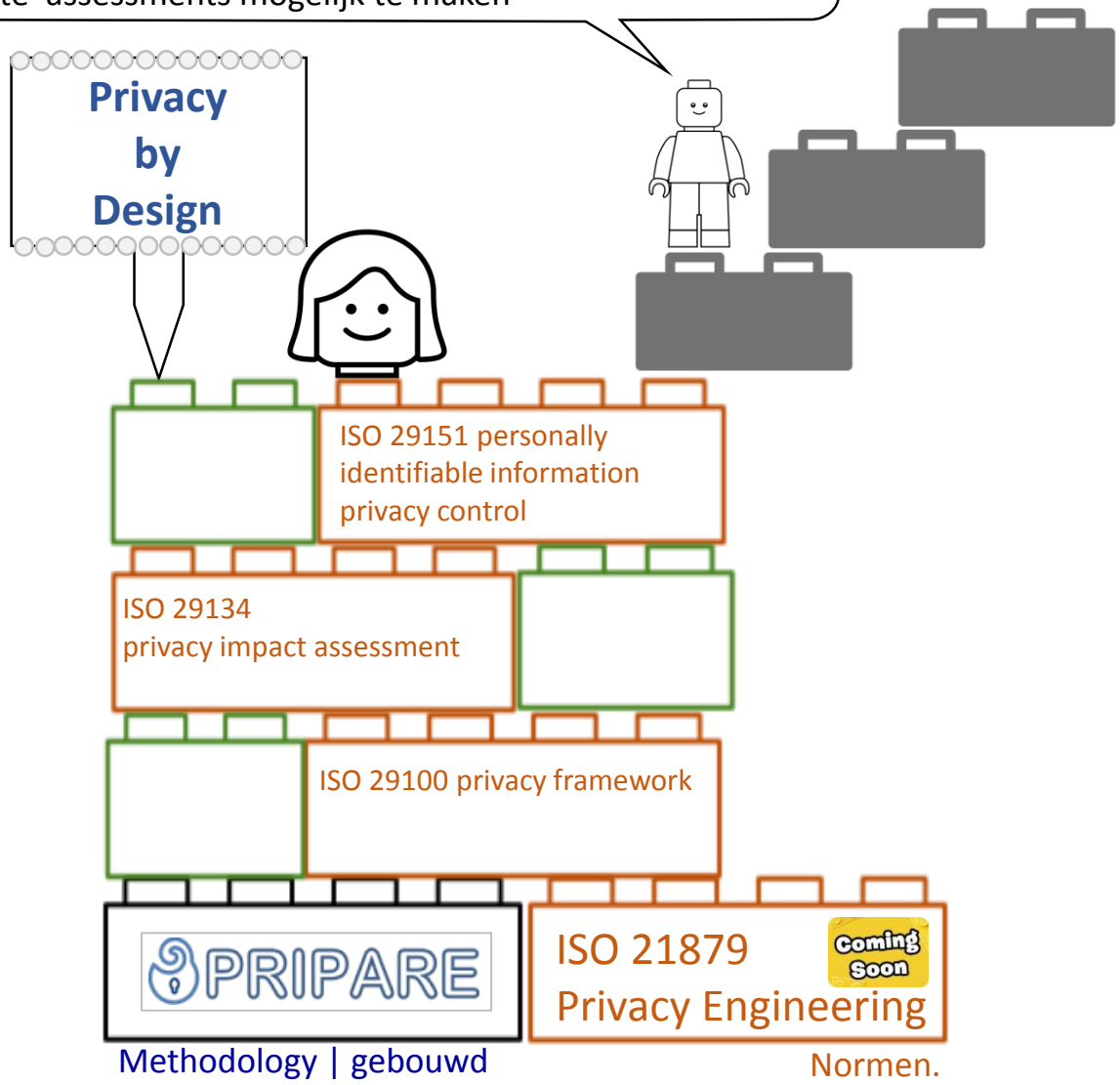
EuroPriSe European Privacy Seal TECHNICAL EXPERT

Voorbeelden:

- *European Privacy Seal for Siemens Healthcare GmbH)*
- *European Privacy Seal for Lidl's Central Cash Auditing (ZKP)*

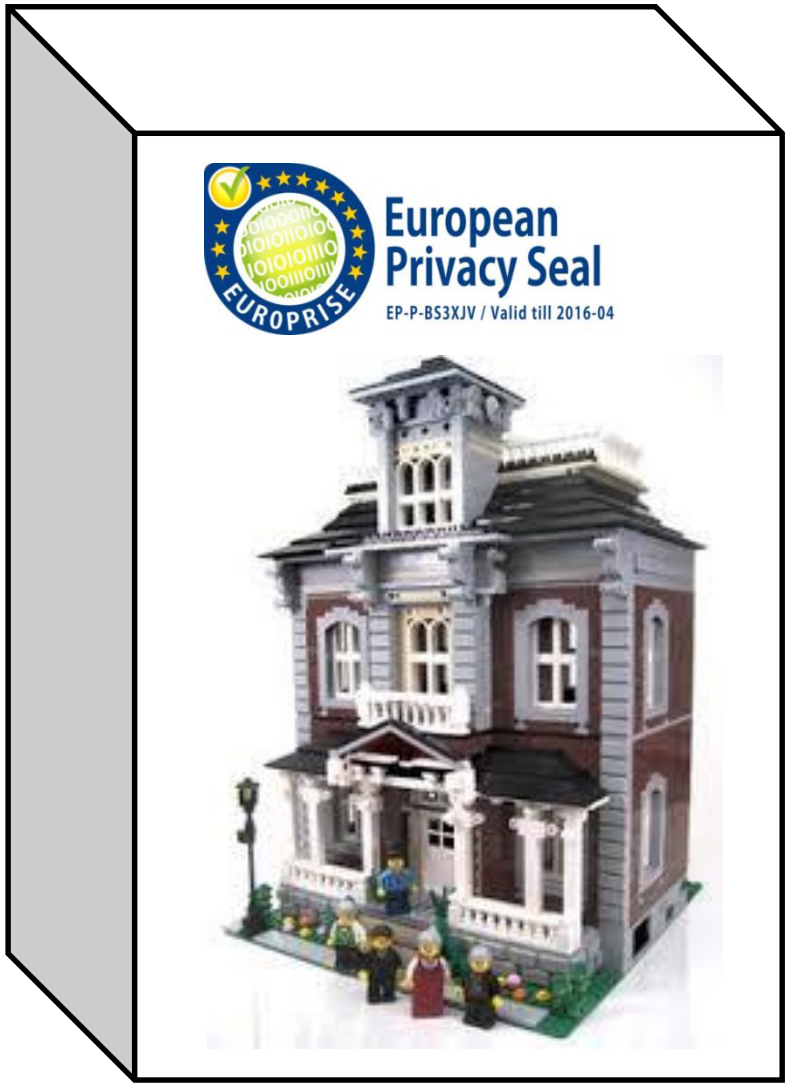
Euro Certificering van IT producten of of IT gebaseerde services

Privacy by Design helpt:
- om aan de normen van een euro certificering te gaan voldoen
- efficiënte assessments mogelijk te maken



Methodology | gebouwd

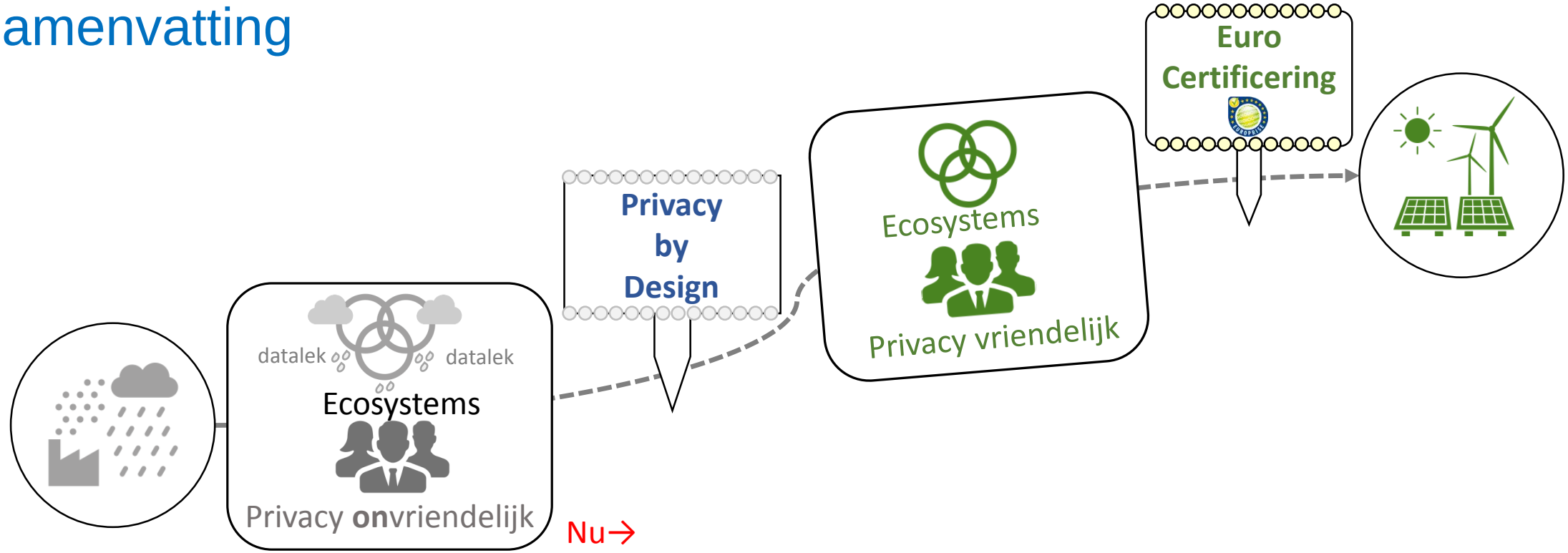
Normen.



Product of service certificering

Privacy | het nieuwe groen

Samenvatting



- Start nu met een gestructureerde invoering van Privacy by Design
- Kies daarbij voor normen, standaarden en referentiemodellen, die bij de organisatie passen, en de ecosystemen waar de organisatie deel van uitmaakt
- Bepaal welke certificeringen relevant (kunnen) zijn voor de organisatie en de partners en leveranciers in de ecosystemen
- Zorg voor een administratieve vastlegging waarmee kan worden aangetoond dat de privacy maatregelen op orde zijn, en die tevens de basis vormen om op een efficiënte wijze assessments te kunnen uitvoeren.

Privacy | het nieuwe groen

Neem voor vragen en informatie contact op met:

| Richard Claassens
| Richard.Claassens@ygdra.com
| https://nl.linkedin.com/in/richardclaassens
| +31(0)626965796

Privacy | het nieuwe groen

Bronnen:

#	Slide 10 t/m 25 zijn gebaseerd op:	Auteurs:
1	Addressing Privacy in Smart Cities (First Webinar), georganiseerd door EIP-SCC Citizen Focus https://eu-smartcities.eu/sites/all/files/Addressing%20Privacy%20in%20Smart%20Cities%20-%20Antonio%20Kung%20-%20Master.pdf	Antonio Kung Antonio Skarmeta Chris Cooper
2	PRIPARE | Privacy Management in Smart cities and Communities Version: v0.20 Date: 01/9/2016 Confidentiality: Public https://eu-smartcities.eu/sites/all/files/PRIPARE%20recommendations%20for%20Smart%20cities.pdf	Antonio Kung
3	PRIPARE | Privacy- and Security-by-Design Methodology Handbook Version: V1.00 Date: 31 December 2015 http://pripareproject.eu/wp-content/uploads/2013/11/PRIPARE-Methodology-Handbook-Final-Feb-24-2016.pdf	Alberto Crespo García (ATOS) Nicolás Notario McDonnell (ATOS) Carmela Troncoso (Gradiant) Daniel Le Métayer (Inria) Inga Kroener (Trilateral) David Wright (Trilateral) José María del Álamo (UPM) Yod Samuel Martín (UPM)