INFORMATIE BEVEILIGINGS DIENST

AVG Borgingsproduct 2.0

18 maart 2021

Borgingsproduct 1.0 (& 2.0)

- Criteria om de AVG te vertalen naar een kwaliteitscyclus voor gegevensbescherming voor gemeentelijke processen
- 7 thema’s >>
- ‘Levend’ document: **feedback gemeenten**, wet- en regelgeving, jurisprudentie etc

AVG Borgingsproduct 2.0

- Behoefte van gemeenten (webinar 9/2020):
  (1) aan privacyvolwassenheidsniveaus
  (2) een tool om de staat van privacy te monitoren

- Alle controls van versie 1 gegoten in volwassenheidsniveaus 1 t/m 5 (ad hoc, herhaalbaar, bepaald, beheerst, geoptimaliseerd)

- Nieuwe controls uit het PbD-instrumenten en de ISO27701

- Ter inspiratie: IAPP, CIP, Amsterdam, Den Haag

- Gemeentespecifiek (raad/college, transparantie, DPIA)

Risicogebaseerde aanpak

Waarom

1. Een hulpmiddel in eerste instantie voor de proceseigenaren om AVG-controls te implementeren (organisatiebreed en binnen afdelingen) en grip te houden (geen momentopname)
2. Sturingsinformatie voor het management (ambitieniveau)
3. Efficiënter werken door de organisatie / kwaliteit dienstverlening

4. ‘Kapstok’ document: privacyproducten aan controls koppelen
5. Vergelijkingen maken tussen (afdelingen van) gemeenten (gezonde competitie)
6. Bruikbare inzichten op lokaal, regionaal en nationaal niveau > inzicht in waar behoefte aan bestaat (door gemeenten en VNG/IBD)

7. Last but not least: imagoverbetering en een morele verplichting

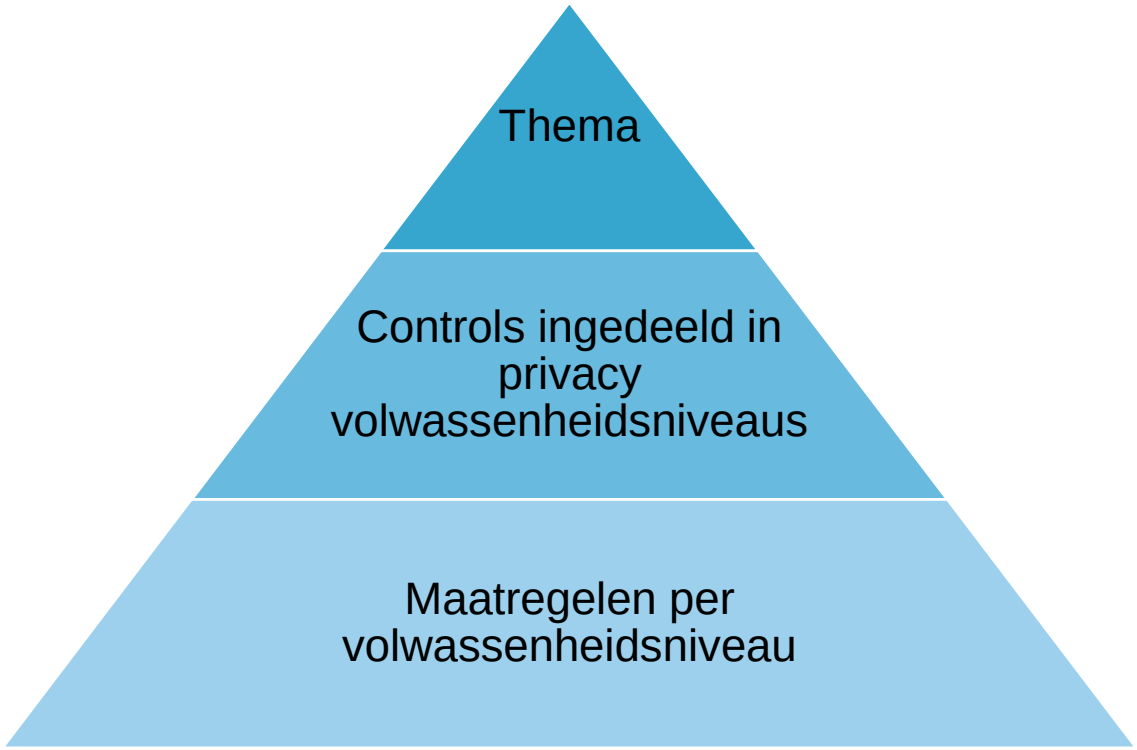
Wie

- Proceseigenaren > meten waar de organisatie staat, met ondersteuning PO
- Management > ambitieniveau bepalen
- Het college of gemandateerde > ambitieniveau vaststellen
- FG > met de resultaten van de proceseigenaren (ongevraagd) adviseren

Opbouw

1. Beleid
2. Organisatorische inbedding
3. Processen
4. Rechten van betrokkenen
5. Samenwerking
6. Beveiliging
7. Verantwoording

P en O-maatregelen



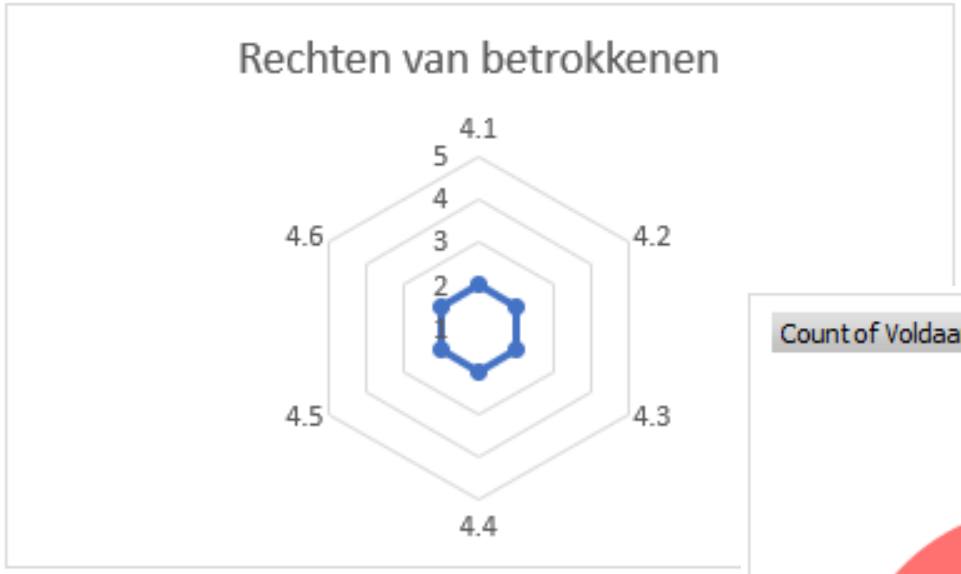
1 Ad hoc	• Geen of onduidelijke privacyrollen en -verantwoordelijkheden • Geen of nauwelijks beheersmaatregelen aanwezig • Reactief en sturing n.a.v. incidenten • Grote afhankelijkheid van één of enkele privacyfunctionarissen • Onbewust onbekwaam
2 Her-haalbaar	• Privacyrollen en -verantwoordelijkheden toegewezen • Beheersmaatregelen zijn aanwezig, maar worden op informele wijze uitgevoerd • Standaarden en formats aanwezig: juist en in duidelijke taal • Bewust onbekwaam
3 Bepaald	• (Privacy)medewerkers tonen eigenaarschap, d.w.z. dat de rollen en verantwoordelijkheden actief worden opgepakt • Beheersmaatregelen worden consistent en gestructureerd uitgevoerd en zijn gedocumenteerd • Er wordt aantoonbaar aan verplichtingen voldaan • Verwerkingsverantwoordelijke bestuursorganen nemen beslissingen mede op grond van risicoanalyses zoals een DPIA. • Er is een duidelijke samenhang met informatiebeveiliging • Bewust bekwaam
4 Beheerst	• De effectiviteit van beheersmaatregelen wordt periodiek geëvalueerd in een PDCA-cyclus • Er wordt proactief geïnformeerd door de proceseigenaar over de realisering van de geconstateerde benodigde verbeteringen in een PDCA-cyclus • In een jaarlijkse evaluatie blijkt een correcte PDCA-cyclus • Bewust bekwaam
5 Geopti-maliseerd	• Toekomstgericht • Proactieve houding van het college en het bestuur • Het verantwoordelijk management verzoekt aan de FG om hun verantwoording van een oordeel te voorzien. • Privacy wordt gezien als een vanzelfsprekendheid • Er wordt continue gezocht naar verbetering, zoals in de vorm van (interne of externe) tooling • Privacy wordt gezien als een kans of unique selling point (USP) • Er wordt verbinding gezocht met andere concerndisciplines • Kennis en ervaringen worden actief gedeeld met gemeenten en andere relevante organisaties waardoor best practices in gemeentenland ontstaan • Onbewust bekwaam

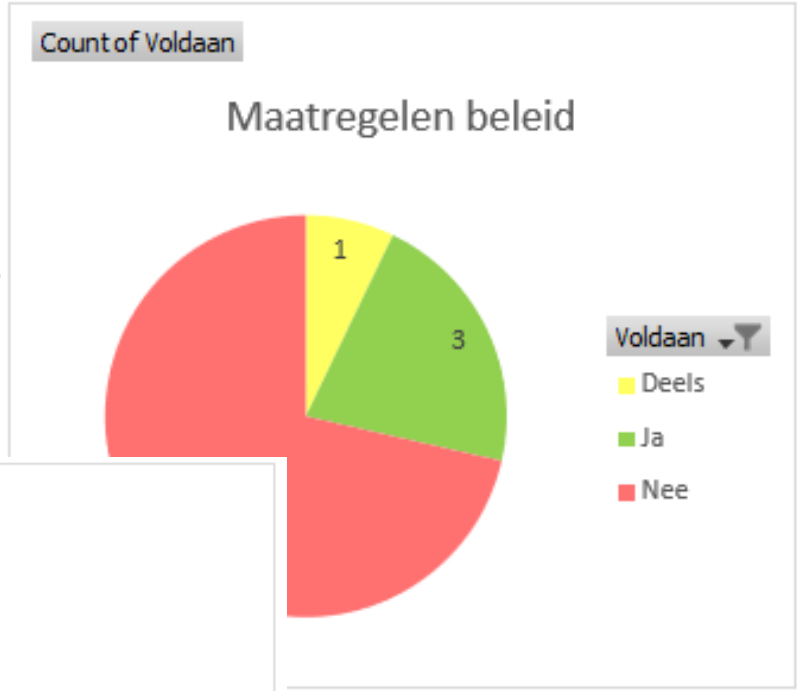
Samenhang met BIO (voorbeelden)

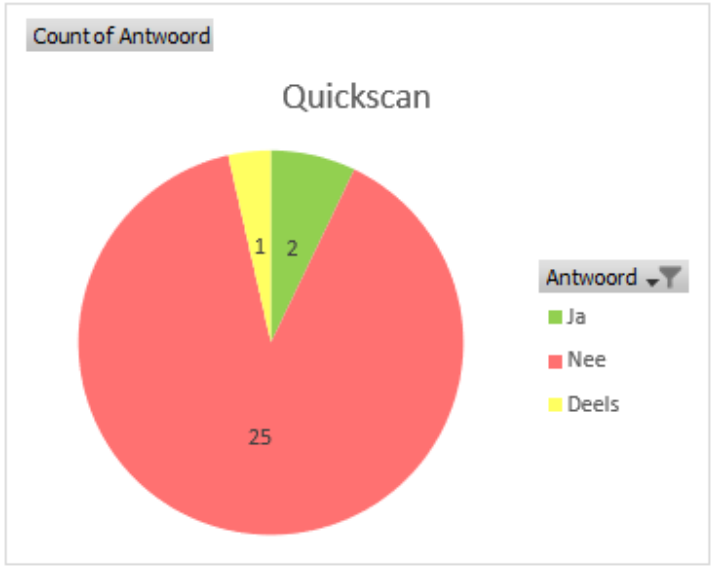
1.0	2.0	BIO
6.1 De staat van informatiebeveiliging en de implementatie ervan wordt onafhankelijk en periodiek, of zodra zich belangrijke veranderingen voordoen, beoordeeld.		BIO Control 18.2 “Informatiebeveiligingsbeoordelingen
6.2 Persoonsgegevens zijn opgenomen binnen het classificatiesysteem.	Maatregel 20.6.3.7 (Persoonsgegevens worden structureel opgenomen in een classificatiesysteem.	BIO Control 8.2 “Informatieclassificatie”. Relevante IBD producten: Handreiking Dataclassificatietoets BIO gemeenten
6.8 Er is een beleid over testen met persoonsgegevens		BIO Control 14.3 “Testgegevens”

Grafieken


Thema's
Beleid
Processen
Organisatorische inbedding
Rechten van betrokkenen
Samenwerking
Beveiliging
Verantwoording
5
4
3
2
1


Rechten van betrokkenen
4.1
4.2
4.3
4.4
4.5
4.6
5
4
3
2
1


Count of Voldaan
Maatregelen beleid
1
3
Voldaan
Deels
Ja
Nee


Count of Antwoord
Quickscan
1
2
25
Antwoord
Ja
Nee
Deels

INFORMATIE
BEVEILIGINGS
DIENST

Demo

INFORMATIE BEVEILIGINGS DIENST

Vragen of verbetervoorstellen?

- VNG Privacyforum
- privacy@vng.nl