ISACA®

Vertrouwen in en waarde uit informatiesystemen

Netherlands Chapter

A recognized global leader in
IT governance, control and assurance

Ronde tafel – Privacy Frameworks

5 november 2018

iRISK

Agenda

1. Opening - Kennisgroep Privacy (Fokke Jan)
2. Met een privacyraamwerk (beter) in control ?(Ronald)
3. NOREA - Privacy Control Framework (Jan)
4. CIP - Privacy Baseline & Maturity Model (Marcel)
5. ISACA - Privacy Framework & hulpmiddelen (Menno)
6. Do’s & Don’ts bij toepassing Frameworks in de praktijk (Menno)
7. Privacy stellingen voor discussie
8. Sluiting (Fokke Jan)

ISACA®
Vertrouwen in en waarde uit informatiesystemen
Netherlands Chapter

A recognized global leader in
IT governance, control and assurance

1. Opening - Kennisgroep Privacy

iRISK

2. Met een privacyraamwerk (beter) in control ?

Privacy & AVG:

met een privacyraamwerk (beter) in control ?

Ronald Koorn, ISACA ronde tafel, 5 november 2018

Korte historie privacyraamwerken in NL

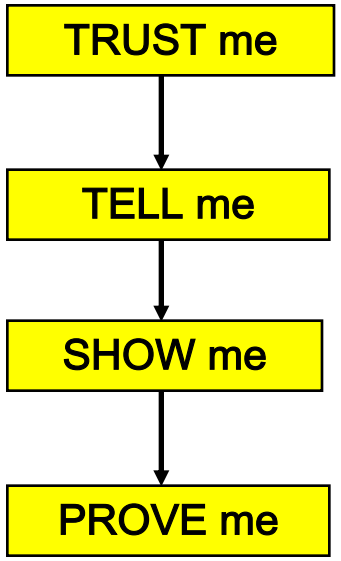
- Wpr: Advies Beveiliging Persoonsgegevens (RK, 1994)
- Wpr: 1e formele privacyaudit (RK & KPMG, 1995)
- Wbp: Beveiliging van persoonsgegevens (RK, AV23, 2001)
- Wbp: Quickscan, Zelfevaluatie en Raamwerk Privacy Audit (RK, 2001)
- Wbp: Contouren voor Compliance & Richtlijn 3600 voor Privacy Audit Proof (NOREA & NIVRA/NBA, 2005 – 2006)
- Wbp: Richtsnoeren Beveiliging van persoonsgegevens (CBP, 2013)
- AVG: Privacy Baseline (CIP, 2017)
- GDPR: Privacy Principles and Program Management Guide (ISACA, 2017)
- GDPR: GDPR Implementation Guide (ISACA, 2018)
- AVG: Privacy Control Framework (NOREA, 2018)

- Overigen: EuroPrise, AICPA/CPA Canada (GAPP & SOC2/3), KPMG, BSi, NEN, ISO…etc.

© 2018 KPMG Advisory N.V., registered with the trade register in the Netherlands under number 33263682, is a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Nut & noodzaak privacyraamwerken

- **Volledigheid AVG-dekking**
- **Gestructureerde set ‘good practices’**
- **Onderbouwing van Binding Corporate Rules en Code of Conducts**
- **Vertaalslag privacybeleid → operatie (samenhang processen – mensen – techniek)**
- **Borging in PDCA-cyclus**
- **Invulling accountability / privacyverantwoording**
- **Kunnen mappen van meerdere compliancegebieden**
- **Gestandaardiseerd vertrouwensniveau in ketens & samenwerkingsverbanden en bij uitbesteding**
- **Interoperabiliteit**
- **Audit- of certificeringscriteria**



© 2018 KPMG Advisory N.V., registered with the trade register in the Netherlands under number 33263682, is a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

Er is echter ook aantal beperkingen/nadelen

- **Keurslijf**
- **Omvang & impact / kosten van toepassing**
- **Onderbelicht zijn van privacy managementsysteem**
- **Weinig/geen aandacht voor ‘soft controls’, een essentieel fundament van privacy**
- **Ontstaan van teveel raamwerken**
- **Geeft beperkt antwoord op privacy-uitdagingen:**
  - Hoever reikt mijn verantwoordelijkheid in deze keten?
  - Hoe organiseer ik inzage- en verwijderverzoeken in ons IT-landschap?
  - Met welke partijen zijn verwerkersovereenkomsten nodig?
  - Welk niveau privacybewustzijn is toereikend?
  - Wat zijn de wettelijke bewaartermijn voor al onze informatie?
  - Hoe pas ik Privacy by Design toe?

KPMG

© 2018 KPMG Advisory N.V., registered with the trade register in the Netherlands under number 33263682, is a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

Toepassingsgebieden

1. **Implementatieproject → maatregelen per eis**

2. **Operatie → volledige opname in beleid, richtlijnen, procedures, systemen, e.d.**

3. **Interne nulmeting/review/audits → vertaling raamwerk in audit werkprogramma**

4. **Externe privacy-assurance / AVG-certificering → normatiek**

© 2018 KPMG Advisory N.V., registered with the trade register in the Netherlands under number 33263682, is a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

3. NOREA – Privacy Framework

NOREA
Privacy Control Framework

…Op weg naar “In Control” …

Jan de Heer

5 november 2018

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Ter relativering … D-day 25 mei 2018

Brenno de Winter
@brenno

Following

Het is 25 mei AVG-dag. Ondanks al het gejammer is de zon opgekomen, varen er boten en rijden de treinen nog. De aarde is niet vergaan. 😂

Translate Tweet

11:03 PM - 24 May 2018

Agenda

- Beroepsgroep NOREA
- Ontstaans–geschiedenis van het PCF
- Waarom een NOREA PCF ?
- Grondslag – doelstelling – gebruikers
- Informatiemanagement als uitgangspunt
- Structuur van het PCF

NOREA, de beroepsorganisatie van IT-auditors

- **Opgericht in 1992** (dus lustrumviering 25 jaar NOREA in 2017)
- 1682 registerleden – RE's
- 238 aspirant–leden, d.w.z. in opleiding
- 118 geassocieerde leden, d.w.z. interesse in vakgebied maar geen IT–auditopleiding genoten

- **Doelstellingen NOREA**
  - ✓ Bevorderen kwaliteit beroepsbeoefening
  - ✓ Bevorderen ontwikkeling vakgebied
  - ✓ Behartigen gemeenschappelijke belangen leden

Vaktechnische Ontwikkeling – vanuit NOREA

- Professionele ontwikkeling, ondersteund door Werk– en Kennisgroepen:
- Vaktechnische Commissie
- Commissie Beroepsregels
- **Werkgroep Assurance**
- **Kennisgroep Privacy**
- **Kennisgroep Cybersecurity**
- Kennisgroep Betalingsverkeer
- Kennisgroep ICT & Zorg
  Kennisgroep Software Development
- Kennisgroep Keteninformatiemanagement
- Werkgroep DigiD–Assessment
- Werkgroep IT & Financial Audit
- Zie **www.norea.nl**

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Een stukje geschiedenis – PCF

- 2001: Raamwerk Privacy Audit (door 'Samenwerkingsverband Audit Aanpak' onder verantwoordelijkheid CPB)
- 2002: ZekeRE Privacy (NOREA)
- 2006: Richtlijn 3600 Assurance–opdrachten met betrekking tot Persoonsgegevens (NBA, NOREA)
- 2006: Keurmerk 'Privacy Audit Proof'(NBA, NOREA, AP)
- 2016: Addendum NOREA Privacy Audit 2016 bij Richtlijn 3600n (NOREA)
- 2017: Besluit NOREA Bestuur i.o.m. KG Privacy en Vaktechnische Commissie om zowel Raamwerk als Richtlijn voor privacy audits te vernieuwen, mede in het licht van de AVG.
- **2018: 1 mei – Norea Guide 'Privacy Control Framework' (PCF)**

Waarom nu een “Privacy Control Framework”?

- Belangrijk: (nog) geen breed gedragen Europees referentie kader
- Vaststellen van de mate van compliance met privacy principes en –wetgeving
- Identificeren van verbeterpunten – implementatie
- Versterken van aantoonbaarheid van compliance (*accountability)*
- Geven van *zekerheid* aan management en stakeholders over privacybeheersing
- Onderscheid in de markt

Privacy Control Framework (PCF) - Grondslag - Doelstelling

- **Grondslag** – basis Privacy Control Framework (PCF):
  - ✓ Voortzetting van Referaat in het kader van afstuderen RE–studie door Ali Ougajou en Maurice Koetsier (ESAA)
    zie ook: Publicatie in "De IT–auditor"
  - ✓ Vervolgens gemodificeerd en aangepast – aansluiting met Assurance & AVG–GDPR

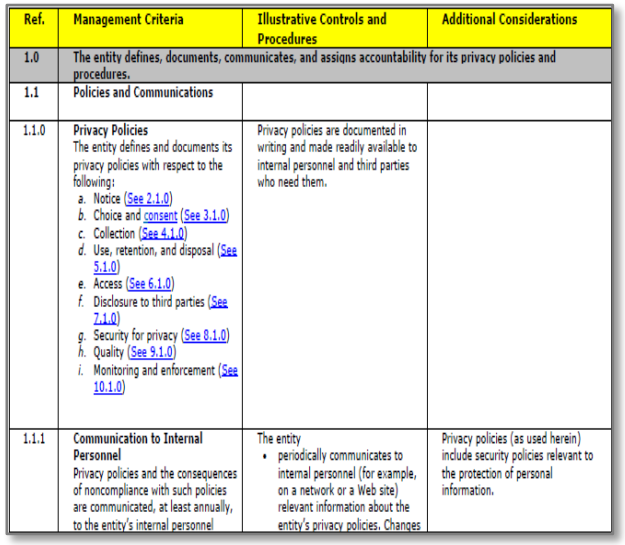
- **Doelstelling** – Privacy Control Framework (PCF) V1.0:
  - ✓ Objectieve beoordeling over hoe een organisatie omgaat met persoonsgegevens
  - ✓ Gebaseerd op risicobenadering en context–based
  - ✓ Gebaseerd op 'Best Practice' Privacy frameworks
  - ✓ Integratie benadering – Privacy – in samenhang met informatiemanagement
  - ✓ Inclusief aansluiting met belangrijke elementen van de AVG/GDPR
  - ✓ Lifecycle benadering – rondom verwerking van persoonsgegevens
  - ✓ inclusief Assurance gebaseerd op "Norea richtlijn 3000" –– A(ttestation of D(irect) reporting)

Gebruikers van Privacy Control Framework

Toepassing van het PCF – er worden **3 soorten gebruikers** onderscheiden:

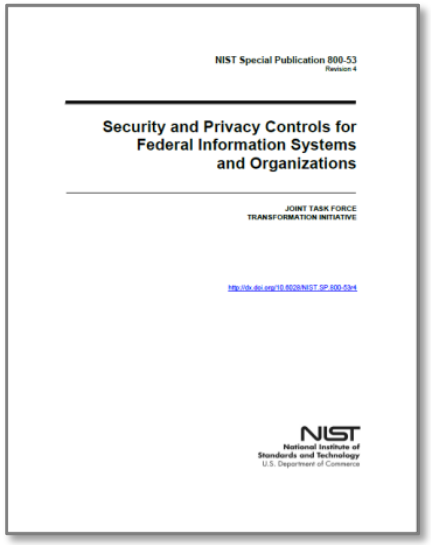
- De IT-auditor die de privacymaatregelen van een entiteit en het behalen van privacydoelstellingen beoordeelt, met als doel de mate van privacybeheersing of AVG-voorbereiding te beoordelen en tot een advies te komen;
- De IT-auditor die een privacy assurance-opdracht uitvoert en op basis van deze werkzaamheden een rapport uitbrengt, overeenkomstig 'assurance-standaard 3000'. De verwerking van persoonsgegevens kan op basis van een positief assurance-rapport desgewenst worden gecertificeerd als 'Privacy Audit Proof™';
- Andere professionals (zoals risicomanagers, functionarissen voor de gegevens-bescherming, beveiligings- en/of privacymedewerkers) die de privacy-impact of de stand van zaken van de AVG-implementatie in een entiteit wensen te beoordelen.

Grondslag PCF - Privacy Frameworks en Good Practices



Ref.	Management Criteria	Illustrative Controls and Procedures	Additional Considerations
1.0	The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.		
1.1	Policies and Communications		
1.1.0	**Privacy Policies** The entity defines and documents its privacy policies with respect to the following: a. Notice (See 2.1.0) b. Choice and consent (See 3.1.0) c. Collection (See 4.1.0) d. Use, retention, and disposal (See 5.1.0) e. Access (See 6.1.0) f. Disclosure to third parties (See 7.1.0) g. Security for privacy (See 8.1.0) h. Quality (See 9.1.0) i. Monitoring and enforcement (See 10.1.0)	Privacy policies are documented in writing and made readily available to internal personnel and third parties who need them.	
1.1.1	**Communication to Internal Personnel** Privacy policies and the consequences of noncompliance with such policies are communicated, at least annually, to the entity's internal personnel	The entity • periodically communicates to internal personnel (for example, on a network or a Web site) relevant information about the entity's privacy policies. Changes	Privacy policies (as used herein) include security policies relevant to the protection of personal information.

GAPP Framework



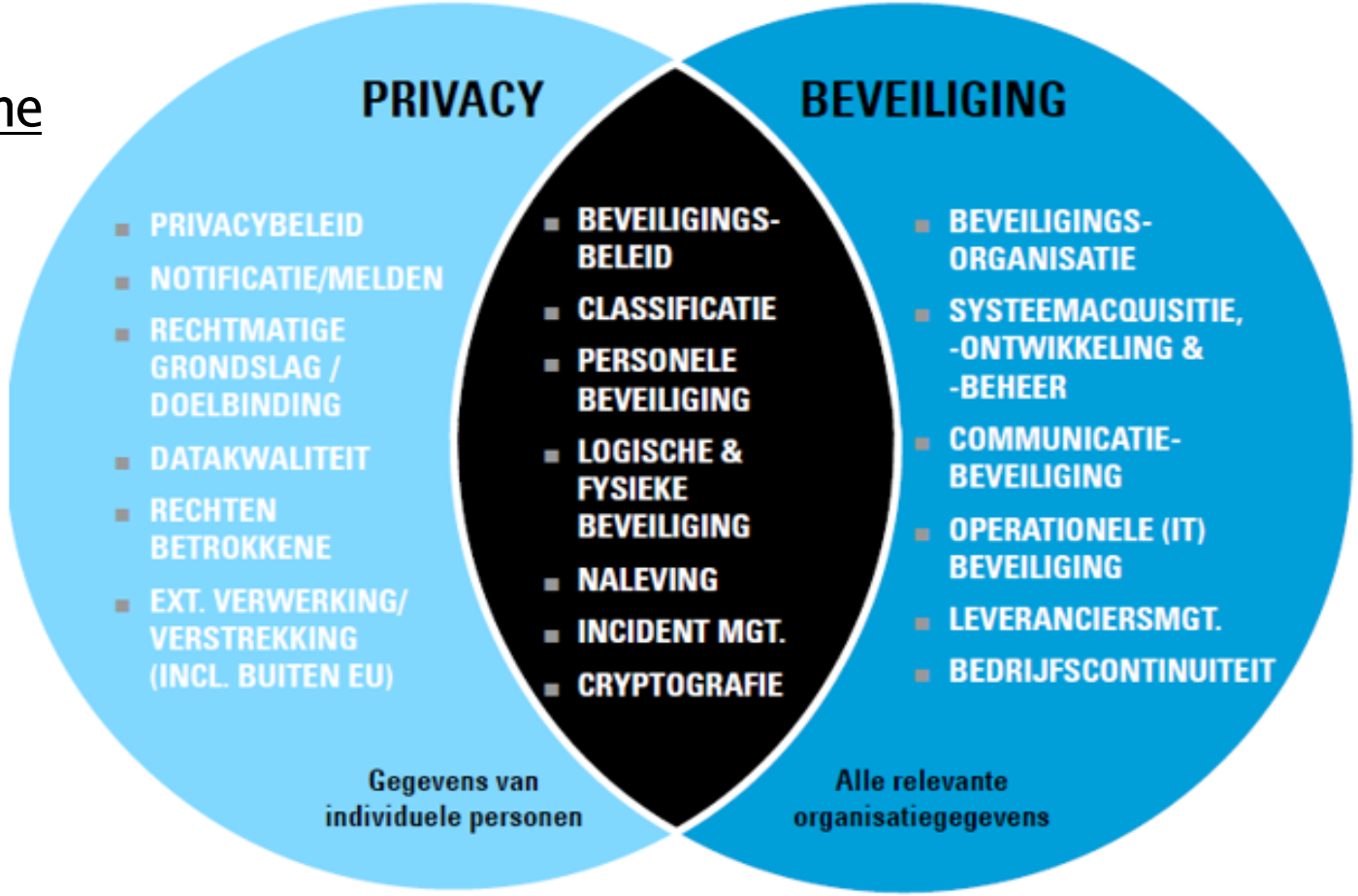
NIST SP800-R54 Privacy Control Catalog

NOREA 3600

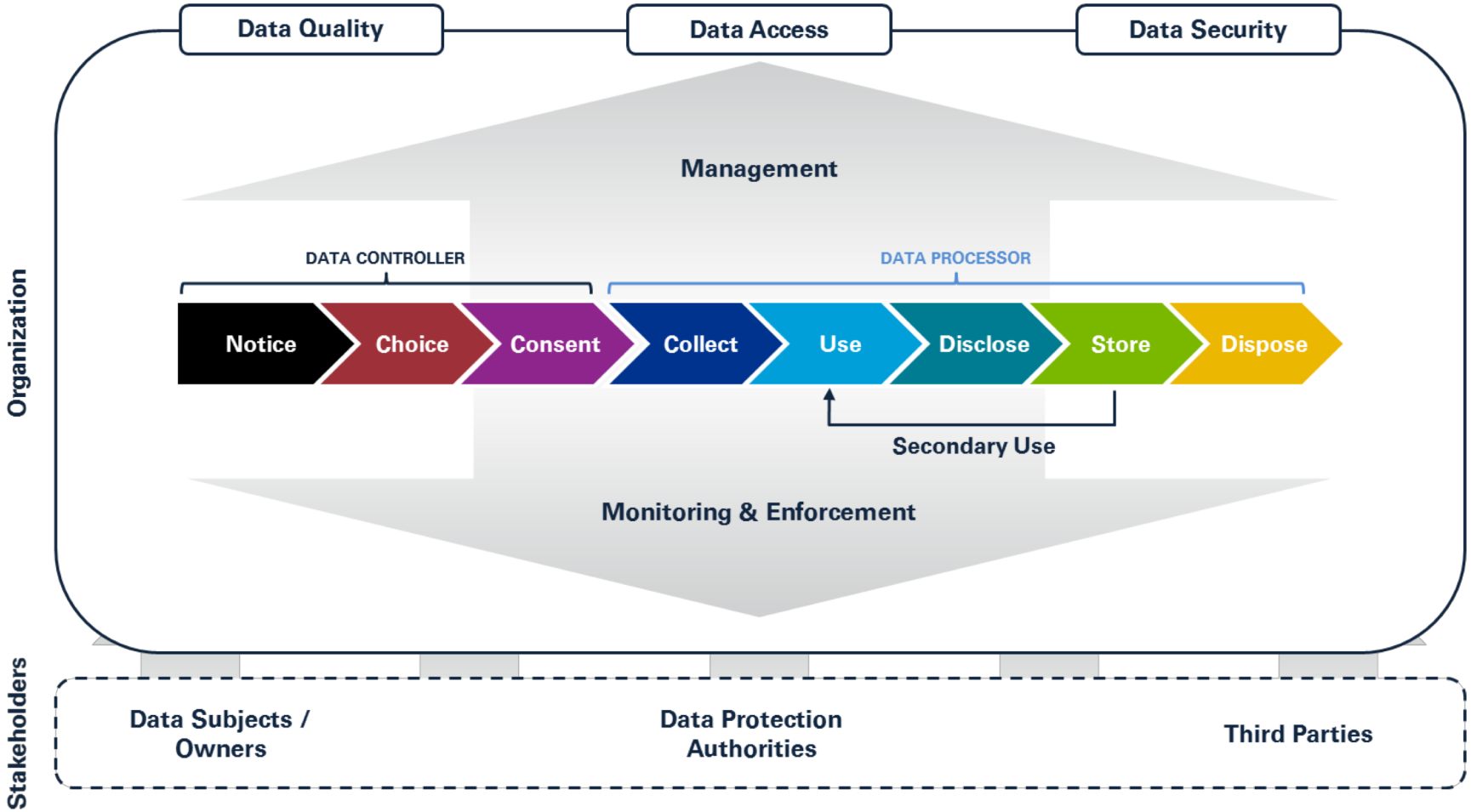
EuroPriSe Framework

Informatiemanagement als uitgangspunt

- Visie op privacy:
  - dient breder te zijn dan alleen juridische of technische perspectief
- Nadruk op praktische implementatie
  - Focus op beveiliging & privacy
- Dient Informatiemanagement te zijn:
  - Schakel tussen IT en bedrijfsvoering
  - Dataflow staat hierin centraal



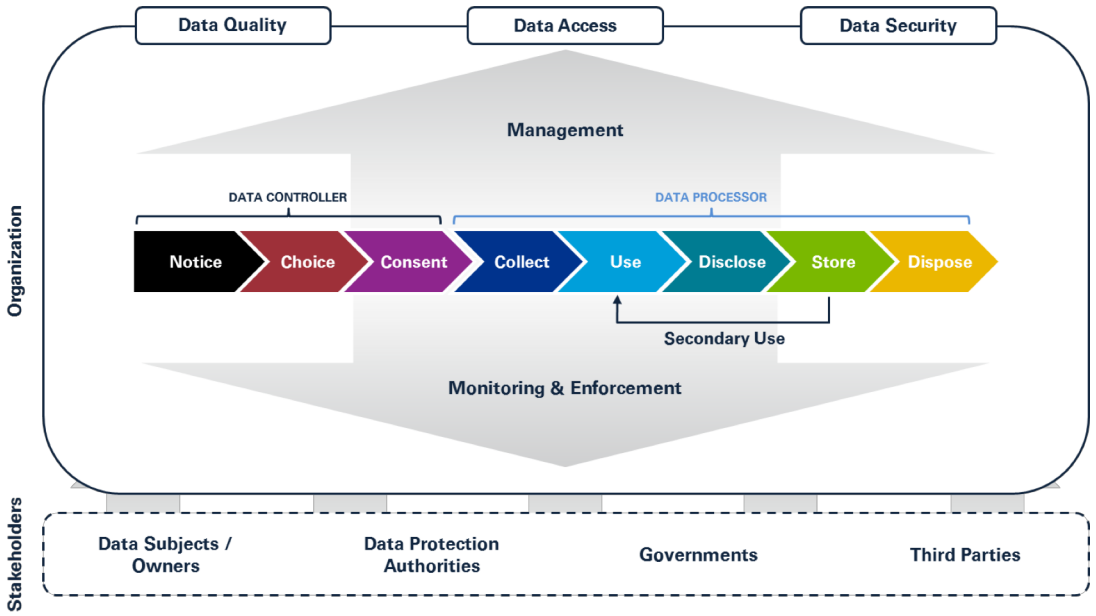
Informatielevenscyclusmodel - zie Annex 2 - PCF



NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Aansluiting “Privacy control objectives & controls ” met “Informatielevenscyclusmodel”

Structurering
Privacy Control objectives & controls binnen informatielevenscyclusmodel



Lifecycle phase	ID	Tag	Topic	Control objective	# Controls
Management	01.1, 01.1a, 01.1b	PPO	Privacy Policy	The entity has established and communicated a policy that states its objectives and responsibilities regarding privacy and is in line with accepted privacy principles and applicable laws and regulations.	5
	01.2, 01.2a	DRR	Definition of roles and responsibilities	The entity has established and implemented clear roles and responsibilities regarding the safeguarding of personal data and the achievement of privacy objectives.	5
	01.3	PDI	Personal Data Identification and classification	The entity understands and documents which personal data is stored and processed and identifies and treats personal data appropriately. Measures to safeguard personal data take into account the differences in sensitivity in personal data, leading to identification of risks and compliance with laws and regulations.	4
	01.4	RMA	Risk Management	The entity systematically and periodically identifies, assesses, and mitigates factors that endanger the achievement of privacy objectives.	5
	01.5	PIA	Data Protection Impact Assessments	The privacy-related impact of new products and services and their use within the entity is systematically identified, assessed and addressed.	6
	01.6	PIB	Privacy Incident and Breach Management	The entity adequately detects and handles privacy-related incidents; privacy-related incidents are responded to appropriately as to limit the consequences and to take measures to prevent future breaches.	9
	01.7	SCO	Staff competences	Staff in positions with access to or control over personal data and personal data processes have the necessary privacy competences to adequately perform their duties.	4

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Voorbeeld: “Control objectives” en “Controls”

Data Protection Impact Assessments (PIA)

Control objective:

The privacy-related impact of new products and services and their use within the entity is systematically identified, assessed and addressed.

Information Lifecycle Management phase: **Management**

Controls:		*Evidence/testing:*
PIA01	The entity deploys a managed and documented process to carry out an assessment of the impact on privacy regarding new or significantly changed processes, products and services.	
PIA02	The assessment takes into account the risks to data subject privacy presented by the changes envisaged, and the measures to mitigate these risks.	
PIA03	The assessment takes into account the purposes of processing in relation to the necessity and proportionality of processing personal data.	
PIA04	The process ensures that all relevant stakeholders are involved in the assessment, and that specific guidelines of the supervisory authority regarding assessment criteria are adhered to.	
PIA05	The entity documents all systems and software that process personal data and a history of changes applied to them.	
PIA06	The entity’s change management process assures that approved privacy measures from the assessment have been implemented before the change is executed.	

Related GDPR key elements:

- Data Protection Impact Assessment

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Aansluiting PCF met belangrijke artikelen uit de AVG-GDPR

- ✓ De aansluiting met kernelementen van de AVG–GDPR is geborgd – zie Annex 1– PCF

GDPR key element	GDPR article(s)
Privacy Principles	5
Lawfulness of Processing	6
Conditions for Consent	7
Rights of the data subject	12-19
Right to data portability	20
Privacy By Design / by Default	25
Responsibilities of controller and processor	24, 28
Records of processing activities	30
Security of processing	32
Personal Data Breach	33, 34
Data Protection Impact Assessment (DPIA)	35
Data Protection Officer (DPO)	37-39
Transfers of personal data to third countries or international organisations	44-50

- ✓ Kernelementen AVG geïnspireerd door:
  - ❖ "In 10 stappen voorbereid op de AVG" – van Autoriteit Persoonsgegevens (AP)

4. CIP – Privacy Framework

centrum informatiebeveiliging en privacybescherming

Samen – werken aan informatieveiligheid & Privacy

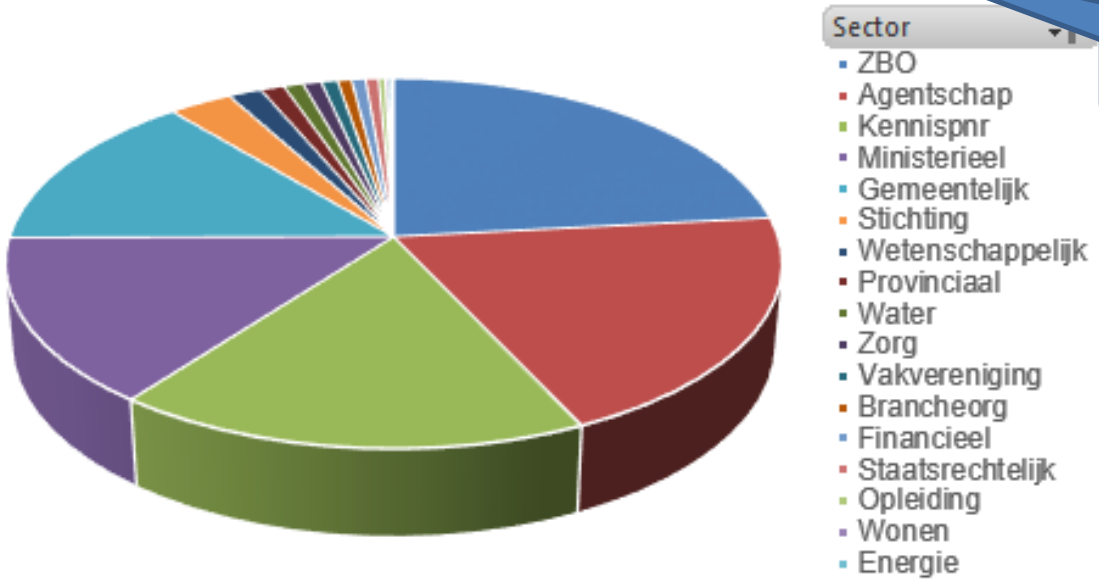
ISACA
5 november 2018

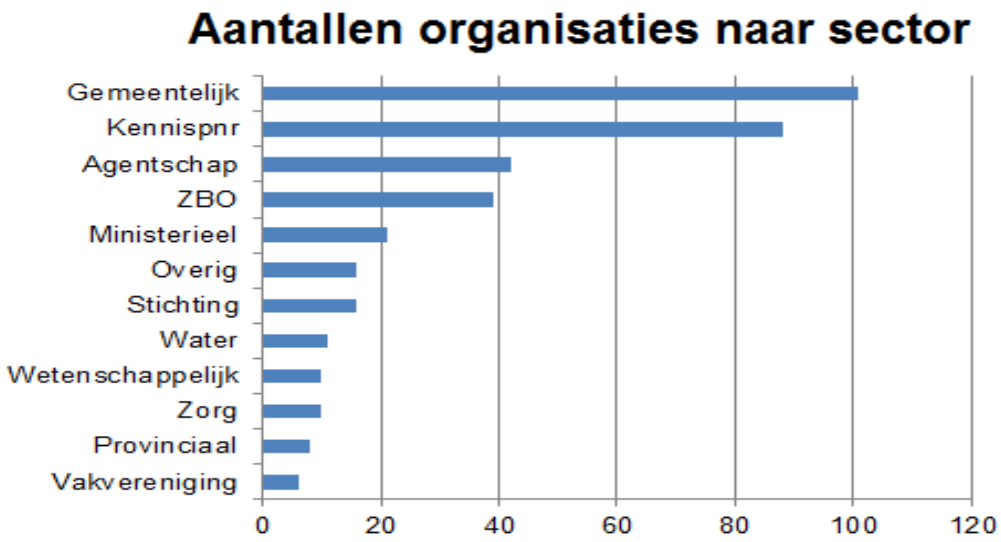
Marcel Koers / CIP

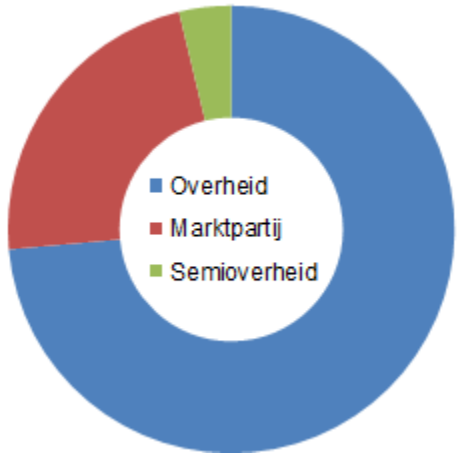
Samenstelling CIP-Netwerk 30-5-18

2412 personen in het CIP netwerk

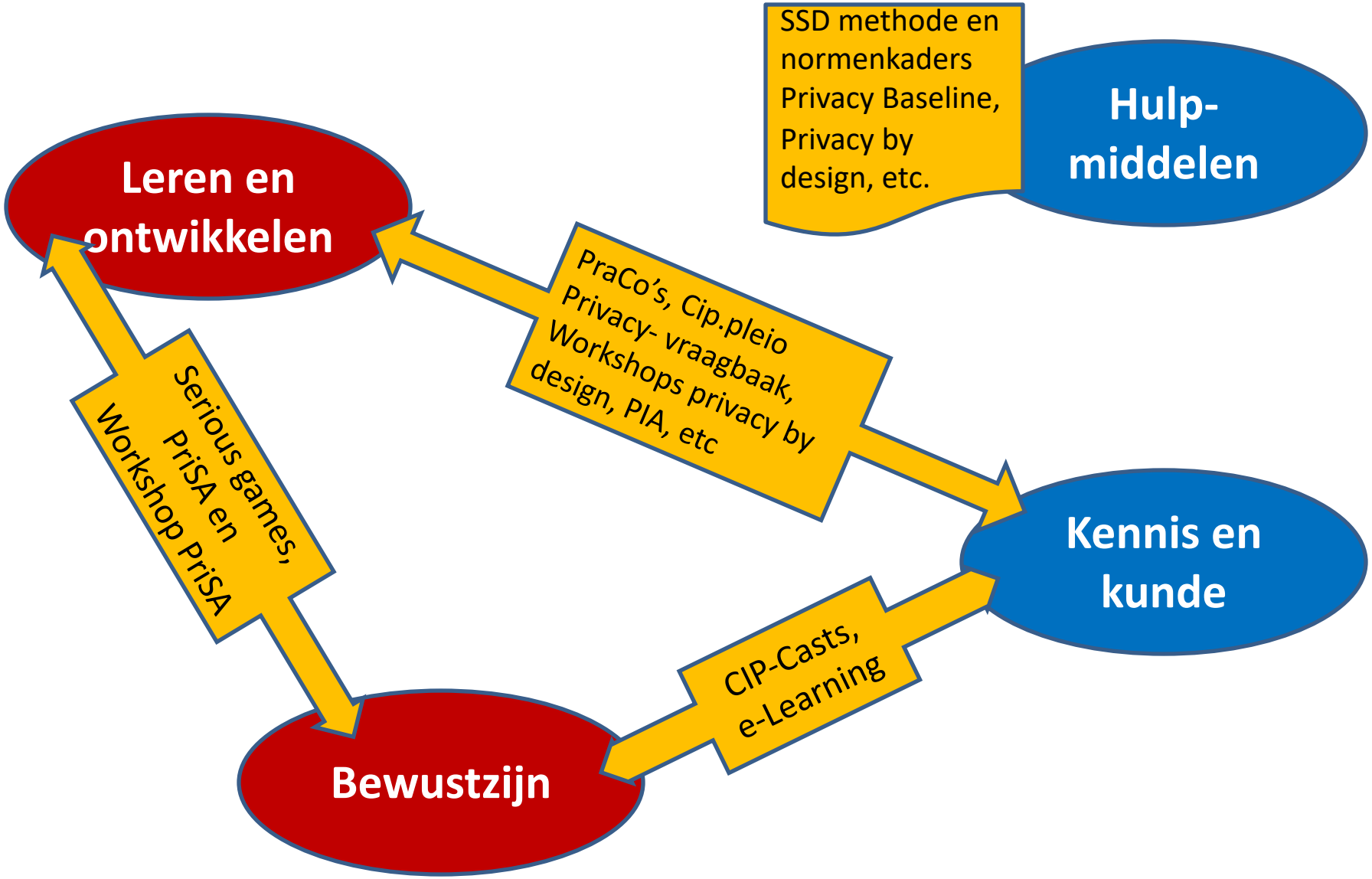
Nu ruim 2700 personen







“Responsible Behavior”



Aanleiding is een vraag uit de CIP community:

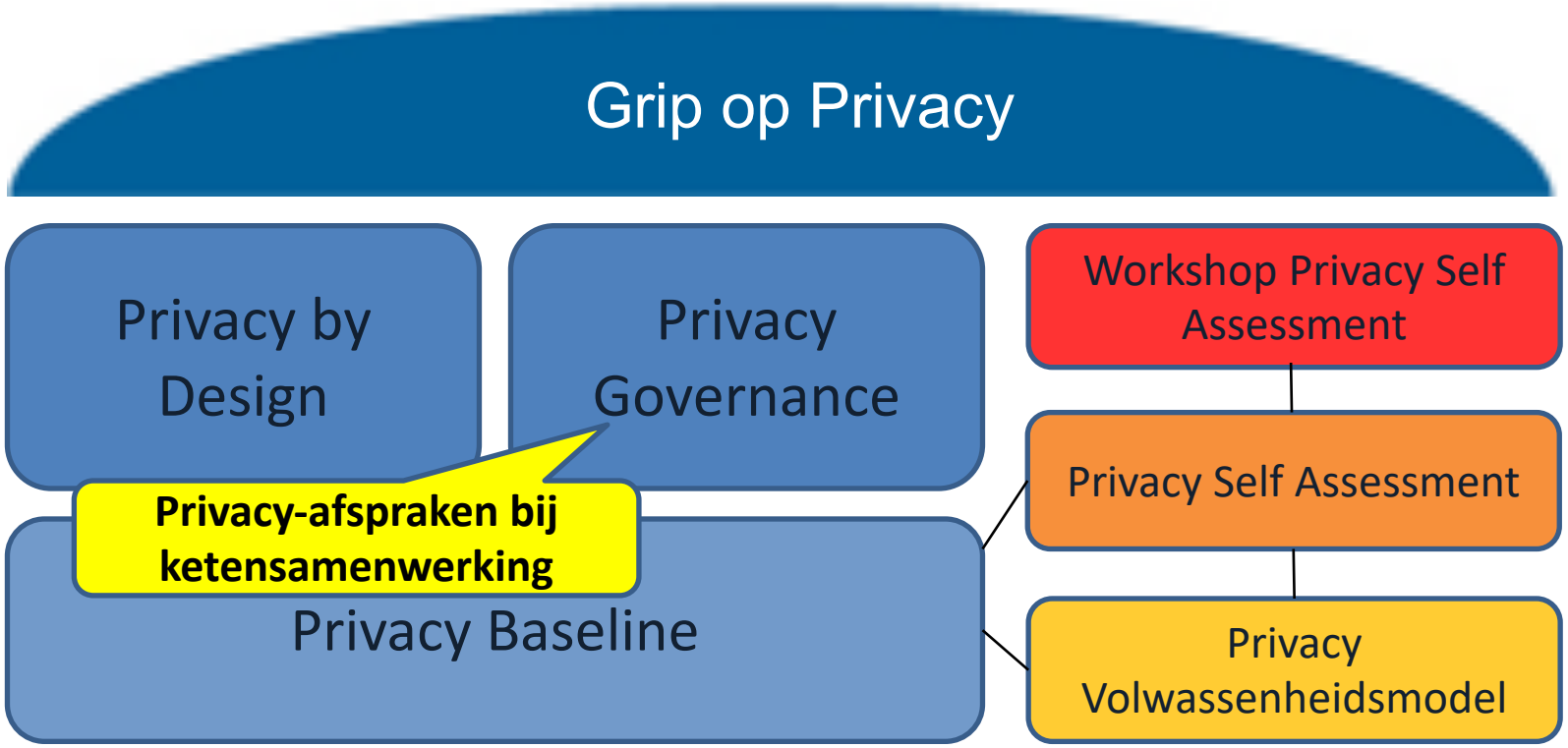
Kunnen jullie eens opschrijven hoe dat nou moet, met die privacy?

Hoe moeten organisaties er mee werken?

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

Grip op Privacy

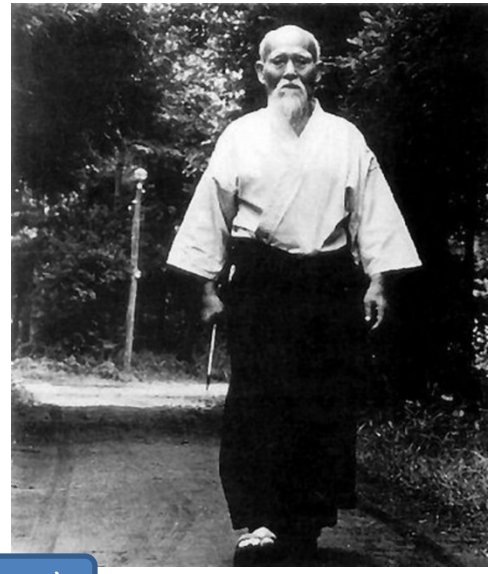
CIP-handreikingen om in control te komen



Het benutten van de kracht van de organisatie

Filosofie van Aikido:
Aikido is een lange tijd onopgemerkt gebleven. Inmiddels wordt aikido niet alleen beschouwd als een van de meest subtiele en verfijnde krijgskunsten maar vanaf een zeker niveau tevens als een effectieve discipline voor de ontwikkeling, integratie en toepassing van het totale menselijke potentieel, fysiek, mentaal en spiritueel.
…….

Basisprincipes:
- kamae (lichaamshouding) — Mindset (Grip op Privacy)
- ma-ai (ruimtelijk bewustzijn en afstand) — Prisa
- sen (timing) — Volwassenheidsmodel
- ki no nagare (vloeiende beweging) — PbD, Privacygovernance



Oprichter Aikido:
Morihei Ueshiba

Bronnen:
https://www.aikido.school/nl/filosofie/
https://nl.wikipedia.org/wiki/Aikido

Grip op Privacy maakt een andere mindset mogelijk

Tijdwinst en kostenbesparing

trainingen

Experts ontmoeten elkaar

Actief privacymanagement

Actief privacymanagement

Privacy Baseline

Stakeholders ontmoeten elkaar

PriSA en workshop PriSA

CIP Handreikingen: PbD en Privacy- Goverance, Privacybescherming in ketens

Volgen van gerichte kennissessies

CIP Praco Privacy, CIP vraagbaak, ……

COBIT Management guidelines

Gekeken naar:

- De taken en doelstellingen:

Privacy Baseline

- Kritische succesfactoren (KSF's) (het mogelijk maken van de doelstellingen):

Privacy Governance

- Metrieken (het meetbaar maken van de doelstellingen):

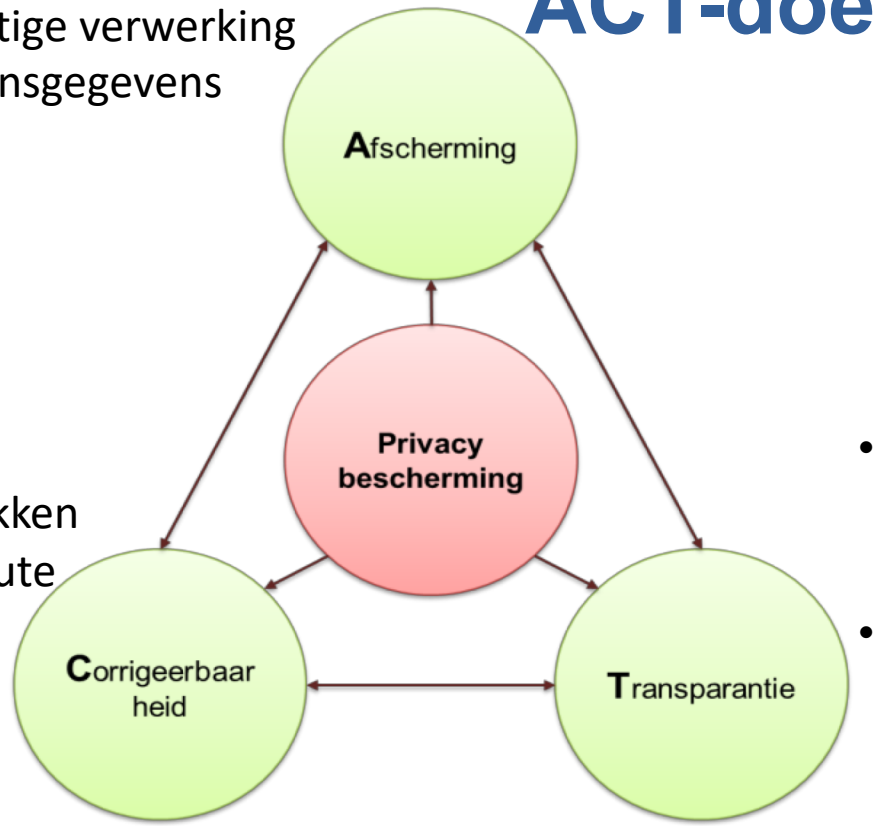
Privacy Volwassenheidsmodel

Privacybescherming: meer dan IB: ACT-doelen

Privacy beschermen
=
ACT-doelen realiseren

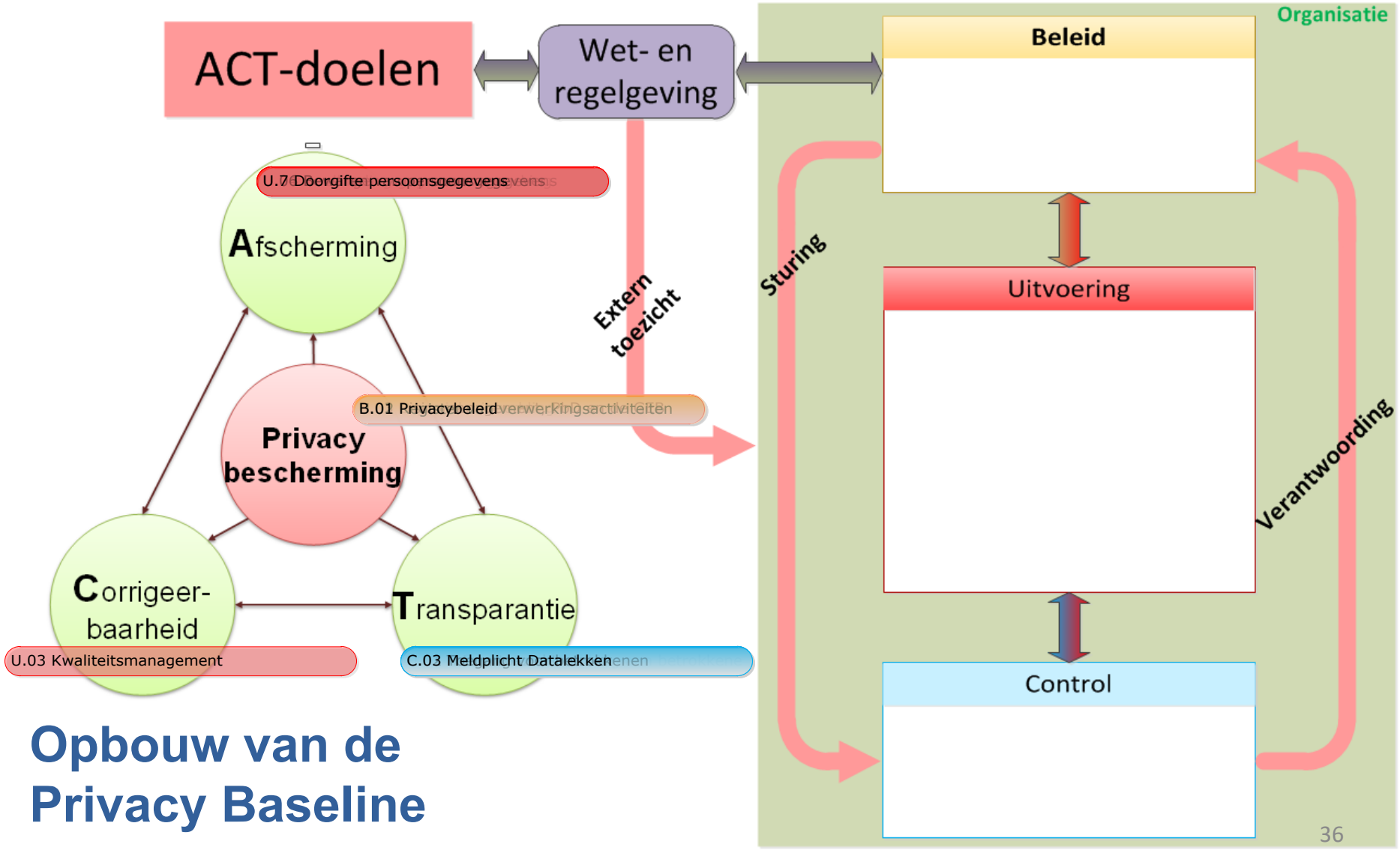
Voorkomen van:

- onrechtmatige verwerking van persoonsgegevens



- Voorkomen van benadeling betrokken personen door foute en ongewenste verwerking

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



Opbouw van de Privacy Baseline

U.06 Bewaren van persoonsgegevens			
Criterium	Door het treffen van de nodige maatregelen hanteert de organisatie voor persoonsgegevens een bewaartermijn die niet wordt overschreden.		
Doelstelling	Het doel van 'Bewaren persoonsgegevens' is te borgen dat persoonsgegevens niet langer worden bewaard dan noodzakelijk voor het te bereiken doel.		
Risico	Onnodig bewaarde persoonsgegevens kunnen worden verwerkt voor andere dan de oorspronkelijke doelen.		
Referentie	Avg	Uitvoeringswet Avg	
	Art. 5, lid 1e	Art. 43	
Maatregelen/indicatoren			
/01 Nodige maatregelen			
/01.01	Als de bewaartermijnen verlopen, zijn de gegevens vernietigd of geanonimiseerd.		
/01.02	De verantwoordelijke bepaald na elke verwerking van persoonsgegevens of er nog redenen zijn om de betreffende persoonsgegevens te bewaren.		
/02 Bewaartermijn			
/02.01	Van alle persoonsgegevens is de bewaartermijn vastgesteld en bekrachtigd.		
/02.02	De bewaartermijn is de maximale periode waarin de persoonsgegevens noodzakelijk worden bewaard om het doel van de verwerking te bereiken of niet langer dan de termijn die verankerd is in sectorspecifieke wetgeving[164].		
/02.03	Als in sectorspecifieke wetgeving een bewaartermijn is vastgelegd voor specifieke persoonsgegevens, dan geldt die bewaartermijn.		
/02.04	Wanneer persoonsgegevens voor langere perioden worden opgeslagen, dan worden ze louter met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden verwerkt[165] en zijn voor de rechten en vrijheden van de betrokkene ("opslagbeperking") passende waarborgen getroffen in overeenstemming met de Avg[166].		

SIVA-schrijfstijl voor audit-referentiekaders

(Wiekram Tewarie)

Privacy Volwassenheidsmodel

- Per criterium uit de Privacy Baseline zijn 5 niveaus beschreven
- Volwassenheidsniveaus zijn meetbaar gemaakt
- Iedere organisatie bepaald zijn eigen ambitieniveau

norm: minimaal niveau 3

- Voor kleine, middelgrote en grote organisaties

‘goed huisvaderschap’

- **Ambitieniveau wordt bespreekbaar**

Handreiking Privacy Governance

De principes van Aikido zijn verder ingevuld

- Principes van verandermanagement:
  Met als doel de kracht van de organisatie te benutten.

- Toegespitst op de ‘zachte’ veranderfactoren:
  “een wet maakt niet vanzelf goede privacybescherming.”

- Daarbij: kritische succesfactoren:
  Het bieden van handvaten om de criteria uit de privacy Baseline te realiseren.

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.

Hoe is de Avg geconcretiseerd in het privacybeleid?

Uitleg: Privacybeleid

(Kies het meest formele / hoogste niveau in de organisatie dat volgens u van toepassing is.)

- ○ Er is **geen concretisering** van de Avg.
- ○ Op verwerkingsniveau zijn **informeel** richtlijnen beschikbaar.
- ○ Binnen de organisatie zijn richtlijnen **vastgelegd**.
- ○ Organisatiebreed zijn beleid en richtlijnen **eenduidig** beschikbaar en **formeel vastgesteld**.

Worden de wettelijke beginselen van de AVG toegepast?

Uitleg: Wettelijke beginselen

(Kies het meest formele / hoogste niveau in de organisatie dat volgens u van toepassing is.)

- ○ Beslissingen over het toepassen van de wettelijke beginselen worden op **ad hoc** basis genomen.
- ○ Beslissingen over het toepassen van de wettelijke beginselen worden **op verwerkingsniveau informeel** genomen.
- ○ Beslissingen over het toepassen van de wettelijke beginselen worden **op afdelingsniveau** genomen en **vastgelegd**.
- ○ Beslissingen over het toepassen van de wettelijke beginselen worden **organisatiebreed eenduidig** en **formeel** genomen en **vastgesteld**.

- ☐ De juistheid en de eenduidigheid van de beleidsbeslissingen wordt op afdelingsniveau bewaakt.
- ☐ De juistheid en de eenduidigheid van de beleidsbeslissingen wordt organisatiebreed formeel bewaakt.

- ☐ 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 is vastgesteld.
- ☐ De kwaliteit (zoals actualiteit en bruikbaarheid) van het beleid en het beleidsproces is meetbaar en inzichtelijk op ieder niveau.

- ☐ Het hoogste management stuurt (waar nodig) bij op de kwaliteit van het beleid en de beleidsprocessen.

Klik hier om naar de START pagina te gaan

Klik hier om naar het volgende criterium te gaan

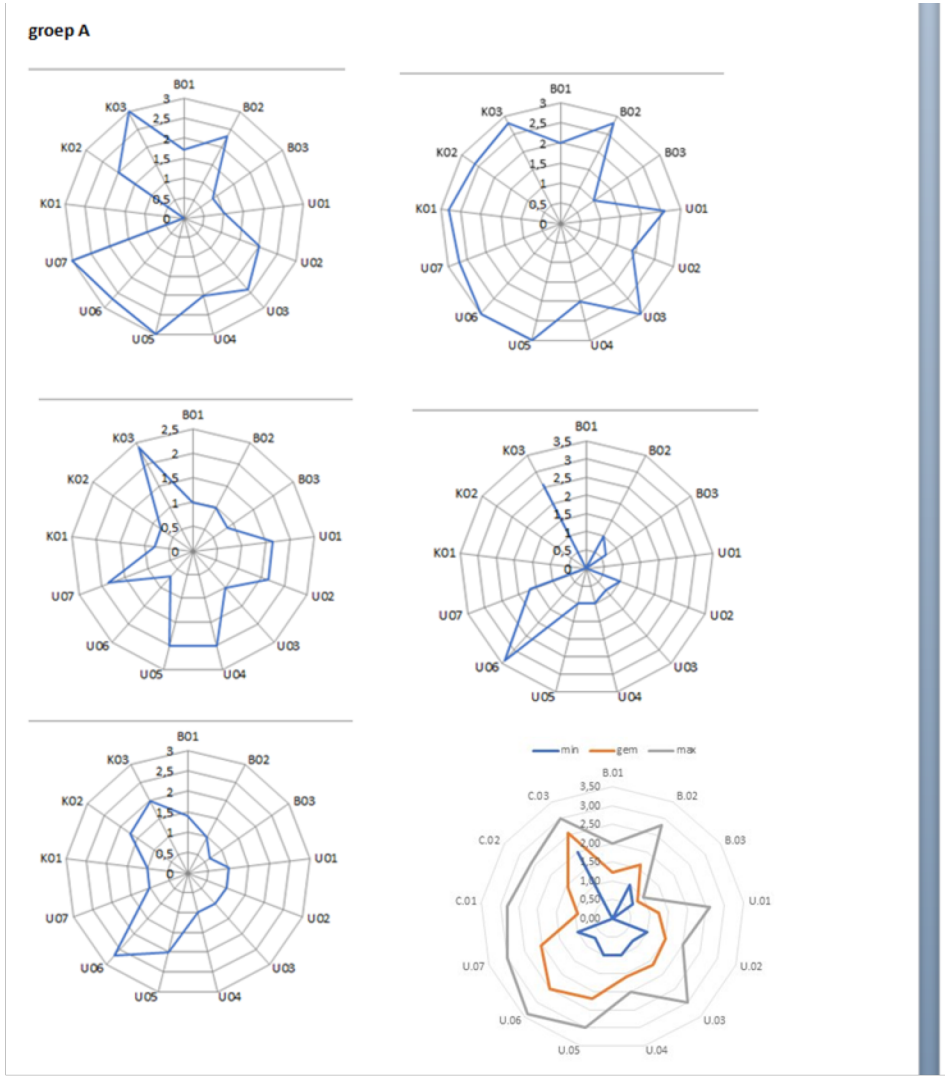
binnen uw

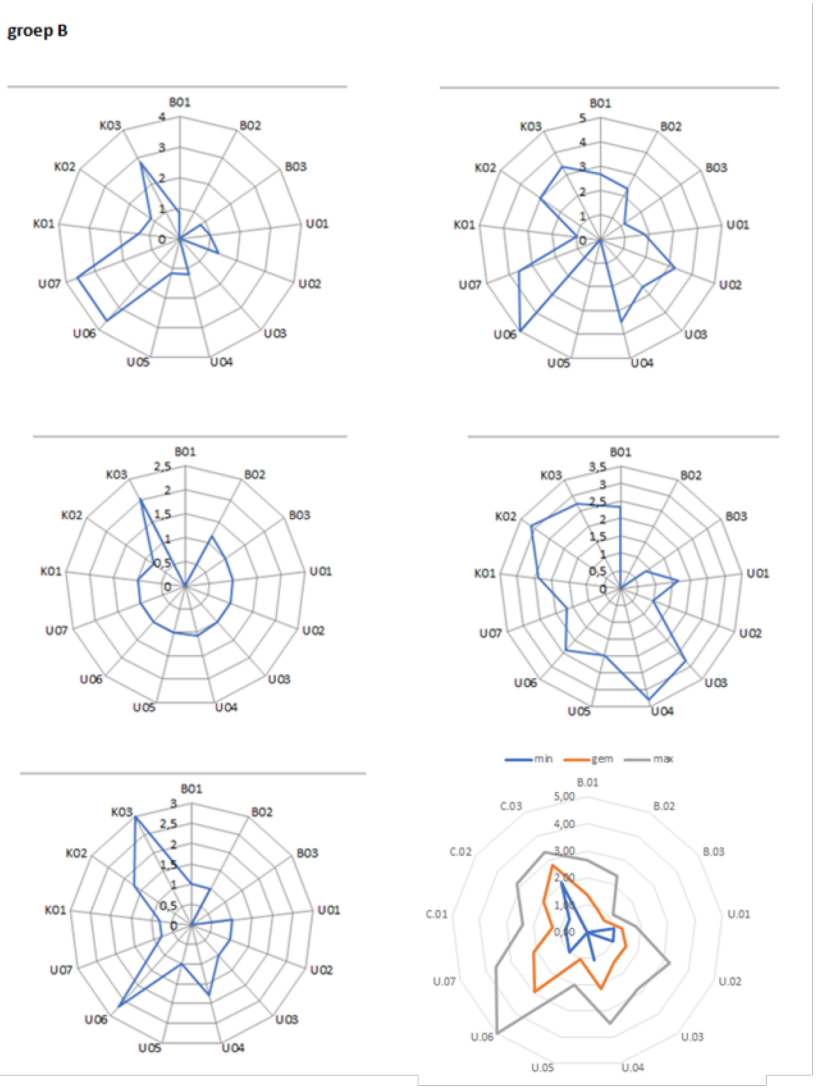
olders

vacy Self
sment

Groepsconsolidatie

Groepsoverzicht





Groepsconsolidatie

Prioritering verschilpunten

Op de volgende vragen zijn verschillende antwoorden gegeven.
De vragen staan op volgorde van gewicht van de vragen en het verschil in antwoorden.
Via de tabbladen kunt u een eigen volgorde bepalen.

In de workshop behandelde vragen verwijderen uit de lijst ☐

criterium	vraag	volwassenheids-niveau	prioiteit	De vewijzigingen naar de vragen:
U06	1	1-3	25,4	Selecteer hier de vraag om te behandelen
U01	1	1-3	22,7	Selecteer hier de vraag om te behandelen
C01	1	1-3	22,0	Selecteer hier de vraag om te behandelen
U07	1	1-3	19,4	Selecteer hier de vraag om te behandelen
U05	1	1-3	16,3	Selecteer hier de vraag om te behandelen
B01	1	1-3	16,3	Selecteer hier de vraag om te behandelen
B03	1	1-3	14,5	Selecteer hier de vraag om te behandelen
B02	1	1-3	12,4	Selecteer hier de vraag om te behandelen
U02	1	1-3	12,3	Selecteer hier de vraag om te behandelen
B01	2	1-3	11,7	Selecteer hier de vraag om te behandelen
U06	2	1-3	11,3	Selecteer hier de vraag om te behandelen
B02	2	1-3	11,0	Selecteer hier de vraag om te behandelen
U01	2	1-3	10,9	Selecteer hier de vraag om te behandelen
U05	2	1-3	9,4	Selecteer hier de vraag om te behandelen
U02	2	1-3	9,4	Selecteer hier de vraag om te behandelen
C01	2	1-3	8,9	Selecteer hier de vraag om te behandelen
U04	1	1-3	8,7	Selecteer hier de vraag om te behandelen
U03	1	1-3	8,4	Selecteer hier de vraag om te behandelen
U03	3	1-3	8,2	Selecteer hier de vraag om te behandelen
B03	5	1-3	7,5	Selecteer hier de vraag om te behandelen
C02	1	1-3	7,2	Selecteer hier de vraag om te behandelen

Groepsconsolidatie

Voorbeeld nog niet behandelde criterium/vraag

In groen de ‘gemiddelde’ groepskeuze

Het advies o.b.v. groepsinvulling en doelniveau

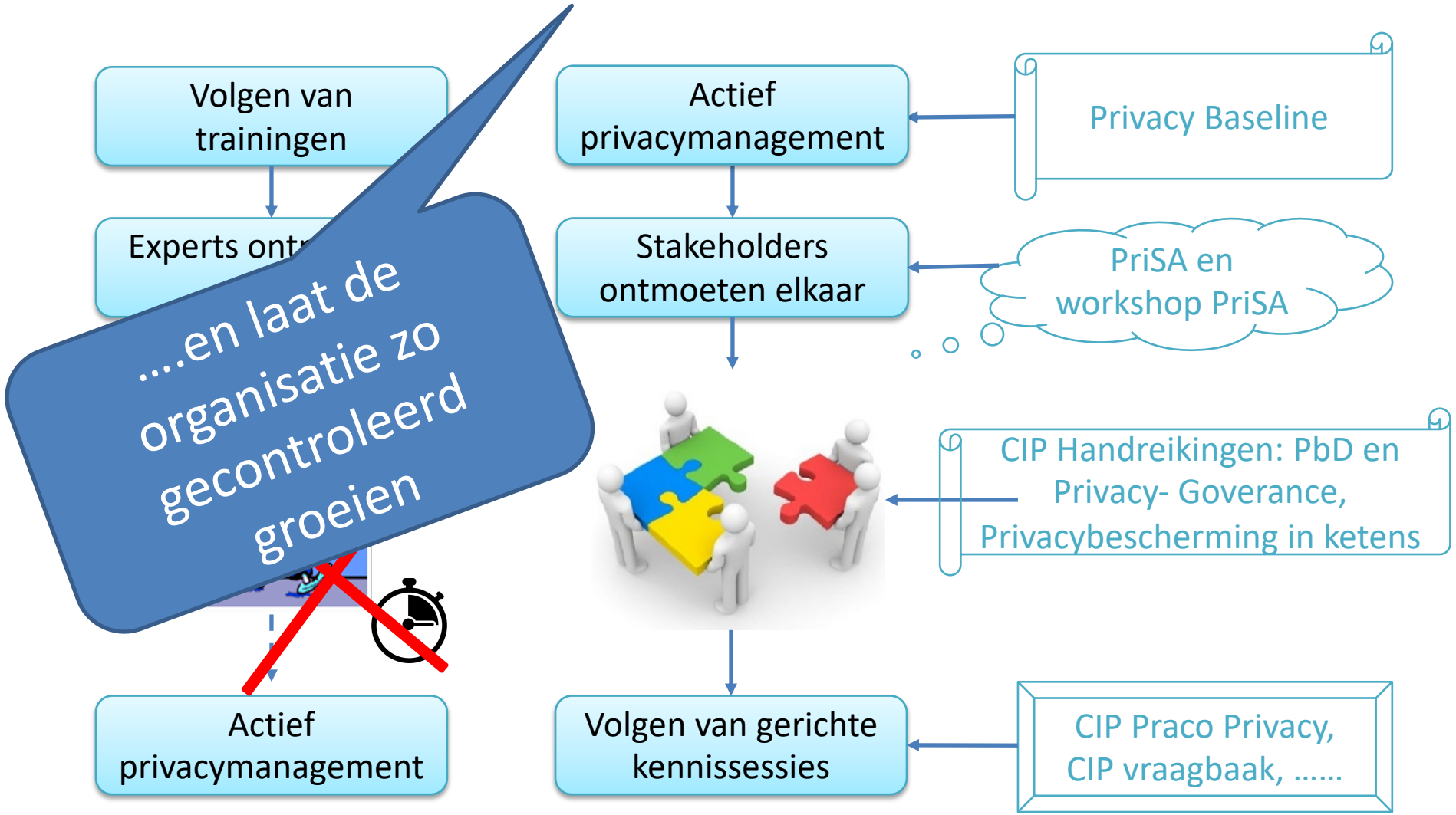
B.01 Privacybeleid

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

			Verdeling van de antwoorden	Antwoorden gegeven door:	Ruimte voor notities (De notities worden in het advies meegenomen.)
Hoe is de Avg geconcretiseerd in het privacybeleid?	Er is geen concretisering van de Avg.	0			Het beleid en de procedures worden op organisatieniveau eenduidig vastgelegd en f en organisatiebreed gebruikt (conform B.01/01).
Uitleg: Privacybeleid	Op verwerkingsniveau zijn **informeel** richtlijnen beschikbaar.	1	3	MW4 MW6 Mw8	Kan wel zijn maar bij afdeling X is dat nog lang niet op orde want ….
	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			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
Uitleg: Wettelijke beginselen	Beslissingen over het toepassen van de wettelijke beginselen worden **op verwerkingsniveau informeel** genomen.	1	2	jan Mw8	Notitie:
	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.)	Besl… het toepassen van de wettelijke beginselen worden …enduidig en **formeel** genomen en **vastgesteld**.	3	1	marie	
	…duidigheid van de beleidsbeslissingen wordt op …kt.	2	3	Eens: MW4 MW6 Mw8 Oneens: piet jan marie	De juistheid en de eenduidigheid van de beleidsbeslissingen worden op afdelingsnive Notitie:
	…heid van de beleidsbeslissingen wordt op ….	3	3	Eens: piet marie MW6 Oneens: jan MW4 Mw8	De juistheid en de eenduidigheid van de beleidsbeslissingen worden in een procedur formeel bewaakt. Notitie:
	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	

En doe de workshop samen met collega’s

Grip op Privacy benut de kracht van de organisatie



De suite blijkt enorm aan te slaan:

- Veel gemeenten zetten de Privacy Baseline in;
- Andere overheden, zoals de SVB, maken gebruik van de Privacy Baseline;
- Bij de Auditdienst Rijk speelt het een rol bij de evaluatie van de stand van zaken van het privacy management in het Rijk;
- Belangstelling is er bij een aantal ministeries.

Factoren die bijdragen aan het succes:

- De Privacy Baseline doet niets af aan de AVG:
  - Gericht op praktisch gebruik en is **geen indikking van de AVG** (dus geen vervlakking),
  - Bevat alleen de voor organisaties **relevante delen van de AVG**.
- De producten zijn **ontwikkeld** in het breed vertegenwoordigde CIP-netwerk:
  - **Professionals en juristen** uit de markt en de overheid
  - De **kennis uit het netwerk is verwerkt**
  - Heeft zo een **groot draagvlak**.
- De producten zijn **open source** en dus voor iedereen om niet te gebruiken. Sterker, men kan ze **gebruiken in eigen producten en diensten** (die ook beschikbaar is voor iedereen).
  Voorbeelden hiervan zijn:
  - **Privacy Company**, die een keurmerk heeft ontwikkeld o.b.v. de Privacy Baseline en hem ook in het eigen GRC-tool heeft verwerkt;
  - **Mexon Technology**, die een Engelse versie van de Privacy Baseline heeft gemaakt;
  - **Gemeente Westland** die een op Excel gebaseerd GRC-instrument heeft gemaakt o.b.v. de Privacy Baseline.
  - ……..

De Websites

centrum informatiebeveiliging en privacybescherming
Voorpagina
Mijn pagina's
Toevoegen
Groepen
Beheer
Filesender
Voeg een widget toe aan je pagina
Collega's zoeken
Zoek Specialisten
Handig !!
CIP Agenda
Alert Online 2015 van start
Snel naar ...
Twelo's
https://cip.pleio.nl/
Home
Voor wie
Producten
Workshops
Over CIP
Contact
Samenwerken aan informatieveiligheid en privacybescherming.
Over CIP →
Voor wie
Participanten →
Kennispartners →
www.cip-overheid.nl
Grip op Secure Software Development

ISACA®
Vertrouwen in en waarde uit informatiesystemen
Netherlands Chapter

A recognized global leader in
IT governance, control and assurance

5. ISACA – Privacy Framework & hulpmiddelen

iRISK

1 ISACA – Privacy Framework

COBIT® 5
AN ISACA® FRAMEWORK

ISACA – Privacy program

1 – Privacy program life cycle

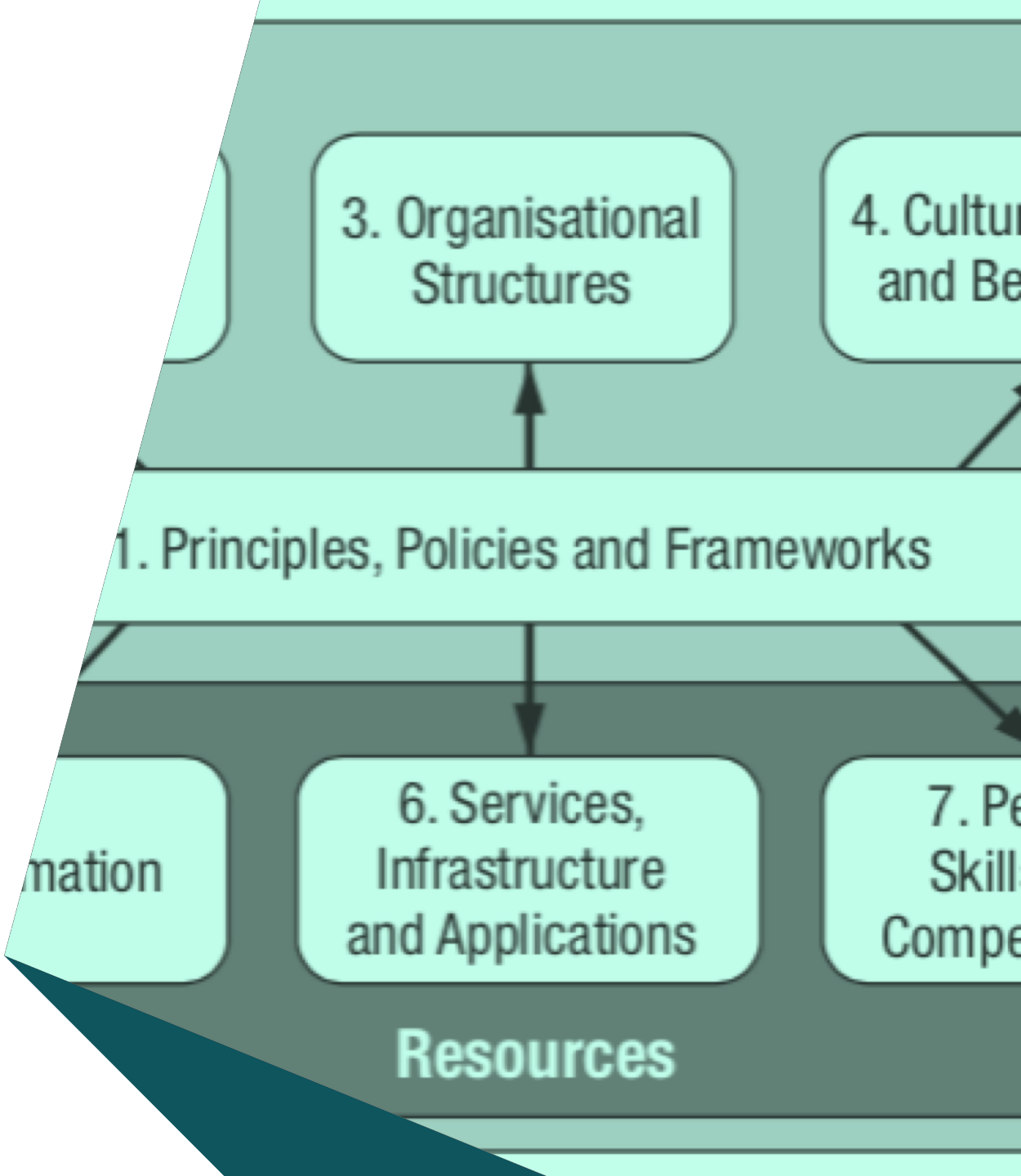
7 – Privacy enablers

- Beleid en richtlijnen
- Processen (IT & Privacy)
- Organisatie structuur
- Cultuur & Gedrag
- Informatie & data
- Diensten, infrastructuur en applicaties
- Mensen, vaardigheden en competenties

14 – Privacy principes

79 – Privacy doelstellingen

210 – Privacy control activiteiten



ISACA – Privacy program life cycle

Fase 1 – Identificeer de uitgangspunten (strategie, PIA, operationele aanpak, management buy-in)

Fase 2 – Beoordeel huidige situatie (enablers, scope activiteiten, ontwikkel risk scenario's)

Fase 3 – Vastleggen uitgangspunten (beleid, ISACA principles, richtlijnen)

Fase 4 – Ontwikkel een implementatie plan (business case, project schema, KPI's & monitoring, benefits)

Fase 5 – Implementeren uitgangspunten (executive support, business support, dagelijkse operatie integreren)

Fase 6 – Valideer succesvolle implementatie (doel bereikt, verbeteracties)

Fase 7 – Ontwikkel onderhoudbare privacy operatie (continue verbetering, meet effectiviteit, gebruik "life cycle" aanpak)

iRISK

ISACA

GDPR DATA PROTECTION IMPACT ASSESSMENT TEMPLATE

For more information, go to www.isaca.org/GDPR-DPIA

Privacy Impact Assessment

A. Description of the Processing (Art. 35(7)(a))	[Name of Enterprise Here] Enter answers to questions / prompts in column A.	[Sample answers for fictional ABC Corporation]
1. Nature, scope, [illegible] the proc[illegible] (Recital 90):		A network application used to monitor employee activities within ABC Corporation's physical and network facilities to ensure safety and compliance with legal and policy requirements
2. List of in-scope personal data items:		Data reflects: 1) employee activities around work stations 2) employee network activities (login/logout, applications used, associated dates/times/durations/locations, etc.) 2) internet activities (sites visited/duration of visits/IP addresses/dates/times/locations, etc.) made through the company's network 3) phone calls (incoming/outgoing phone numbers/dates/times/durations/locations, etc.)
3. Recipients of personal data items (if not applicable, indicate N/A):		Data controllers: management whose job responsibilities require such data; IT support personnel Data processors: * contracted physical safety/security vendor ACME Co. * contracted managed systems security vendor ABC Net Security * contracted phone systems vendor XYZ Telco
4. Period for which the personal data will be stored (e.g. in hours, days, weeks or years, etc.):		Data will be stored as follows: 1) Physical monitoring: for at least 6 months and in compliance with legal requirements 2) Network monitoring: for at least 1 year and in compliance with legal requirements 3) Phone calls: for at least 3 months and in compliance with legal requirements
5. Func[illegible]		The application was created in-house by company IT personnel. The application imports data from three different vendors: * Physical safety/security data, video, audio and photo files from vendor ACME Co. are collected through an API from the ACME cloud-based system. [illegible] ata is [illegible] job responsibilities.

PRIVACY FRAMEWORK'S EEN BOZE DROOM?!

iRISK

Privacy Impact Assessment

Data Protection Impact Assessment (DPIA) & alysis Questions	Which of the following answers best applies to your enterprise? Please enter a letter below. For "NA", provide an explanation. A: Yes, we've completely addressed all points and are managing. Associated risks are sufficiently mitigated, or accepted and approved by management. There are no gaps with respect to GDPR requirements. B: We've mostly addressed the points but still have a few actions outstanding; then we plan to manage. A few risks remain to be mitigated or accepted; and/or there are a few gaps with respect to GDPR requirements. C: We completed a few activities to address the points; but many remain to be addressed. Then we will manage. Most risks have not been mitigated, and/or most GDPR requirements are not satisfied. D: We have not done anything to address the points. No risks have been explicitly	Associated Personal Data Security Risk & GDPR Mitigation Safeguards Actions List or describe actions the enterprise will take to mitigate identified security risks and/or GDPR compliance gaps. If no security risk or gap mitigation is planned, please explain briefly.	Associated Data Subject Privacy Harm Risk-mitigation Actions List or describe actions the enterprise will take to mitigate identified harm risks. If no harm risk mitigation is planned, please explain briefly.	Assessment Results for Priva Summarize findings for the p the following points (as app * Summary totals of answers These totals will indicate the activities in your privacy ma * Statement of risks and gap the answers), along with arr * Summary of risk and privac * Additional information to management regarding each
u have documented and enforced privacy and security policies (and g procedures) to provide choices, where appropriate, to data regarding use of their personal data? t obtained before using personal information for specific purposes, ed by GDPR? **R Art. 6(1)**	**A**	We have the following safeguards in place: * Documented policies and procedures for the facility, internet use and phone use monitoring. * Training for the policies and procedures. * Technology has been implemented within the surveillance systems to give notice to those within our facilities of the surveiling activities. At the entrance to our facilities we give notification that if the individual does not want to be surveilled they should not enter the facilities. * For the types of monitoring and surveillance implemented, no consent is necessary for entering the facilities or for monitoring network use to access the internet, as confirmed with GDPR supervisory authorities. Personnel understand these are conditions of employment. * For the phone calls we give notice and obtain consent. * Identification verification is obtained where necessary. * Data is retained according to the information given in the Introduction. Planned actions: None at this time.	We have the following harm prevention controls in place: * Documented policies and procedures detail how the data can and cannot be used. * Controls do not allow data to be shared to others without obtaining authorization for such sharing. * Data is irreversibly deleted upon reaching the end of the retention date or legal requirement, whichever arrives first. * We have cyber liability insurance to cover personal data breaches. * We have documented and implemented breach response plans in place. Planned actions: None at this time.	1. Choice & Consent Summary a. Maturity & Risk Levels # of Level A answers: 1 # of Level B answers: # of Level C answers: 1 # of Level D answers: # of Level E answers: # of Level F answers: # of NA answers: 1 b. Summary of Risk Levels, Risk * Technology has not yet been i manager will be responsible for position (4 weeks from the date Position/person(s)/team assig c. Summary of Privacy Harm Ris * Technology has not yet been i privacy manager will be respons this position (4 weeks from the Position/person(s)/team assig d. Additional Information: The automate the management of
nsents (once obtained) appropriately documented and maintained? ents be easily provided upon request by data subjects and/or ate authorities? **Art. 7(1), Art. 7(2)**	**C**	We have the following safeguards in place: * Documented policies and procedures for obtaining consents. * Training for the policies and procedures. * Technology not yet been implemented to fully manage the consents. The new privacy manager will be responsible for accomplishing this. Planned actions: Implement technology to fully manage the consents.	We have the following harm prevention controls in place: * Documented policies and procedures detail how the data can and cannot be used. * Controls do not allow data to be shared to others without obtaining authorization for such sharing. * Data is irreversibly deleted upon reaching the end of the retention date or legal requirement, whichever arrives first.	
enterpris ave you c s to colle **escriptions, comments and additional information for each d column, as appropriate.**		will start in four weeks from the date on this DPIA. He will be responsible for		applicable; all GDPR requiremen Principle.

PRIVACY FRAMEWORK'S EEN BOZE DROOM?!

iRISK

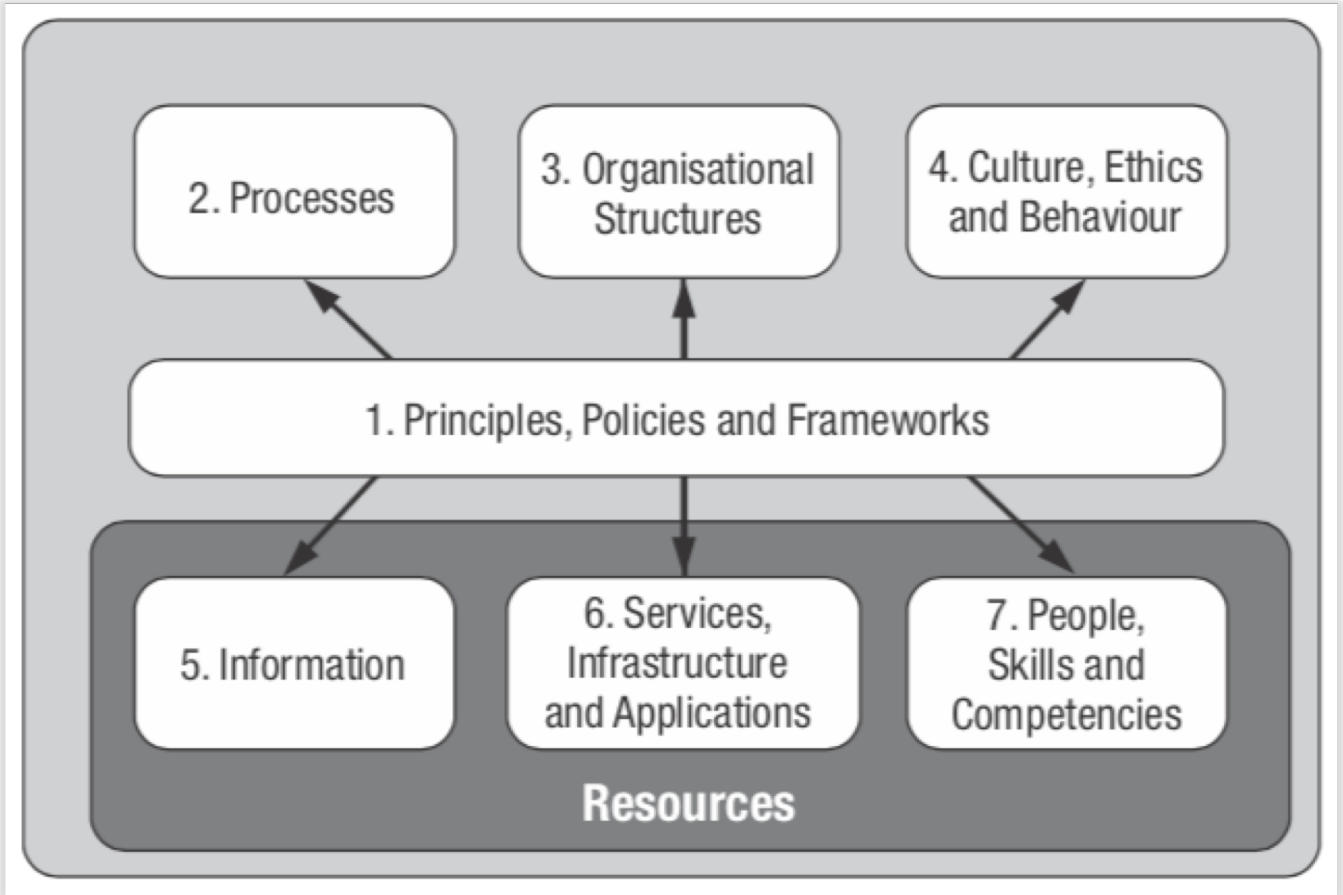
Fase 3. Privacy Principles

ISACA PRIVACY PRINCIPLES	RELATED GDPR ARTICLES
1. Choice and Consent	Article 6: Lawfulness of processing Article 7: Conditions for consent Article 8: Conditions applicable to child's consent in relation to information society services
2. Legitimate Purpose Specification and Use Limitation	Article 5: Principles relating to processing of personal data Article 6: Lawfulness of processing Article 10: Processing of personal data relating to criminal convictions and offences Article 22: Automated individual decision-making, including profiling Article 39: Tasks of the data protection officer
3. Personal Information and Sensitive Information Life Cycle	Article 5: Principles relating to processing of personal data Article 6: Lawfulness of processing Article 9: Processing of special categories of personal data Article 21: Right to object Article 25: Data protection by design and by default Article 35: Data protection impact assessment Article 89: Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes
4. Accuracy and Quality	Article 5: Principles relating to processing of personal data Article 16: Right to rectification
5. Openness, Transparency and Notice	Article 5: Principles relating to processing of personal data Article 12: Transparent information, communication and modalities for the exercise of t rights of the data subject Article 13: Information to be provided where personal data are collected from the data Article 14: Information to be provided where personal data have not been obtained fro Article 15: Right of access by the data subject Article 21: Right to object
	Article 7: Conditions for consent Article 12: Transparent information, communication and modalities for the exercise data subject Article 14: Information to be provided where personal data Article 15: Right of

1. Choice and consent
2. Legitimate purpose specification and use limitation
3. Personal information and sensitive information life cycle
4. Accuracy and quality
5. Openness, transparency and notice
6. Individual participation
7. Accountability
8. Security safeguards
9. Monitoring, measuring and reporting
10. Preventing harm
11. Third party/vendor management
12. Breach management
13. Security and privacy by design
14. Free flow of information and legitimate restriction

iRISK

Privacy Enablers –
(APO10.1) Supplier relationships and contracts.



iRISK

Fase 5. Proces - Identify and evaluate supplier relationships and contracts (APO10.1)

- **Conduct privacy impact assessments for suppliers** with access to personal information and define the privacy risk and harms profiles.
- **Define the supplier relationship** and privacy requirements based on the privacy risk and harms profiles.
- **Identify high, medium and low privacy risk suppliers** and establish oversight appropriate to corresponding levels of risk.

Fase 5. Organisation structure

Chief Privacy Officer (CPO)/Data Privacy Officer (DPO)

Mandate, Operating Principles, Span of Control and Authority Level

Figure 7 lists the characteristics of the CPO/DPO.

Figure 7—Characteristics of the CPO/DPO

Area	Characteristic
Mandate	The overall responsibility of the enterprise privacy management program
Operating principles	Depending on a variety factors within the enterprise, the CPO/DPO may report to the CEO, chief operating officer (COO), chief information officer (CIO), chief risk officer (CRO), general counsel or other senior executive management. The CPO/DPO is the liaison between executive management and the privacy management program. The CPO/DPO should also communicate and coordinate closely with key business stakeholders to address information protection needs. The CPO/DPO must: • Have an accurate and strong understanding of the business strategic vision • Have a strong understanding of privacy risk and privacy harms • Have a strong understanding of legal requirements for privacy protections • Be an effective communicator • Collaborate successfully with the chief information security officer (CISO) in areas where privacy overlaps with information security • Be adept at building effective relationships with business leaders • Be able to translate business objectives into privacy management requirements
Span of control	The CPO/DPO is responsible for: • Establishing and maintaining a privacy management program • Defining and managing a privacy risk management plan and privacy harms management plan • Monitoring and reviewing the privacy management program

Fase 5. Culture & Ethics

Behaviors

Each of the following behaviors occurs in an enterprise at two levels: the organizational level, where behaviors are determined by the values (ethics, culture or attitude) by which the enterprise wants to live, and the individual level, where behaviors are defined by the personal values (ethics, culture or attitude) of the individual.

Behavior 1: Privacy is practiced in daily operations.

Privacy is part of the enterprise's daily functioning.

- At the organizational level, the behavior indicates that privacy protection is accepted as a business imperative in organizational goal setting.
- At the individual level, the individual cares about the well-being of the enterprise and the well-being of individuals associated with personal information, and applies privacy protection techniques to his/her daily operations, while recognizing where to apply the privacy principles.

Fase 5. Information

- Privacy management strategy
- Privacy management budget
- Privacy management plan • Posted privacy notices
- Privacy policies
- Privacy principles
- Privacy standards
- Privacy procedures
- Privacy forms

- Privacy protection requirements, which can include:
  - Privacy protection configuration requirements
  - SLA/OLA privacy protection requirements
  - Privacy clauses within the business partner contracts
- Privacy training and awareness material
- Privacy management review reports, which include:
  - PIA reports
  - Privacy management audit findings
  - Privacy management maturity reports
  - Privacy-related risk management information, such as:

Fase 5. Service & Infrastructure

- Privacy management architecture
- Privacy training & awareness
- Individual access to privacy data
- Privacy protection development

iRISK

Fase 5. Skills

Figure 58—Experience, Education and Qualifications for Privacy Governance	
Requirement	**Description**
Experience	• Several years of experience in privacy, information security and, ideally, IT/business management, including experience in: – Creating, implementing and measuring privacy policies, standards and procedures – Achieving privacy compliance with external regulations and other legal requirements – Aligning privacy strategy with corporate governance goals – Creating privacy policies that align with business needs and make use of information security safeguards, and devising methods to measure the effectiveness of the policies – Communicating with executive leadership
Qualifications	• Demonstrated experience in and understanding of how to manage compliance governance programs, and demonstrated understanding of privacy principles and how to effectively implement them within an organization • Possible certifications to support qualifications include: CISM, Certified in the Governance of Enterprise IT® (CGEIT®), CRISC or one of the available privacy certifications

Fase 6. implementatie - Supplier Management” (APO10)

APO10 - Doelstelling: regelmatige beoordeling van verwerkers op de werking van hun privacy maatregelen

Privacy Indicator:

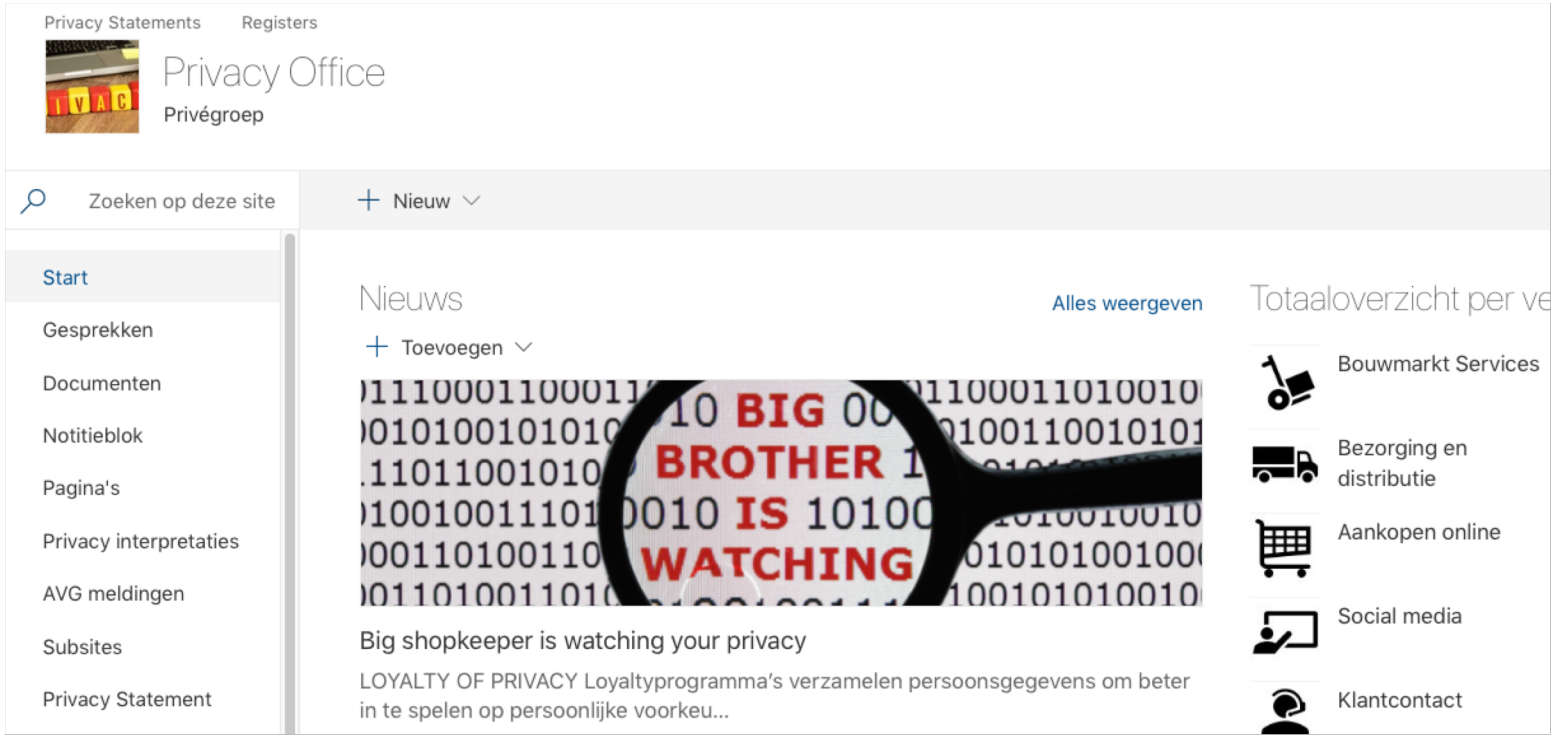
- Percentage positieve verwerkers beoordeling;
- Aantal datalekken veroorzaakt door verwerker;
- Aantal events veroorzaakt door verwerker die leiden tot een datalek;
- Frequentie van datalekken bij/door verwerker;
- Percentage verwerkers dat afgelopen jaar een beoordeling heeft gehad;
- Percentage verwerkersovereenkomsten waarin privacy management staat beschreven;
- Aantal privacy gerelateerde incidenten per verwerker (geen datalek)

10. Manage suppliers.

APO10 Manage Suppliers	Area: Management Domain: Align, Plan and Organize
COBIT 5 Process Description Manage IT-related services provided by all types of suppliers to meet enterprise requirements, including the selection of suppliers, management of relationships, management of contracts, and reviewing and monitoring of supplier performance for effectiveness and compliance.	
COBIT 5 Process Purpose Statement Minimize the risk associated with nonperforming suppliers and ensure competitive pricing.	
Primary Privacy Principles Involved • Principle 3: Personal Information and Sensitive Information Life Cycle • Principle 7: Accountability • Principle 9: Monitoring, Measuring and Reporting • Principle 10: Preventing Harm • Principle 11: Third-party/Vendor Management • Principle 13: Security and Privacy by Design	
APO10 Privacy-specific Process Goals and Metrics	
Privacy-specific Process Goals	**Related Metrics**
1. Suppliers and contracts are assessed regularly and appropriate privacy risk and harm mitigation plans are provided.	• Percentage of suppliers meeting agreed-on privacy protection requirements • Number of privacy breaches caused by suppliers • Number of information security and other types of supplier events leading to privacy breaches • Frequency of privacy breaches with suppliers • Number of independent privacy management program reviews of suppliers • Percentage of suppliers who have had a PIA or similar assessment in the past year
2. Suppliers recognize privacy management as an important business enabler.	• Percentage of supplier contracts specifying privacy management requirements • Number of privacy-related incidents related to suppliers • Percentage of suppliers used who have experienced privacy-related incidents

iRISK

Fase 7. operations - Dagelijkse operatie Supplier Management (APO10)



iRISK

2 Voelt de consument zich gehoord?

Volkskrant artikel

De Bijenkorf (geslaagd plaats 1)
De Bijenkorf heeft een uitgebreide privacyverklaring op de website, met tien antwoorden op vragen over hoe en waarom de winkelketen data verzamelt, wat die ermee doet, naar wie het gaat en hoe ze die beschermen.

Albert Heijn (gezakt)
We hebben een gepersonaliseerde bonuskaart, dus Albert Heijn weet bijna alles van ons. Maar de grootgrutter maakt er een potje van. Op de webpagina's met privacybeginselen is geen privacy-mailadres te vinden. Daarvoor moet de klant eerst 62 pagina's downloaden. Op pagina 61 staat het eindelijk: privacy@ah.nl. Na twee weken komt er antwoord: AH wil een kopie van een paspoort. Volgende stap: AH wil dat je een brief stuurt. Per post …

iRISK

Klachten ontvangen bij Autoriteit Persoonsgegevens

Welke type betrokken melden deze klachten?

- Consumenten
- Leveranciers
- Medewerkers

Ruim 600 mensen dienen privacyklacht in bij AP

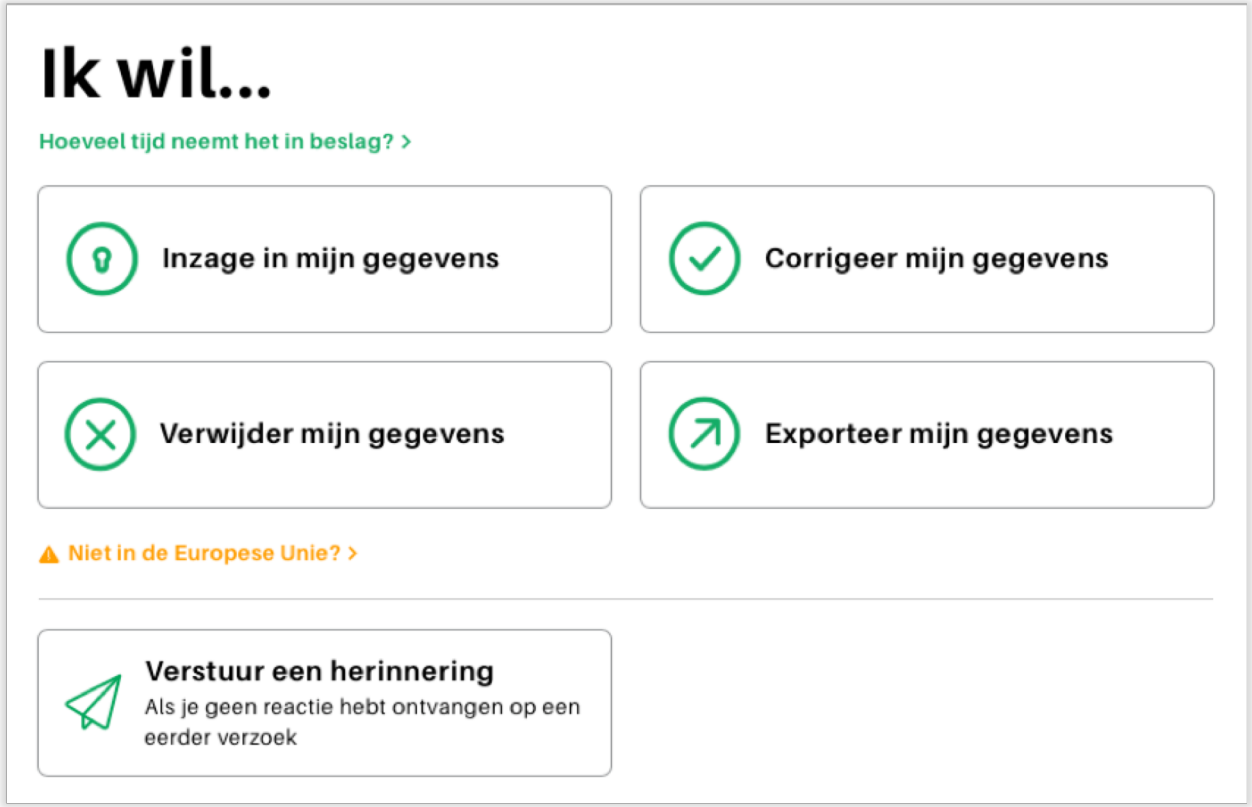
Nieuwsbericht / 29 juni 2018

Categorie:
Klacht over gebruik persoonsgegevens

Sinds 25 mei zijn de privacyrechten van mensen versterkt en kan iedereen een privacyklacht indienen bij de Autoriteit Persoonsgegevens (AP). Ruim 600 mensen hebben dat inmiddels gedaan. De AP heeft nu de eerste 400 klachten geanalyseerd. Wat opvalt is dat veel mensen problemen ondervinden met het verwijderd krijgen van hun persoonsgegevens. Bijna een derde van de klachten gaat hierover. Daarnaast klagen mensen dat zij hun gegevens niet mogen inzien en over ongewenste verstrekking van hun gegevens aan derden. Het grootste deel van de klachten gaat over bedrijven (87%). De AP heeft alle klachten in behandeling.

iRISK

Bits of Freedom
Check je gegevens



iRISK

Bits of Freedom
Opgenomen Retailers

De Bijenkorf
Magazijn De Bijenkorf' B.V.

Functionaris Gegevensbescherming
Magazijn De Bijenkorf' B.V.
Hoogoorddreef 11
1101 BA AMSTERDAM
NETHERLANDS

info@debijenkorf.nl

Albert Heijn
Albert Heijn B.V.

Klantenservice
Albert Heijn B.V.
Provincialeweg 11
1506 MA ZAANDAM
NETHERLANDS

privacy@ah.nl

Tele2
Tele2 Nederland B.V.

Privacy
Tele2 Nederland B.V.
Postbus 289
2400 AG ALPHEN AAN DEN RIJN
NETHERLANDS

privacy.nl@tele2.com

HEMA
HEMA B.V.

HEMA B.V.
NDSM-straat 10
1033 SB AMSTERDAM
NETHERLANDS

hemaklantenservice@hema.nl

Aldi
ALDI Holding B.V.

Coördinator voor gegevensbescherming
ALDI Holding B.V.
Postbus 147
4100 AC CULEMBORG
NETHERLANDS

InShared
InShared Nederland B.V.

Relatiebeheer
InShared Nederland B.V.
Postbus 408
3830 AL LEUSDEN
NETHERLANDS

privacymanager@achmea.nl

H&M
H & M Hennes & Mauritz GBC AB

Data Protection Officer
H & M Hennes & Mauritz GBC AB
Mäster Samuelsgatan 46
SE-106 38 STOCKHOLM
SWEDEN

dataprotection.nl@hm.com

3 Do’s & Don’ts

DO’s
Privacy Framework

1. Kies voor een implementatie life cycle strategie;
2. Start met een risico gebaseerde Privacy Impact inschatting;
3. Kies voor privacy principes die passen bij de organisatie;
4. Selecteer allen de privacy controle activiteiten uit verschillende frameworks die de privacy risico’s echt minimaliseren voor de organisatie;
5. Zorg voor business participatie/ multi disciplinair (taskforce, ambassadeurs, verantwoordelijke);
6. Faciliteer de juiste tools (sharepoint registers) en handige richtlijnen;
7. Zorg voor een communicatie platform en vertrouwen voor verantwoordelijke;
8. Start altijd met een context-analyse bij Privacy vraagstukken;
9. “Kill the stove-pipes”

DON’Ts
Privacy Framework

1. Geloof niet dat Security gelijk is aan Privacy!
2. Gooi beleidsrichtlijnen over de schutting van de business
3. Vergeet Juridische zaken mee te nemen
4. Directie laten tekenen zonder bewustwording
5. Vertrouw op “latente” kennis van de business op gebied van privacy
6. Verwerkersovereenkomsten van derden ongezien tekenen

6. Privacy Framework stellingen

3 Stellingen

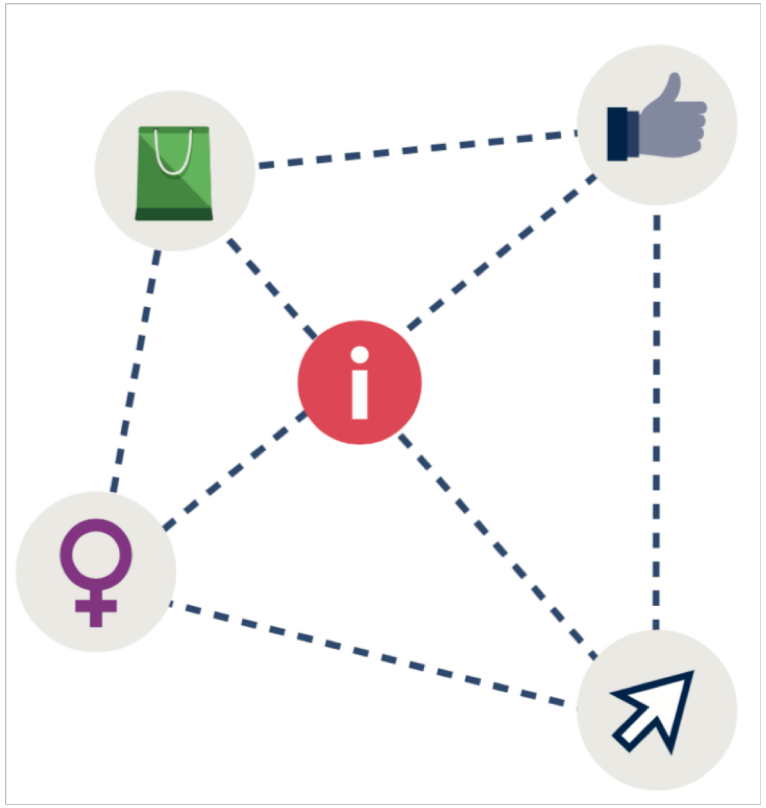
Frameworks leveren voor consumenten geen extra veiligheid op!

iRISK

Frameworks maken bijzondere persoonsgegevens vogelvrij!

iRISK

Privacyjuristen begrijpen nut van FRAMEWORKS nog niet, derhalve vergt het minimaal 2 jaar om PRIVACY FRAMEWORK goed in een organisatie toe te passen!



iRISK

Uw sprekers:

- Fokke Jan
- Jan de Heer (www.Norea.nl)
- Ronald Koorn (www.KPMG.nl)
- Marcel Koers (www.Uwv.nl)

- Menno Borst (www.iRiskiT.nl)
  (menno.borst@iRiskit.nl)