privacy1

dat delen we

Voorstellen

IT-Jurist, PhD RuG
UMCG, LifeLines,...
Privacy, EPD, Ketens, Blockchain,...

IAPP; CIPP/E, CIPM, CIPT
ePrivacy

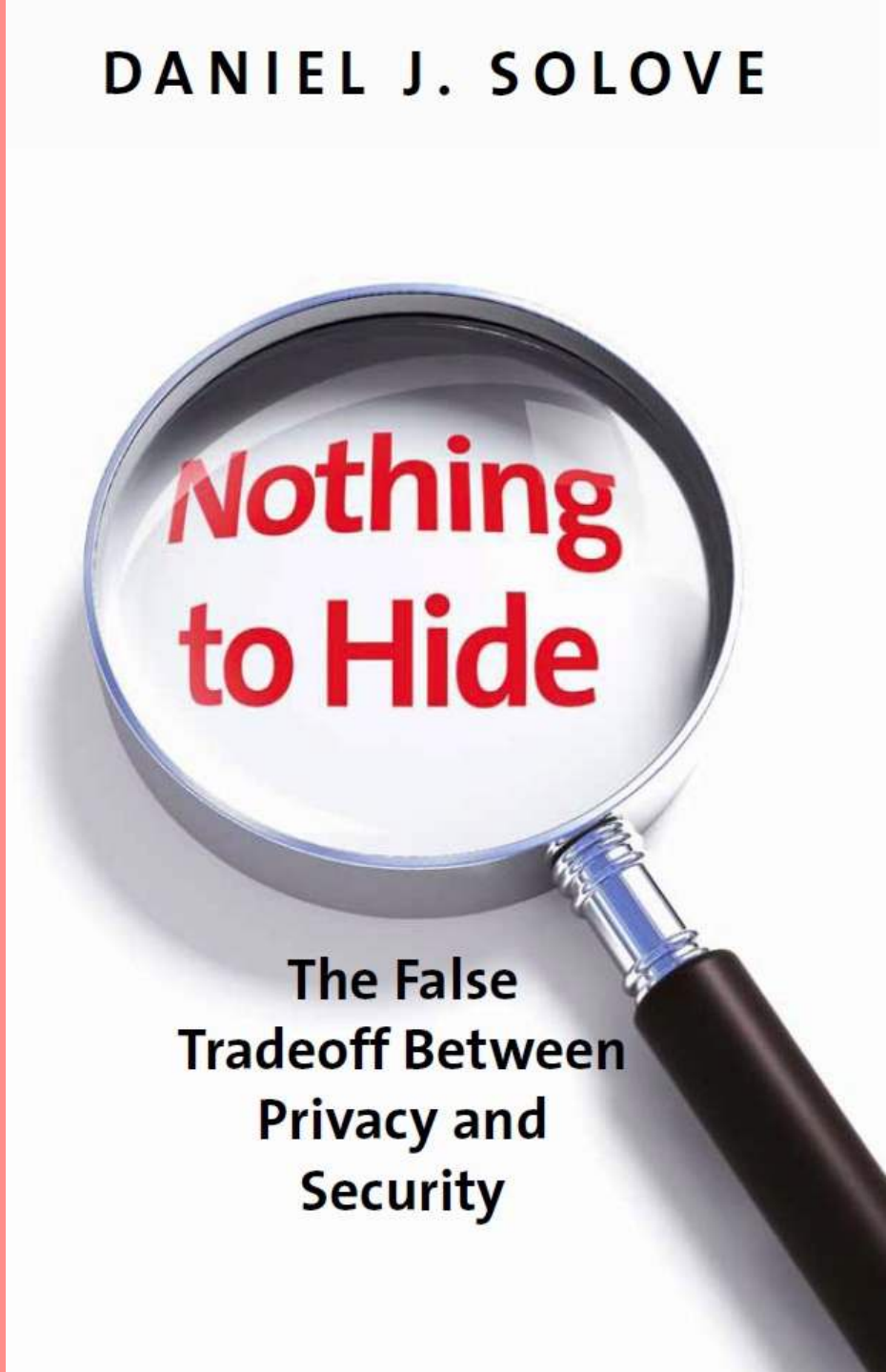

DUTCH
HACKING HEALTH
privacy1

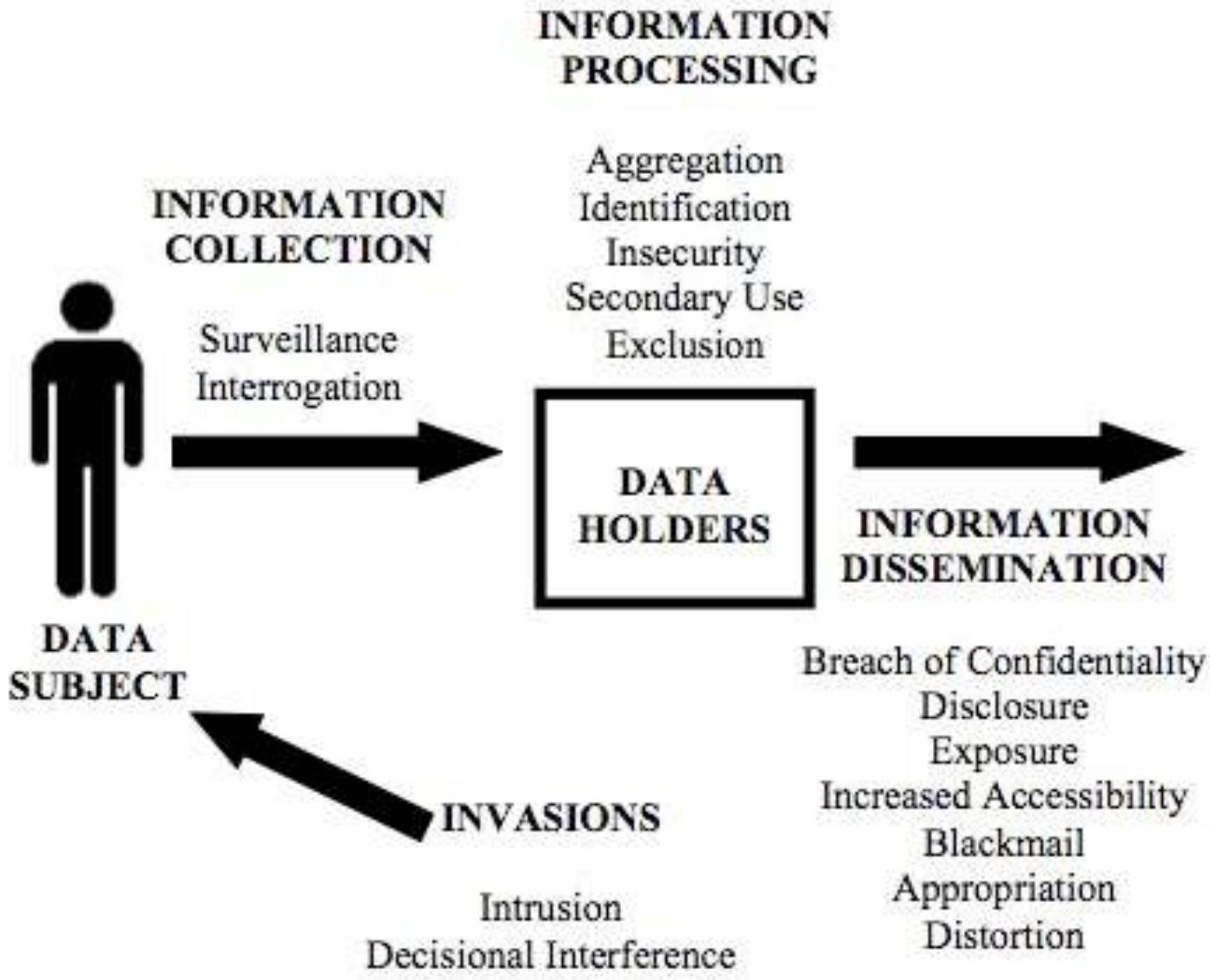

HACKING HEAL
I'M HACKING HEAL


StudyBits
Power to Share

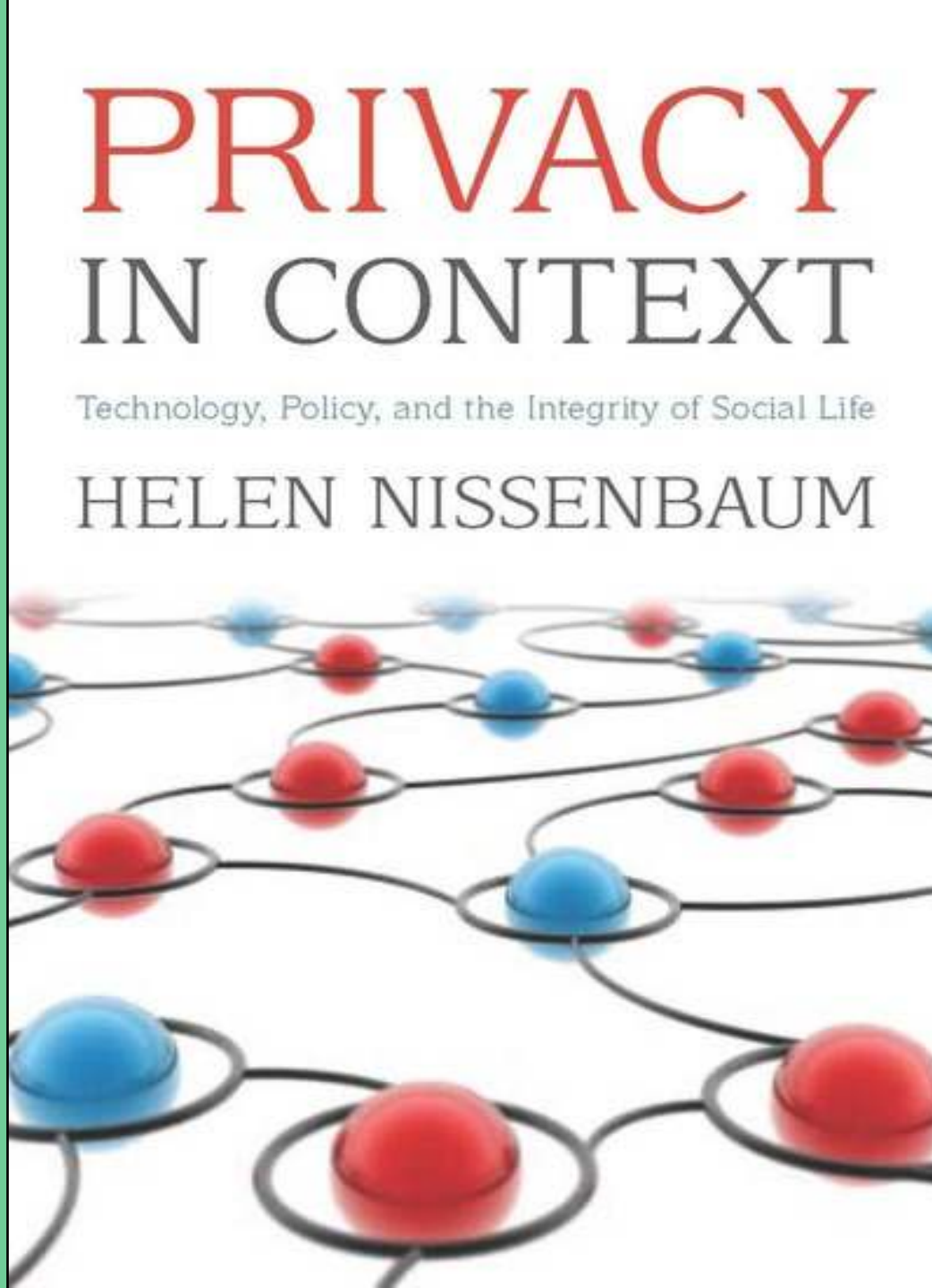
privacy1

Privacy1 zet zich in voor een wereld waarin iedereen zichzelf kan zijn, waar zij erop kunnen vertrouwen dat persoonsgegevens zorgvuldig en vertrouwelijk worden gebruikt.




INFORMATION PROCESSING
Aggregation
Identification
Insecurity
Secondary Use
Exclusion
INFORMATION COLLECTION
Surveillance
Interrogation
DATA HOLDERS
INFORMATION DISSEMINATION
DATA SUBJECT
Breach of Confidentiality
Disclosure
Exposure
Increased Accessibility
Blackmail
Appropriation
Distortion
INVASIONS
Intrusion
Decisional Interference

Privacy = contextuele integriteit



Programma

Klassieke gegevensuitwisseling

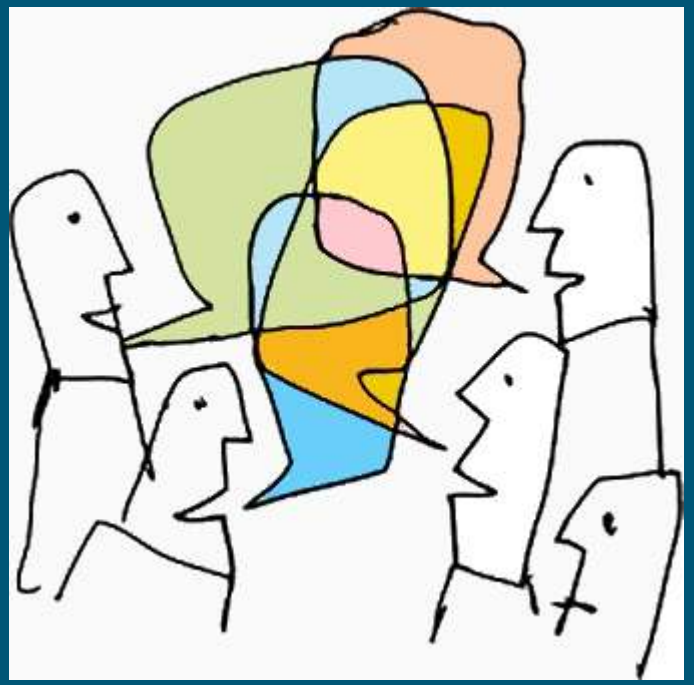
Privacy problemen in ketens:

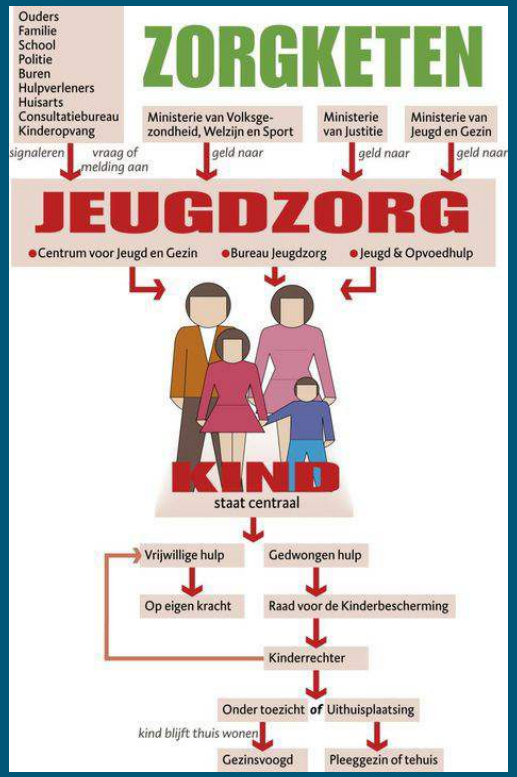
Rollen & verantwoordelijkheden & grondslag

Alternatief? Ketentheorie, PMM + privacy by design

privacy 1

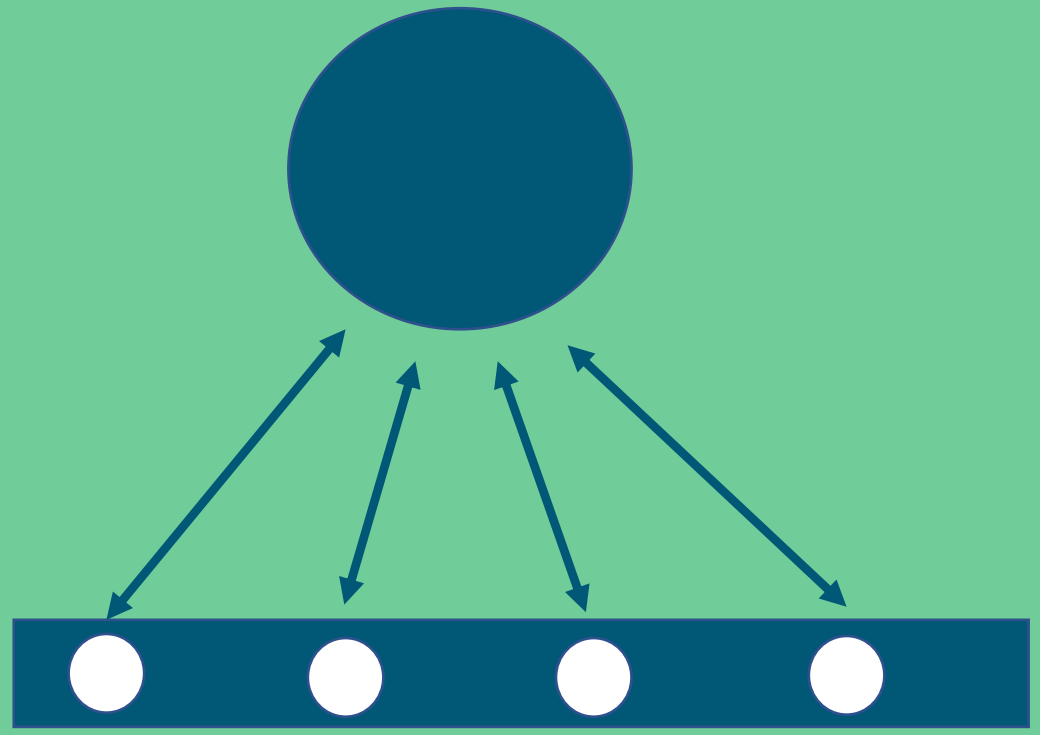
Ketens





privacy 1

Informatisering (klassiek)



Centraal

Dataminimalisatie

Grondslag

Beveiliging

Problemen

Verantwoordelijke?
Grondslag?

Toestemming als grondslag?

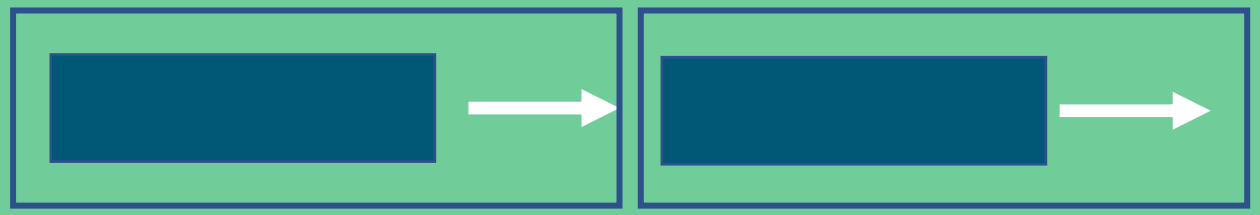
Rolverdeler

Verwerker
Verantwoordelijke
-alleen
-samen met anderen

Verwerker-verantwoordelijke

Verantwoordelijke-Verwerker

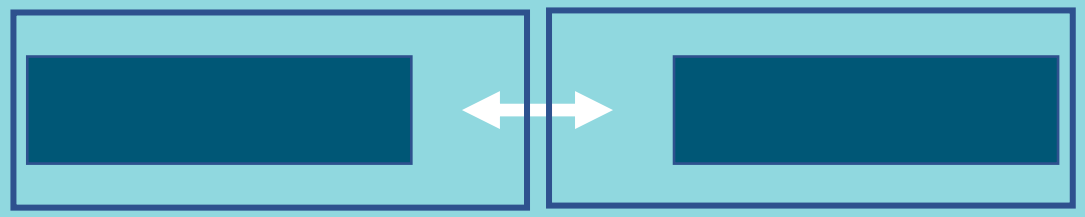
Verwerkerovereenkomst



Verantwoordelijke-Verantwoordelijke

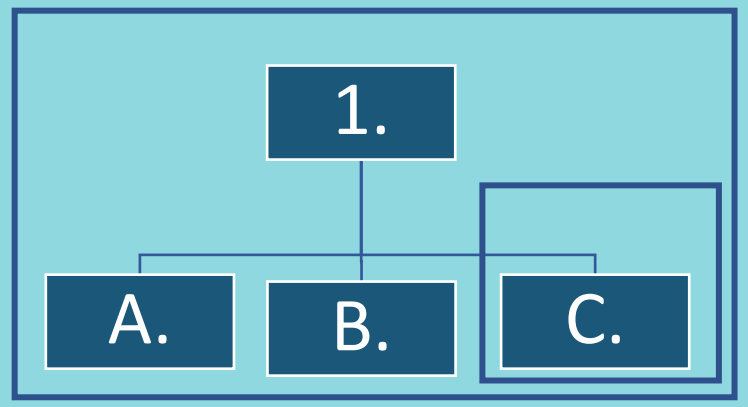
Geen overeenkomst

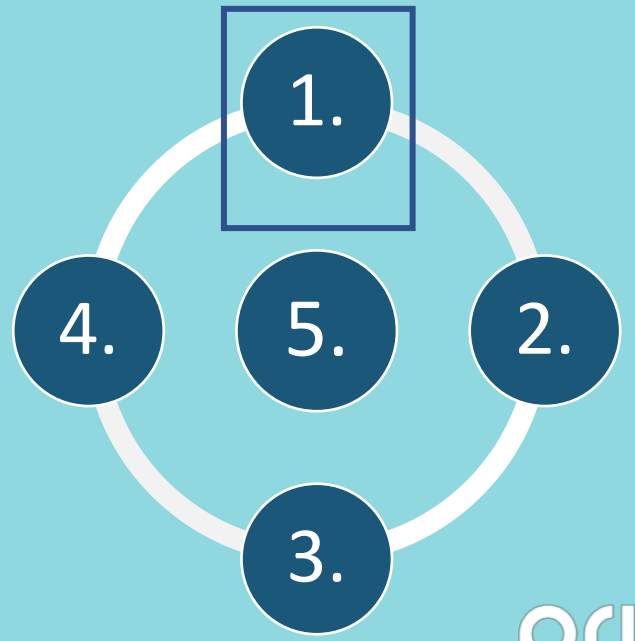
Gezamenlijk verantwoordelijk



Verdeling van aansprakelijkheden (regres)

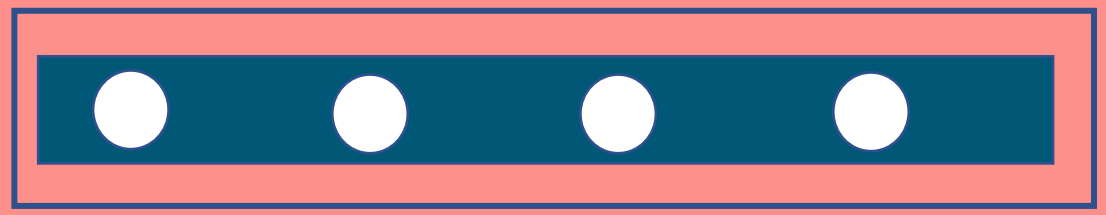
Gezamenlijke regeling





privacy 1

Gemeenschappelijk verantwoordelijk



Hoofdelijk aansprakelijk

Convenant

privacy 1

Alternatieven

2 soorten ketens

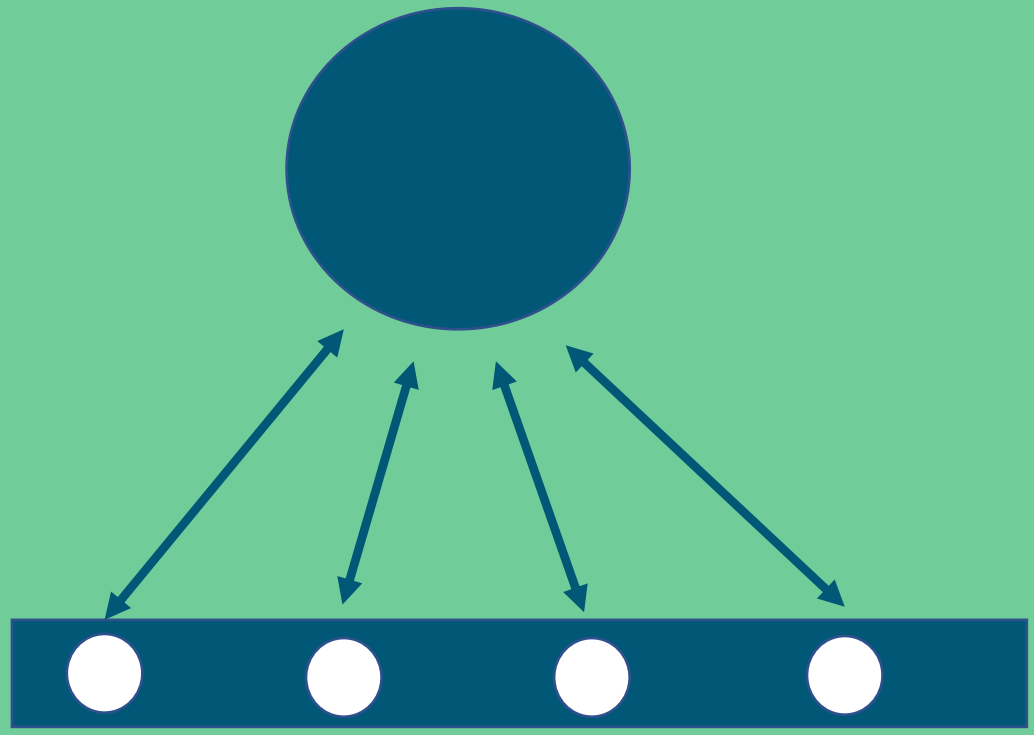
2 niveaus!

2 soorten verantwoordelijkheden

	Coordinatie mechanisme Processtructuur	**Productieproces-standaardisatie**	**Product-standaardisatie**	**Standaardisatie deskundigheden**	**Standaardisatie werkwijze**	**Keteninformatie systeem**	**Informsele afstemming**
1	**Eenvoudige keten** Lineaire ketens en convergente of divergente varianten *Feedforward*	X	X	X	X		
2	**Complexe keten** Knoopstructuur *Feedback and feedforward*	X	X	X	X	X	X

Informatiseren op 2 niveaus

Ketenniveau



Grondvlak

Ketentheorie

Een keten is een moeilijk terrein door:

-geen overkoepelend gezag
-gemeenschappelijke belangen vaak beperkt en onduidelijk
-irrationaliteit en onvoorspelbaarheid troef
-het dominant ketenprobleem is de ‘baas’ in de keten!

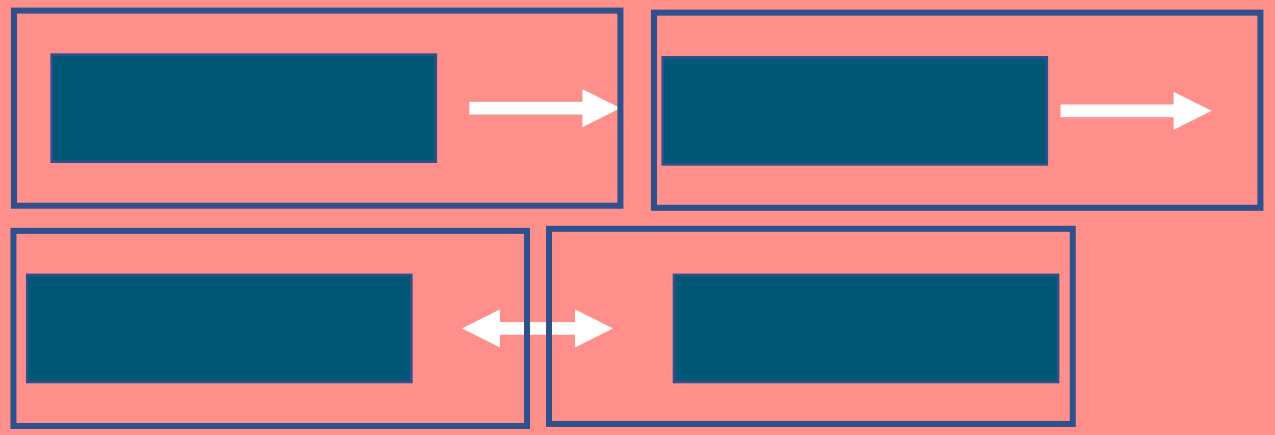
Niveauvergissing

Grootschalige stelsels werken in de praktijk anders dan kleinschalige! Voorbeelden: HAP, nationale patiëntdossier EPD (nu: LSP), biometrische visa, EU-uitwisseling van strafvonnissen, Sociaal domein

Niveaugebonden privacy principes

Verantwoordelijke
Verwerker
Grondslag (toestemming)

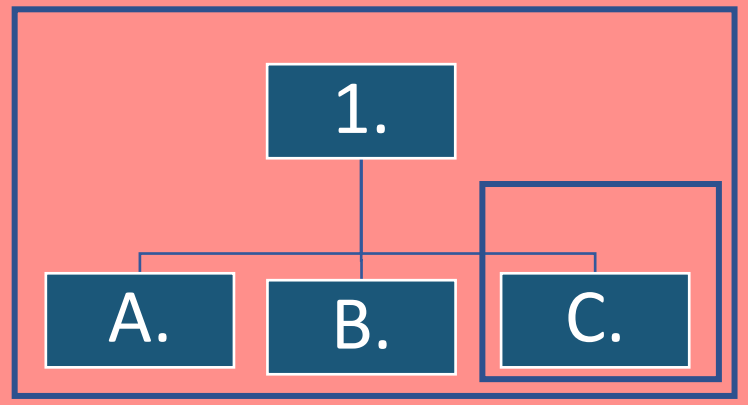
Eenvoudige keten/ push

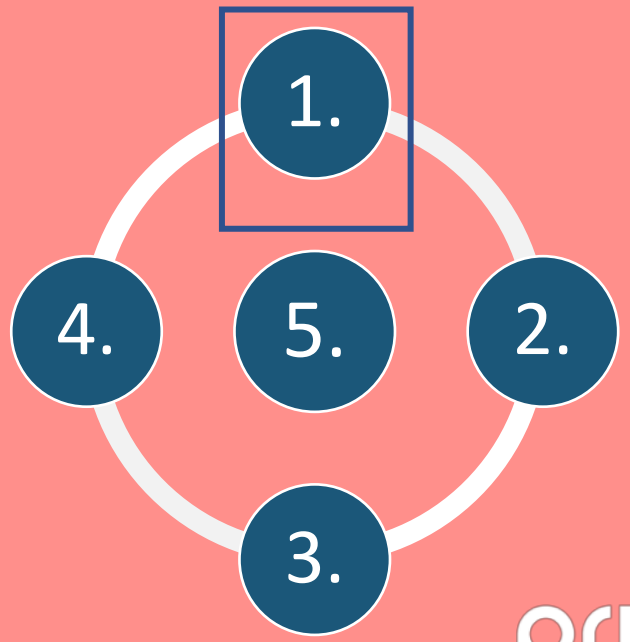


Verenigbaar doel

Grondslag

Gezamenlijke regeling (t.o.v. Betrokken





privacy 1

AVG principes

		Ad hoc informeel	Bewust	Gedefinieerd	Voorspelbaar
1	**Rollen en verantwoordelijkheden**	Ad hoc verwerker-overeenkomst	Procedure verwerker-overeenkomst	Contract management	+ Actualisatie
2	**Register van verwerkingen** persoonsgegevens / bijzondere persoonsgegevens (PIA; zie 5) documentatie	Geen / niet vastgelegd overzicht	Statisch register / risico-inventarisatie o.i.d	Procedure register	+ Actualisatie (Monitor)
3	**Privacy functionarissen**	Geen/ FG/ PO (ad hoc)	FG/ PO/ SO (functiescheiding	Privacy management	+ Business case
4	**Gerechtvaardigd doel** doelbepaling / rechtmatige grondslag	Gekozen	Omschreven per proces	Geïmplementeerd per proces	Geactualiseerd (Monitor)
5	**Dataminimalisatie**	Nice to have	Need to know	PIA	PIA + PDCA
6	**Juist en volledig**	Gefragmenteerd	Op afdelingsniveau	Bedrijfsbreed overzicht	+ Actualisatie (Monitor)
7	**Transparantie**	Privacy statement	Privacy statement die past bij realiteit	Geheel van informati-everplichtingen	PDCA
8	**Rechten van betrokkenen** inzage / correctie & aanvulling verwijdering / vergeten / dataportabiliteit	0/.. van de 5, ad hoc afhandeling	Alle 5 (procedures)	Procedures + implementatie	PDCA
9	**Maatregelen** organisatorisch (vertrouwelijkheid/ geheimhouding etc.) technisch / meldplicht datalekken / bewaartermijnen	Bewustwording presentatie (ad hoc) oid. Privacybeleid/ IB-beleid etc.	Risico inventarisatie Training op afdelings-niveau Per afdeling geïm-plementeerd beleid	Bedrijfsbrede training Afdelingsbreed geïmplementeerd beleid (schonen)	0-meting + elearning Risk-based sturing schonen
10	**Doorgifte**	Landen passend beschermingsniveau (let op: cloud etc.)	Contracten	Geïmplementeerde waarborgen (uit contracten); procedure	PDCA

verantwoordelijke | verwerker

Variant 1

Een tandartsenpraktijk laat de betaling van salarissen van zijn personeel verzorgen door Infomedics. Deze verwerkt ten behoeve van de tandartsen persoonsgegevens van medewerkers en is daarom verwerker.

Het is in deze situatie van belang om een verwerkersovereenkomst af te sluiten tussen beide partijen, waarin duidelijke afspraken worden gemaakt over onder andere:
- De (soorten) persoonsgegevens van welke (soorten) betrokkenen;
- Het doel (duidelijk omschreven);
- Duur van de verwerking;
- Welke beveiligingsmaatregelen worden getroffen (inclusief het melden van datalekken) om de gegevens te beschermen tegen ongeoorloofd gebruik;
- Na einde verwerking: de vernietiging/ retourprocedure.

Overige voorbeelden: Hosting-provider, mailingorganisaties.

1

verantwoordelijke → verantwoordelijke

Variant 2

Een tandartsenpraktijk verstrekt bepaalde gegevens van zijn medewerkers aan de Belastingdienst en ook aan een Pensioenfonds. Alle partijen zijn aan te merken als verantwoordelijke, aangezien bij beide partijen een nieuwe verantwoordelijkheid ontstaat.

De tweede variant kenmerkt zich doordat het doel en de middelen van de ene verantwoordelijke zijn overgegaan naar het doel en de middelen van de andere verantwoordelijke. Er begint bij de tweede verantwoordelijke dus een nieuwe verantwoordelijkheid, omdat deze verantwoordelijke een eigen grondslag heeft om de persoonsgegevens van deze betrokkene te verwerken. In deze situatie hoeft geen verwerkersovereenkomst afgesloten te worden.
Beide partijen zijn immers geheel gebonden aan de AVG.

Overige voorbeelden: Reisbureau-Vliegtuigmaatschappij-Hotel (tenzij in 1 pakket aangeboden; dan: gezamenlijk verantwoordelijke).

2

verantwoordelijke verantwoordelijke

Variant 4

Via een fraudedetectiesysteem kunnen het UWV en DUO zien welke betrokkenen zowel een uitkering als een studiefinanciering hebben aangevraagd (deze combinatie is niet toegestaan). Beide partijen zijn verantwoordelijke voor het geheel. In een convenant kunnen gezamenlijke afspraken worden gemaakt.

Bij deze variant hebben verschillende verantwoordelijken een gemeenschappelijk systeem waarop zij persoonsgegevens verwerken. In deze situatie bepalen zij gezamenlijk het doel en de middelen van de verwerking.
Alle partijen zijn hoofdelijk aansprakelijk voor het geheel.

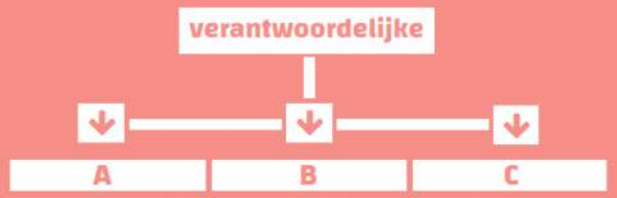
4

verantwoordelijke ← → verantwoordelijke

Variant 3

Een tandartsenpraktijk verstrekt aan de Arbodienst gegevens van medewerkers die verzuimbegeleiding nodig hebben. Er gaan bepaalde gegevens van medewerkers over en weer en beide werken conform eigen wettelijke kaders. De tandartsenpraktijk en de Arbodienst zijn beide zelfstandig verantwoordelijke voor de gegevens van medewerkers, maar ook voor de verstrekking tussen beide. Er is sprake van een gezamenlijke verantwoordelijkheid. Overige voorbeelden: Werving- en selectie, kredietscoremaatschappijen, verzekeraars (incl. tussenpersonen).

3a



**Een aantal tandartsen zijn werkzaam voor een zorginstelling (ziekenhuis) en gebruiken voor de dossiers het elektronisch patiëntendossier.
Iedere tandarts heeft op basis van zijn beroep een zelfstandige verantwoordelijkheid voor de gegevens van zijn eigen patiënten. Daarnaast is het ziekenhuis verantwoordelijke van de gegevens van alle patiënten.
Het ziekenhuis kan bij eventueel onrechtmatig gebruik van patientgegevens de individuele tandarts aanspreken.**

3b

Een bank deelt betaalgegevens (berichten) van zakelijke klanten met andere banken. De zakelijke klanten en de bank zijn gezamenlijk verantwoordelijke voor de verwerking, de bank voor het systematische/ technische deel (maakt berichtenverkeer mogelijk) en de klanten voor de inhoud van het bericht.

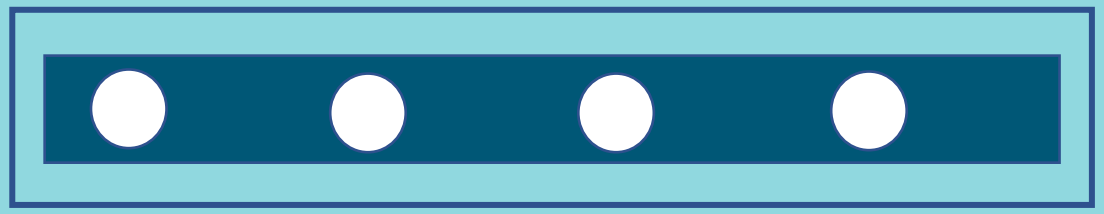
Overig voorbeeld: Telecomprovider.

3c

Gemeenschappelijke verwerking (nieuw)

Pull/ complexe keten

Grondslag?



-> dkp &

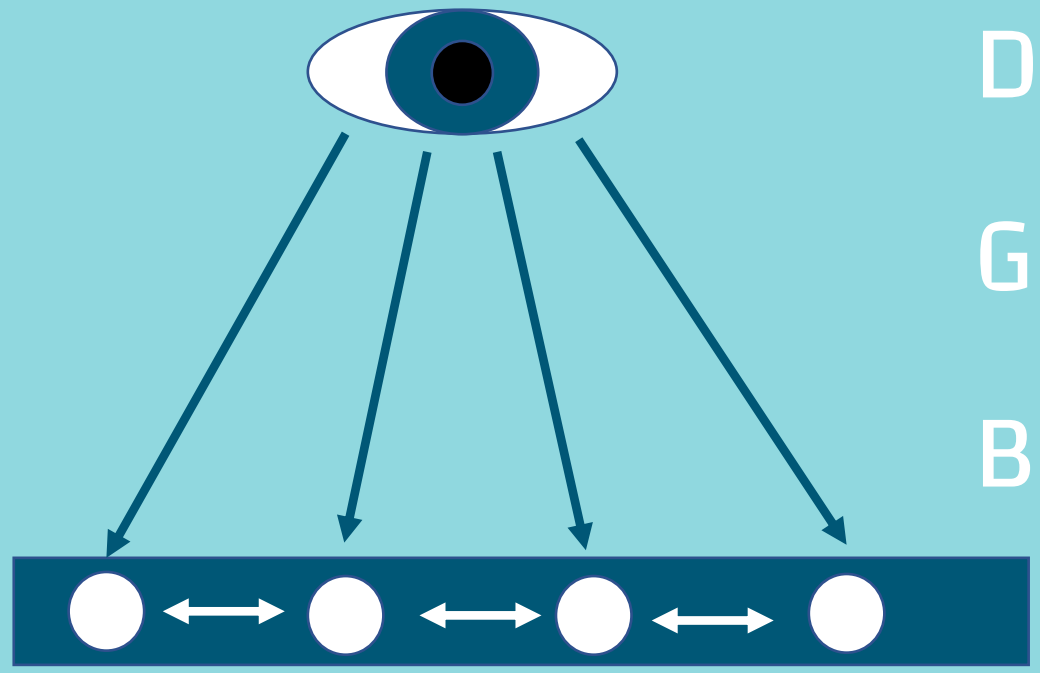
hoofdelijke aansprakelijkheid

Dominant Ketenprobleem

1. Een probleem dat overal in de keten voelbaar is, en dat geen van de partijen op eigen kracht kan oplossen.
2. Alleen goede samenwerking kan voorkómen, dat stelselmatig falen de keten als geheel in opspraak brengt.
3. Een gecoördineerde aanpak moet het hebben van het krachtenveld dat een dominant ketenprobleem oproept.

privacy 1

Informatisering (ketentheorie)



Communicatie

Dataminimalisatie (dkp)

Grondslag

Beveiliging

Privacy by design bij het ontwerp

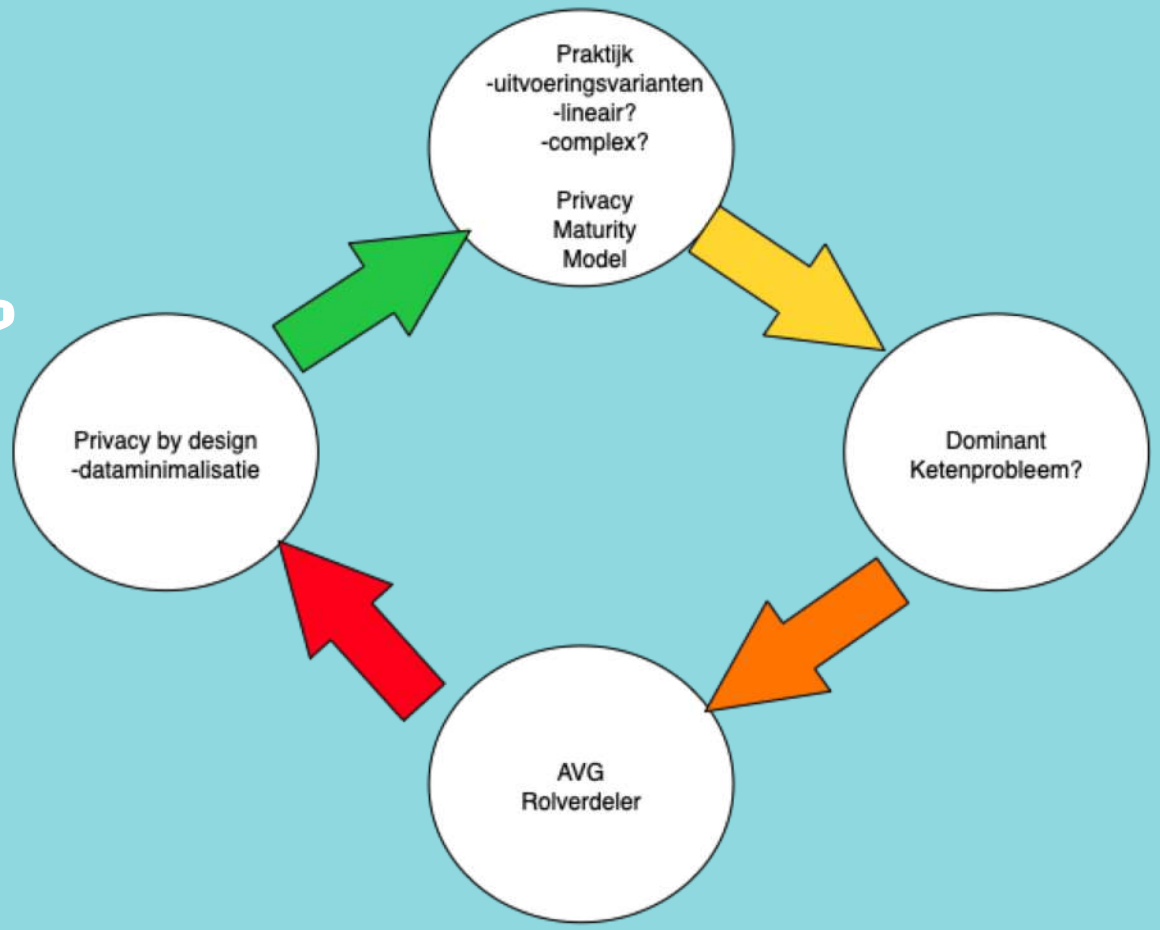
Klassieke manier van informatisering (push and pull) en de privacyrisico's:
Actoren bepalen; wet zegt: doelbinding (in zorg: behandelrelatie)
Brede toestemming versus accountability
Problemen vinden van een verantwoordelijke/ bewerker
Privacy by design door KI = get the right on the right moment

Privacyconcepten op schaal

Verantwoordelijke in wet- en regelgeving 1:1 ontbreekt in de keten;
optie: dkp?
Verwerking (doelbinding, grondslag) versus niveauvergissing?
Doelbinding versus her/ de-contextualisering
Grondslag/ Toestemming 1:1; dkp?
Van halen naar brengen (decentralisatie); kale infrastructuur (get the right on the right moment)

Conclusies

Praktijk (PMM/ PbD) +
Ketendenken (dkp) =
vorm -> AVG-rolverdeler?



Aanbevelingen

DKP als gemeenschappelijk verantwoordelijke?
Nieuwe verwerking op niveau vd keten!
Nieuwe doelbinding/ DKP
Nieuwe grondslag (geen toestemming!)
'Krijgen' ipv *push* of *pull*

privacy 1

Privacy concept	Kernbegrip	Schaal?	Uitwerking
Verantwoordelijke	Ontbreken van gezag	Kleinschalig, gebaseerd op bronbestand	Dominant ketenprobleem als verantwoordelijke
Verwerking	Niveauvergissing	Kleinschalig, gebaseerd op bronbestand	Op ketenniveau ontstaat een nieuwe verwerking.
Doelbinding	Decentralisatie	Kleinschalig, gebaseerd op bronbestand	Gegevens kunnen een andere betekenis krijgen op het ketenniveau.
Rechtmatige grondslag, toestemming	Dominant ketenprobleem (dkp)	Kleinschalig, gebaseerd op een één-op-één relatie met verantwoordelijke en verwerking.	n:n, er zal een 'eigen' gerechtvaardigds doel moeten zijn voor de nieuwe verwerking op het ketenniveau, het dkp kan daar behulpzaam bij zijn.
Dataminimalisatie	Decentraal communiceren van noodzakelijke gegevens	Kleinschalig, gegevens zijn context-gebonden	Door risico's van de – en her-contextualisering kan een kale infrastructuur beter passen bij beginsel van proportionaliteit.