Kenissessie Privacy (by Design)

NORA en CIP

14 november 2017

NORA
Nederlandse Overheid
Referentie Architectuur

Welkom!

Programma

13.20 Introductie

14.20 Case-study

15.00 Terugkoppeling case-study en doorontwikkeling privacy in de NORA

16.00 Presentatie ontwikkelingen NORA 2017 en aansluitend borrel

Bij wat voor organisatie werk je?

Werk je vooral in projecten of meer in beleid/advies?

Zie je de AVG vooral als lust of als last?

Wie beschouwt zichzelf al als privacy expert?

centrum informatiebeveiliging en privacybescherming

Grip op Privacy

Als de architect zijn werk goed doet:

Win-win voor organisatie en privacybescherming

NORA , 14 november 2017

Marcel Koers en Ruud de Bruijn

Agenda

- Intro CIP
- AVG
- Grip op Privacy
- 10 redenen
  om nog eens naar uw rol te kijken

Privacy onder architectuur?

Stelling:

Ik bouw als architect in het belang van de organisatie.

Checks vanuit privacybescherming:

✓ De architect houdt zich aan de (privacy) wet- en regelgeving

✓ De architect benut de principes van Privacy by Design

Art 25 AVG (PbD):
Een claim op architecten!
(Begrijp de AVG en Privacy by Design principes)

Nuttige bronnen

Privacy Engineering:

Proactively Embedding Privacy, by Design

PbD

www.privacybydesign.ca

AUTORITEIT
PERSOONSGEGEVENS

CIP

centrum
informatiebeveiliging
en privacybescherming

Intro CIP

Aanleiding en doelen

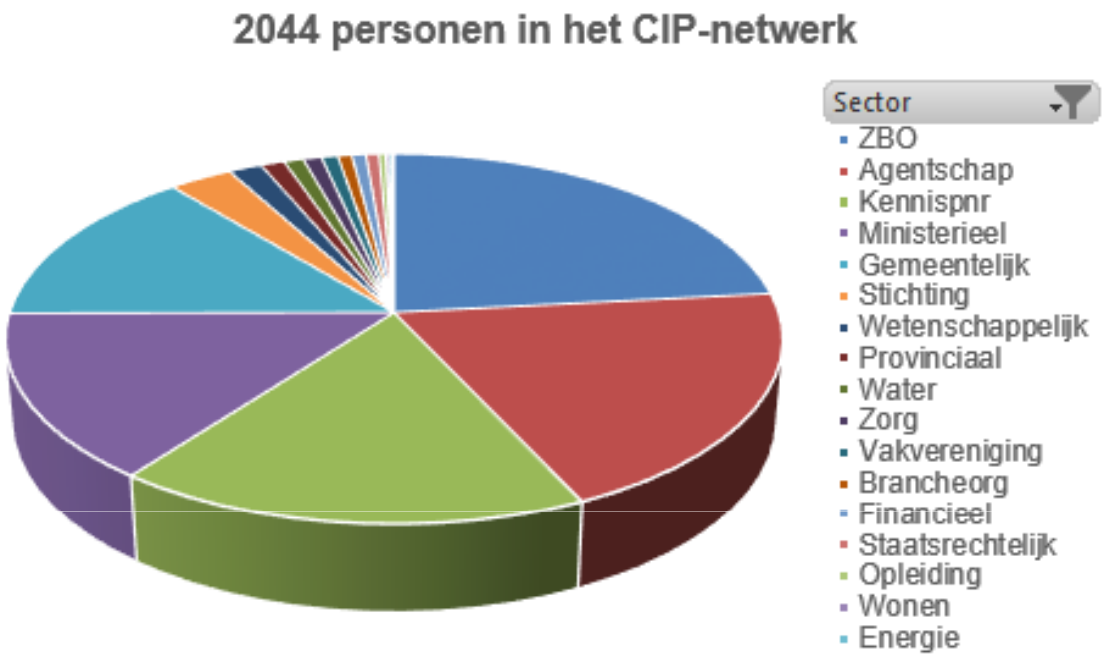
Aanleiding voor de overheid

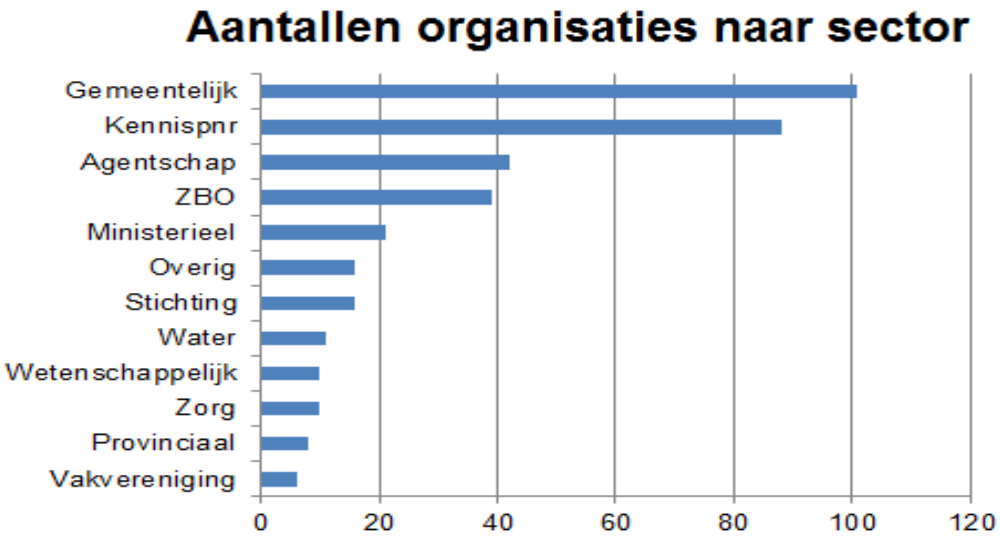
- Toenemende afhankelijkheid van het internet, mobile devices,ed.
- Toenemende (organisatiegraad van) cyber crime

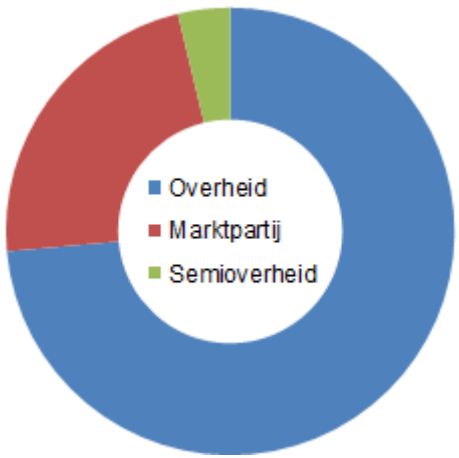
De overheid organiseert zich en CIP faciliteert dit door:

- Bundeling kennis/krachten: door het bouwen aan een IB-community in de overheid
- Aanbieden/toegankelijk maken van kennis en practices
- Werken aan gezamenlijke afspraken en normatiek

Samenstelling CIP-Netwerk 1-9-17







Algemene Verordening Gegevensbescherming (AVG)

In het Engels heet de Algemene Verordening Gegevensbescherming (AVG)
General Data Protection Regulation (GDPR)

OPP en de Avg

de avg: moet je daar wat mee?

CIP: samen – werken aan informatieveiligheid

Avg Algemeen

Ingang
25 mei2016

Start handhaving
25 mei 2018

Avg volgt filosofie Wbp

Vervangt Wbp

"AVG is een verduidelijking van de Universele Verklaring van de Rechten van de Mens (UVRM)"

Kernwaarden Avg:

- De betrokkene (burger, klant, ..) voorop
- Organisatie heeft aantoningsplicht rechtmatige verwerking
- Gegevensminimalisatie

Avg inrichtingsniveau

Highlights	Toepassingsgebied
Registerplicht/verantwoordingsplicht	Voor alle verwerkingen van persoonsgegevens
Privacy by Design	Bij ontwerp nieuwe systemen/processen
Gegevensbeschermingseffectbeoordeling	Bij verwerkingen met hoog risico
Verwerkerovereenkomsten	Bij uitbesteding verwerkingen van persoonsgegevens
Functionaris Gegevensbescherming	Verplicht voor overheidsorganisaties

Avg verwerkingsniveau

Highlights	Toepassingsgebied
Inregelen vergeetrecht en dataportabiliteit	Voor alle verwerkingen van persoonsgegevens
Inregelen inzagerecht	Voor alle verwerkingen van persoonsgegevens
Informatiebeveiligingsmaatregelen treffen (risico gebaseerd)	Voor alle verwerkingen van persoonsgegevens
Logging & Monitoring	Voor alle verwerkingen van persoonsgegevens
Meldplicht Datalekken (verruimd tot ook bijhouden niet meldenswaardige lekken)	

Wie is er bang voor de privacywetgeving?

CIO.nl:
De investering die bedrijven doen
in GDPR -compliance,
kan over een veel bredere linie voordeel opleveren,
mits het de juiste investeringen zijn.

Grip op Privacy

Grip op privacy: hoe?

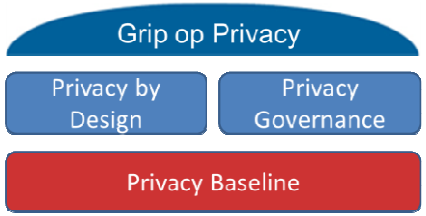
Een ogenschijnlijk eenvoudige vraag uit de CIP community:

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?

Candleproblem



Problem: Fix the lit candle to the wall so that it will not drip wax onto the table below.

Oplossing

Grip op Privacy

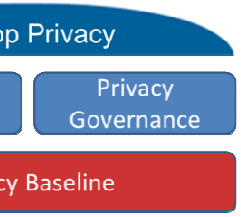
Privacy by Design

Privacy Governance

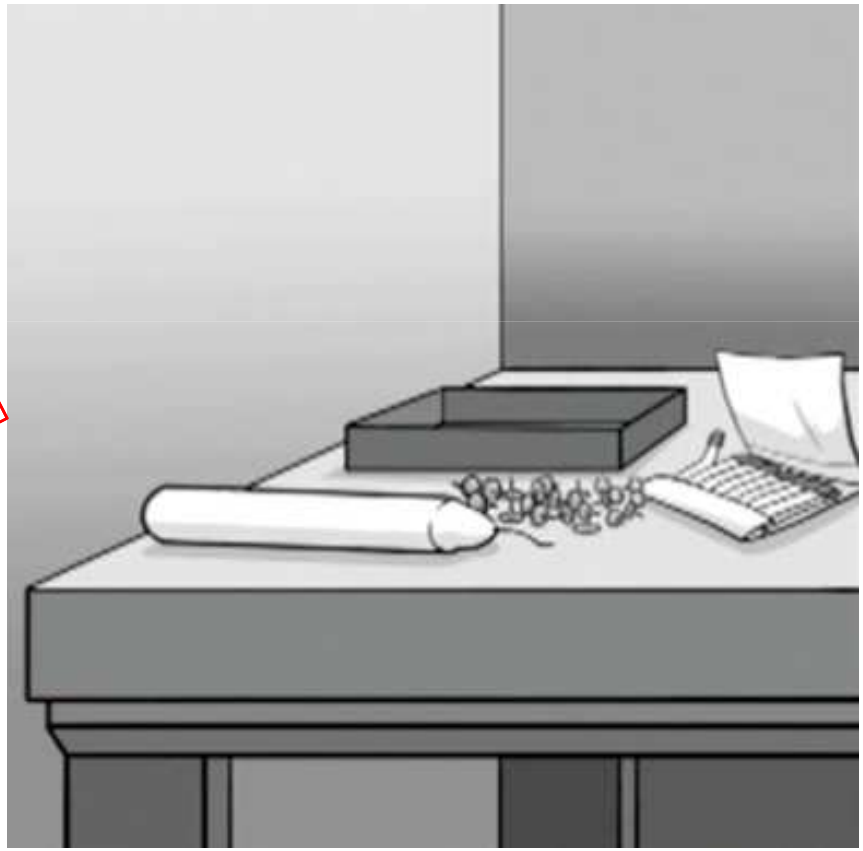
Privacy Baseline

.

Zelfde eisen, beter gestructureerd



Geen nieuw normenkader



.

Grip op privacy: versimpel!

- AVG: wollig beschreven als ‘extra eisen’
- CIP idee: Privacy Baseline
  - ‘vertaal’ de AVG naar het format van een hanteerbaar normenkader
  - gebruik SIVA format: eenduidig, ontdubbeld, compleet en uniform
  - laat het normenkader aansluiten op de bedrijfsvoering

Het verbetert de bedrijfsvoering

- De boodschap:

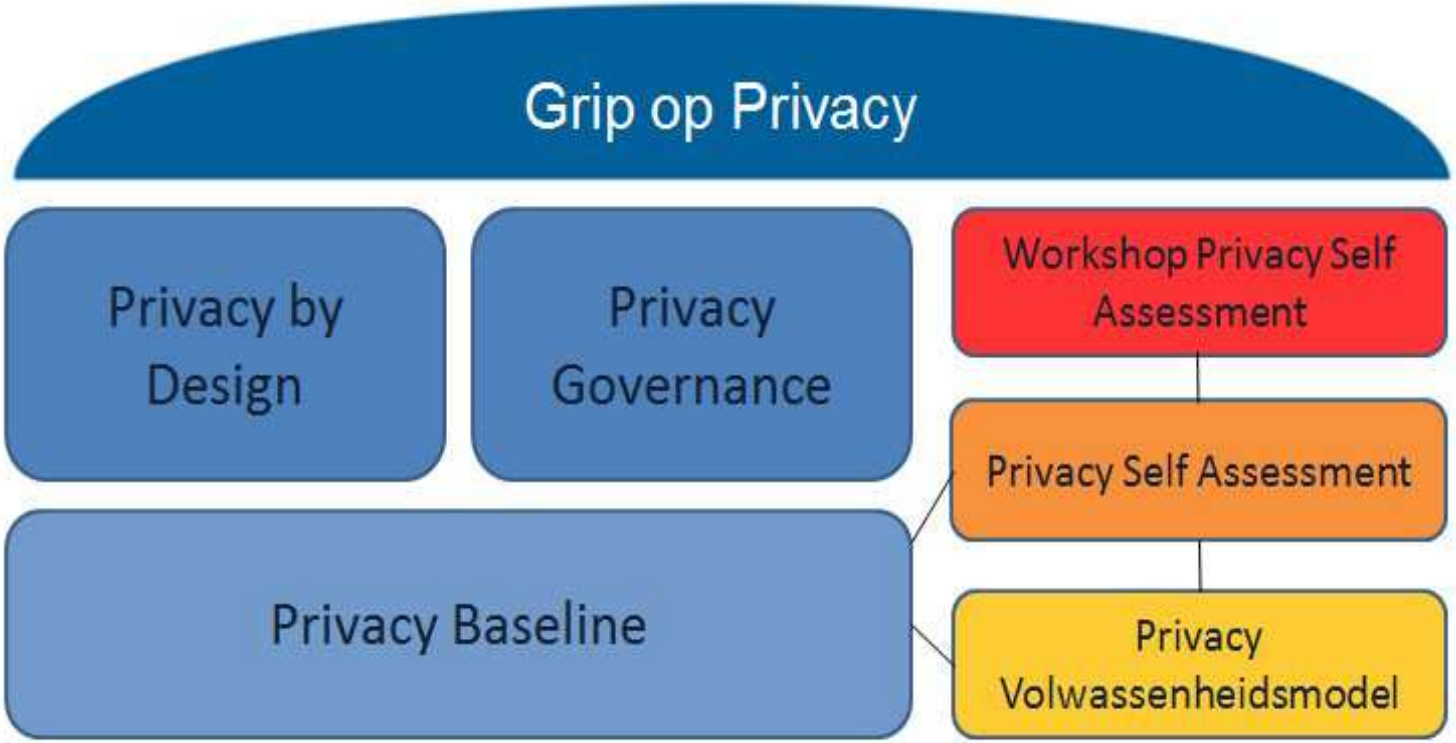
  volg de aanwijzingen van de Privacy Baseline op en
  je voldoet ‘automatisch’ aan de AVG

- Hulpmiddelen bij uitvoering:
  - Handleidingen Privacy by Design en Priravy Governance en
  - Privacy Selfassessment tool voor de stakeholders

Door het doen van de juiste investeringen

Avg Highlights

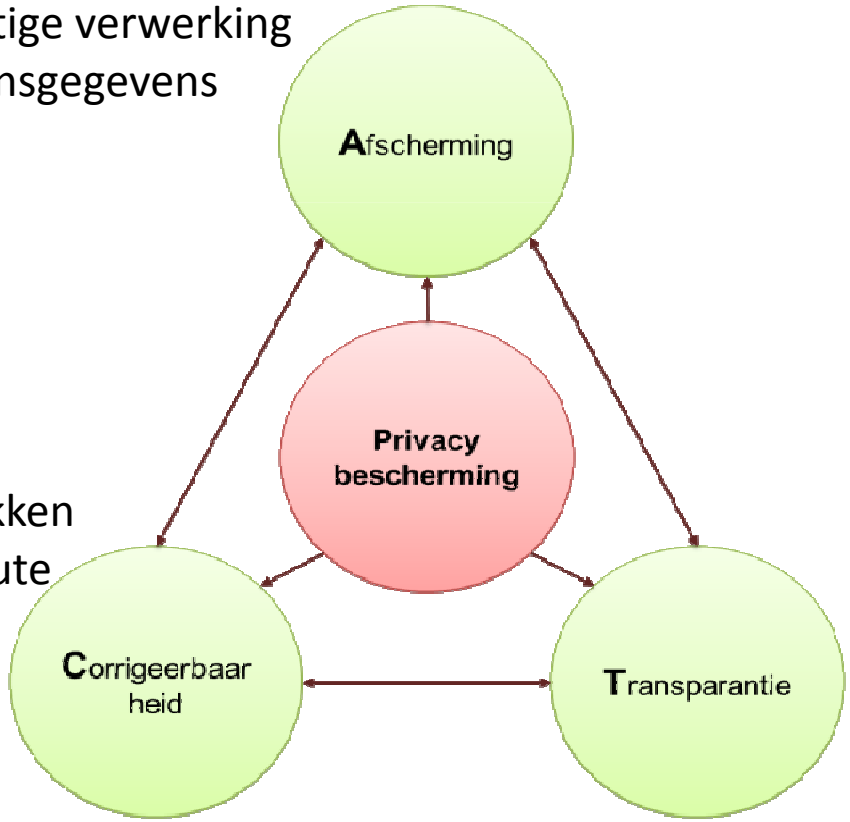
Grip op Privacy: CIP-handreikingen om in control te komen



Privacy beschermen
=
ACT-doelen realiseren

Voorkomen van:

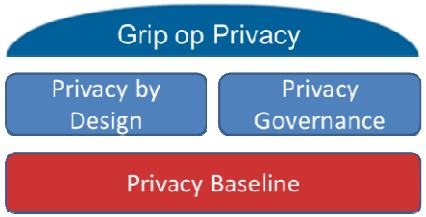
- onrechtmatige verwerking van persoonsgegevens
- datalekken



- Voorkomen van benadeling betrokken personen door foute en ongewenste verwerking

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

ACT-doelen vertaalt naar organisatie-doelen



- CIP heeft de wet- en regelgeving ontrafeld
- De ordening van de normen maakt privacy-governance mogelijk
- De normen maken de wet bespreekbaar:
  - Geven aan <u>wat</u> <u>waar</u> gedaan moet worden.
  - Beschrijven de doelstellingen, de risico's en de vereisten om de doelstellingen te bereiken.

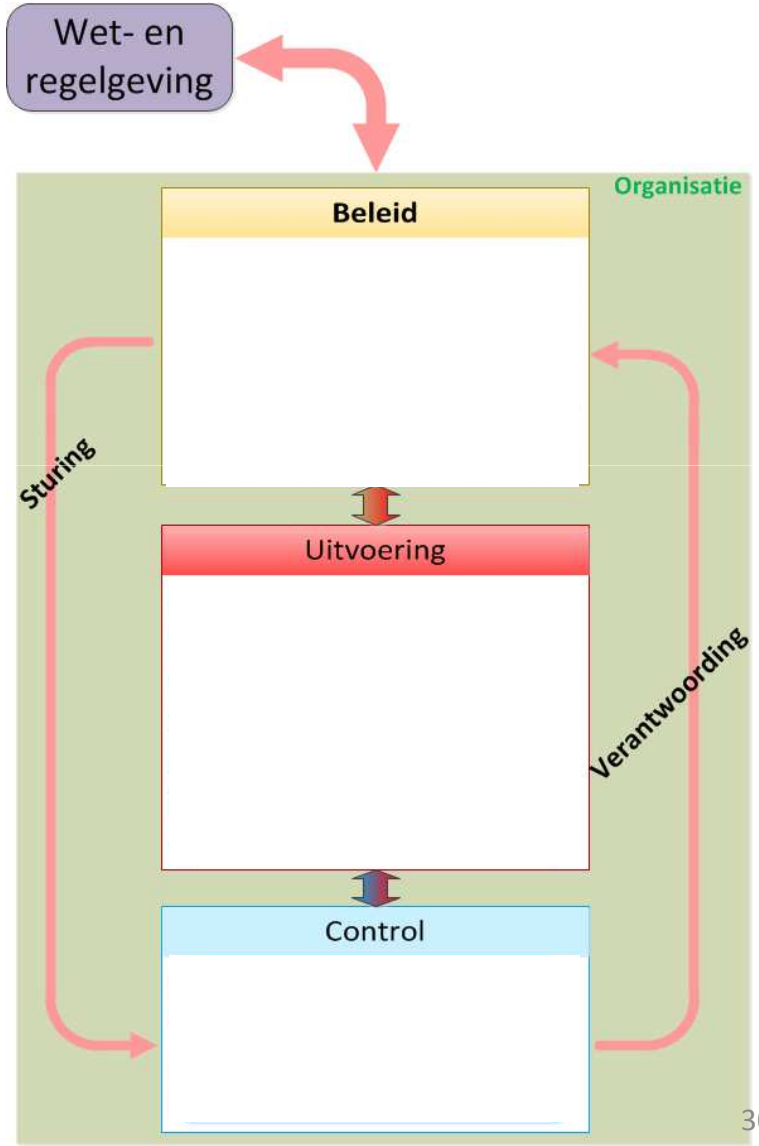
Privacy Baseline

Criteria zijn opgedeeld naar:

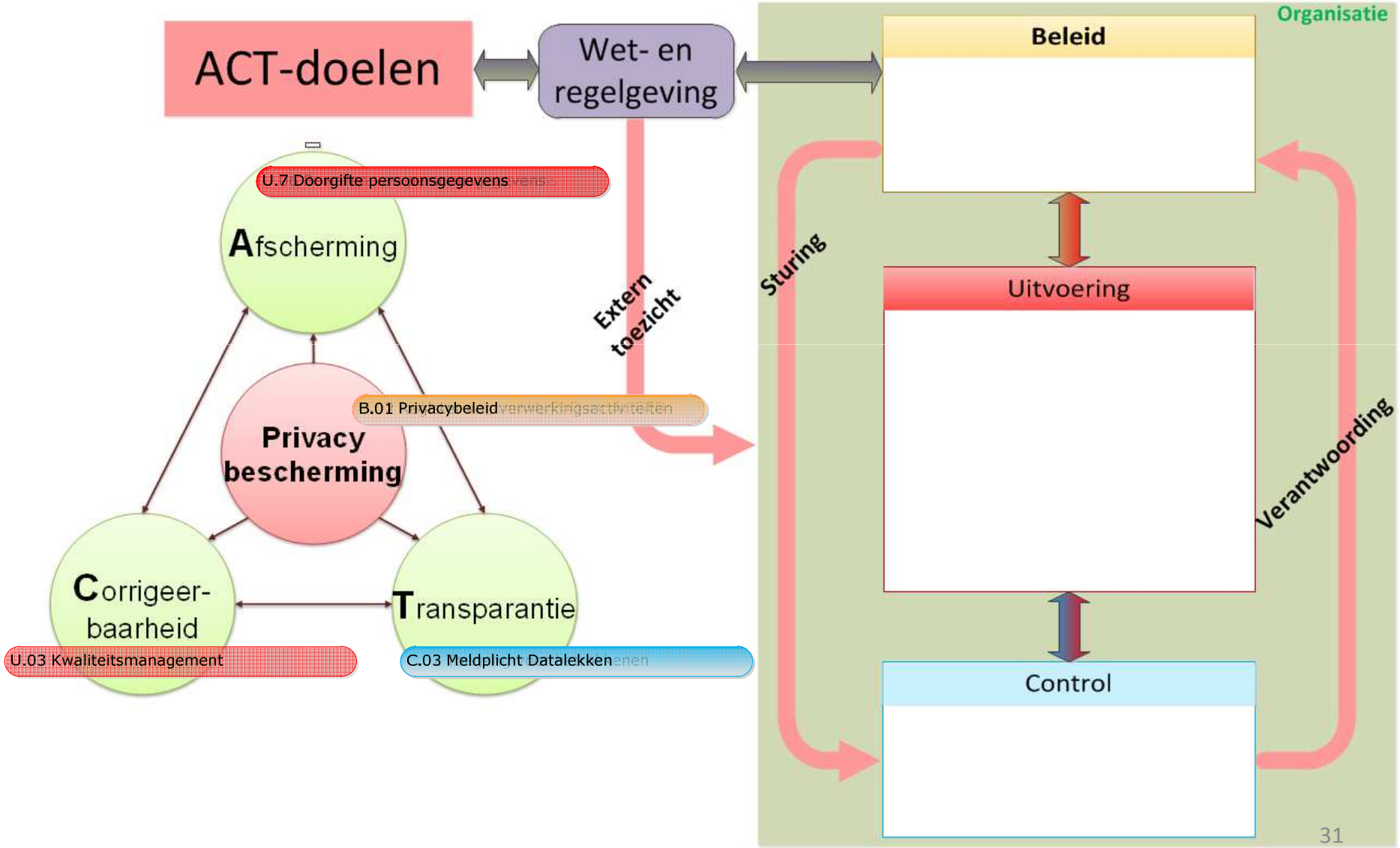
- **Beleid:**
  Geeft richting en kaders
- **Uitvoering:**
  Verwerkt persoonsgegevens
- **Control:**
  Toont compliancy aan

Resultaat:

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



Opbouw van de Privacy Baseline

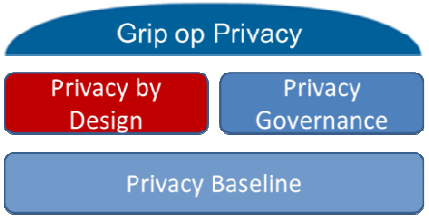


Hoe komen de handleidingen tot stand?

- Werkgroep met 20-tal deelnemers uit de CIP community
- Samenstelling kan wisselen
- Veel kennis voorhanden
- Inhoud aangedragen en gevraagd door:
  - leden van de werkgroep
  - interviews bij organisaties
  - Privacy Vraagbaak

Vraaggericht en Aanbodgericht

Handleiding Privacy by Design

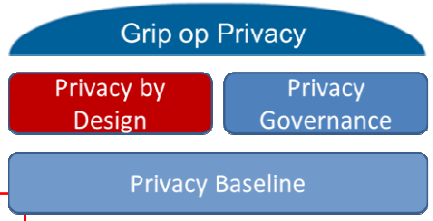


- Maakt ontwerpers bewust van het belang van privacy
- Handvaten om de bescherming om de ACT-doelen mee te nemen in de ontwerpfasen en het ontwerp
- Ondersteunt zowel het formele als het creatieve proces
- Proactieve aanpak, voorkomt hoge kosten van aanpassingen achteraf
- Een betere bedrijfsvoering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

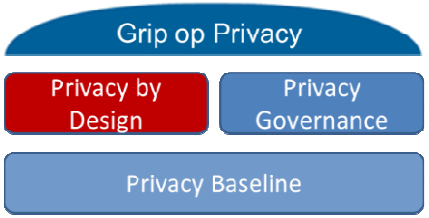
maar ook:

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

Inrichtingsprincipes voor het ontwerp

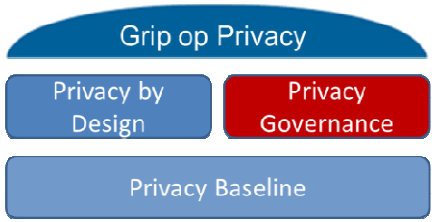


- Architectuurprincipes: Hoe wordt het ontwerp een succes?
  - Waar moet op gelet worden om aan de criteria te voldoen
  - Reduceren van de complexiteit
  - Beschikbare technologieën
- Extra principes bij de inzet van mobiele apparaten

Handvaten voor de "bouw"

De handvaten helpen de ontwerper bewust keuzen te maken

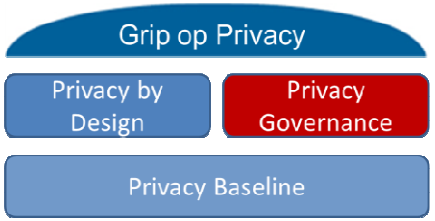
Handleiding Privacy Governance



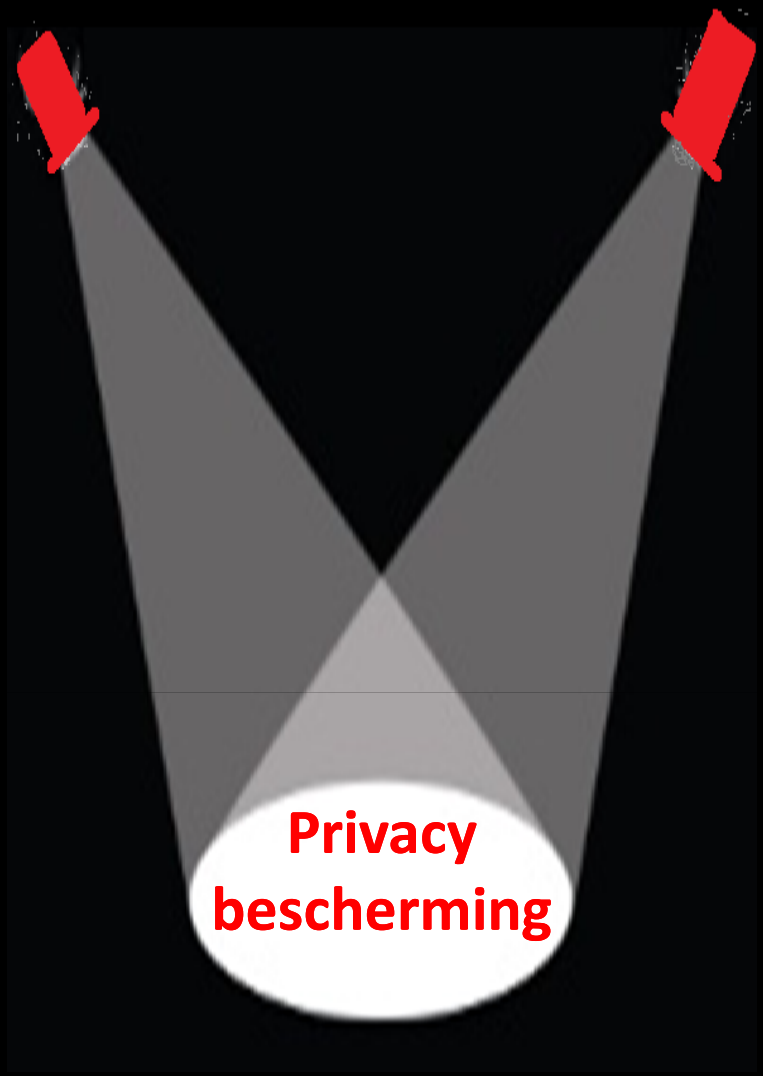
- Privacybescherming verhoogt de kwaliteit van de bedrijfsvoering door het leveren van betere diensten. Dit vraagt om sturing en een groeipad.
- De Handleiding Privacy Governance geeft u handvaten om grip te krijgen op de privacybescherming.
- Het Privacy Volwassenheidsmodel helpt u het ambitieniveau te kiezen en als organisatie daar naartoe te groeien.
- De handleiding en het volwassenheidsmodel geven sturing aan een veranderperspectief, waarbij de kracht van de organisatie wordt benut.

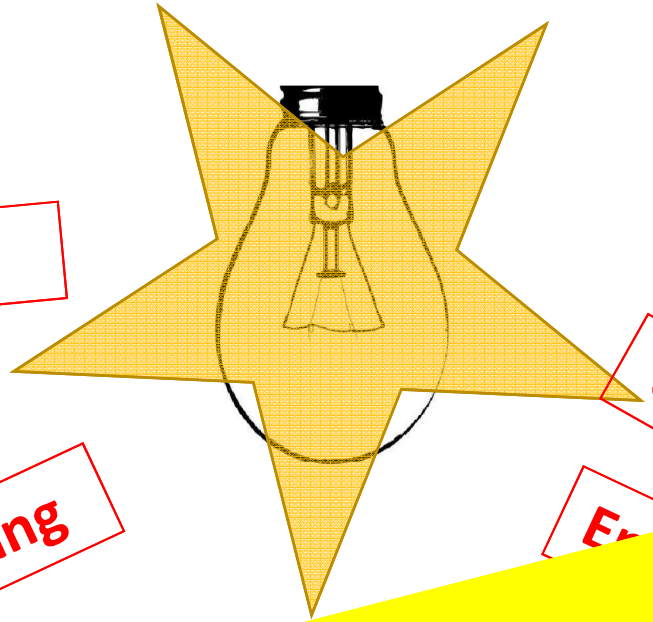
Iedere organisatie bepaalt zelf het ambitieniveau

Privacy Governance: hoe?



- Principes van verandermanagement om de kracht van de organisatie te benutten.
- Toegespitst op de ‘zachte’ veranderfactoren: een wet maakt niet vanzelf goede privacybescherming.
- Wel: kritische succesfactoren: je wil natuurlijk wel ergens komen en dat kunnen vaststellen.


Privacy
bescherming



Procesontwerp

Ketenafspraken

centraal

Beleidsvorming

Informatiebeveiliging

Privacybescherming:

De organisatie heeft meestal al veel op eigen kracht geregeld

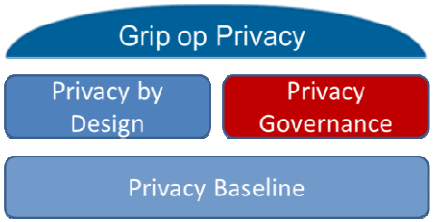
Audits

Externe invloeden

Governance

Security by Design

Handleiding Privacy Governance



Als voorbeeld: COBIT management guidelines

1. Doelstelling van de processen

2. Key Succes Factoren

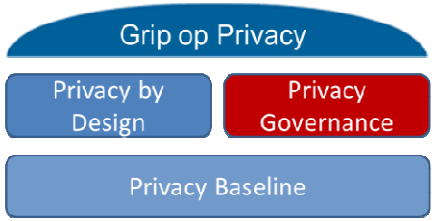
3. Key Goal Indicatoren

Deze staan als indicatoren in de Privacy Baseline

4. ~~Key Performance Indicatoren~~

Principes van verandermanagement om de kracht van de organisatie te benutten.

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

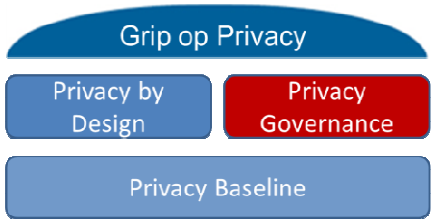
- Voor (kleine,) middelgrote en grote organisaties

‘goed huisvaderschap’

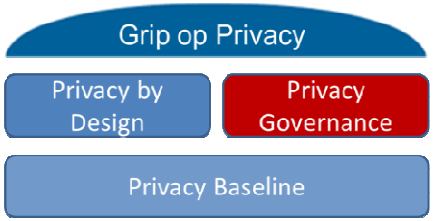
- **Ambitieniveau wordt bespreekbaar**

Volwassenheidsniveaus

Volwassenheidsniveaus:



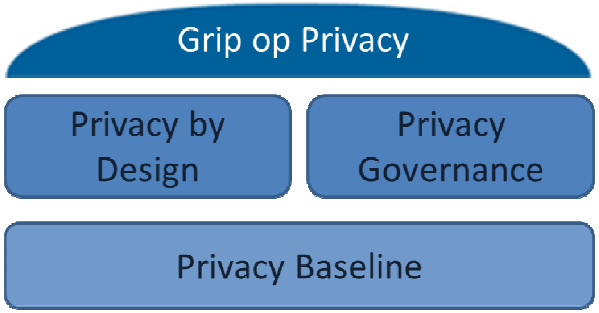
Privacy Selfassessment



- **Beantwoord de vragen van de Privacy Selfassessment**
  - Ontdek het volwassenheidsniveau van de organisatie
- **Kies uw ambitieniveau**
  - Ontdek op welke punten privacy nog aandacht moet krijgen binnen uw organisatie
- **Maak het grip op privacy krijgen bespreekbaar**
  - Vergelijk en bespreek de scores en de ambities van de stakeholders
  - PriSA -workshop

Nog steeds bang?

- **Grip op Privacy maakt de aanpak transparant.**
- **Grip op Privacy geeft u de handvaten.**



- **Grip op Privacy maakt door de juiste investeringen uw bedrijfsvoering beter.**
- **Grip op Privacy hoeft u alleen nog maar toe te passen.**
- **Nog niet overtuigd?**
  Voer de Privacy Selfassessment uit.

Niet bang
en
nog niet overtuigd van de noodzaak?

10 redenen voor architecten om PbD alsnog toe te passen:

1. Privacy by Default is niet toegepast.
2. De noodzaak van de verwerking en de opslag van de gegevens liggen niet vast.
3. Van de doorgiften liggen de wettelijke grondslag en de waarborgen niet vast.
4. De complexiteit van de gegevensverwerking is te hoog, waardoor het corrigeren van foutieve gegevens niet mogelijk is.
5. De levenscyclus van persoonsgegevens is niet meegenomen in het ontwerp.
6. Het hoe en waarom de betrokkenen wel of niet worden geïnformeerd over verwerkingen ligt niet vast.
7. De persoonsgegevens zijn niet overdraagbaar.
8. De architectuur benut niet of beperkt de mogelijkheden van encryptie.
9. Bij het maken van ontwerpkeuzen is men zich niet bewust geweest van hoe keuzen de persoonlijke levenssfeer van betrokkenen kunnen beïnvloeden.
10. Om aan te kunnen tonen dat de verwerking aan de Avg voldoet vraagt om dure audits.

10 redenen voor architecten om PbD alsnog toe te passen:

1. Privacy by Default is niet toegepast.
2. De noodzaak van de verwerking en de opslag van de gegevens liggen niet vast.
3. Van de doorgiften liggen de wettelijke grondslag en de waarborgen niet vast.
4. De complexiteit van de gegevensverwerking is te hoog, waardoor het corrigeren van foutieve gegevens niet mogelijk is.
5. De levenscyclus van persoonsgegevens is niet meegenomen in het ontwerp.
6. Het hoe en waarom de betrokkenen wel of niet worden geïnformeerd over verwerkingen ligt niet vast.
7. De persoonsgegevens zijn niet overdraagbaar.
8. De architectuur benut niet of beperkt de mogelijkheden van encryptie.
9. Bij het maken van ontwerpkeuzen is men zich niet bewust geweest van hoe keuzen de persoonlijke levenssfeer van betrokkenen kunnen beïnvloeden.
10. Om aan te kunnen tonen dat de verwerking aan de Avg voldoet vraagt om dure audits.

De Websites

centrum informatiebeveiliging en privacybescherming
Voorpagina
Mijn pagina's
Toevoegen
Groepen
Beheer
Filesender
Alert Online 2015 van start
Handig !!
Collega's zoeken
Zoek Specialisten
Online CIP-ers
CIP Agenda
Twelo's
Snel naar ...
https://cip.pleio.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
www.cip-overheid.nl

Workshop

Privacy by Design door architecten

De bevindingen zijn van toepassing op één van de verwerkingen

Je vraagt zich daarbij mogelijk af:

- Heb ik voldoende sturing gegeven in de vorm van gehanteerde principes?
- Heb ik daarbij voldoende duidelijkheid gegeven aan de ontwerpers?
- Heb ik dat op het juiste moment gedaan?

….en je wordt gevraagd te reageren op de bevindingen.

Wat is handig bij de workshop

1. Weten wat de wettelijke vereisten zijn.
   - Toegang tot de Privacy Baseline
   - (Toegang tot de handleiding Privacy by Design)

2. Weten welke architectuurprincipes er zijn om sturing te geven aan PbD.
   - Toegang tot de NORA architectuurprincipes
   - Kennis van de architectuurprincipes van uw organisatie.

3. Beschrijving van de case.

"Meedoen is belangrijker dan op argumenten te winnen"

Terugkoppeling case-studies

Door NORA en CIP gezette stappen:

Privacy in de NORA

Dit is de goedgekeurde versie van deze pagina. Er is geen nieuwere versie.

NORA > Privacy in de NORA

Om te toetsen hoe privacy geborgd is in de NORA zijn de basis en afgeleide principes nagelopen door het Centrum voor Informatiebeveiliging en Privacybescherming (CIP). Bijkomend doel van deze exercitie is om een idee te krijgen over of de (afgeleide) principes van de NORA voldoende houvast bieden vanuit het perspectief van privacy. Hieronder vind je een overzicht van de principes die bijdragen aan het borgen van privacy en de rationale daarachter. Heb je op of aanmerkingen op deze lijst, laat dat dan vooral weten aan ons via nora@ictu.nl

Privacy in de Basis Principes

Aan privacy gerelateerde Basis principes:

- BP08 vertrouwelijkheid
- BP06 Transparant
- BP09 Betrouwbaar
- BP01 Proactief
- BP07 Noodzakelijk

Het Basisprincipe 8 vertrouwelijkheid is de belangrijkste doelstelling voor overheden in NORA, die bescherming van persoonsgegevens borgt. Want: 'De dienstverlener garandeert dat informatie alleen toegankelijk is voor bevoegde personen en alleen wordt gebruikt voor het doel waarmee zij is verzameld.'

Basisprincipe 6 Transparant transparant is een voorwaarwaarde om voor controleerbaarheid. Als het onbekend is waarvoor persoonsgegevens worden gebruikt is het lastig om te toetsen of dit rechtmatig wordt gedaan.

Basisprincipe nummer 9 Betrouwbaar heeft vooral betrekking op de juistheid en daarmee betrouwbaarheid van gegevens. Maar afnemers mogen er ook van uitgaan dat de dienstverlener zich aan de afspraken houdt, bijvoorbeeld in het geval van privacy de Wbp en vanaf 25 mei 2018 de AVG.

Proactief (BP01) is de grondhouding van privacy by design. Als organisatie denk je proactief na over hoe je gegevensverwerkingsprocessen zo inricht dat de privacy geborgd is in het ontwerpen van de informatiehuishouding.

BP07 Noodzakelijk stelt dat afnemers niet worden geconfronteerd met onnodige vragen. Daarmee is dit principe gekoppeld aan het afgeleide principe 'eenmalige uitvraag'. Dit stimuleert de overheid om reeds beschikbare informatie optimaal te gebruiken. Daarmee staat dit principe soms op gespannen voet met het afgeleide principe 'doelbinding' en dus met het borgen van privacy.

Privacy in de Afgeleide Principes

Doelbinding

doelbinding (AP15) beschrijft dat het doel waarmee gegevens worden gebruikt verenigbaar moet zijn met het doel waarmee ze verzameld zijn. Dit moet voorkomen dat persoonsgegevens voor andere dan de 'welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden' worden gebruikt. Deze doelbinding kan vast worden gelegd in de meta-data Afspraken vastgelegd(AP28).

Informatiebeveiliging

AP's 40- 44 zijn recent toegevoegd om ervoor te zorgen dat informatiebeveiliging beter geborgd is in de NORA. Informatiebeveiliging en privacy liggen als thema's dicht bij elkaar, goede informatiebeveiliging is een randvoorwaarde voor het garanderen van privacy. Daarmee zijn de nieuwe informatiebeveiliging AP's 42, 43 en 44 essentieel voor het borgen van privacy. Waarbij AP43 vertrouwelijkheid direct bijdraagt aan de realisatie van het BP08 Vertrouwelijk. AP44 draagt vooral bij aan de transparantie (BP06). En Integriteit (van gegevens)AP42 houdt vooral verband met de betrouwbaarheid van de gegevens (BP09).

Gebruikersperspectief

Vanuit het gebruikersperspectief wordt privacy versterkt door inzicht in je eigen gegevens door Transparante dienstverlening AP25, Afnemer heeft inzage AP26 en controleerbaarheid AP44. Daarmee is Verantwoording dienstlevering mogelijk AP30. Er moet sowieso met vertrouwelijkheid AP43 met informatie worden omgegaan .

By design

AP24 Proactief realiseert BP01 Proactief en daarmee het 'by design' aspect van privacy by design. De AP's 27-34 zorgen ervoor dat privacy by design bestuurlijk geborgd is doordat; in de keten is Een verantwoordelijke organisatie AP27, Afspraken vastgelegd AP28 en De dienstverlener voldoet aan de norm AP29. Hierdoor is Verantwoording dienstlevering mogelijk AP30. De kwaliteit van de dienst wordt via een PDCA-cyclus in besturing kwaliteit AP31 verder geborgd. Sturing kwaliteit op het hoogste niveau AP32 betekend dat dit op het hoogste niveau belegd is. De kwaliteitscriteria, standaarden en best practices zijn vertaald in een Baseline kwaliteit diensten AP33 en de dienstverlener legt bestuurlijke verantwoording af over de mate van transparantie en control via AP34: Verantwoording besturing kwaliteit.

Aan privacy gerelateerde Afgeleide Principes:

- AP05 Nauwkeurige dienstbeschrijving
- AP15 doelbinding
- AP16 Identificatie informatie-objecten
- AP17 Informatie-objecten systematisch beschreven
- AP19 Perspectief gebruiker
- AP24 Proactief aanbieden
- AP25 Transparante dienstverlening
- AP26 Afnemer heeft inzage
- AP27 Een verantwoordelijke organisatie
- AP28 Afspraken vastgelegd
- AP29 De dienstverlener voldoet aan de norm
- AP30 Verantwoording dienstlevering mogelijk
- AP31 PDCA-cyclus in besturing kwaliteit
- AP32 Sturing kwaliteit op het hoogste niveau
- AP33 Baseline kwaliteit diensten
- AP34 Verantwoording besturing kwaliteit
- AP42 Integriteit (van gegevens)
- AP43 vertrouwelijkheid
- AP44 Controleerbaarheid

Categorieën: Onderwerpen | Privacy | Thema's

https://www.noraonline.nl/wiki/Privacy_in_de_NORA

Relaties Baseline Principes CIP en Afgeleide Principes

De relaties tussen de baseline en de afgeleide principes zijn soms behoorlijk 1-op-1, maar soms vereist de bedoelde overeenkomst enige lenigheid van denken. Dit komt door de uiteenlopende herkomst en scope van de NORA en Privacy Baseline. U01 Doelbinding en AP15 Doelbinding zijn bijvoorbeeld één op één te vertalen. Voor de doorgifte van persoonsgegevens is ook AP15 Doelbinding van belang, maar dit privacy baseline principe is terug te vinden in nog vier AP's.

Hieronder staat een overzicht van de gevonden common ground tussen de Privacy Baseline Principes aan de linkerkant en de Afgeleide Principes aan de rechterkant. De eventuele toelichting van de relatie vind je in het midden. Heb je op of aanmerkingen? Schroom deze dan niet te melden via: nora@ictu.nl.

Privacy Baseline Principe	Beschrijving relatie	NORA principe
B.01: Privacybeleid	Van de dienst (in AVG-termen: de gegevensverwerking) is duidelijk hoe de privacy wordt gewaarborgd.	AP05: Nauwkeurige dienstbeschrijving
B.01: Privacybeleid	Het privacybeleid is op het hoogste niveau van de organisatie goedgekeurd en geldt daarmee voor de gehele organisatie, waardoor de samenhang over der verschillende domeinen heen en voor de gehele dienstenportfolio geldt.	AP32: Sturing kwaliteit op het hoogste niveau
B.01: Privacybeleid	Borging vindt plaats in een cyclisch beleidscyclus. Deze is in het privacybeleid vastgelegd.	AP31: PDCA-cyclus in besturing kwaliteit
B.01: Privacybeleid	In het beleid is vastgelegd aan welke baseline het dienstenportfolio moet voldoen, zodat duidelijk is aan welke kwaliteitscriteria wordt voldaan. Het volwassenheidsmodel helpt de baseline te hanteren.	AP33: Baseline kwaliteit diensten
B.02: Organieke inbedding	De verantwoordelijkheden zijn in de TVB van de organisatie vastgelegd. Deze TVB is op het hoogste niveau vastgesteld.	AP32: Sturing kwaliteit op het hoogste niveau
B.03: Risicomanagement Privacy by Design en de GEB		AP34: Verantwoording besturing kwaliteit
B.03: Risicomanagement Privacy by Design en de GEB	De risico's en de genomen maatregelen, bestaande uit de gehanteerde baseline en de benodigde aanvullende maatregelen zijn duideljk. Om het passend zijn van de maatregelen in de tijd te borgen vindt er continu management plaats, waarbij de resultaten worden meegenomen in de criteria B.01 Privacybeleid en B.02 Organieke inbedding.	AP33: Baseline kwaliteit diensten
C.01: Intern toezicht		AP44: Controleerbaarheid
C.01: Intern toezicht	Toezicht maakt het de verantwoordelijke van de gegevensverwerking mogelijk om op ieder niveau verantwoording te kunnen afleggen over de kwaliteit van de privacyborging.	AP34: Verantwoording besturing kwaliteit

Vragen aan de zaal:

Gebruik je de Afgeleide Principes van de NORA?

…bij de start van een project?

Heb je behoefte aan aanpassing van de afgeleide principes?

Heb je best practices die je wilt delen?

Heb je andere ideeën over betere borging van privacy in de NORA?