

JAARRAPPORTAGE GEGEVENSBE SCHERMING GEMEENTE BEEK 2024

Jaarrapportage voor de gemeenteraad

Definitief
Functionaris Gegevensbescherming
Veerle van Hees
25-03-2025

Inhoudsopgave

SAMENVATTING.....	2
INLEIDING	4
LEESWIJZER	5
DEEL 1. VERANTWOORDING COLLEGE AAN GEMEENTERAAD	6
DEEL 2. TERUGBLIK OP 2024.....	7
1. HET PRIVACYBELEID	7
2. PROCESSEN.....	10
3. ORGANISATORISCHE INBEDDING	10
4. RECHTEN VAN BETROKKENEN	11
5. SAMENWERKING.....	12
6. BEVEILIGING	12
7. VERANTWOORDING.....	12
8. CONCLUSIE	14
DEEL 3. VOORUITKIJKEN NAAR 2025	15
1. HET PRIVACYBELEID	15
2. PROCESSEN.....	15
3. ORGANISATORISCHE INBEDDING	16
4. RECHTEN VAN BETROKKENEN	16
5. SAMENWERKING.....	16
6. BEVEILIGING	16
7. VERANTWOORDING.....	16
8. CONCLUSIES.....	17

Samenvatting

Deze jaarrapportage gegevensbescherming gemeente Beek gaat over gegevensbescherming conform de Algemene Verordening Gegevensbescherming (hierna: AVG) én de Wet politiegegevens¹ (hierna: Wpg). De Wpg spreekt overigens niet van persoonsgegevens maar over politiegegevens.

Gemeenten hebben veel kennis uitgewisseld en producten met elkaar gedeeld, zowel online (bijvoorbeeld via het VNG privacy forum) 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, zo ook de berichtgeving over de functie Functionaris Gegevensbescherming. De overheid heeft 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 van B&W en de gemeenteraad. Het college is verantwoordelijk voor het merendeel van de verwerkingen van persoonsgegevens in onze gemeente. Dit brengt verplichtingen met zich mee. BOA's verwerken de politiegegevens onder beheer van hun werkgever. Daarmee is conform de Wpg de werkgever de verwerkingsverantwoordelijke.

In deze jaarrapportage is beschreven welke acties en maatregelen in 2024 zijn genomen om de doelstellingen en beginselen uit de AVG/Wpg te behalen en te waarborgen. Ook bevat dit document aandachtspunten en actiepunten voor het jaar 2025. Adequaat omgaan met persoonsgegevens is een blijvend proces en zal dan ook aandacht blijven vergen van zowel bestuur, management als medewerkers.

In 2024 is tijd en aandacht uitgegaan naar het uitvoeren van DPIA's, het verwerkingregister, het algoritmeregister, gebruik ChatGPT, het zelfstandig uitvoeren en oplossen van privacy vraagstukken, procedure rechten van betrokkenen, het bijhouden van verwerkersovereenkomsten, afhandeling van datalekken en inzageverzoeken en bewustwordingscampagnes zoals de veiligheid tweeweekse. Daarnaast zijn de netwerken zowel extern, intern als met omliggende gemeenten gebruikt waar nodig. Door inhuur van een externe Functionaris Gegevensbescherming is voldaan aan de splitsing in de uitvoering en toezicht taken in de normenkaders en bij de uitvoering van DPIA's.

Al enige jaren wordt met het Privacy Management System (PMS) in het integraal beheerssysteem gewerkt. Dit is gebaseerd op het PDCA-kwaliteitsmodel en omvat het privacy VNG normenkader en het Norea Wpg normenkader. Voor beheersjaar 2025 is in het PMS een meting en Gap analyse uitgevoerd over zowel het privacy VNG normenkader als over het Norea Wpg normenkader. In deze rapportage zijn de bevindingen uit deze metingen opgenomen. Voorheen gebruikten we het VNG privacy normenkader 1.0. De nieuwe meting is uitgevoerd in het nieuwe privacy VNG normenkader 3.0. Dit is een nieuwere versie en wijkt behoorlijk af van versie 1. Versie 1 heeft 65 normen terwijl versie 3.0 er 155 heeft. Details vanuit de inhoud komen nadrukkelijker in beeld bij versie 3.0. De reden voor de overstap naar versie 3.0 is dat deze ingaat op meer details en verfijning waardoor er in 2025 op onderdelen nog winst te behalen is. Er kan geen vergelijking met versie 1 gemaakt worden omdat nu meer op details gemeten wordt. Versie 1 gaat uit van een volwassenheidsniveau, versie 3.0 gaat is het streven dat aan alle normen wordt voldaan.

In een tijdlijn is de score:

- 2021: v1: score 70%
- 2022: v1: score 75%
- 2023: v1: score 82%
- 2024: v1: score 95%
- 2025: v3: score 81%

¹ Voor BOA's geldt voor de uitvoering van opsporingstaken een strenger privacy regime, de Wet politiegegevens (Wpg). Voor toezicht taken geldt de AVG, de BOA's werken dus met twee privacy regimes.

De resultaten van de laatste meting voor het privacy VNG normenkader 3.0 laten zien dat al in grote mate aan dit normenkader 3.0 wordt voldaan. De resultaten van de metingen voor het Norea Wpg normenkader zijn ruim voldoende en dat is mede te danken aan de aanschaf van de BRS applicatie.

Samenvattend heeft de gemeente Beek in 2024 veel werk verzet op het gebied van gegevensbescherming en zal in 2025 in het teken staan om aan de slag te gaan met verbeterpunten die volgen uit het nieuwe privacy VNG normenkader.

Inleiding

De gemeente Beek dient zorgvuldig om te gaan met persoonsgegevens. We verwerken immers bij de uitoefening van onze taken veel informatie. Niet alleen persoonlijke informatie van eigen inwoners, maar ook van andere burgers, medewerkers, externen en zakenrelaties.

In de AVG/Wpg wordt het wettelijk kader beschreven voor het verwerken van persoonsgegevens als politiegegevens. Zo dient de gemeente transparant te zijn welke gegevens zij verwerkt en voor welk doel. Persoonsgegevens en politiegegevens 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/politiegegevens tegen te gaan en daardoor een onrechtmatig gebruik van deze persoons/politie gegevens te voorkomen. Daarnaast heeft de gemeente ook te maken met tal van privacyregels in sector specifieke 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 Burgemeester en Wethouders (college van B&W) als van de gemeenteraad vindt een groot aantal verwerkingen van persoonsgegevens plaats. Het gaat hierbij om persoons/politie gegevens 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 Gegevensbescherming (FG). Op 1 januari 2021 hebben de bestuursorganen van de gemeente Beek Veerle van Hees aangesteld als FG². In Q1 van 2024 is Werny Berns aangesteld als externe FG om te voldoen aan het gestelde in artikel 37, 38 en 39 van de AVG. Waarbij de focus ligt op de uitvoering van de FG taken daar waar een ongewenste samenloop van taken en verantwoordelijkheden dreigt.

De FG ziet erop toe dat de AVG/Wpg 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 persoons/politie gegevens. 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 en bevindingen en doet hij naar aanleiding daarvan aanbevelingen. Dit jaarverslag is bedoeld voor de gemeenteraad enerzijds als controlerend orgaan van het college van B&W anderzijds als zelfstandig verwerkersverantwoordelijke.

² Hiermee worden de drie bestuursorganen van de gemeente bedoeld: de burgemeester, het college van burgemeester en wethouders en de gemeenteraad.

Leeswijzer

Deze jaarrapportage bestaat uit drie onderdelen.

Het eerste deel betreft de verantwoording van het college aan de gemeenteraad van de gemeente Beek

In het tweede deel wordt teruggekeken naar het jaar 2024. Wat heeft de gemeente bereikt op het gebied van gegevensbescherming? Welke maatregelen zijn er genomen om te voldoen aan de AVG en de Wpg?

In het derde deel worden aanbevelingen gedaan om gegevensbescherming en privacy in het jaar 2025 naar een hoger niveau te tillen. Hierbij wordt waar nodig tevens aandacht geschonken aan de technische en organisatorische middelen die nodig zijn om dit niveau te bereiken.

De gegevens uit de meting en gap analyses en verantwoordingsrapportages uit het privacy management systeem voor de AVG en Wpg normenkaders zijn verwerkt in deze jaarrapportage.

Deel 1. Verantwoording College aan gemeenteraad

Het college van B&W heeft de jaarrapportage gegevensbescherming gemeente Beek 2024 van de FG ontvangen. Dit is een vergelijkbaar document als deze jaarrapportage gegevensbescherming gemeente Beek 2024. Voor beide voorbeelden is een VNG sjabloon gehanteerd.

Met het Privacy Management Systeem (PMS) is de gemeente Beek in staat om zich tijdig en rechtmatig te verantwoorden. Aan de hand van privacy normenkaders wordt jaarlijks een meting en gap analyse uitgevoerd. Deze helpt bij het beheren van belangrijke bedrijfsprocessen op gebied van privacybescherming. Het PMS bevat een PDCA-cyclus (Plan-Do-Check-Act) en standaardrapportages voor het monitoren van de voortgang.

Het college van B&W heeft de verklaring van toepasselijkheid die volgt uit de Meting en Gap analyse in het PMS bij de verantwoordingsrapportage ontvangen en vastgesteld.

Deel 2. Terugblik op 2024

In dit deel van de rapportage zal worden teruggeblikt op hetgeen de gemeente in 2024 heeft bereikt en welke werkzaamheden zijn verricht.

Het eerste deel van het jaar 2024 stond voor wat betreft privacy in het teken van algoritmen, ChatGPT, bewustwordingstrainingen, aanstelling externe FG om te voldoen aan het gestelde in artikel 37, 38 en 39 van de AVG. Hierbij ligt de focus op de uitvoering van de FG taken daar waar een ongewenste samenloop van taken en verantwoordelijkheden dreigt met de huidige werkzaamheden van de interne FG.

1. Het privacybeleid

Het privacybeleid is een kader waarin de gemeente Beek aangeeft aan welke principes zij zich houdt bij de verwerking van persoonsgegevens. Het laat zien hoe de gemeente omgaat met persoonsgegevens en welke maatregelen zij treft om te voldoen aan de relevante wet- en regelgeving.

In 2022 is het privacy beleid aangepast aan de Wpg. De privacyverklaring op de website is eveneens aangepast aan de Wpg. Via een DigiD formulier kunnen burgers hun rechten van betrokkenen uitoefenen. Ook kunnen burgers deze formulieren van de website downloaden. Daarnaast is een separaat privacyprotocol ondermijning voor binnengemeentelijke gegevensdeling opgesteld.

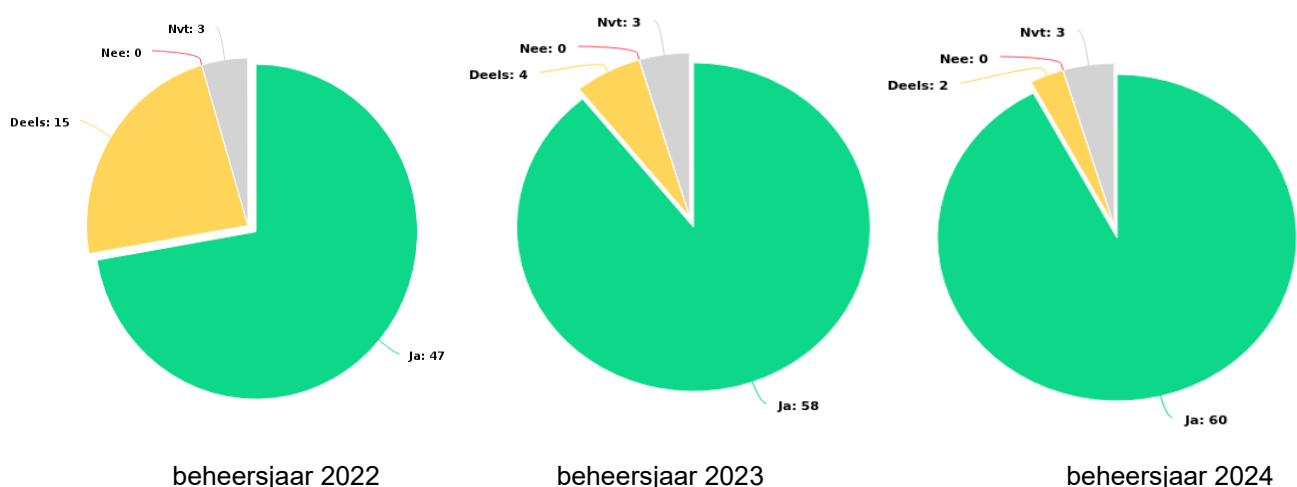
In 2023 is een privacyprotocol cameratoezicht opgesteld. In 2023 zijn de 'review' taken, in het integraal beheersysteem waarin de AVG en Wpg normenkaders staan, uitgevoerd door een senior consultant van Key2control die ervaring heeft met beide normenkaders.

Voor het beheersen, verbeteren en verantwoorden van de uitvoeringskwaliteiten in diverse bedrijfsprocessen is er een beleidsplan integrale beheersing opgesteld dat samen met deze rapportage aan het college ter goedkeuring wordt aangeboden.

AVG

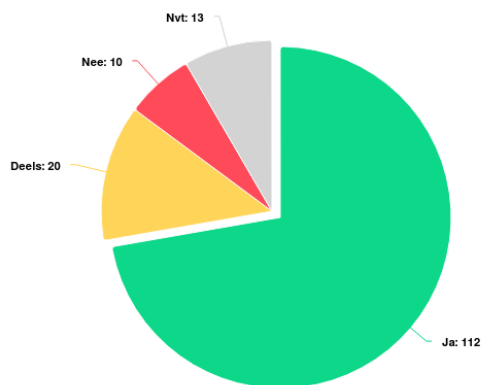
In december 2024 en januari 2025 is de nieuwe meting en gap analyse in het integraal beheersysteem uitgevoerd voor het VNG privacy 3.0 normenkader.

De resultaten van de metingen voor de beheersjaren 2022, 2023 en 2024 in het VNG privacy 1.0 normenkader zijn als volgt grafisch weergegeven:



Figuur 1 VNG privacy 1.0 normenkader

De resultaten van de metingen voor het beheersjaar 2025 in het VNG privacy 3.0 normenkader zijn als volgt grafisch weergegeven:



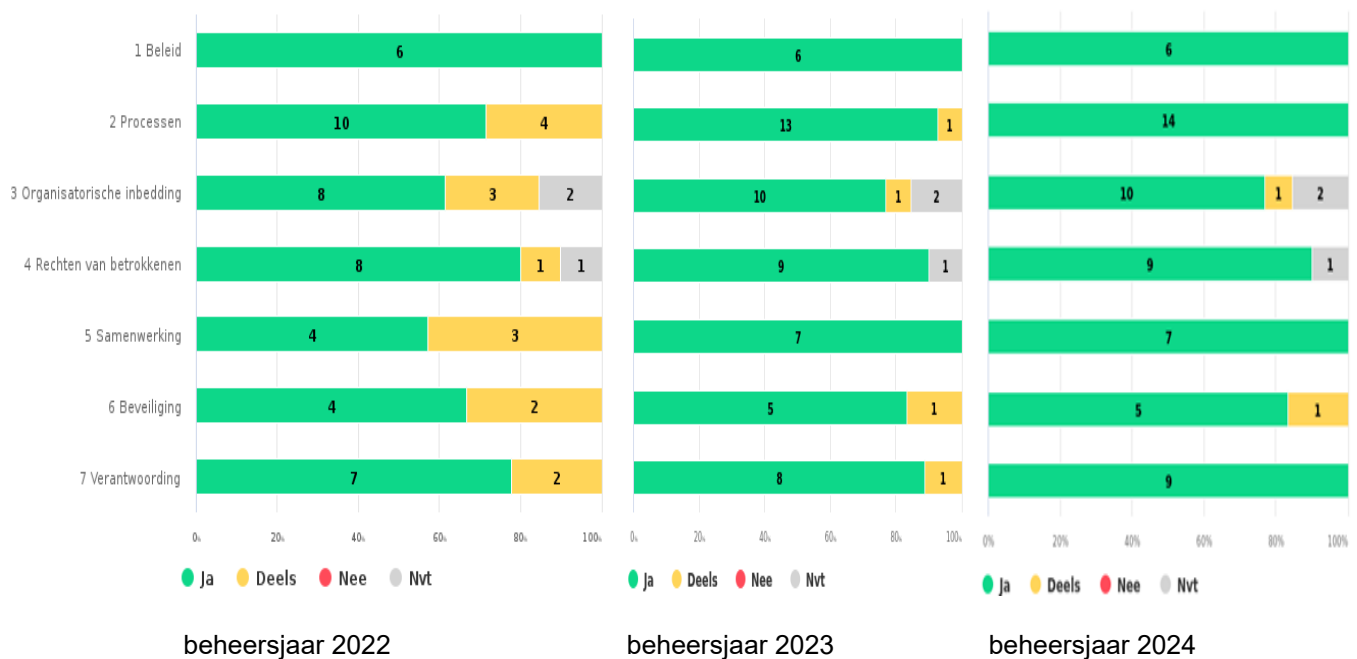
Beheersjaar 2025

Figuur 2 VNG privacy 3.0 normenkader

Analyse AVG metingen

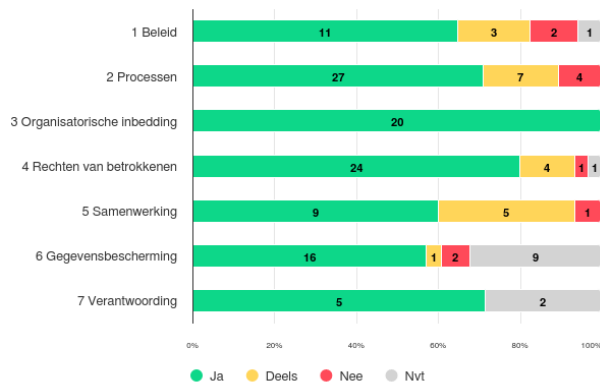
Bovenstaande toont aan dat de gemeente Beek in zeer hoge mate voldoet aan VNG privacy 3.0 normenkader meting, maar een aantal verbeteringen noodzakelijk zijn.

Verdeeld over de aandachtsgebieden in het VNG privacy 1.0 normenkader ziet dit er als volgt uit voor beheersjaren 2022, 2023 en 2024:



Figuur 3 VNG privacy 1.0 normenkader

Verdeeld over de aandachtsgebieden in het VNG privacy 3.0 normenkader ziet dit er als volgt uit voor het beheersjaar 2025:

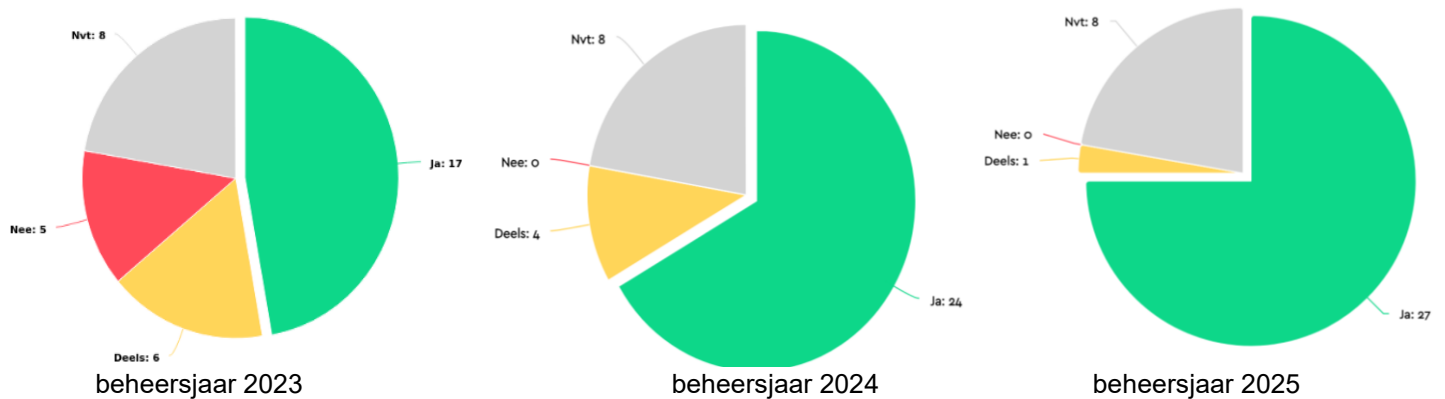


Beheersjaar 2025

Figuur 4 VNG privacy 3.0 normenkader meting

Wpg

Het Wpg normenkader is eind 2021 aangeschaft. De eerste meting is over beheersjaar 2022 uitgevoerd. In december 2023 is de nieuwe meting en gap analyse in het integraal beheersysteem uitgevoerd voor het Norea Wpg normenkader. De resultaten van de metingen voor de beheersjaren 2023, 2024 en 2025 zijn als volgt grafisch weergegeven:

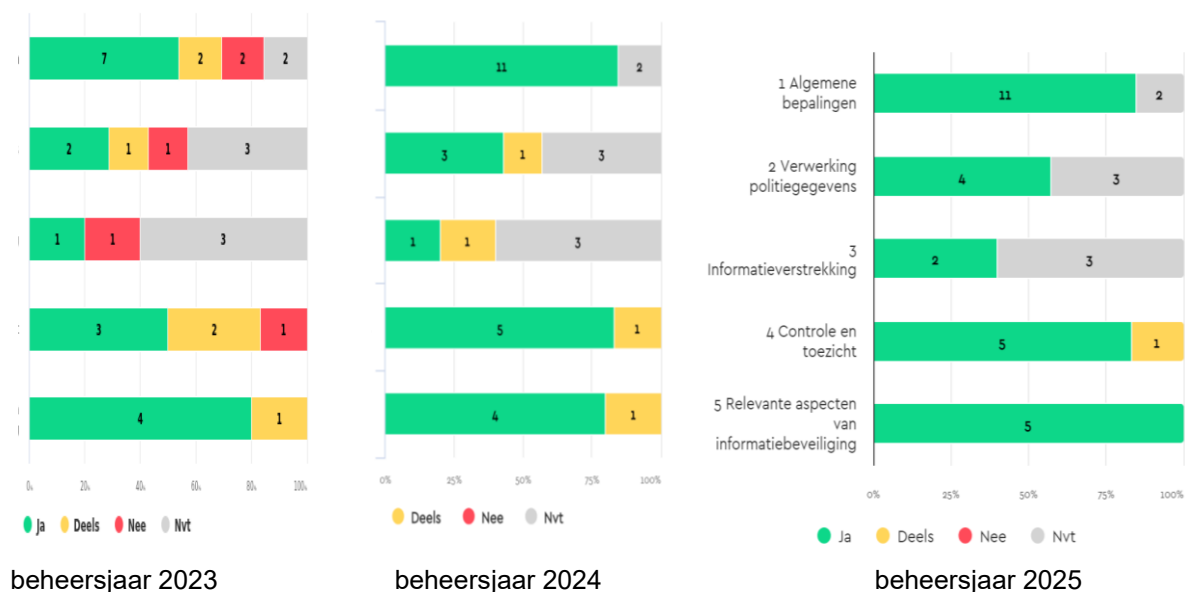


Figuur 5 Norea Wpg normenkader

Analyse Wpg metingen

voor het beheersjaar 2022 voldeed de gemeente onvoldoende aan het NOREA Wpg normenkader. De basis was nog niet op orde. In 2023 zijn de nodige Quick wins en verbeteringen doorgevoerd en is BRS voor de boa's aangeschaft. De meting voor beheersjaar 2024 en 2025 laat zien dat de gemeente de basis nu goed op orde heeft.

Verdeeld over de aandachtsgebieden in het Wpg normenkader ziet dit er als volgt uit voor beheersjaren 2023 en 2024 en 2025:



Figuur 6 Norea Wpg normenkader

2. Processen

De verwerkingen van persoonsgegevens van de gemeente Beek dienen te voldoen aan de AVG/Wpg. 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 gemeente in gevallen verplicht zijn om een gegevensbeschermingseffectbeoordeling (DPIA³) uit te voeren. De procedure DPIA is uitgewerkt en vastgelegd en is in 2022 aangepast aan de Wpg.

In 2024 zijn de onderstaande DPIA's uitgevoerd:

2024
Herhaling: Aanvraag hulp bij het huishouden in iSamenleving, getoetst door externe FG
Herhaling: Aanvraag jeugdhulp iSamenleving, getoetst door externe FG
Herhaling: Aanvraag rijbewijs en verhuizing in iBurgerzaken, getoetst door externe FG
Externe DPIA Ethos telling dak- en thuisloosheid waar wij aan meedoen van Hogeschool Utrecht, getoetst door FG
DPIA Regionaal expertise team VNG: niet van toepassing, geen gebruik van gemaakt.
DPIA Gebruik inpandige foto's in WOZ proces VNG: WOZ is uitbesteed aan de BsGW, niet van toepassing
DPIA VNG inburgering, niet van toepassing wordt uitgevoerd door Vidar
Pre DPIA mijnoverzicht berichtenbox, getoetst door externe FG
Pre DPIA Visma Idella, getoetst door externe FG
Pre DPIA Chat GPT, getoetst door externe FG

3. Organisatorische inbedding

Voor een goede en juiste uitvoering is het van belang dat eenieder binnen de organisatie op de hoogte is van de beginselen van de AVG en het belang van privacy. Voor de boa's geldt dat ze op de hoogte moeten zijn van de Wpg. Organisatorische inbedding betekent het toewijzen van taken, verantwoordelijkheden en bevoegdheden en bewustzijn creëren.

³ De gegevensbeschermingseffectbeoordeling wordt ook wel afgekort tot DPIA (Data Protection Impact Assessment).

Op Beekipedia zijn berichten geplaatst ter bewustwording. Daarnaast is in de veiligheid tweeweeke aandacht aan privacy en informatiebeveiliging besteed. In de leeracademie gemeente Beek zijn jaarlijks verplichte e-learnings op gebied van privacy, informatieveiligheid en integriteit.

Daarnaast wordt via diverse kanalen aandacht besteed aan privacy. In de koffiekwartiertjes wordt indien nodig extra aandacht gevraagd voor privacy. De Functionaris Gegevensbescherming heeft frequent overleggen met de gemeentesecretaris. Datalekken worden in MT ingebracht. Jaarlijks wordt verantwoording afgelegd aan MT, het college van B&W en aan de gemeenteraad. De FG heeft nauw contact met de Chief Information Security Officer (CISO). De FG heeft diverse repeterende overleggen, zowel in- als extern.

4. Rechten van betrokkenen

De gemeente dient degene van wie zij de persoonsgegevens verwerkt (betrokkene) zowel actief als passief te informeren over het verwerken, de wijze van het verwerken, de grondslag en de maatregelen die zij neemt om onrechtmatige toegang en - verwerking te voorkomen. Daarnaast stelt de AVG/Wpg 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, deze is in 2022 aangepast aan de Wpg.
- De privacyverklaring op de website is eveneens aangepast aan de Wpg. Via een DigiD formulier kunnen burgers hun rechten van betrokkenen uitoefenen. Ook kunnen burgers deze formulieren van de website downloaden.

Er zijn in 2024 vier verzoeken rechten van betrokkene ingediend. Voor de Wpg zijn geen verzoeken van betrokkenen ingediend. Hoewel het niet de hoofdmotivatie is voor de meeste AVG-verzoeken, zijn twee van de gevallen hoogstwaarschijnlijk mensen die de gemeente aansprakelijk proberen te stellen voor privacy schendingen. Als een gemeente niet correct met persoonsgegevens is omgegaan, kan dat nml. leiden tot klachten of zelfs schadeclaims.

Er zijn in 2023 twee verzoeken van betrokkenen ingediend voor de AVG. Voor de Wpg zijn geen verzoeken van betrokkenen ingediend.

5. Samenwerking

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/Wpg. 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. Daarnaast heeft de VNG een sjabloon verwerkersovereenkomst voor de Wpg opgesteld. De gemeente Beek neemt de VNG sjablonen onverkort over. De FG adviseert welk sjabloon wanneer noodzakelijk is.

Wat is ook al weer een verwerkersovereenkomst? Klik op deze link voor uitleg:

<https://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. Er is een Regionaal Privacy Overleg, privacy/CISO overleg Westelijke Mijnstreek, daarnaast houdt VNG FG intervisie sessies.

6. Beveiliging

Vanuit het algemene behoorlijkheidsbeginsel, het integriteitsbeginsel en het vertrouwelijkheidsbeginsel is het essentieel dat de gemeente Beek passende technische en organisatorische maatregelen neemt ter beveiliging van persoonsgegevens. Daarnaast geldt er onder de AVG/Wpg 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). De procedure datalek is uitgewerkt en is intern gecommuniceerd, deze is in 2022 aangepast aan de Wpg.

De FG heeft in 2024 11 meldingen van incidenten waarbij persoonsgegevens betrokken zijn ontvangen, waarvan twee meldingen bij de Autoriteit Persoonsgegevens zijn gemeld. Overige veiligheidsincidenten worden niet meer in deze lijst meegenomen. De FG heeft in 2023 19 meldingen van mogelijke inbreuken ontvangen. Echter waren dit niet allemaal incidenten waarbij persoonsgegevens betrokken waren. Bij de Autoriteit Persoonsgegevens zijn 4 datalekken gemeld. Voor de Wpg zijn in 2024 wederom geen datalekken geregistreerd.

7. Verantwoording

De AVG en de Wpg legt de verantwoordelijkheid bij de organisatie 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 het college van B&W aan moet kunnen tonen dat de verwerkingen van persoonsgegevens voldoen aan de beginselen van de AVG, de Wpg en aan de relevante wet- en regelgeving.

Verwerkingsregister

Het VNG verwerkingregister is in gebruik als verwerkingregister totdat de iNavigator volledig is gevuld. Met de iNavigator wordt grip gekregen op de informatiehuishouding. De kern is een overzicht van alle processen die de gemeente Beek uitvoert. Daarnaast wordt het ook gebruikt door ICT waarin alle applicaties worden geplaatst en aan processen gekoppeld. INavigator is nog niet volledig aangevuld voor wat betreft de werkprocessen vanuit de applicaties van Samenleving.

Privacy Management System (PMS)

In 2021 is voor het eerst gewerkt met de module Privacy Management System (PMS) van de applicatie Key2Control. Dit systeem is gebaseerd op het PDCA-kwaliteitsmodel en omvat het privacy VNG normenkader. Eén jaar later is eveneens het Norea Wpg normenkader aangeschaft. Naast deze normenkaders bevat Key2Control ook de normenkaders 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..

Toezicht op autorisaties

Om ongeoorloofde inzage in persoonsgegevens tegen te gaan is het belangrijk dat autorisaties regelmatig worden getoetst en bijgehouden door de applicatiemedewerkers. Dit is een van de punten die ook in het functioneel applicatiebeheer (FAB) staan. Hiervoor is een autorisatiematrix opgesteld, die de applicatiebeheerder hierbij helpt. Een controle op autorisaties is noodzakelijk vanuit verschillende disciplines, vanuit informatieveiligheid, rechtmatigheid en privacy. De afspraak is dat de applicatiebeheerders hierover verantwoording afleggen aan de Chief Information Security Officer en niet drie keer dezelfde vraag ontvangen uit de organisatie.

AI en het algoritme register

Artificial Intelligence (AI) is een geautomatiseerd systeem dat taken uitvoert waar vroeger menselijke intelligentie voor nodig was. AI-systemen werken met in software beschreven algoritmen (instructiereeksen). De systemen herkennen patronen en nemen dan zelf beslissingen. En net zoals mensen worden ze door te oefenen steeds beter. De regering wil dat de overheid algoritmes verantwoord gebruikt.

Mensen moeten erop kunnen vertrouwen dat algoritmes voldoen aan de waarden en normen van de samenleving. En er moet uitleg zijn over hoe algoritmes werken. Dat doet de overheid door algoritmes voor het gebruik te controleren op hoe ze werken en op eventuele discriminatie en willekeur daarbij. Wanneer de overheid open is over algoritmes en hun toepassing, kunnen burgers, organisaties en media haar kritisch volgen en controleren of ze de wet en de regels volgt. Het aanleveren van informatie over algoritmes is nu nog niet verplicht voor overheidsorganisaties. Die verplichting komt er wel aan. Gemeenten moeten in de toekomst algoritmen aanmelden in het Centrale Algoritmeregister van de Nederlandse overheid. Steeds meer overheden doen al mee en publiceren in dit Algoritmeregister van de overheid informatie over hun impactvolle algoritmes en algoritmes met een hoog-risico volgens de aanstaande Europese AI Verordening. Uitgangspunt is dat overheden zelf verantwoordelijk zijn voor het opstellen en het beheer van hun algoritmes in het Algoritmeregister. Het Algoritmeregister ondersteunt daarbij met hulp, handreikingen, tools en een publicatiestandaard.

Onderzocht is in welke applicaties algoritmen voorkomen en of dit impactvolle algoritmen zijn die in het Algoritmeregister van de overheid moeten worden gepubliceerd. Dit algoritmeregister focust op impactvolle algoritmes (waaronder hoog risico AI-systemen) en geeft de bezoeker inzicht in hoe deze algoritmes werken. De eerste twee algoritmen zijn inmiddels hierin geplaatst.

Wel of geen AI-tools voor je werk gebruiken?

Ook de gemeente Beek kan er niet meer om heen: Kunstmatige intelligentie (AI) en soortgelijke diensten veroveren de wereld. Deze AI-tools, waaronder taalmodel ChatGPT dat supersnel teksten maakt met de hulp van AI, bieden verschillende kansen om werk sneller gedaan te krijgen en het kan een mooi hulpmiddel zijn voor verschillende type werkzaamheden. Daarom zijn er een aantal principes voor gebruik AI-tools geformuleerd en gedeeld in de organisatie welke een voorwaarde zijn om verantwoord om te gaan met deze nieuwe technologie. Tevens zijn bewustwordingssessies over gebruik van ChatGPT aangeboden waarin extra aandacht voor privacy is benoemd.

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. Naast de jaarlijkse interne audits dient de gemeente ook eens in de 4 jaar een externe audit uit te voeren en aan de Autoriteit Persoonsgegevens te verstrekken.

8. Conclusie

In 2024 is tijd en aandacht uitgegaan naar het uitvoeren van DPIA's, het verwerkingregister, het algoritmeregister, gebruik ChatGPT, het zelfstandig uitvoeren en oplossen van privacy vraagstukken, procedure rechten van betrokkenen, het bijhouden van verwerkersovereenkomsten, afhandeling van datalekken en inzageverzoeken en bewustwordingscampagnes zoals de veiligheid tweewEEKSE. Daarnaast zijn de netwerken zowel extern, intern als met omliggende gemeenten gebruikt waar nodig. Door inhuur van een externe Functionaris Gegevensbescherming is voldaan aan de splitsing in de uitvoering en toezicht taken in de normenkaders en bij de uitvoering van DPIA's.

Er zijn ook aandachtspunten voor de organisatie 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 3. Vooruitkijken naar 2025

Gegevensbescherming onderdeel laten worden van de organisatie 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.

1. Het privacybeleid

In het Privacy Management System (PMS) is het integraal beheerssysteem gewerkt. Dit is gebaseerd op het PDCA-kwaliteitsmodel en omvat het privacy VNG normenkader en het Norea Wpg normenkader. Voor beheersjaar 2025 is in het PMS een meting en Gap analyse uitgevoerd over zowel het privacy VNG normenkader als over het Norea Wpg normenkader. In deze rapportage zijn de bevindingen uit deze metingen opgenomen. Voorheen gebruikten we het privacy VNG normenkader 1.0. De nieuwe meting is uitgevoerd in het nieuwe privacy VNG normenkader 3.0. Dit is een nieuwere versie en wijkt behoorlijk af van versie 1. Versie 1 heeft 65 normen terwijl versie 3.0 er 155 heeft. Details vanuit de inhoud komen nadrukkelijker in beeld bij versie 3.0. De reden voor de overstap naar versie 3.0 is dat deze ingaat op meer details en verfijning. Er kan geen vergelijking met versie 1 gemaakt worden omdat nu meer op details gemeten wordt. Versie 1 gaat uit van een volwassenheidsniveau, versie 3.0 gaat is het streven dat aan alle normen wordt voldaan.

In figuur 1 t/m 6 zijn de resultaten van de metingen in het PMS voor het privacy VNG normenkader 3.0 en het NOREA Wpg normenkader grafisch weergegeven. Zo wordt een goed beeld verstrekt van de vorderingen die zijn gemaakt. Hieruit volgen de jaarplannen 2025 en de verklaring van toepasseljkheid.

De resultaten van de laatste meting voor het privacy VNG normenkader 3.0 laten zien dat al in grote mate aan het normenkader 3.0 wordt voldaan. De resultaten van de metingen voor het Norea Wpg normenkader zijn ruim voldoende en dat is mede te danken aan de aanschaf van de BRS applicatie. Zie de cirkeldiagrammen in figuur 2 op pagina 7.

Het 'Privacybeleid en -reglement voor gemeente Beek 2023-2025' wordt in 2025 herzien.

Onderstaande punten uit de nieuwe meting hierin meegenomen:

- Het privacybeleid beschrijft de taken en verantwoordelijkheden privacybeleid
- Beleidsdocumenten afstemmen met privacybeleid
- Inventarisatie domein specifiek privacybeleid
- Vaststellen domein specifiek privacybeleid
- In beleid opnemen dat het management verantwoordelijk is om keuzes te maken op het gebied van privacyrisico's, zoals het treffen van mitigerende maatregelen en het accepteren van restisico's

Daarnaast wordt in 2025 in samenwerking met de Chief Information Security Officer een logging beleid opgesteld.

2. Processen

Een Data Protection Impact Assessment (DPIA) is noodzakelijk wanneer een gegevensverwerking waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van personen. De procedure DPIA zal worden geëvalueerd en waar nodig geactualiseerd. Acceptatiecriteria voor privacy risico's worden vastgesteld, goedgekeurd, gedocumenteerd en toegepast. De procedure DPIA wordt nogmaals geëvalueerd of hier voldoende invulling aan is gegeven. Indien wordt afgeweken van het advies van de FG dient dit schriftelijk te worden vastgelegd en meegenomen in procedure. Stel in de procedure eveneens vast welke functionaris beslissingsbevoegd is ten aanzien van dit besluit.

Waar noodzakelijk uitvoeren van gegevensbeschermingseffectbeoordelingen (DPIA's). Naar aanleiding van een analyse van het verwerkingregister worden van een aantal verwerkingen DPIA's uitgevoerd.

In 2025 zullen de onderstaande DPIA's (opnieuw) worden uitgevoerd.

2025
DPIA Nieuwe applicatie afdeling Samenleving
DPIA Nieuwe applicatie personeelsdossiers
DPIA Integrale toegang Sociaal Domein
DPIA Cameratoezicht openbare ruimte
Herhaling: DPIA Schulddienstverlening

3. Organisatorische inbedding

In de online leeracademie gemeente Beek worden wederom privacy iBewustzijn modules verplicht gesteld. Er is sinds 2024 een module Wpg beschikbaar voor boa's ter bewustwording. Op Beekipedia zal regelmatig het onderwerp ter sprake worden gebracht. De veiligheid tweeweekse zal vervolg krijgen in 2025.

De organisatie evalueert periodiek of betrokkenen tijdig en volledig de verplichte informatie ontvangen en waar nodig wordt dit bijgesteld.

4. Rechten van betrokkenen

De procedure rechten van betrokkenen is in 2022 aangepast aan de Wpg. Burgers kunnen hier een beroep op doen schriftelijk danwel online via de privacyverklaring op de website. Deze procedure zal in 2025 worden geëvalueerd en indien nodig geactualiseerd. Hierbij wordt opgemerkt dat de Autoriteit Persoonsgegevens extra aandacht heeft voor de afhandeling van inzageverzoeken. Onlangs is verschenen het Europees onderzoek van de European Data Protection Board (EDPB) 'Inzageverzoeken vaak niet goed afgehandeld' d.d. 22 januari 2025.

5. Samenwerking

Huidige samenwerkingen worden gecontinueerd en aandacht voor samenwerkingsverbanden.

6. Beveiliging

Er is een procedure DPIA's opgesteld. Deze zal in 2025 worden geëvalueerd en indien nodig geactualiseerd.

7. Verantwoording

Door aanschaf van het VNG privacy en het NOREA Wpg normenkader in het PMS kan aantoonbaar worden gemaakt dat de gemeente voldoet aan de AVG en de Wpg.

Op verzoek zijn beschikbaar de onderstaande detailrapporten:

- | | |
|-------------------------------|-------------------------------|
| 1. Meting en GAP analyse 2025 | privacy VNG normenkader |
| 2. Jaarrapportage 2025 | privacy VNG normenkader |
| 3. Meting en GAP analyse 2025 | privacy NOREA Wpg normenkader |
| 4. Jaarrapportage 2025 | privacy NOREA Wpg normenkader |

Het college heeft de Verklaring Van Toepasselijkheid (VVT) voor zowel het privacy VNG normenkader 3.0 als het privacy NOREA Wpg normenkader vastgesteld.

8. Conclusies

Op het gebied van privacy en gegevensbescherming is er in 2025 zeker nog winst te behalen. Vooral de onderstaande punten behoeven in 2025 extra aandacht.

Evaluatie beleid en processen

In 2025 zal het privacy beleid, de procedure DPIA, rechten van betrokkene, en datalekken worden geëvalueerd en indien nodig geactualiseerd. Daarnaast zal in samenwerking met de CISO een loggingbeleid worden opgesteld. Een crisiscommunicatieplan voor datalekken met hoge impact is noodzakelijk.

De FG is verder betrokken bij de uitvoering van de strategische toekomstvisie sociaal domein en de impact op werkprocessen. Samen met FG wordt in beleidskader privacywetgeving en integrale toegang geformuleerd.

De uitvoering van een gegevensbeschermingseffectbeoordeling (DPIA) is noodzakelijk bij de verwerking van persoonsgegevens vanwege een hoog privacy risico.

De FG is betrokken bij de nieuwe aanbestedingen voor applicaties waarin persoonsgegevens verwerkt worden en een gegevensbeschermingseffectbeoordeling noodzakelijk is.

De uitvoering van een gegevensbeschermingseffectbeoordeling (DPIA) is noodzakelijk bij de verwerking cameratoezicht openbare ruimte vanwege een hoog privacy risico. Samen met FG wordt hiervoor een beleidskader privacywetgeving en cameratoezicht geformuleerd.

Verwerkingregister

Periodiek dient toezicht op de juistheid van het verwerkingsregister plaats te vinden. Dit zal een toevoeging worden in het te actualiseren privacybeleid.

Algoritmeregister

Periodiek dient toezicht op de juistheid van het algoritmeregister plaats te vinden. Dit zal een toevoeging worden in het te actualiseren privacybeleid.

Externe Wpg Audit

De Wpg bepaalt dat de gemeente als werkgever van boa's de externe Wpg audit 2 jaar na inwerkingtreding van de auditverplichting voor de eerste keer moet laten uitvoeren. En daarna iedere 4 jaar. Dat betekent dat de eerstvolgende externe Wpg audit zich richt op de omgang met politiegegevens in de periode 1 januari 2022 t/m 31 december 2024. Het jaar 2021 ins in de eerste audit meegenomen en hoeft daarom niet nogmaals te worden meegenomen. (zie <file:///G:/Download/20250205-faq-handreiking-wpg-versie-10.pdf>)

De AP moet de audit rapportage tussen 1 maart 2025 en 1 maart 2026 hebben ontvangen.

Datagedreven werken

Data gedreven werken stelt de gemeente in staat gericht te reageren op vragen, beter beleid te ontwikkelen en efficiënter te werken. De omgang van privacy bij datagedreven werken is een terugkerend punt van aandacht.

Een DPIA is een belangrijk instrument, maar privacy borging bij datagedreven werken vraagt om een bredere aanpak. Door een combinatie van DPIA's, privacy vriendelijk ontwerpen, transparantie en beveiligingsmaatregelen kan de gemeente verantwoord en AVG-conform datagedreven werken.

Logging en ongeoorloofde inzage in gegevens

Om ongeoorloofde inzage in persoonsgegevens tegen te gaan is het belangrijk dat er binnen een applicatie gelogd wordt. Alleen loggen is echter onvoldoende, er zal ook controle op logging moeten plaats vinden. Logging is een van de punten die ook in het functioneel applicatiebeheer (FAB) staan. Hiervoor zal in 2025 nader beleid worden vastgesteld. Dit zal langs de ondernemingsraad moeten.

Overige punten

Met name het oppakken van de maatregelen die volgen uit het privacy NOREA Wpg en VNG AVG normenkader, het uitvoeren (en herhalen) van DPIA's, beantwoorden van privacy vraagstukken (gevraagd en ongevraagd), aanvullen verwerkingregister, bijhouden van verwerkersovereenkomsten, bewustwordingsacties op gebied van informatieveiligheid en privacy verdienen aandacht.

Bewustwording

Voorbeelden uit organisatie van datalekken als onderdeel van het bewustwordingsprogramma ten aanzien van privacy incidenten.

Toets werking

Bij periodieke toetsing controleert de FG de opzet, bestaan en werking van gegevensverwerkende processen en andere initiatieven. Het gebruik van een AVG-prestatielijst bevordert het inzicht in het aantal verwerkingen en bijbehorende meetbare activiteiten. Dit draagt bij tot bewustwording en tot een betere afstemming met uit te voeren beheeractiviteiten. De FG houdt hiermee toezicht op de werking van gegevensverwerkende processen.