JAARRAPPORTAGE GEGEVENSBESCHERMING GEMEENTE BEEK 2021

Jaarrapportage voor de gemeenteraad

Functionaris Gegevensbescherming

Veerle van Hees

31-12-2021

Samenvatting

Het jaar 2021 was een interessant jaar voor de AVG. De AVG is inmiddels geïmplementeerd en gemeenten hebben veel kennis uitgewisseld en producten met elkaar gedeeld, zowel online (bijvoorbeeld via het VNG privacyforum) als offline (bijvoorbeeld via de IBD regiobijeenkomsten). Ontwikkelingen in rechtspraak en wetgeving hebben enige duidelijkheid geboden bij de vele open normen uit de AVG. De verhoogde aandacht voor het beschermen van de privacy van burgers stond hierin centraal. De overheid heeft hierin een belangrijke voorbeeldfunctie.

De verantwoordelijkheden voor de gemeente Beek voor het verwerken van persoonsgegevens van burgers liggen in hoofdlijnen bij drie bestuursorganen: de burgemeester, het college en de gemeenteraad. Het leeuwendeel van de verwerkingen gebeuren onder verantwoordelijkheid van het college.

De gemeenteraad is zelf verantwoordelijk voor de verwerkingen van persoonsgegevens binnen de gemeenteraad en de griffie. Dit brengt verplichtingen met zich mee. In deze jaarrapportage wordt beschreven welke acties en maatregelen de gemeenteraad Beek in 2021 heeft genomen om de doelstellingen en beginselen uit de AVG te behalen en te waarborgen. Ook bevat dit document aandachtspunten en actiepunten voor het jaar 2022. Adequaat omgaan met persoonsgegevens is een blijvend proces en zal dan ook aandacht blijven vergen van zowel bestuur, management als medewerkers.

Samenvattend heeft de gemeente in 2021 veel werk verzet op het gebied van gegevensbescherming.

Veel tijd en aandacht is gegaan naar het uitwerken van werkprocessen rechten van betrokkenen, DPIA, datalekken, uitvoeren van DPIA’s en het aanvullen van de iNavigator, het zelfstandig uitvoeren en oplossen van privacy vraagstukken en bewustwordingscampagnes. Daarnaast zijn de netwerken zowel intern als met omliggende gemeenten aangescherpt en gebruikt waar nodig.

In 2021 is voor het eerst met het Privacy Management System (PMS) gewerkt in een integraal beheerssysteem. Dit is gebaseerd op het PDCA-kwaliteitsmodel en omvat het VNG privacy normenkader. Voor beheersjaar 2021 is in het PMS een eerste meting uitgevoerd over het VNG privacy normenkader. De meting over het privacy VNG normenkader voor het beheersjaar 2022 is inmiddels afgerond. In deze rapportage zijn bevindingen uit deze metingen opgenomen. Te zien is dat in grote mate aan het VNG privacy normenkader wordt voldaan, er een stuk minder stuurvragen zijn waar deels aan wordt voldaan en er geen stuurvragen meer zijn waar niet aan wordt voldaan.

Naast de AVG zijn er ook bijzondere privacy wetten voor BOA’s bij de uitvoering van opsporingstaken. Daarvoor geldt een strenger privacy regime, de Wet politiegegevens (Wpg). Voor toezicht taken geldt de AVG, de BOA’s werken met twee privacy regimes. Hiervoor is het Wpg normenkader in ons Privacy Management System aangeschaft. Voor beheersjaar 2022 is een eerste meting uitgevoerd. Uit die meting voor het NOREA Wpg normenkader blijkt dat er nog veel stuurvragen zijn waar niet of deels aan wordt voldaan.

Inhoudsopgave

INLEIDING **4**

Leeswijzer 4

DEEL 1. VERANTWOORDING COLLEGE AAN RAAD **5**

DEEL 2. TERUGBLIK OP 2021 ..... **6**

1. Het privacybeleid 6
2. Processen 7
3. Organisatorische inbedding 7
4. Rechten van betrokkenen 7
5. Samenwerking 7
6. Beveiliging 8
7. Verantwoording 8
8. Conclusie 9

DEEL 2. VOORUITKIJKEN NAAR 2022 ..... **10**

1. Het privacybeleid 10
2. Processen 11
3. Organisatorische inbedding 11
4. Rechten van betrokkenen 11
5. Samenwerking 11
6. Beveiliging 11
7. Verantwoording 11
8. Conclusies 11

Inleiding

De gemeente dient zorgvuldig om te gaan met persoonsgegevens. Gemeenten verwerken immers bij de uitoefening van hun taken veel informatie. Niet alleen persoonlijke informatie van eigen inwoners, maar ook van andere burgers, medewerkers, externen en zakenrelaties. In de AVG wordt het wettelijk kader beschreven voor het verwerken van persoonsgegevens. Zo dient de gemeente transparant te zijn welke persoonsgegevens zij verwerkt en voor welk doel. Persoonsgegevens mogen alleen worden verwerkt wanneer dit in overeenstemming is met het doel waarvoor zij zijn verzameld en gegevens mogen niet langer bewaard worden dan strikt noodzakelijk. Bovendien moet de gemeente passende technische en organisatorische beveiligingsmaatregelen treffen om onrechtmatige toegang tot deze persoonsgegevens tegen te gaan en daardoor een onrechtmatig gebruik van deze persoonsgegevens te voorkomen. Daarnaast heeft de gemeente ook te maken met tal van privacyregels in sectorspecifieke wetgeving. Dit alles heeft gevolgen voor de inrichting van processen en systemen in en van de gemeente.

Onder de verantwoordelijkheid van zowel het college van B&W als de gemeenteraad vindt een groot aantal verwerkingen van persoonsgegevens plaats. Het gaat hierbij om persoonsgegevens van eigen inwoners, inwoners van andere gemeenten, zakenrelaties, medewerkers en externen. De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de privacyregels in Nederland. Daarnaast dient de gemeente Beek te beschikken over een interne toezichthouder: de Functionaris voor de Gegevensbescherming (FG). 1 januari 2021 hebben de bestuursorganen van de gemeente Beek Veerle van Hees aangesteld als FG[1].

De FG ziet erop toe dat de AVG intern wordt nageleefd. Het college dient erop toe te zien dat de FG naar behoren en tijdig wordt betrokken bij alle gelegenheden die verband houden met de bescherming van persoonsgegevens. Daarnaast dient de FG ondersteund te worden door hem toegang te verschaffen tot persoonsgegevens en verwerkingen daarvan en hem de benodigde middelen ter beschikking te stellen voor het vervullen van de taak en het in standhouden van zijn deskundigheid.

De FG brengt jaarlijks een verslag uit aan de verwerkingsverantwoordelijke van zijn werkzaamheden, bevinden en aanbevelingen. Dit jaarverslag is bedoeld voor de gemeenteraad enerzijds als controlerend orgaan van het college van B&W, anderzijds als zelfstandig verwerkingsverantwoordelijke.

Leeswijzer

Deze jaarrapportage bestaat uit drie onderdelen. In het eerste deel zal een samenvatting worden gegeven van de rapportage die de FG heeft opgesteld voor het college van B&W van de gemeente Beek.

In het tweede en derde deel zal worden aangegeven in hoeverre de verwerkingen van persoonsgegevens door de gemeenteraad voldoet aan de AVG.

In het tweede deel wordt teruggekeken naar het jaar 2021. Wat heeft de gemeenteraad bereikt op het gebied van gegevensbescherming? Welke maatregelen zijn er genomen om te voldoen aan de AVG?

In het derde deel worden aanbevelingen gedaan om gegevensbescherming en privacy in het jaar 2022 naar een nog hoger niveau te tillen. Hierbij wordt waar nodig tevens aandacht geschonken aan de technische en organisatorische middelen die nodig zijn om dit hogere niveau te bereiken.

[1] Hiermee worden de drie bestuursorganen van de gemeente bedoeld: de burgemeester, het college van burgemeester en wethouders en de gemeenteraad.

Deel 1. Verantwoording College aan Raad

Het college van B&W heeft de jaarrapportage gegevensbescherming gemeente Beek 2021van de FG ontvangen. Dit is een vergelijkbaar document als deze jaarrapportage gegevensbescherming, beide naar voorbeeld van VNG sjabloon.

In de rapportage aan B&W wordt tevens verwezen naar het Privacy Management Systeem waarin het privacy VNG en privacy NOREA Wpg normenkader zijn opgenomen. Hierin staat het privacy normenkader en sinds kort is het Wpg normenkader aangeschaft. Het college van B&W heeft de specifieke detailrapporten ontvangen en het college heeft de Verklaring Van Toepasselijkheid (VVT) en de jaarplannen 2022 voor zowel het privacy VNG normenkader als het privacy NOREA Wpg normenkader vastgesteld en ondertekend. Tevens heeft het college kennis genomen van de voortgangsrapportage 2021 voor het VNG Privacy normenkader en de meting en gap analyses 2022 voor beide normenkaders.

Deel 2. Terugblik op 2021

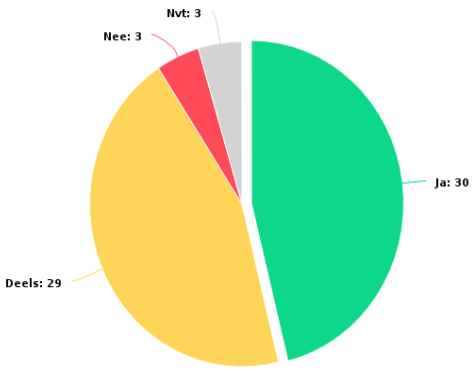
Het eerste deel van het jaar 2021 stond voor wat betreft privacy volledig in het teken van het van kracht worden van de AVG. In dit deel van de rapportage zal worden teruggeblikt op hetgeen de gemeente in 2021 heeft bereikt en welke werkzaamheden zijn verricht.

1. Het privacybeleid

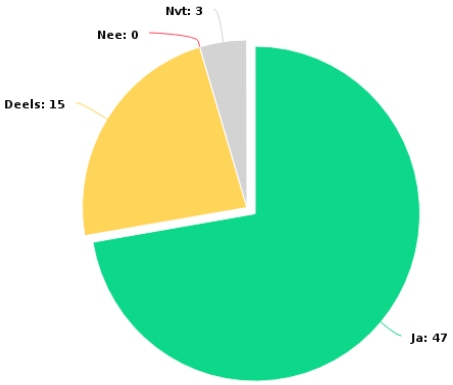
Het privacybeleid is een kader waarin de gemeenteraad van de gemeente Beek aangeeft aan welke principes hij zicht houdt. Het laat zien hoe de gemeenteraad omgaat met persoonsgegevens en welke maatregelen hij treft om te voldoen aan de wet- en regelgeving.

In 2021 is het privacy beleid niet aangepast. De privacyverklaring op de website is aangepast. Via een DigiD formulier kunnen burgers hun rechten van betrokkenen uitoefenen. Ook kunnen burgers deze formulieren van de website downloaden.

Het resultaat van de Privacy meting nummer 1 voor het beheersjaar 2021 en van meting nummer 2 voor het beheersjaar 2022 over het privacy VNG normenkader is als volgt grafisch weergegeven:



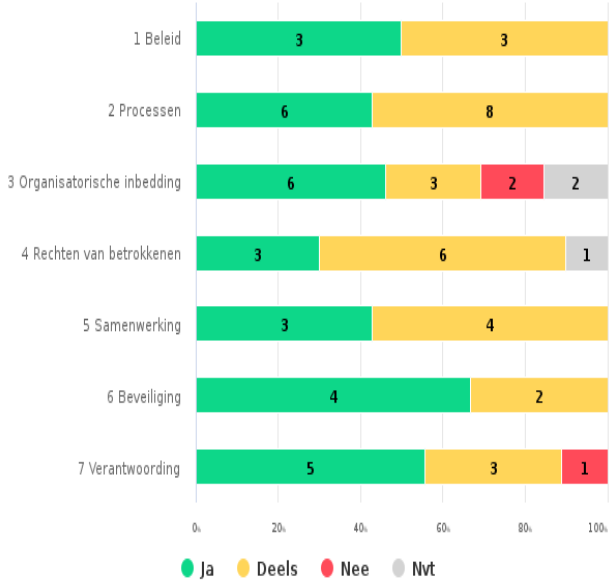
privacy VNG meting beheersjaar 2021



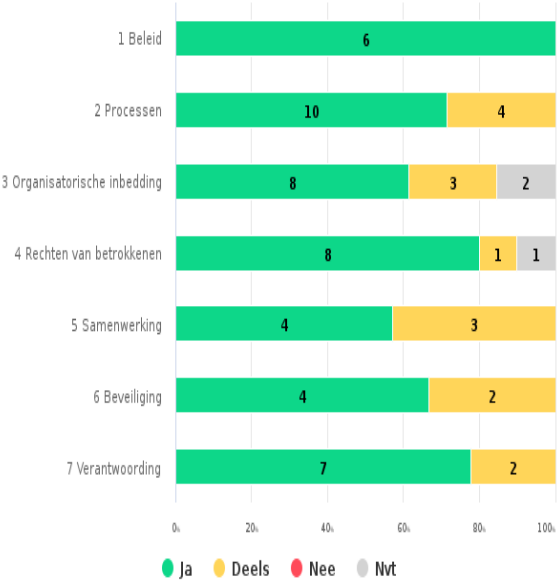
Privacy VNG meting beheersjaar 2022

Figuur 1

Verdeeld over de aandachtsgebieden in het normenkader ziet dit er als volgt uit voor meting 1 en meting 2:



Privacy VNG meting beheersjaar 2021



Privacy VNG meting beheersjaar 2022

Figuur 2

2. Processen

De verwerkingen van persoonsgegevens van de gemeenteraad van de gemeente Beek dienen te voldoen aan de AVG. Dit houdt in dat de werkprocessen die persoonsgegevens bevatten getoetst en ingericht moeten worden volgens de volgende beginselen: behoorlijkheid, transparantie, doelbinding, dataminimalisatie, opslagbeperking, juistheid, integriteit en vertrouwelijkheid. Daarnaast kan de gemeenteraad in gevallen verplicht zijn om een gegevensbeschermingseffectbeoordeling (DPIA[2]) uit te voeren.

De procedure DPIA is uitgewerkt en vastgelegd.

In 2021 zijn de onderstaande DPIA's uitgevoerd:

- Gewijzigde Wet Schuldhulpverlening (WSH)
- MyCorsaNxT
- Siem/SOC
- Verbindingsknooppunt Informatie en Advies (VIA)

De DPIA Liber is verplaatst naar 2022, vanwege capaciteitsgebrek.

3. Organisatorische inbedding

Voor een goede en juiste uitvoering is het van belang dat eenieder binnen de gemeenteraad op de hoogte is van de beginselen van de AVG en het belang van privacy. Organisatorische inbedding betekent het toewijzen van taken, verantwoordelijkheden en bevoegdheden en bewustzijn creëren.

De procedure datalek is uitgewerkt en is intern gecommuniceerd.

Een Privacy pubquiz is gehouden in februari 2021 teneinde bewustwording te creëren onder medewerkers op een ludieke manier. Ook op Beekipedia zijn geregeld berichten geplaatst ter bewustwording. Daarnaast zijn de drie leercirkels, informatiebeveiliging, privacy en integriteit afgerond.

4. Rechten van betrokkenen

De gemeenteraad dient degene waar de gegevens van verwerkt worden (de betrokkene) zowel actief als passief te informeren over het verwerken, de wijze van het verwerken, de grondslag en de maatregelen genomen worden om onrechtmatige toegang en verwerking te voorkomen. Daarnaast stelt de AVG betrokkenen in staat om middels een aantal rechten controle en invloed uit te oefenen over zijn of haar persoonsgegevens.

De procedure rechten van betrokkenen is uitgewerkt en is intern gecommuniceerd.
De privacyverklaring op de website is aangepast. Via een DigiD formulier kunnen burgers hun rechten van betrokkenen uitoefenen. Ook kunnen burgers deze formulieren van de website downloaden.

Er zijn in 2021 geen verzoeken van betrokkenen ingediend.

5. Samenwerking

De gemeenteraad van de gemeente Beek werkt op meerdere beleidsterreinen, in verschillende bedrijfsfuncties, in diverse rollen en hoedanigheden samen met (mede) overheden en private organisaties. In veelvoorkomende gevallen zal er sprake zijn van een verwerking van persoonsgegevens tussen partijen: ontvangen van persoonsgegevens, verzenden van persoonsgegevens, maar ook het opslaan van en inzage hebben in persoonsgegevens valt onder dit begrip. Deze verwerkingen dienen dan ook te voldoen aan de AVG. De gemeenteraad van de gemeente Beek dient dan ook afspraken te maken met deze andere partijen.

De VNG heeft naast het sjabloon 'standaard verwerkersovereenkomst' nu ook modelovereenkomsten voor "gezamenlijke' en 'zelfstandige verwerkersverantwoordelijkheid' opgesteld. De gemeente Beek neemt de VNG sjablonen onverkort over. De FG adviseert welk sjabloon wanneer noodzakelijk is.

[2] De gegevensbeschermingseffectbeoordeling wordt ook wel afgekort tot DPIA naar de Engelse term Data Protection Impact Assessment.

Wat is ook al weer een verwerkersovereenkomst? Klik op de onderstaande link voor uitleghttps://www.rovid.nl/ap/comm/2019/ap-comm-20190705-idbimpp50-web-hd.mp4

Op diverse manieren wordt informatie ingewonnen danwel gedeeld via diverse gremia.
De FG van de gemeente Beek werkt met diverse gemeenten en in diverse in en externe samenwerkingsverbanden nauw samen.

6. Beveiliging

Vanuit het algemene behoorlijkheidsbeginsel, het integriteitsbeginsel en het vertrouwelijkheidsbeginsel is het essentieel dat de gemeenteraad van de gemeente Beek passende technische en organisatorische maatregelen neemt ter beveiliging van persoonsgegevens. Daarnaast geldt er onder de AVG een meldplicht datalekken. Dit houdt in dat incidenten – waaronder inbreuken – op de beveiliging onder omstandigheden gemeld dienen te worden aan de AP en/of de betrokkene(n).

In 2021 zijn negen datalekken geregistreerd.
Twee datalekken zijn gemeld bij AP en bij betrokkenen.

7. Verantwoording

De AVG legt de verantwoordelijkheid bij de gemeenteraad zelf om aantoonbaar te maken dat deze voldoet aan de privacyregels. Door te voldoen aan de verantwoordingsplicht, levert de organisatie een belangrijke bijdrage aan de bescherming van het grondrecht van mensen op privacy. Dit betekent dat de gemeenteraad aan moet kunnen tonen dat de verwerkingen van persoonsgegevens voldoen aan de beginselen van de AVG en aan de andere relevante wet- en regelgeving.

iNavigator
De iNavigator dient als verwerkingsregister (verplichting volgt uit AVG art 30). Tevens maakt het gebruik van de iNavigator dat er één vaste plek is waar de informatiehuishouding is vastgelegd en wordt beheerd en van waaruit het vervolgens beschikbaar wordt gesteld aan applicaties als zaaksystemen. De processen worden momenteel door DIV en FG aangevuld.

Privacy Management System (PMS)
In 2021 is de eerste keer gewerkt met de module Privacy Management System (PMS). Dit systeem is gebaseerd op het PDCA-kwaliteitsmodel en omvat het privacy VNG normenkader. Naast het privacy VNG normenkader zit hier ook de normenkaders in voor informatiebeveiliging en informatiebeheer. Dit integraal beheersysteem stelt ons in staat om het proces van privacy management, zodanig in te richten dat de kwaliteit van beleidsuitgangspunten, procedures en risico's aantoonbaar geborgd wordt ten behoeve van de dagelijkse uitvoering én er een blijvend proces van continu verbeteren in gang wordt gezet. Naast de maatregelen die volgen uit de normen worden ook de maatregelen die uit de DPIA's naar voren komen hierin verwerkt.

Wet politiegegevens
Sinds 1 januari 2019 zijn de aangepaste Wet politiegegevens (Wpg) en Wet justitiële en strafvorderlijke gegevens (Wjsg) van kracht. Deze wetten zijn samen met de daaronder vallende besluiten de Nederlandse implementatie van de Europese richtlijn gegevensbescherming opsporing en vervolging (EU) 2016/680. De doorgevoerde aanpassingen in de Wpg hebben onder andere gevolgen voor het regime waar de verwerking van persoonsgegevens door buitengewoon opsporingsambtenaren (BOA's) onder vallen.

BOA's kunnen meerdere taken en bevoegdheden hebben waarbij rekening moet worden gehouden met verschillende wet- en regelgeving. In het kader van de verwerking van persoonsgegevens door BOA's kunnen twee regimes van toepassing zijn. Voorheen vielen de verwerkingen van persoonsgegevens door BOA's altijd onder de Algemene verordening gegevensbescherming (AVG), maar door aanpassingen in de Wpg kan nu ook de Wpg van toepassing zijn. In de Wpg en het bijbehorende besluit voor BOA's - het Besluit politiegegevens voor buitengewoon opsporingsambtenaren (BpgBoa) - staat dat de Wpg van toepassing is op gegevensverwerkingen door BOA's voor de uitvoering van hun opsporingstaak. Toezicht valt onder de AVG.

De Wet politiegegevens heeft dus invloed op de BOA taken. Een nieuw privacy NOREA Wpg normenkader in het PMS is aangeschaft voor de jaarlijks wettelijk verplichte Wpg interne meting. Ook is de gemeente verplicht een externe audit uit te laten voeren (zie artikel 33 Wpg, artikel 6:5 Bpg en artikel 3 Regeling periodieke audit politiegegevens). De datum voor het indienen van deze eerste externe audit bij de AP is uitgesteld tot december 2022.

8. Conclusie

In 2021 heeft de gemeenteraad heel wat werk verzet om de AVG te implementeren in de organisatie, de systemen en de processen. De volgende procedures zijn opgesteld en intern gecommuniceerd: procedures voor datalekken, procedure rechten van betrokkenen, procedure DPIA. De privacyverklaring is verbeterd voor de uitoefening van de rechten voor betrokkenen door burgers. De taken die uit de eerste privacy meting in het PMS naar voren kwamen zijn afgehandeld.

De aanschaf van een nieuw privacy NOREA Wpg normenkader voor de Wpg moet zorgen dat we ook aantoonbaar kunnen gaan voldoen aan de Wpg. Dit zijn privacy regels waar de BOA's mee te maken hebben bij de uitvoering van de opsporingstaken.

Daarnaast is regelmatig aandacht besteed aan bewustwording, het aanvullen van het verwerkingsregister en het opbouwen van de samenwerking met nieuwe CISO.

Ook in 2021 is veel thuis gewerkt door Corona. Er zijn geen significante gevolgen van het vele thuiswerken gesignaleerd, wel blijkt dat er minder datalekken zijn gemeld.

Er zijn ook aandachtspunten voor de gemeenteraad om aantoonbaar te kunnen voldoen aan de AVG. In het tweede deel van de rapportage zullen aanbevelingen worden gedaan om gegevensbescherming nog meer in te bedden in de organisatie.

Deel 2. Vooruitkijken naar 2022

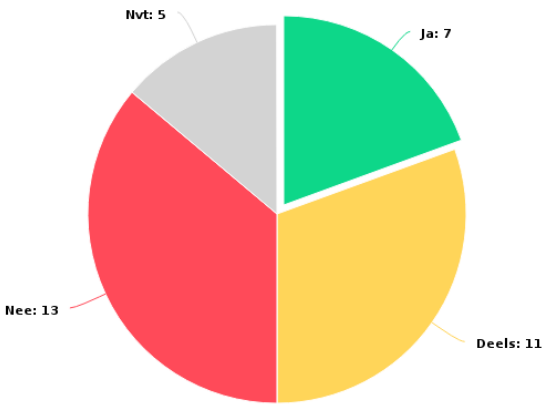
Gegevensbescherming onderdeel laten worden van de processen en systemen van de gemeenteraad, en daarmee aantoonbaar voldoen aan de relevante wet- en regelgeving, is geen afvinklijst, maar een continu proces. Het vraagt om structurele borging van dit onderwerp. Waar het jaar 2021 in het teken stond van verbeteren van diverse processen aan de AVG, het uitvoeren van de taken uit het PMS om de eerste hobbels te nemen om uiteindelijk aantoonbaar te kunnen voldoen aan deze wet, zal 2022 in het teken staan van aanpassen gegevensbescherming vanuit de kaders en procedures uit de Wet politiegegevens (Wpg).

1. Het privacybeleid

De meting en gap analyse voor het beheersjaar 2022 is uitgevoerd aan de hand van het privacy VNG normenkader en het privacy NOREA Wpg normenkader in het Privacy Management System (PMS).

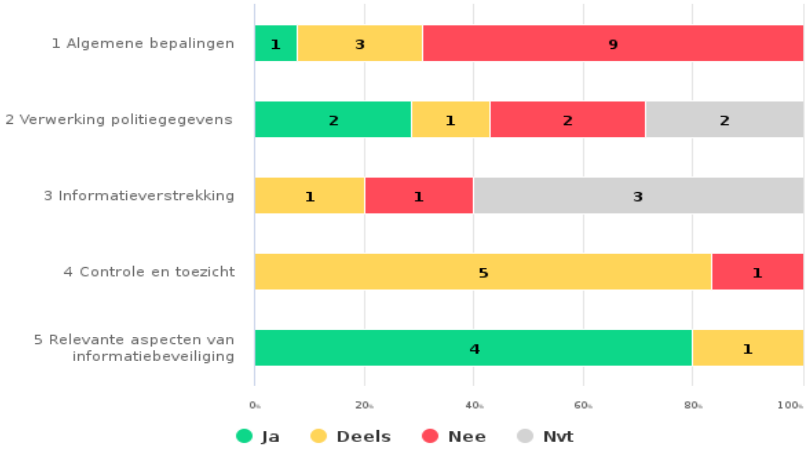
In figuur 1 en 2 zijn de resultaten van het PMS voor wat betreft het privacy VNG normenkader voor beheersjaar 2022 naast de meting voor beheersjaar 2021 grafisch weergegeven. Zo wordt een goed beeld verstrekt van de vorderingen die zijn gemaakt.

Voor het nieuwe privacy NOREA Wpg normenkader is voor het eerst een meting en GAP analyse uitgevoerd voor beheersjaar 2022. In onderstaande figuur is de meting voor beheersjaar 2022 voor het privacy NOREA Wpg normenkader grafisch weergegeven.



Privacy NOREA Wpg meting beheersjaar 2022
Figuur 2

Verdeeld over de aandachtsgebieden in het Wpg normenkader ziet dit er als volgt uit:



Privacy NOREA Wpg meting beheersjaar 2022
Figuur 3

2. Processen

De privacy procedures en beleidsdocumenten dienen te worden aangepast aan de Wpg. Daarnaast dient het privacy protocol RIEC te worden opgesteld.

3. Organisatorische inbedding

In januari starten we met een online cyberquiz,'What the H@ck', daarna zal in de leeracademie gemeente Beek een module privacy ibewustazijn verplicht worden gesteld. Op Beekipedia zal regelmatig het onderwerp ter sprake worden gebracht.

In het introductieprogramma voor de nieuwe raadsleden wordt privacy en informatiebeveiliging opgenomen.

4. Rechten van betrokkenen

De procedure rechten van betrokkenen dient te worden aangepast aan de Wpg.

5. Samenwerking

Huidige samenwerkingen worden gecontinueerd en aandacht voor samenwerkingsverbanden.

6. Beveiliging

Waar noodzakelijk uitvoeren van gegevensbeschermingseffectbeoordelingen (DPIA's). O.a. voor de Nieuwe wet inburgering,het zaaksysteem Liber, het nieuwe digitale personeelssysteem en evaluatie DPIA Squit.

7. Verantwoording

Middels deze jaarrapportage legt de FG verantwoording af aan de gemeenteraad. De conclusies uit het Privacy Management System (PMS) zijn hierin meegenomen.

8. Conclusies

Op het gebied van privacy en gegevensbescherming is er in 2022 zeker nog winst te behalen. Met name het oppakken van de maatregelen die volgen uit het NOREA Wpg normenkader verdienen het komend jaar extra aandacht. Te meer daar er een verplichte externe audit vanuit de Wpg moet worden uitgevoerd en overhandigd aan de Autoriteit Persoonsgegevens.