

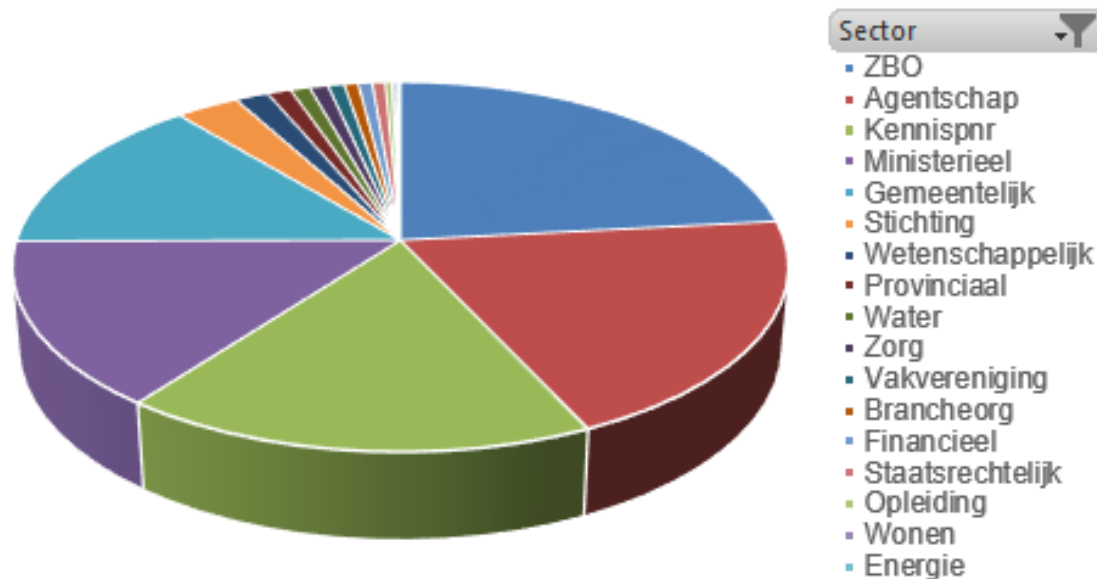
# **Samen – werken aan informatieveiligheid & Privacy**

**PILab-ECP-CIP stoppen er energie in.**

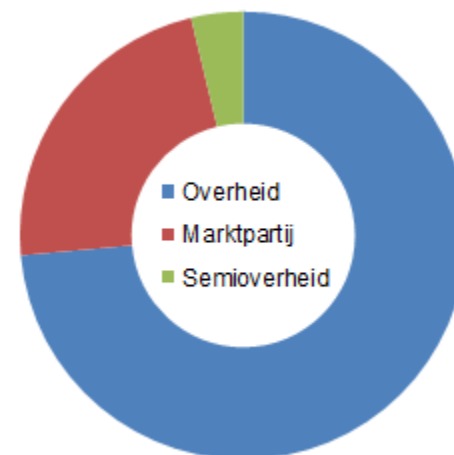
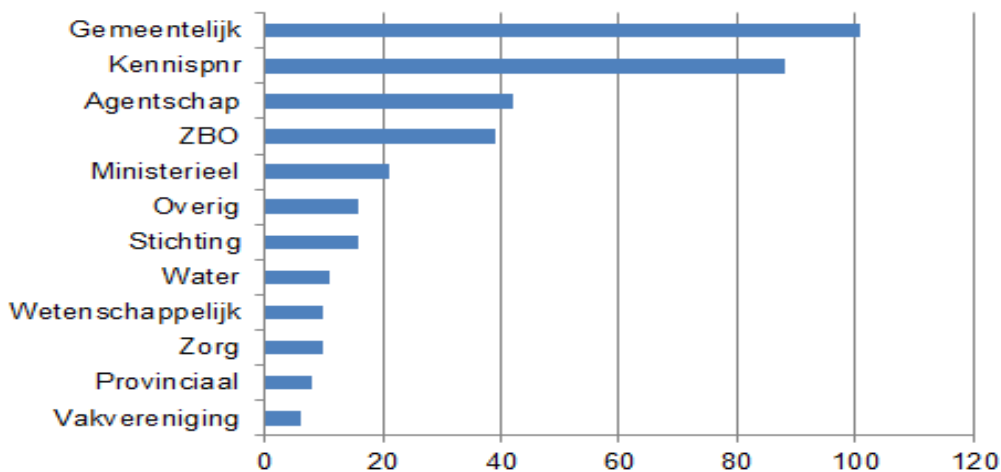
**7-11-2017**

# Samenstelling CIP-Netwerk 1-9-17

2044 personen in het CIP-netwerk



## Aantallen organisaties naar sector



# De PDC in Context

## CIP-activiteiten en producten

### Weerbaarheid

### Herstelvermogen

#### Bevorderen SAMEN DOEN

- > Practitioners Communities voor: SSD, BIR, Awareness, Inkoop, privacy
- > Diverse werkgroepen
- > Workshops: SSD, Priv. Self Assessment
- > Privacy Vraagbaak

- > Snelle onderlinge bereikbaarheid in CIP-netwerk via [cip.peio](http://cip.peio).
- > Verbinding met NCSC.
- > Moderatie Serious Games CIP

#### Product Aanbod

- > SSD-producten, KSL, div. handreikingen
- > BIR-OP en Thema-uitwerkingen
- > Grip op Privacy + Priv.Normenkader
- > PIA-paper en practices
- > Grip op Veilige Inkoop
- > e-Learningmodules,
- > CIP-Casts, etc

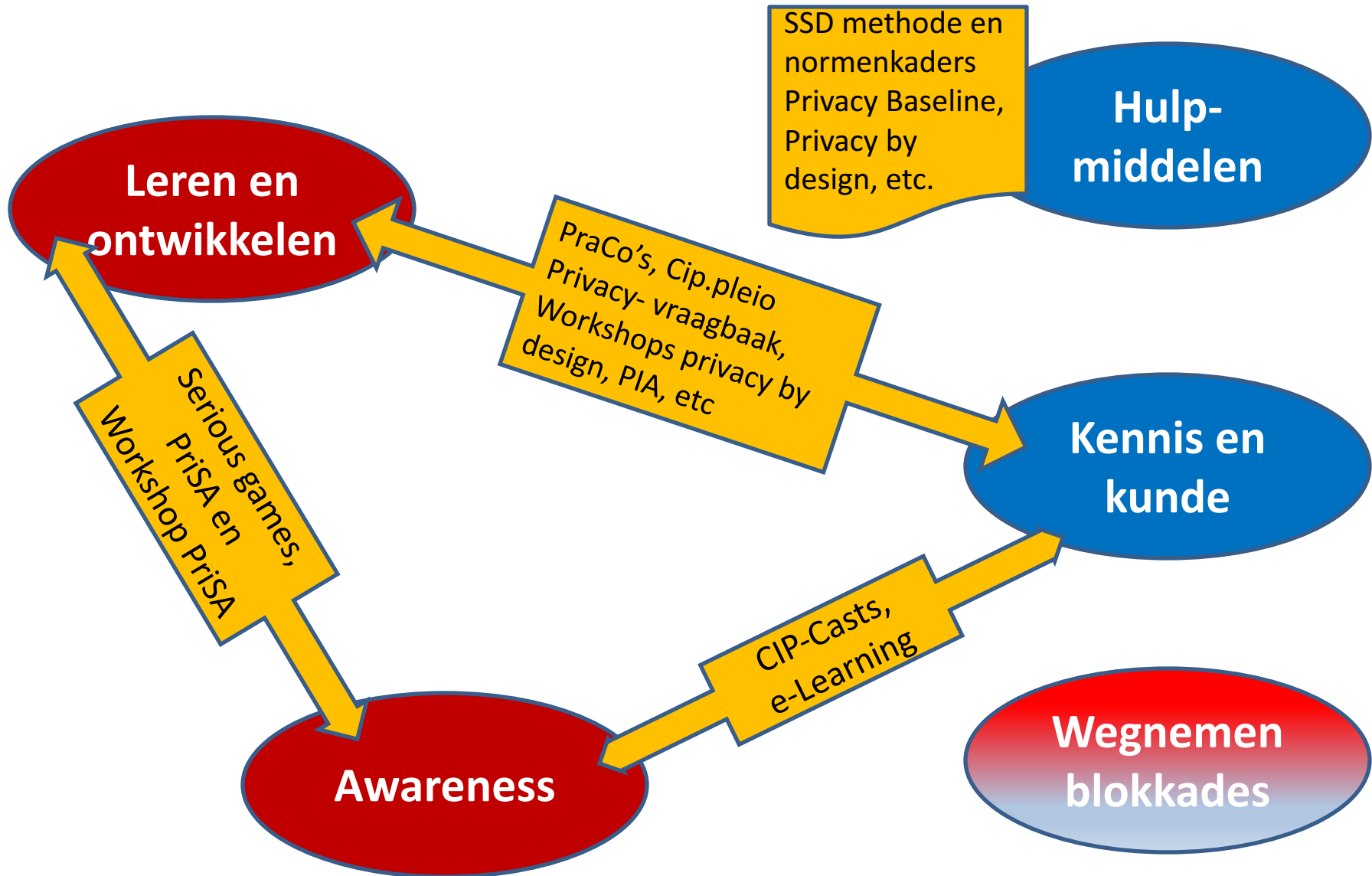
- > Serious game: Crisis Rijksdienst
- > Serious game: Crisis Gemeente
- > Netwerk game
- > Model Protocol Crisis Communicatie

#### Basis- werkvormen Kennisdeling

- > 4 Domeingroepen,
- > Kennissessies,
- > Conferenties
- > [Cip.pleio.nl](http://Cip.pleio.nl)

- > Subcommunity Cyber Security Platform (Sinds Opzet Rijks-ISAC slapend)
- > Opgezet: Rijks-ISAC

# Responsible Behavior



# De Websites

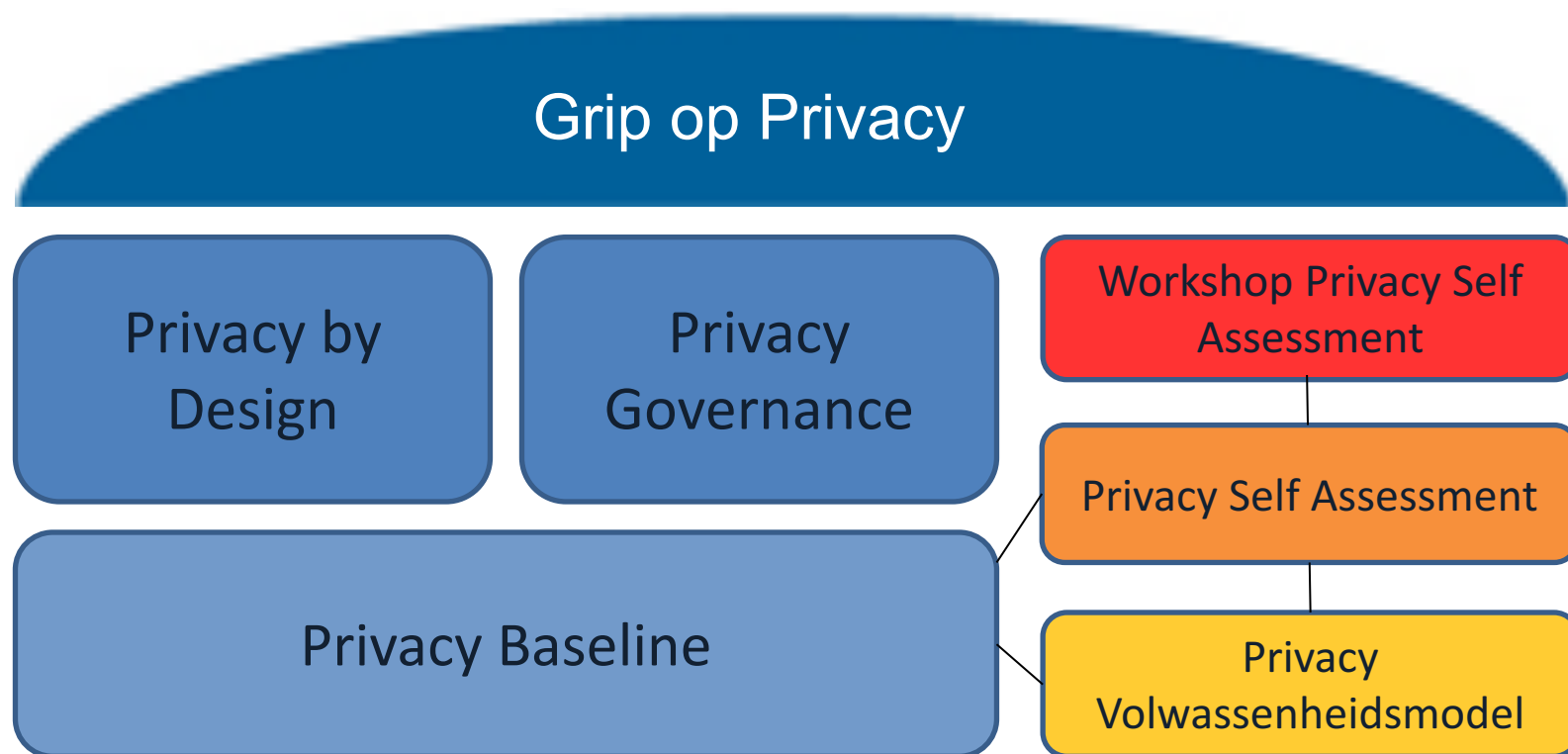


# Kernwaarden van de Avg

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

# Grip op Privacy

## CIP-handreikingen om in control te komen



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.

**Doe de Privacy Self Assessment**

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
<b>IN IEDER GEVAL uw sector:</b>	<b>een keuze uit de lijst &gt;&gt;&gt;</b>



# Workshop Privacy Self Assessment

## Voorbeeld nog niet behandelde criterium/vraag

B.01 Privacybeleid		niveau:	Verdeling van de antwoorden	Antwoorden gegeven door:	Ruimte voor notities (De notities worden in het advies meegenomen.)
 <p>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.</p>					
<p>Hoe is de Avg geconcretiseerd in het privacybeleid?</p> <p><b>Uitleg: Privacybeleid</b></p> <p>(Kies het meest formele / hoogste niveau in de organisatie dat volgens u van toepassing is.)</p>	<input type="radio"/> Er is geen concretisering van de Avg.	0			<p>Het beleid en de procedures worden op organisatieniveau eenduidig vastgelegd en in organisatiebreed gebruikt (conform B.01/01).</p> <p>Notitie:</p>
	<input type="radio"/> Op verwerkingsniveau zijn <b>informeel</b> richtlijnen beschikbaar.	1	3	MW4 MW6 Mw8	
	<input type="radio"/> Binnen de organisatie zijn richtlijnen <b>vastgelegd</b> .	2			
	<input type="radio"/> Organisatiebreed zijn beleid en richtlijnen <b>eenduidig</b> beschikbaar en <b>formeel vastgesteld</b> .	3	1	marie	
<p>Hoe worden de wettelijke beginselen toegepast?</p> <p><b>Uitleg: Wettelijke beginselen</b></p> <p>(Kies het meest formele / hoogste niveau in de organisatie dat volgens u van toepassing is.)</p>	<input type="radio"/> Beslissingen over het toepassen van de wettelijke beginselen worden op ad hoc basis genomen.	0			<p>Beleidsbeslissingen over het toepassen van de wettelijke beginselen worden gebaseerd op privacybeleid op organisatieniveau, volgens de procedures die op organisatieniveau vastgelegd zijn. De beslissingen worden op organisatieniveau formeel vastgesteld (conform B.01/02).</p> <p>Notitie:</p>
	<input type="radio"/> Beslissingen over het toepassen van de wettelijke beginselen worden op verwerkingsniveau <b>informeel</b> genomen.	1	2	jan Mw8	
	<input type="radio"/> Beslissingen over het toepassen van de wettelijke beginselen worden op verwerkingsniveau <b>formeel</b> genomen en <b>vastgelegd</b> .	2	3	piet MW4 MW6	
	<input type="radio"/> Beslissingen over het toepassen van de wettelijke beginselen worden op verwerkingsniveau <b>eenduidig</b> en <b>formeel</b> genomen en <b>vastgesteld</b> .	3	1	marie	
<input type="checkbox"/> De eenduidigheid van de beleidsbeslissingen wordt op afdelingsniveau <b>formeel</b> bewaakt.		2	3	Eens: MW4 MW6 Mw8 Oneens: piet jan marie	De juistheid en de eenduidigheid van de beleidsbeslissingen worden op afdelingsniveau formeel bewaakt.
<input type="checkbox"/> De eenduidigheid van de beleidsbeslissingen wordt op afdelingsniveau <b>informeel</b> bewaakt.		3	3	Eens: piet marie MW6 Oneens: jan MW4 Mw8	De juistheid en de eenduidigheid van de beleidsbeslissingen worden in een procedureel proces formeel bewaakt.
<input type="checkbox"/> Ontwikkelingen in relevante wet- en regelgeving worden actief door de organisatie gevolgd, zodat de impact op het beleid bekend is alvorens de wet- en regelgeving wordt toegepast.		4	4	Eens: piet MW4 marie	

**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

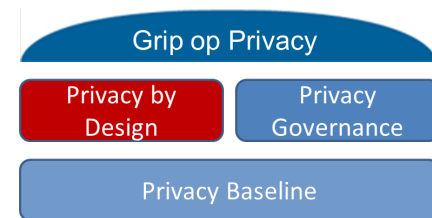
- datalekken en geslaagde hackpogingen vaak het gevolg zijn van zwakheden in software,
- het niet toereikend is een algemene afspraak te maken over de veiligheid van software,
- de opdrachtgever voor ontwikkeling en onderhoud van software een zorgplicht heeft in zijn rol van opdrachtgever en van hem 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 ontleen 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 offerteproses 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. |

# 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.**

# Privacy by design

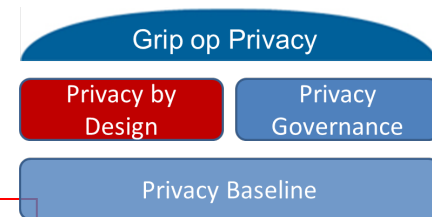


Gaat eigenlijk over:

**Houding en gedrag ontwerpers**

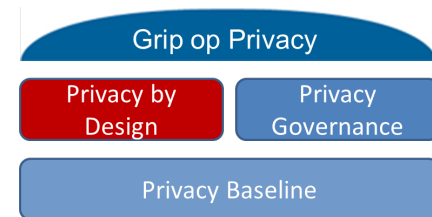
maar ook:

**Waar in het ontwerpproces  
moet aan welk criterium  
gedacht worden**



# Principes in het ontwerpproces

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



Privacy by Design

*The 7 Foundational Principles*

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

Terug naar G-o-P

A large red arrow with a black outline points from the right towards the left, indicating a return to the 'G-o-P' (Grijp op Privacy) framework.