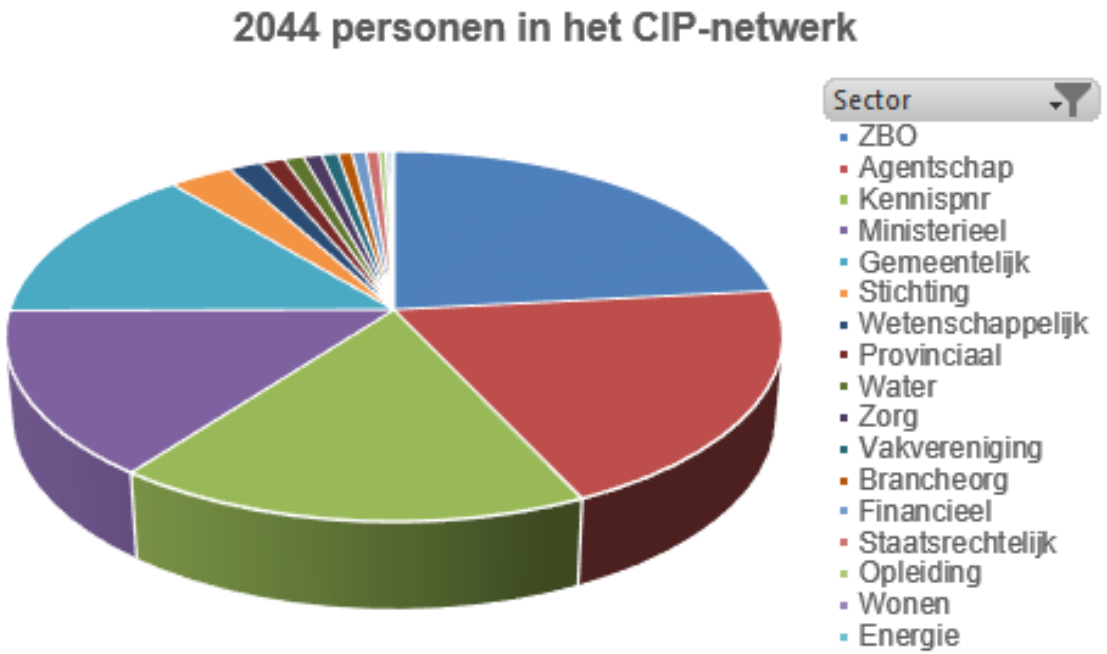
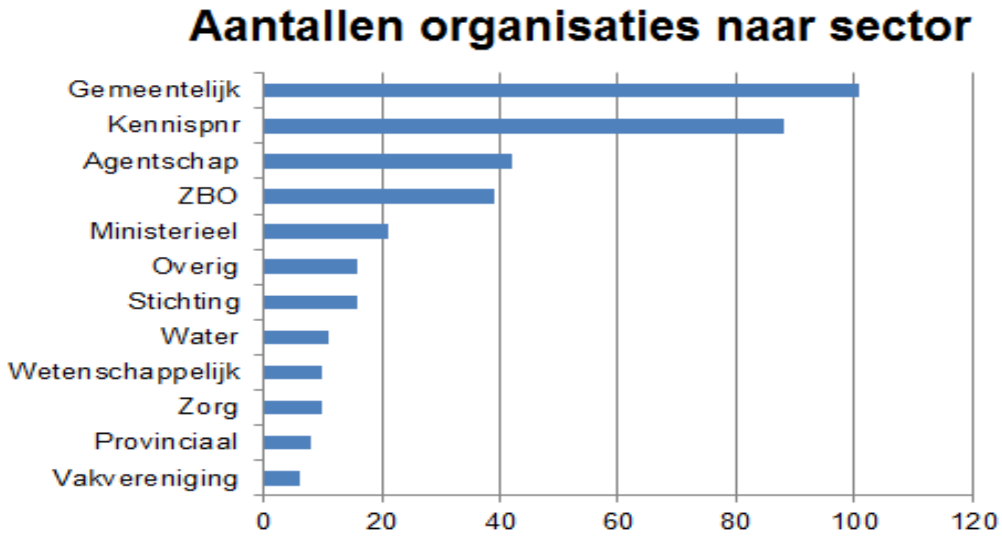
centrum informatiebeveiliging en privacybescherming

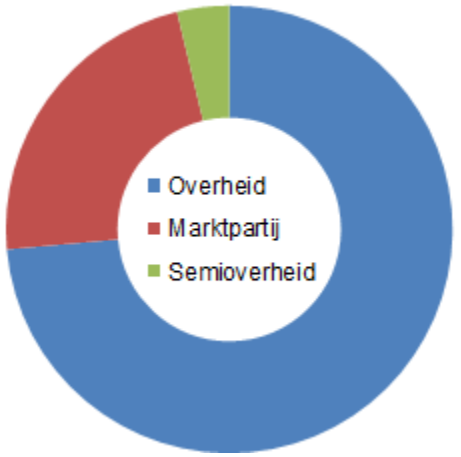
Samen – werken aan informatieveiligheid & Privacy

9 november 2017 PvIB

Samenstelling CIP-Netwerk 1-9-17

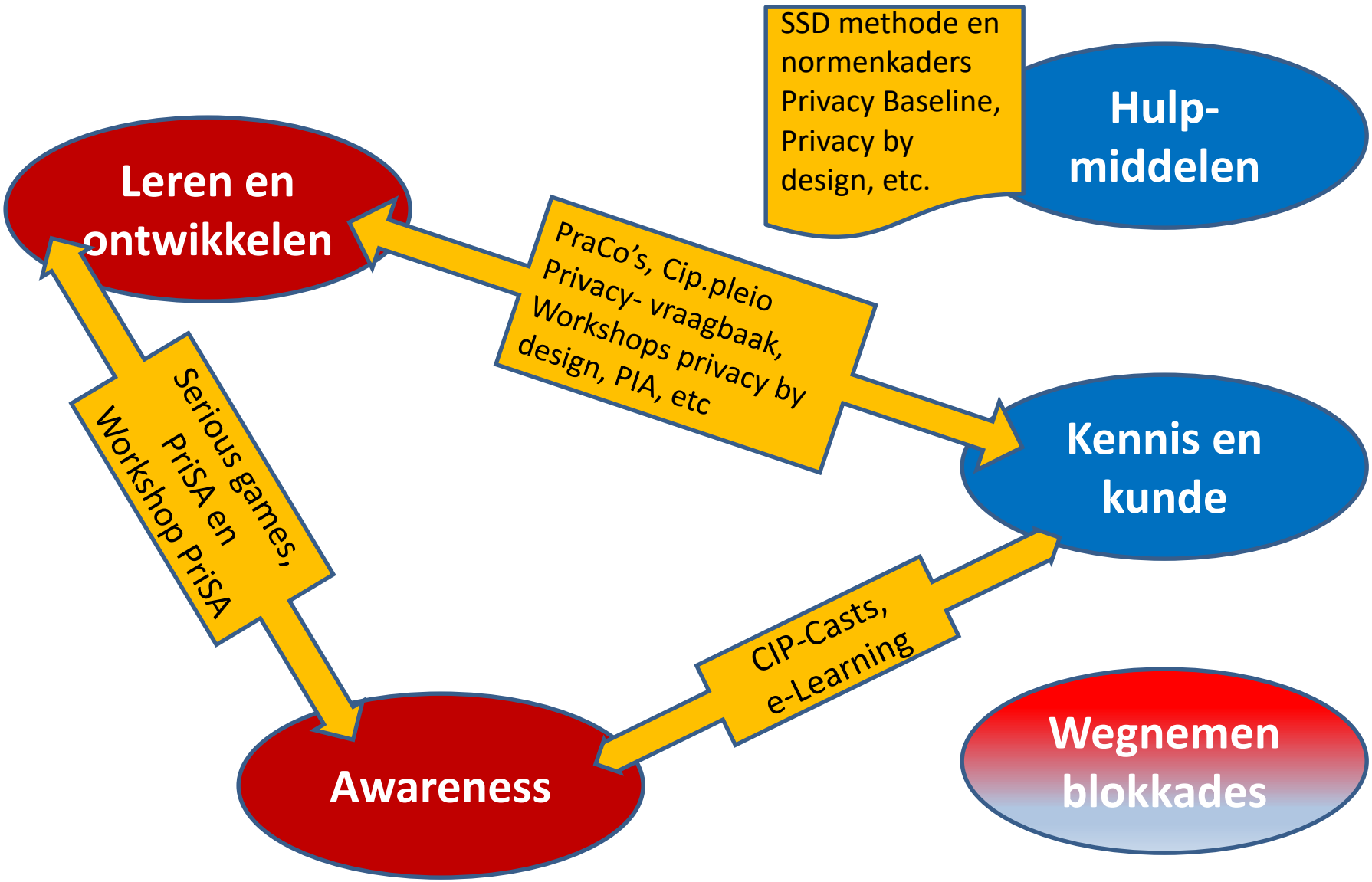






De PDC in Context

Responsible Behavior



De Websites


centrum informatiebeveiliging en privacybescherming
https://cip.pleio.nl/
www.cip-overheid.nl
HOME
CIP
EVENTS
PARTNERS
SSD MANIFESTPARTIJEN
DOWNLOADS
CIP-POST
Centrum voor Informatiebeveiliging en Privacybescherming (CIP)
Snel naar 'Producten'
Snel naar 'CIP-Casts'
Hoe meld ik problemen?
CONFERENTIEDATA

Een paar vragen

- **Wie van jullie is met de Avg bezig?**
- **Wie daarvan heeft de wet gelezen?**
- **Wie is klaar op 25 mei?**

- **Wat is eigenlijk “klaar”?**

De Avg is niet geheel nieuw

- Volgt filosofie Wbp
- Gap met Avg = de achterstand bij de implementatie Wbp (6 juli 2000!) plus enkele nieuwigheden van de AVG

Kernwaarden van de Avg

- De betrokkene (burger, klant, ..) vóórop
- Organisatie heeft aantoningsplicht rechtmatige verwerking
- Gegevensminimalisatie
- Aantoningsplicht zaakjes op orde, bijvoorbeeld:
  - transparantie verwerkingen
  - inzage en correctierecht
  - best effort informatiebeveiliging

Highlights en achtergrondinformatie

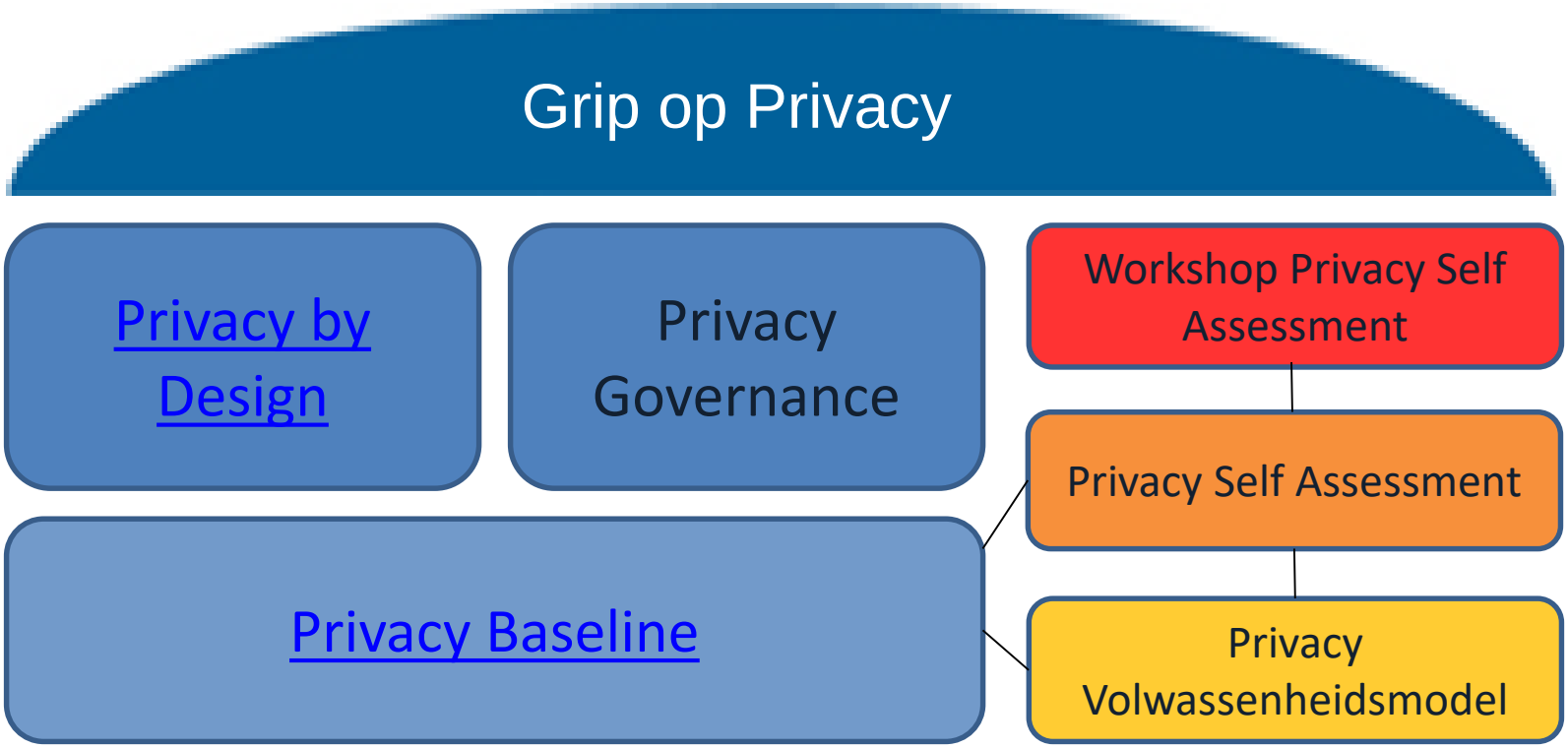
Van AP: In 10 stappen voorbereid: (overview)
https://autoriteitpersoonsgegevens.nl/

Van CIP: Tussen Wbp en Avg: (overview)
https://www.cip-overheid.nl/ (Link in het eerste tekstblok)

Van CIP: Grip-op-Privacy (Handreikingen voor aanpak en self assessment tool)
https://www.cip-overheid.nl/grip-op-privacy/

Grip op Privacy

CIP-handreikingen om in control te komen



Doe de Privacy Self Assessment

De Privacy Self Assessment geeft u een advies.
Het advies gebaseerd op uw antwoorden die u geeft.
Hierbij stellen we alleen die vragen die passen bij uw ambitieniveau.
Het ambitieniveau kan aan de hand van onderstaande figuur gekozen worden.

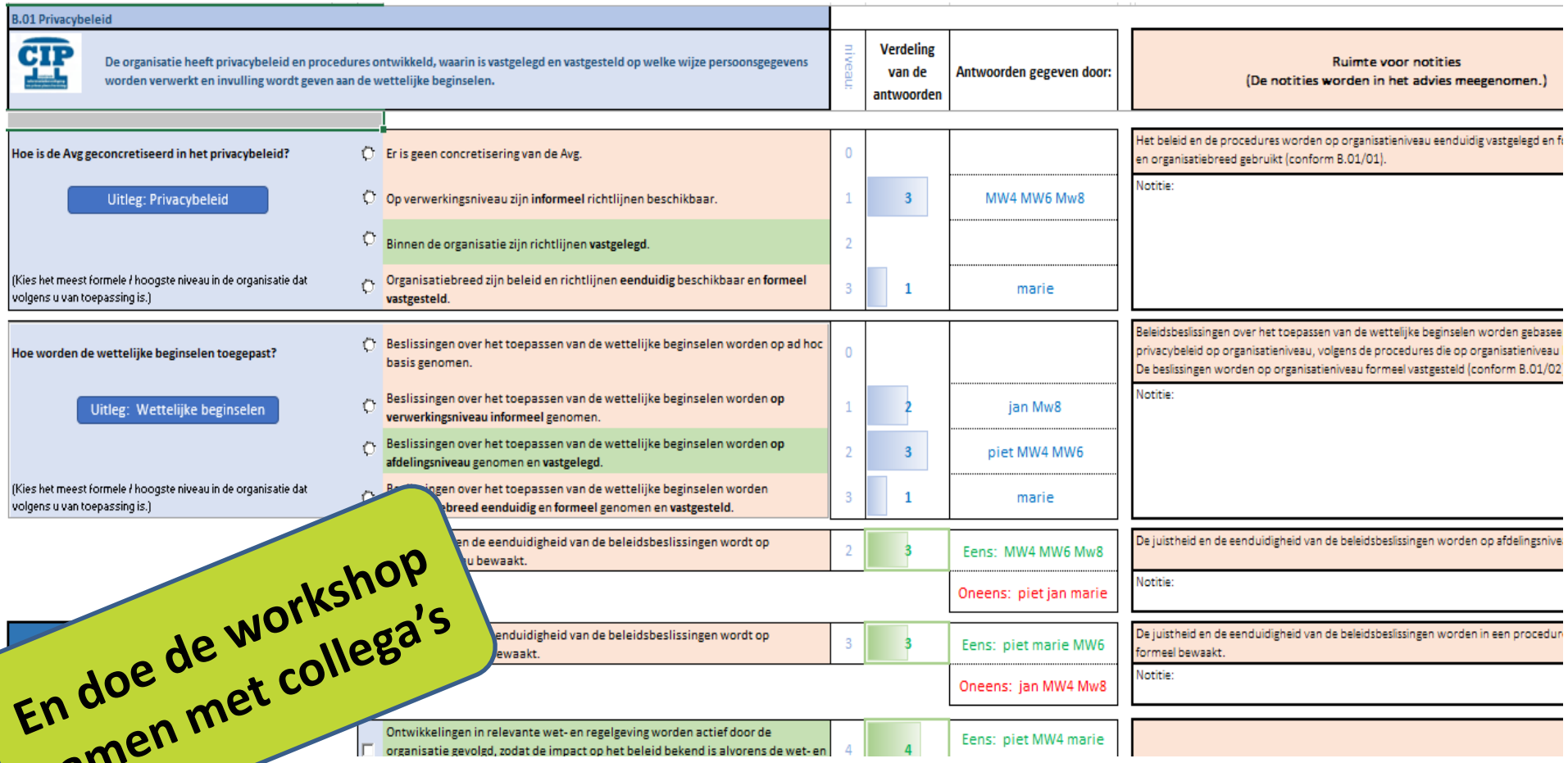
Deze niveau's zijn nader beschreven in het CIP Privacyvolwassenheidsmodel.

Wilt u tbv het delen van de resultaten uw gegevens opgeven?
(de gegevens worden door CIP alleen voor statistische doeleinden gebruikt of intern uw eigen organisatie als u een privacyworkshop houdt)

uw naam:	uw naam
uw functie:	uw functie
uw organisatie:	uw organisatie
IN IEDER GEVAL uw sector:	een keuze uit de lijst >>>

Workshop Privacy Self Assessment

Voorbeeld nog niet behandelde criterium/vraag



B.01 Privacybeleid

De organisatie heeft privacybeleid en procedures ontwikkeld, waarin is vastgelegd en vastgesteld op welke wijze persoonsgegevens worden verwerkt en invulling wordt geven aan de wettelijke beginselen.

		niveau	Verdeling van de antwoorden	Antwoorden gegeven door:
Hoe is de Avg geconcretiseerd in het privacybeleid?	Er is geen concretisering van de Avg.	0		
Uitleg: Privacybeleid	Op verwerkingsniveau zijn **informeel** richtlijnen beschikbaar.	1	3	MW4 MW6 Mw8
	Binnen de organisatie zijn richtlijnen **vastgelegd**.	2		
(Kies het meest formele / hoogste niveau in de organisatie dat volgens u van toepassing is.)	Organisatiebreed zijn beleid en richtlijnen **eenduidig** beschikbaar en **formeel vastgesteld**.	3	1	marie
Hoe worden de wettelijke beginselen toegepast?	Beslissingen over het toepassen van de wettelijke beginselen worden op ad hoc basis genomen.	0		
Uitleg: Wettelijke beginselen	Beslissingen over het toepassen van de wettelijke beginselen worden **op verwerkingsniveau informeel** genomen.	1	2	jan Mw8
	Beslissingen over het toepassen van de wettelijke beginselen worden **op afdelingsniveau** genomen en **vastgelegd**.	2	3	piet MW4 MW6
(Kies het meest formele / hoogste niveau in de organisatie dat volgens u van toepassing is.)	…gen over het toepassen van de wettelijke beginselen worden …**breed eenduidig** en **formeel** genomen en **vastgesteld**.	3	1	marie
	…n de eenduidigheid van de beleidsbeslissingen wordt op …u bewaakt.	2	3	Eens: MW4 MW6 Mw8
				Oneens: piet jan marie
	…enduidigheid van de beleidsbeslissingen wordt op …ewaakt.	3	3	Eens: piet marie MW6
				Oneens: jan MW4 Mw8
	Ontwikkelingen in relevante wet- en regelgeving worden actief door de organisatie gevolgd, zodat de impact op het beleid bekend is alvorens de wet- en	4	4	Eens: piet MW4 marie

Ruimte voor notities
(De notities worden in het advies meegenomen.)

Het beleid en de procedures worden op organisatieniveau eenduidig vastgelegd en f… en organisatiebreed gebruikt (conform B.01/01).

Notitie:

Beleidsbeslissingen over het toepassen van de wettelijke beginselen worden gebasee… privacybeleid op organisatieniveau, volgens de procedures die op organisatieniveau … De beslissingen worden op organisatieniveau formeel vastgesteld (conform B.01/02

Notitie:

De juistheid en de eenduidigheid van de beleidsbeslissingen worden op afdelingsnive…

Notitie:

De juistheid en de eenduidigheid van de beleidsbeslissingen worden in een procedur… formeel bewaakt.

Notitie:

En doe de workshop samen met collega's

En voor het overige ben ik van mening …

Artikel voor de invulling van de zorgplicht op het gebied van software-veiligheid

Overwegende dat

- datalekken en geslaagde hackpogingen vaak het gevolg zijn van zwakheden in software,
- het niet toereikend is een algemene afspraak te maken over de veiligheid van software,
- de opdrachtgever voor ontwikkeling en onderhoud van software een zorgplicht heeft in zijn rol van opdrachtgever en van hem goed opdrachtgeverschap mag worden verwacht,
- de opdrachtnemer (ontwikkelafdeling of softwareproducent) een zorgplicht heeft voor het leveren van veilige software,

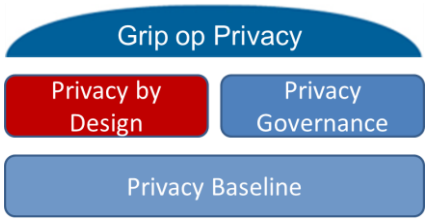
achten opdrachtgever en opdrachtnemer het van belang dat opgeleverde software, zowel nieuw als vernieuwd, voldoet aan een aantal specifieke kenmerken. Deze kenmerken ontlenen wij aan de set van eisen die vastgelegd is in de methode Grip-op-SSD van het CIP.

De wederzijdse zorgplicht voor de veiligheid van de software wordt als volgt ingevuld.

- de opdrachtnemer zal de eisen van Grip-op-SSD meenemen in het offerteproces bij de begroting van de werkzaamheden, en deze implementeren bij de ontwikkeling en het onderhoud van de software,
- De opdrachtgever zal zowel bij de aanbesteding als bij de contractsluiting van softwareontwikkeling en -onderhoud de eisen van Grip-op-SSD meegeven als onderdeel van de non-functional requirements en daarop (laten) toetsen in het acceptatieproces.
- In het geval een van de partijen een risicoafweging maakt die naar diens inzien afwijkingen van de SSD-eisen rechtvaardigt of noodzaakt, bespreken partijen dat en leggen afwijkingen formeel vast.

Vragen
?

Handleiding Privacy by Design



- Maakt ontwerpers bewust van het belang van privacy
- Handvaten om de bescherming om de ACT-doelen mee te nemen in de ontwerpfasen en het ontwerp
- Ondersteunt zowel het formele als het creatieve proces
- Proactieve aanpak, voorkomt hoge kosten van aanpassingen achteraf
- Een betere bedrijfsvoering is het resultaat. Dit leidt tot win-win

Privacy by Design gaat verder dan techniek.
De scope is de gehele verwerking van persoonsgegevens: systemen én bedrijfsprocessen.

Principes in het ontwerpproces

Privacy by Design

The 7 Foundational Principles

Ann Cavoukian, Ph.D.
Information & Privacy Commissioner
Ontario, Canada

1. Proactief i.p.v. reactief; Preventief i.p.v. herstellend
2. Privacy als standaard
3. Privacy geïntegreerd in het ontwerp
4. Volledige functionaliteit – win-win in plaats van compromissen
5. Bescherming tijdens de volledige levenscyclus
6. Zichtbaarheid en transparantie – hou het open
7. Respect voor de privacy – laat de gebruiker centraal staan

Inrichtingsprincipes voor het ontwerp

- Architectuurprincipes: Hoe wordt het ontwerp een succes?
  - Waar moet op gelet worden om aan de criteria te voldoen
  - Reduceren van de complexiteit
  - Beschikbare technologieën
- Extra principes bij de inzet van mobiele apparaten

Handvaten voor de “bouw”

De handvaten helpen de ontwerper bewust keuzen te maken

10 redenen om PbD alsnog toe te passen:

1. De noodzaak van een verwerking of een (redundante) opslag ligt niet vast.
2. Van doorgiften liggen de wettelijke grondslag of de waarborgen niet vast.
3. De complexiteit van de gegevensverwerking is hoog of niet bekend.
4. De levenscyclus van persoonsgegevens is niet meegenomen in het ontwerp.
5. Het hoe en waarom de betrokkenen worden geïnformeerd over verwerkingen ligt niet vast.
6. De persoonsgegevens zijn niet eenvoudig te corrigeren en overdraagbaar.
7. De architectuur benut niet of beperkt de mogelijkheden van encryptie.
8. Privacymaatregelen zijn niet gestandaardiseerd.
9. Toezicht of de verwerkingen voldoen aan de AVG vraagt om dure audits.
10. De architect was zich niet bewust van hoe keuzen de persoonlijke levenssfeer van betrokkenen kan beïnvloeden.

10 redenen voor architecten om PbD alsnog toe te passen:

1. De noodzaak van een verwerking of een (redundante) opslag ligt niet vast.
2. Van doorgif[illegible] liggen de wettelijke grondslag of de waarborgen niet vast.
3. De comp[illegible]it van de gegevensverwerking is hoog of niet bekend.
4. De le[illegible]egenomen in het ont[illegible]
5. Het [illegible]ormeerd over verwe[illegible]
6. De perso[illegible]egevens zijn niet eenvoudig te corrigeren en overdraagb[illegible].
7. De architectuur benut niet of beperkt de mogelijkheden van encryptie.
8. Privacymaatregelen zijn niet gestandaardiseerd.
9. Toezicht of de verwerkingen voldoen aan de AVG vraagt om dure audits.
10. De architect was zich niet bewust van hoe keuzen de persoonlijke levenssfeer van betrokkenen kan beïnvloeden.

Terug naar G-o-P

Aanleiding is een vraag uit de CIP community:

Kunnen jullie eens opschrijven hoe dat nou moet, met die privacy?

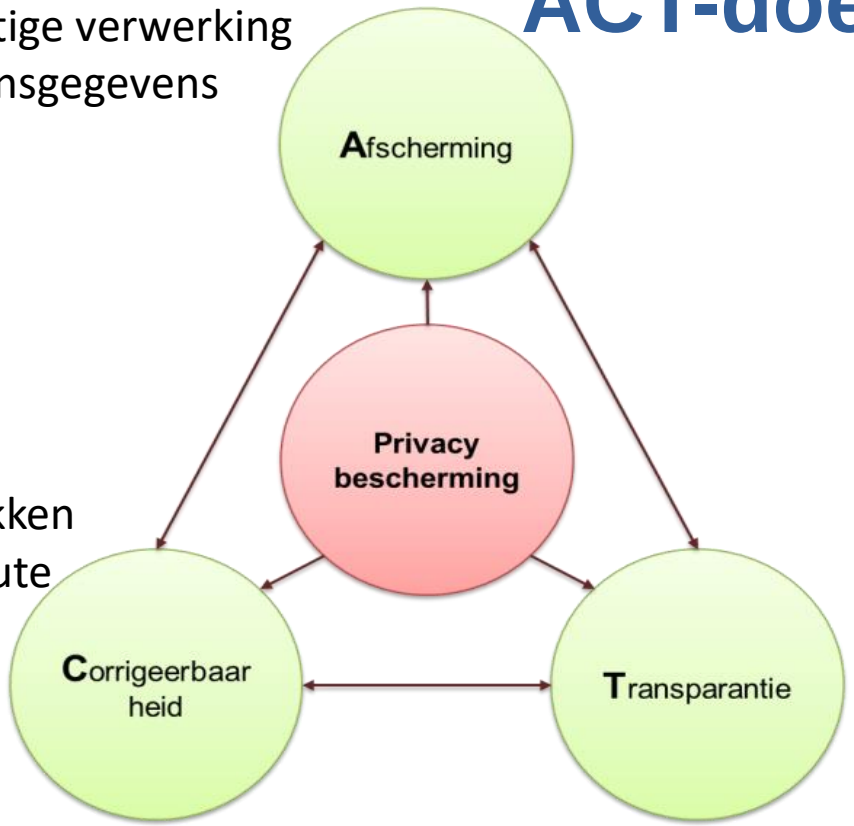
Hoe moeten organisaties er mee werken?

Hoe krijgen we duidelijkheid in de wirwar aan informatie en meningen?

Privacy beschermen
=
ACT-doelen realiseren

Voorkomen van:

- onrechtmatige verwerking van persoonsgegevens
- datalekken



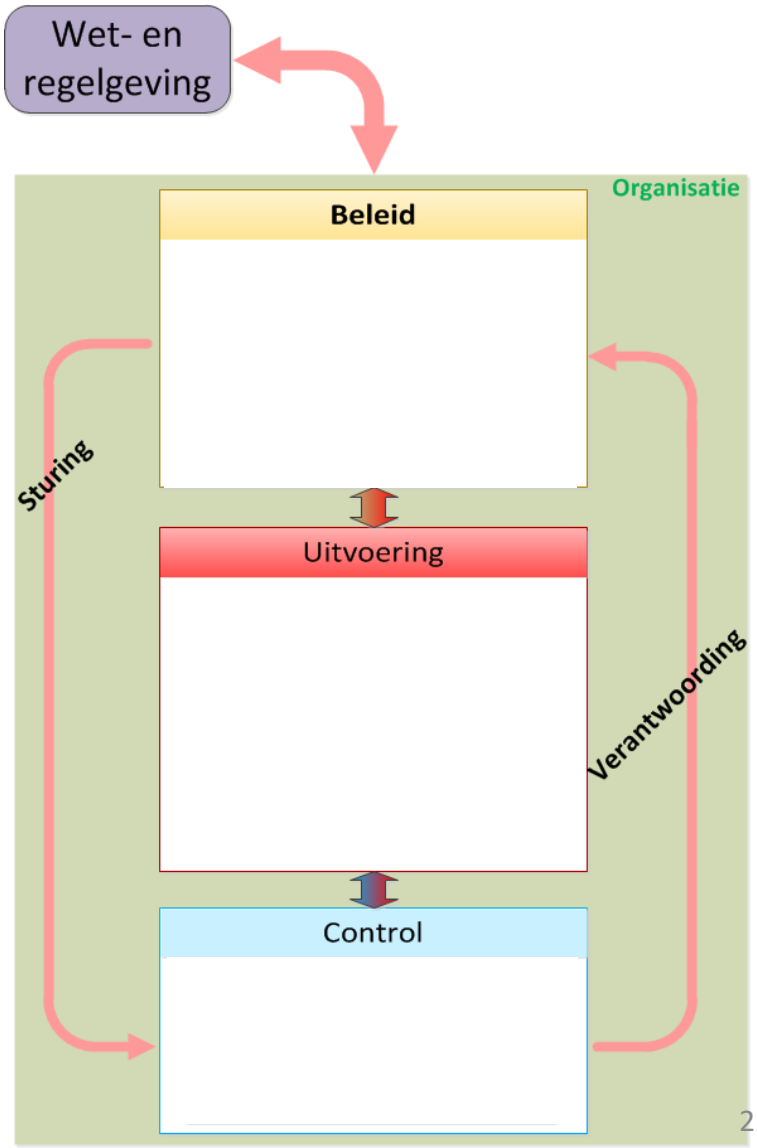
- Voorkomen van benadeling betrokken personen door foute en ongewenste verwerking

- Bieden van inzicht aan betrokkene omtrent juistheid registratie
- In control brengen betrokkene en organisatie

Privacy Baseline

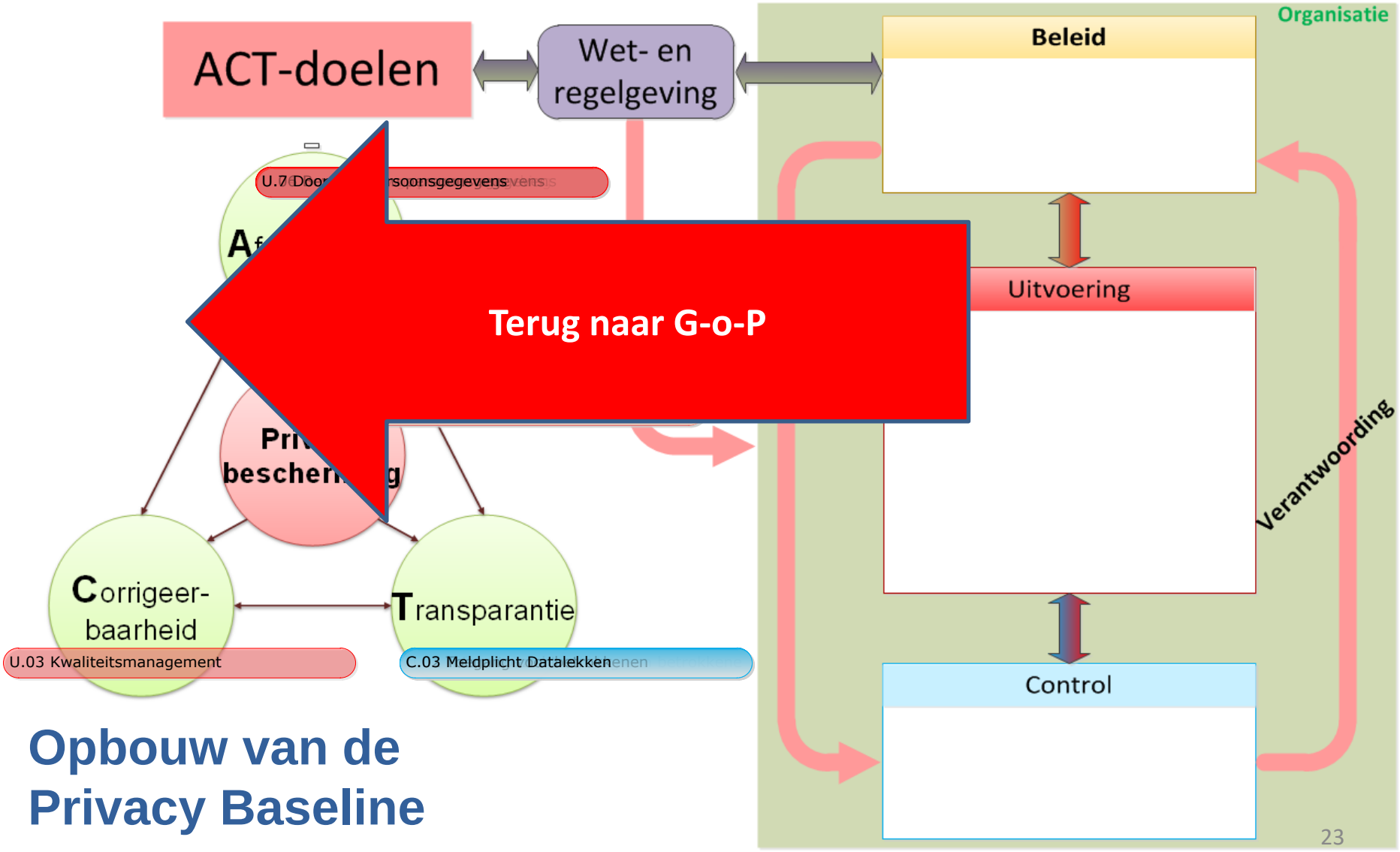
Criteria zijn opgedeeld naar:

- **Beleid:**
  Geeft richting en kaders
- **Uitvoering:**
  Verwerkt persoonsgegevens
- **Control:**
  Toont compliancy aan



Resultaat:

- Lerende organisatie
- Intern en extern toezicht en verantwoording
- Betere kwaliteit van dienstverlening



Opbouw van de Privacy Baseline