Tools voor AVG impact assessment

Bob Hulsebosch

IZO-platform 9-feb-2018

Aanleiding

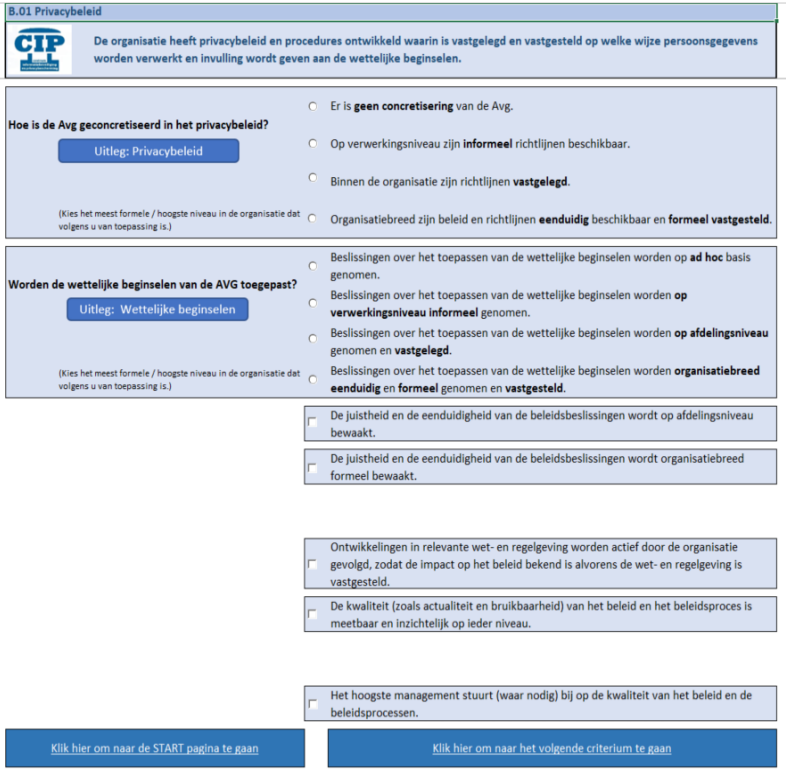
- ZINL: verken de mogelijkheden van AVG-tooling voor ZINL programmamanagers en ketenpartners
  - Overzicht van beschikbare tools
  - Eigen tool voor AVG self-assessment

- Agenda:
  - Overzicht van tools
  - Eigen tool (in ontwikkeling)

Overzicht tools

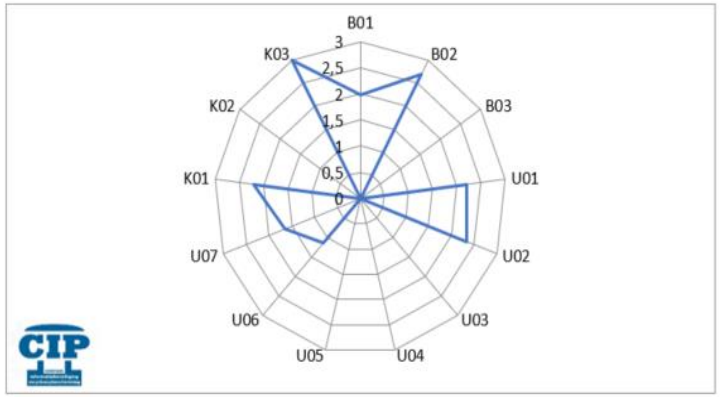
CIP AVG Self Assessment Tool

https://www.cip-overheid.nl/grip-op-privacy/



Het resultaat van het CIP Privacy Selfassessment

Uw ambitieniveau waarop u uw vragen heeft beantwoord is:	4
Uw volwassenheidscore is (gemiddeld)	1,3



Terug naar laatste vraag | Naar begin van de Privacy Selfassessment

U kunt uw doelstellingen voor de korte termijn lager stellen dan uw ambities.

Op niveau wilt u uw doelstellingen realiseren?

(Bedenk: Het niveau mag niet hoger liggen dan het ambitieniveau waarop u de vragen heeft beantwoord.)

Tip om de moed erin te houden: als het uw volwassenheidscore meer dan 1 niveau lager ligt dan uw ambitieniveau, kies dan een doelstellingenniveau dat niet meer dan 1 niveau hoger ligt.

- ○ Niveau 1
- ○ Niveau 2
- ○ Niveau 3
- ○ Niveau 4
- ◉ ~~Niveau 5~~

Tip: de adviezen hieronder passen niet altijd allemaal binnen de gegeven ruimtes. Gebruik de PriSA Rapportgenerator om een goed leesbaar rapport te maken.

De nog na te streven doelstellingen om het gewenste volwassenheidsniveau 5 te bereiken zijn:

AP Stappenplan

https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/2017-11_stappenplan_avg_online_v2.pdf

AUTORITEIT
PERSOONSGEGEVENS

In 10 stappen voorbereid op de AVG

Vanaf 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. Dat betekent dat vanaf die datum dezelfde privacywetgeving geldt in de hele Europese Unie (EU). De Wet bescherming persoonsgegevens (Wbp) geldt dan niet meer.

Wat verandert er?
De AVG versterkt de positie van de betrokkenen (de mensen van wie gegevens worden verwerkt). Zij krijgen nieuwe privacyrechten en hun bestaande rechten worden sterker. Organisaties die persoonsgegevens verwerken krijgen meer verplichtingen. De nadruk ligt – meer dan nu – op de verantwoordelijkheid van organisaties om te kunnen aantonen dat zij zich aan de wet houden.

Wat kan ik doen?
Als organisatie kunt u nu alvast stappen ondernemen om straks klaar te zijn voor de AVG. Om u hierbij te helpen, heeft de Autoriteit Persoonsgegevens de 10 belangrijkste stappen voor u op een rijtje gezet. In het grote AVG-dossier op de website van de AP vindt u de antwoorden op veelgestelde vragen.

Stap 1: Bewustwording

Zorg ervoor dat de relevante mensen in uw organisatie (zoals beleidsmakers) op de hoogte zijn van de nieuwe privacyregels. Zij moeten inschatten wat de impact van de AVG is op uw huidige processen, diensten en goederen en welke aanpassingen nodig zijn om aan de AVG te voldoen. Houd er rekening mee dat de implementatie van de AVG veel kan vragen van de beschikbare menskracht en middelen en begin er daarom op tijd mee.

De Autoriteit Persoonsgegevens (AP) biedt instrumenten die u kunnen helpen om de AVG na te leven, zoals guidelines die zijn opgesteld samen met de andere privacytoezichthouders in Europa.

Bedenk dat de AP uw organisatie sancties kan opleggen van maximaal 20 miljoen euro of 4% van uw wereldwijde omzet als u zich niet aan de nieuwe privacywetgeving houdt.

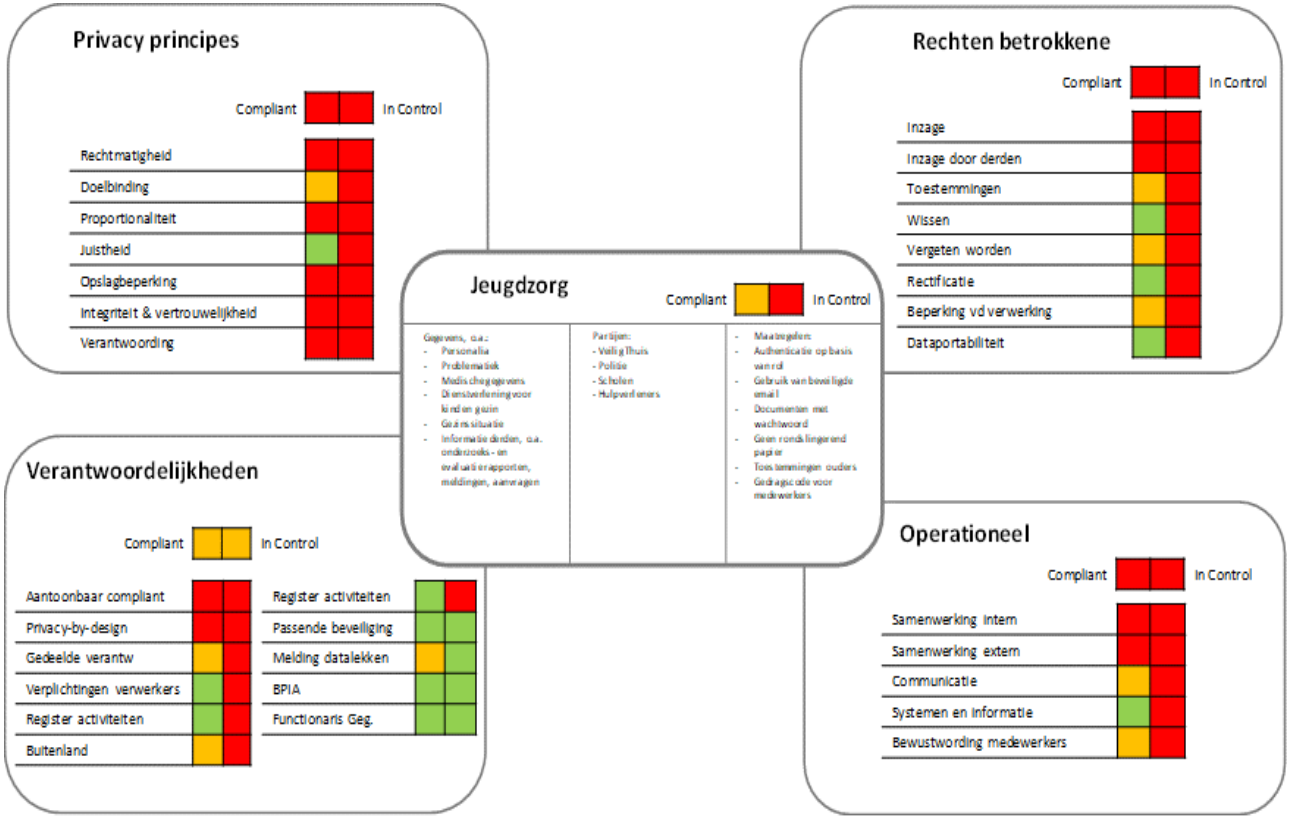
Stap 2: Rechten van betrokkenen

Onder de AVG krijgen de mensen van wie u persoonsgegevens verwerkt meer en verbeterde privacyrechten. Zorg er daarom voor dat zij hun privacyrechten goed kunnen uitoefenen.

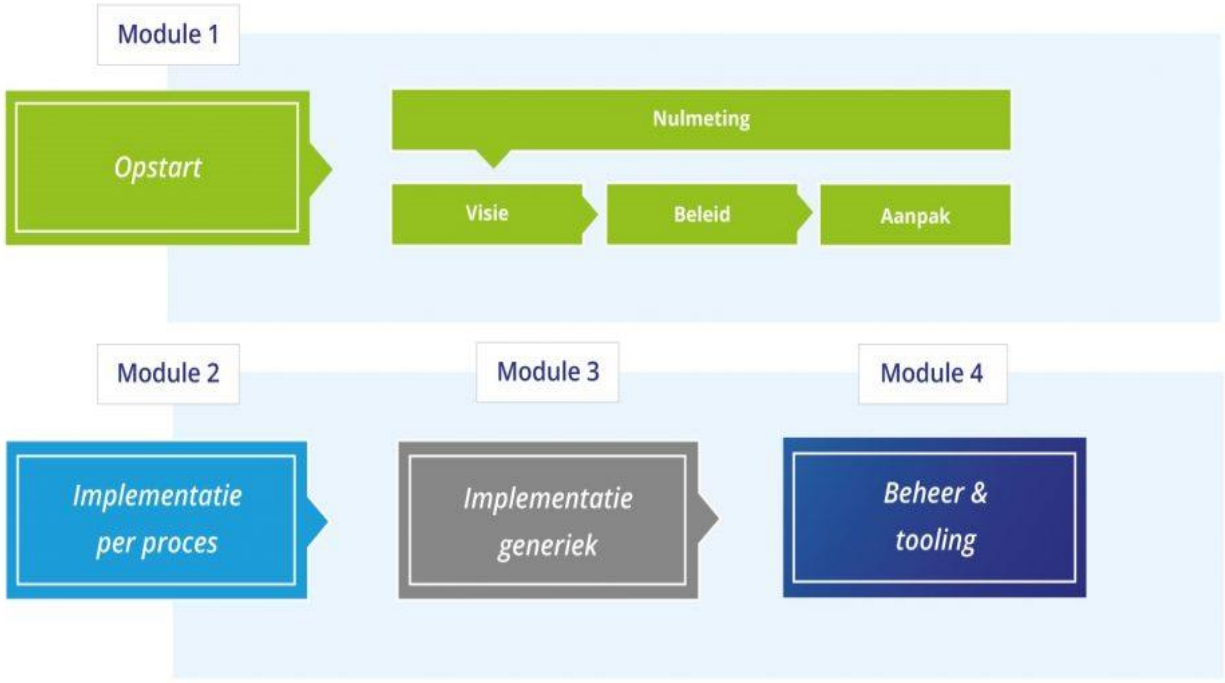
VNG/KING materiaal

- Stappenplan:
  - Stel een Functionaris Gegevensbescherming (FG) aan
  - Stel een privacybeleid op en draag het uit
  - Stel een register van verwerkingen op (en hou het bij)
  - Pas de werkprocessen aan
  - Maak afspraken met derden
- Het stappenplan is hier te vinden: https://vng.nl/files/vng/20171204-vng-king-stappenplan-voorbereiding-avg_.pdf.
- Daarnaast biedt KING ook diverse templates aan, bijvoorbeeld voor de Verwerkersovereenkomst of het Privacy Beleid. Zie https://www.vngrealisatie.nl/secties/privacy/producten/voorbereidingstips-voor-de-komst-van-de-avg

InnoValor AVG impact assessment



PMP Privacy Proof



Handreikingen

- Nederlandse chapter van gecertificeerde informatiebeveiligingsprofessionals (ISC)2: https://chapter.isc2.nl/app/uploads/2017/10/AVG-in-DC-formaat-2.pdf
- Nederland ICT, een verzameling van blogs over de AVG, zie https://www.nederlandict.nl/dossier/avg/
- Privacy Management Partners heeft een goede blogserie over de AVG: https://www.pmpartners.nl/category/kennis/avg/.
- SURF, de ICT-samenwerkingsorganisatie voor het hoger onderwijs en onderzoek, biedt via de website tal van hulpmiddelen aan voor de instellingen. Deze website is hier te vinden: https://www.surf.nl/themas/beveiliging/beleidsondersteuning-privacy/algemene-verondening-gegevensbescherming-avg/index.html. Onderdelen zijn o.a.:
  - Uitwerking AVG (work in progress): https://wiki.surfnet.nl/display/privacy/De+privacyverordening+uitgewerkt
  - Model voor het uitvoeren van een PIA: https://www.surf.nl/themas/beveiliging/beleidsondersteuning-privacy/algemene-verondening-gegevensbescherming-avg/impact-en-riskassessment/index.html
- Privacy modelbeleid: https://www.surf.nl/themas/beveiliging/beleidsondersteuning-privacy/algemene-verondening-gegevensbescherming-avg/privacy-modelbeleid/index.html

Eigen tool

Let wel: is nog in ontwikkeling en ter discussie!

Huidige AVG-tool ZINL

- Uitgangspunten
  - Eenvoudig in gebruik / laagdrempelig
  - Vooral aanzetten tot bewustwording

- Wat doet het wel:
  - Brengt in kaart waar AVG uitdagingen zitten

- Wat doet het (nog) niet:
  - Het leggen van allerlei slimme relaties tussen vragen
    - Bv: Als ‘nee’ bij vraag 2 dan is vraag 5 niet van toepassing
  - Uitsluitsel geven of een FG, register van verwerkingen of DPIA nodig is

Uitkomsten

Het resultaat van het Privacy Selfassessment

Onderstaand is een visuele weergave van de score op het Selfassessment zoals beschreven in de huidige situatie.

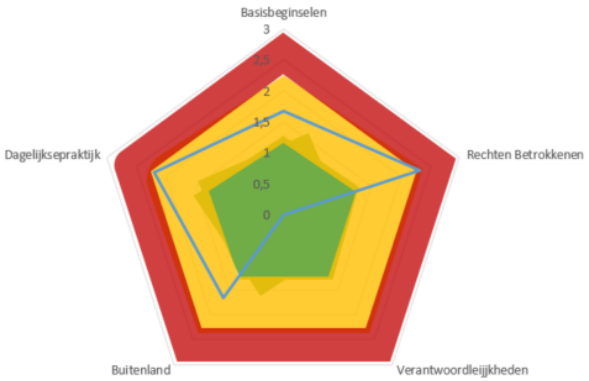
Zorginstituut Nederland

Het object waarover dit assesment wordt uigevoerd is als volgt omschreven:	Een korte beschrijving van het object
Het object heeft als doel om:	Het doel van de dataverwerking is optimale zorg bieden
U heeft aangegeven dat de volgende stakeholder betrokken zijn:	Stakeholders zijn ZINL, CIZ, SVB en UWV

Er vind verwerking plaats van persoonsgegevens en bijzondere gegevens waarbij u de rol vervult als verantwoordelijke

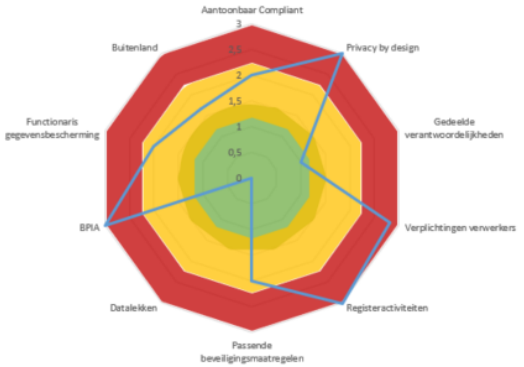
Algemene score

Onderstaande afbeelding is een visuele weergave van uw score op de verschillende gebieden van het assesment. Indien uw scoort in het groene gebied bent u "in control" op dit onderwerp, oranje als uw compliant bent en rood als de privacy van dit onderwerp zich in de kritische zone bevindt. De deelgebieden worden verder gespecificeerd in onderstaande weergaves.

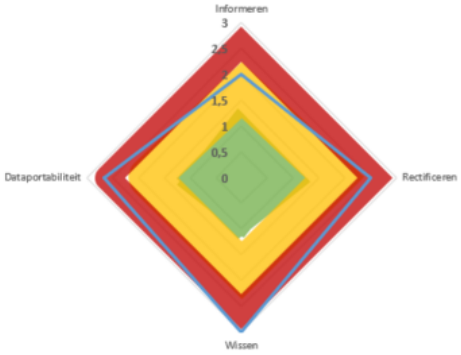


Basisbeginselen

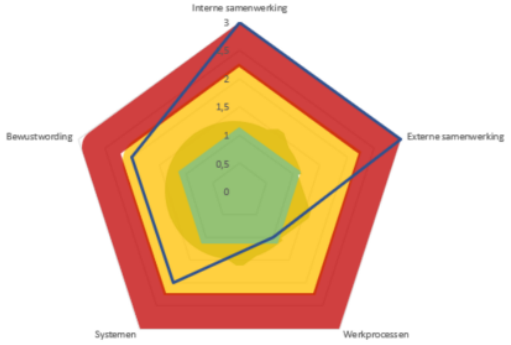
Verantwoordelijkheden



Rechten betrokkene



Dagelijkse praktijk



Wat vinden jullie ervan?

- Wat ontbreekt?
- Wat zou je anders willen zien?
- …