JAARVERSLAG 2024 GEGEVENSBESCHERMING

Opgesteld door de Functionaris Gegevensbescherming

Maart 2025.

Samenvatting

In dit jaarverslag worden bevindingen beschreven over acties en maatregelen die de gemeente in 2024 heeft genomen om de doelstellingen en beginselen uit de Algemene verordening gegevensbescherming (AVG) en de Wet politiegegevens (Wpg) te behalen en te waarborgen. Ook bevat dit document aanbevelingen voor 2025 e.v.
De FG heeft zijn bevindingen naast de eigen waarnemingen mede gebaseerd op het AVG Borgingsproduct 2.0 van het VNG en het selfassessment van het Centrum voor Informatiebeveiliging en Privacybescherming (CIP).

De gemeente Nieuwegein heeft in 2024 weer een aantal stappen gezet in de bescherming van persoonsgegevens. Er kan worden geconcludeerd dat van alle AVG-onderwerpen inmiddels 83% volledig is geïmplementeerd.

Er worden tal van goede initiatieven genomen en acties in de organisatie uitgezet. Alleen ontbreekt het hierin vaak aan een juiste opvolging binnen de teams en organisatie of worden acties onvoldoende gedocumenteerd en beslissingen vaak onvoldoende vastgelegd Hierdoor kan de organisatie moeilijk aantonen dat wordt voldaan aan de geldende privacyregels. Het is gewenst dat de afdelingen en de teams zich aantoonbaar kunnen verantwoorden over hun uitgevoerde taken voor Privacy en Informatieveiligheid. Hiermee zou een belangrijke stap voorwaarts gezet kunnen worden in het privacy volwassenheidsniveau. Dit was ook al een FG-aanbeveling in vorige jaarverslag maar heeft nog niet geleid tot concrete stappen hierin.

Een belangrijke verplichting binnen de AVG is dat aangetoond kan worden dat medewerkers voldoende worden getraind worden en blijven in privacy bewust werken. Bewustwording is belangrijk omdat 80% van de incidenten met persoonsgegevens voortkomt uit menselijk handelen. Omdat uit analyses is gebleken dat te weinig collega's werden bereikt met de huidige bewustwordingsacties, is in 2024 vooral gewerkt aan het herijken van het bewustwordingsplan.

Daarnaast is er extra aandacht geweest voor hoog-risicoverwerkingen en zijn hiervoor DPIA's uitgevoerd zoals voor het cameratoezicht in het Stadhuis en anonimerings-software.

Adequaat omgaan met persoonsgegevens is een blijvend en groeiend proces.
De FG concludeert dat de gemeente Nieuwegein zich over het geheel genomen nog bevindt op volwassenheidsniveau "beheerst" (2), [1]maar dicht ligt tegen het niveau "vastgesteld" (3). Het gaat hierbij vooral om het organisatie breed inzicht krijgen en houden in privacy risico's en vervolgens het managen van deze risico's in de afdelingen en teams. Hierin ligt een belangrijke uitdaging voor de afdelingshoofden en teamleiders samen met hun privacy ambassadeurs, medewerkers en ondersteuning van de Privacy Office.
De FG gaat er nog steeds vanuit dat als voor de AVG/Wpg een adequaat verantwoordingssysteem wordt ingericht, er een belangrijke stap kan worden gezet in de privacy volwassenheid van de organisatie.

[1] Zie hiervoor hoofdstuk 'Groeimodel volwassenheid totale gegevensbescherming AVG en Wpg'.

Wet politiegegevens (Wpg)
Het college van burgemeester en wethouders is ook verwerkingsverantwoordelijke voor het verwerken van persoonsgegevens bij handhavingsactiviteiten van boa's, waarbij sprake is van het opsporen van een strafbaar feit. Het gaat hierbij om de domeinen: openbare ruimte, milieu en leerplicht.

Jaarlijks dient voor het gebruik van politiegegevens een interne Wpg-audit te worden uitgevoerd en vierjaarlijks een externe audit.
Op basis van auditresultaten is een verbeterplan opgesteld over de normen waaraan nog niet volledig wordt voldaan. Eind 2025 dient er weer een extern auditrapport te worden opgeleverd over alle 31 Wpg-normen.

Net zoals in veel gemeenten is vooral gewerkt aan het opstellen en het in uitvoering nemen van de verbeterplannen. Daardoor was over het jaar 2024 nog geen interne audit uitgevoerd. Inmiddels is deze interne audit alsnog begin 2025 uitgevoerd.

Inhoud

Deel A: Borging AVG

De algehele AVG-compliance wordt in de gemeente Nieuwegein gemeten aan de hand van het IBD AVG-borgingsproduct. Het AVG-borgingsproduct kent slechts 3 scores te weten: nog niet gepakt (), gedeeltelijk () of opgepakt (). Om de scope van de scores wat meer te duiden heeft de FG gekozen voor een range van 5 scores. De weergave in een van de 5 bolletjes is een optelsom van de scores van het betreffende onderwerp. Nuances zijn hierbij niet direct zichtbaar.

Aandacht vereist van management	Bijna op schema
In te halen achterstand	Op schema
Opgepakt	

AVG Dashboard

1. Beleid

Het privacy beleid is een kader waarin de gemeente aangeeft aan welke principes zij zich houdt bij de verwerking van persoonsgegevens, hoe de gemeente omgaat met persoonsgegevens en welke maatregelen zij treft om te voldoen aan de relevante wet- en regelgeving. Ter uitvoering van het beleid adviseert de Privacy Office het bestuur, management en medewerkers over allerlei privacy gerelateerde vraagstukken. De Privacy Office heeft daarbij ook een vraagbaakfunctie naar medewerkers toe.

Bevindingen FG

- In 2022 is geïnventariseerd welke beleidsonderdelen moeten worden aangepast of geïntensiveerd. Hiervoor is een spoorboekje ontwikkeld dat onderdeel vormde van het Jaarplan Privacy 2023. Vanaf 2023 zijn er op de verschillende thema's initiatieven genomen als voorbereiding op de genoemde uitwerking, zoals de integrale gegevensverwerking tussen de gemeenschappelijke regeling Werk en Inkomen Lekstroom (WIL) en de gemeente in het lokale werkteam.
- In het laatste kwartaal 2024 is een zorgvuldige voorbereiding gestart voor de aanpassing van het uitgebreide beleidsdocument uit 2018. Dit tegen de achtergrond van de ontwikkelingen en ervaringen van de laatste jaren en het format van de Informatiebeveiligingsdienst (IBD). De verwachting is dat het nieuwe beleid in Q2 van 2025 door het college kan worden vastgesteld.
- De bescherming van personen binnen het sociaal- en veiligheidsdomein is van extra belang gelet op de aard van de persoonsgegevens die worden verwerkt en de mogelijke kwetsbaarheid van de betrokkenen. Hiervoor zal in de loop van 2025 specifiek beleid worden opgesteld.

FG-aanbeveling voor de Privacy Office:

- Maak een implementatieplan voor het nieuw vast te stellen beleid.

FG-aanbeveling voor het Afdelingshoofd en de Privacy Office:

- Geef prioriteit aan de realisatie van een specifiek beleidskader voor het sociaal- en veiligheidsdomein.

2. Bewustwording

Kennis, houding en gedrag (awareness) zijn de belangrijkste pijlers in de privacybescherming. Op het gebied van gegevensbescherming is privacy bewustzijn vaak de achilleshiel van een organisatie. Zelfs als de processen en procedures van een organisatie goed ingericht zijn, zullen maatregelen niet effectief zijn als medewerkers hier niet naar handelen. Daarom is het essentieel om voortdurend aandacht te besteden aan privacy bewustzijn. Het is namelijk niet altijd vanzelfsprekend dat medewerkers begrijpen hoe ze persoonsgegevens moeten beschermen.

Bevindingen FG

- De FG constateert dat met de bestaande bewustwordingsacties – on-boarding nieuwe medewerkers, het Grote Datalekkenspel en de digitale voorziening 'Sir Askalot' - té weinig medewerkers worden bereikt.
- De Privacy Office heeft een concept bewustwordingsplan in voorbereiding met daarin een voorstel voor een verplichtend karakter voor medewerkers. De planning is dat dit plan in Q2 wordt voorgelegd aan het DT.
- De FG ondersteunt dit concept, temeer ook omdat alle datalekken in 2024 te wijten waren aan onzorgvuldig handelen van medewerkers en dat de organisatie moet kunnen aantonen dat alle medewerkers worden betrokken in bewustwordingssessies.
- De FG waardeert de samenwerking tussen de onderdelen Privacy en Informatiebeveiliging op het thema Bewustwording.
- Vanaf februari 2025 is de gemeente, op grond van de Europese AI-Act, verplicht om medewerkers die met AI werken te trainen. Dit omvat ook het gebruik van generatieve AI-tools zoals ChatGPT en Co-pilot.

FG-aanbeveling voor het DT en Afdelingshoofden/ Teamleiders:

- Blijf aandacht houden voor de bewustwording van medewerkers en bestuurders, door:
    - het vaststellen van een nieuwe bewustwordingsplan met een verplichtend karakter;
    - het faciliteren van medewerkers om deel te kunnen nemen in de deelname aan verplichte bewustwordingssessies;
    - periodiek aandacht vragen voor gegevensbescherming tijdens afdeling/teammomenten.
- Blijf als management stimuleren dat aan de voorkant van nieuwe initiatieven de onderwerpen van privacy en informatieveiligheid worden meegenomen.
- Organiseer een training en bewustwording voor medewerkers die met AI werken.

3. Processen

De verwerkingen van persoonsgegevens van de gemeente 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 is de gemeente verplicht zijn om hoog risicoverwerkingen een gegevensbeschermingseffectbeoordeling (DPIA) uit te voeren.

Goed inzicht in de werkprocessen is belangrijk voor een adequate borging van de AVG-vereisten. De PO houdt jaarlijks privacy-talks (interviews). Samen met de afdelingshoofden en teamleiders wordt daarin ingezoomd op mogelijke wijzigingen en ontwikkelingen in hun processen. Hierbij is ook extra aandacht voor de samenwerking rolverdeling tussen de afdelingen en de PO, zodat de proceseigenaren hun verantwoordelijkheid voor verwerking van persoonsgegevens in hun processen zo goed mogelijk kunnen waarmaken. Deze privacy-talks zijn daardoor een belangrijke pijler voor het "in control" kunnen zijn van de privacy-risico's binnen de organisatie.

Bevindingen FG

- In het algemeen is er bij de proceseigenaren nog steeds een positieve ontwikkeling te zien qua bewustzijn over hun processen en de daarbij horende risico's voor de bescherming van persoonsgegevens. De positieve rol van de I-adviseurs is daarin ook belangrijk.
- In 2024 is vooral veel energie gericht op de uitvoering van DPIA's onder meer door het inhuren van externe deskundigheid, zoals bij het CCTV- camera toezicht plan, aanpak woonfraude en anonimiseringssoftware.
- Er is nog geen structureel DPIA-plan. Hierdoor is de organisatie niet in staat te aantoonbaar te voldoen aan de wettelijke verantwoordingsplicht.

FG-aanbeveling voor Afdelingshoofden/Teamleiders samen met de Privacy Office:

- Het is essentieel dat er een jaarlijkse DPIA-planning wordt opgesteld, gekoppeld aan prioriteiten en risico's. Dit maakt het mogelijk om beter toezicht te houden op de implementatie van maatregelen om risico's te verminderen.
- Organiseer een proces voor opvolging van de geïmplementeerde maatregelen en koppel dit aan een risicomanagementsysteem. Dit maakt het mogelijk om de effectiviteit van de maatregelen te toetsen en zo nodig bij te sturen.

4. Risicomanagement

Het beheren van risico's is een doorlopend proces waarbij de risico's met betrekking tot gegevensbescherming worden geïdentificeerd, beoordeeld en op passende wijze worden beheerd. Risicomanagement bij privacy richt zich op het beheersen van risico's die ontstaan tijdens het verwerken, inclusief het verzamelen, opslaan en doorgeven van persoonsgegevens. Door Privacy by Design toe te passen en Data Protection Impact Assessments (DPIA's) uit te voeren, worden de risico's bij de ontwikkeling, implementatie en uitvoering van de gegevensverwerking geanalyseerd en zo veel mogelijk beperkt of weggenomen. Ook geeft het inzicht in de risico's die de organisatie accepteert, waar we geen maatregelen voor hoeven te nemen.

Bevindingen FG

- Er komt steeds meer besef in de organisatie dat het voor een veilig gebruik van persoonsgegevens belangrijk is om het privacy-risicomanagement in samenhang te bezien met de risico's van informatiebeveiliging.

FG-aanbeveling voor het DT en Privacy Office:

- Faciliteer en ondersteun de ontwikkeling van een systeem voor risicomanagement waarvan ook de bescherming van persoonsgegevens onderdeel vormt. Dit systeem zou ook een onderdeel kunnen zijn van een op te zetten verantwoordingssysteem.

5. Organisatorische inbedding

Voor een goede en juiste uitvoering is het van belang dat iedereen binnen de organisatie 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 het creëren van bewustzijn.

Bevindingen FG

- In de organisatie is goed waarneembaar dat de Privacy Ambassadeurs een belangrijke schakel vormen in de bewustwording binnen de afdelingen en de organisatie als geheel. Het is goed om te zien dat bij een aantal privacy-talks met de afdelingshoofden ook de betreffende privacy ambassadeurs aanwezig waren.
- De Privacy Office organiseert periodieke afstemmingsmomenten met de Privacy Ambassadeurs. Door een gebrek aan capaciteit binnen de Privacy Office zijn in 2024 helaas niet alle geplande bijeenkomsten doorgegaan.

FG-aanbeveling voor de Privacy Office:

- Het is belangrijk dat het enthousiasme van de Privacy Ambassadeurs wordt vastgehouden. Blijf daarom een hoge prioriteit geven aan de ondersteuning van de Privacy Ambassadeurs.

FG-aanbeveling voor de Afdelingshoofden en Teamleiders:

- Blijf investeren in het belang van de rol van Privacy Ambassadeur.

6. Rechten van betrokkenen

De gemeente dient degene van wie zij de persoonsgegevens verwerkt (de 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 de betrokkenen in staat om door een aantal rechten controle en invloed uit te oefenen over zijn of haar persoonsgegevens. Denk aan het recht op inzage, verwijdering van gegevens onder voorwaarden of tussenkomst van een mens bij het nemen van besluiten.

Bevindingen FG

- Bij de behandeling van AVG-verzoeken bij Geynwijs is gebleken dat in die gevallen meer persoonsgegevens zijn geregistreerd dan nodig en ook op meerdere opslaglocaties. Hierdoor wordt de afhandeling van AVG-verzoeken onoverzichtelijk en tijdrovend.

FG-aanbeveling voor Afdelingshoofd Geynwijs en Privacy Office:

- Stel een protocol op voor het gebruik van persoonsgegevens in het Sociaal Domein.

7. Gegevensuitwisseling bij samenwerkingsverbanden

De gemeentelijke organisatie werkt op meerdere beleidsterreinen, in verschillende bedrijfsfuncties, in diverse rollen en hoedanigheden samen met (mede) overheden. Deze verwerkingen moeten ook voldoen aan de AVG.
De gemeente dient dus niet alleen intern de gegevensbescherming op orde te hebben, maar ook de bestuurlijke verantwoordelijkheid te kunnen waarmaken voor het maken van goede afspraken met ketenpartners over gegevensbeschermingsbeleid en toetsing daarvan belangrijk.

Bevindingen FG

- In 2024 is vooral ingezoomd op implementatie van een gedeelte (arbeidsinschakeling) van de Participatiewet in het lokale werkteam in afstemming met de Gemeenschappelijke Regeling Werk -en Inkomen Lekstroom. De Privacy Officer heeft namens de Lekstroomgemeenten geparticipeerd in de projectgroep. Vanuit de projectgroep is ook een voorbeeld privacyverklaring ontwikkeld die zal worden opgenomen in de privacyverklaring van de gemeente.
- De taken voor het verwerven van voorzieningen in het kader van de Jeugdwet en de Wmo 2015 zijn door middel van een dienstverleningsovereenkomst en een verwerkersovereenkomst opgedragen aan de Regionale Backoffice Lekstroom (RBL). De RBL is een organisatieonderdeel van de gemeente Houten. Door de RBL wordt verantwoording afgelegd over met name de reguliere processen.
- In de praktijk worden soms onder de vlag RBL, Lekstroombreed initiatieven ontwikkeld waarbij persoonsgegevens worden gebruikt. Niet altijd is duidelijk op welke manier de opdrachtgevende gemeenten -waaronder Nieuwegein- betrokken zijn. Een recent voorbeeld hiervan is de dak- en thuislozentelling.

FG-aanbeveling voor het DT:

- Maak een jaarkalender voor regionale Lekstroom projecten waarin persoonsgegevens worden gebruikt en deel deze met de Privacy Office en voor zover van toepassing met de andere Lekstroomgemeenten.
- Maak afspraken in de organisatie over het monitoren van de afspraken over gegevensbescherming met verbonden partijen.

8. Leveranciersmanagement

De gemeentelijke organisatie kan niet alle taken in eigen beheer uitvoeren. Voor deze taken wordt gebruikt gemaakt van opdrachtnemers die dan namens de gemeente persoonsgegevens verwerken. Omdat de gemeente ook bij uitbesteding verantwoordelijk blijft voor een juist gebruik van deze persoonsgegevens, worden in een verwerkingsovereenkomst afspraken gemaakt met de opdrachtnemers over de bescherming van persoonsgegevens

Bevinding FG

- Het beheer op verwerkersovereenkomsten is nog onvoldoende in de organisatie belegd. Daardoor is de gemeente niet volledig in control van uitbestede taken. Dit geldt in sommige gevallen ook voor verbonden partijen.

FG-aanbeveling voor het DT en de gehele organisatie:

- Maak afspraken in de organisatie over wie het beheer voert op verwerkersovereenkomsten, met andere woorden wie de verwerker aanspreekt op het gevoerde beleid. Een mooi voorbeeld daarvoor is de inrichting van Contract Lifecycle Management (CLM) voor het Datacenter.

9. Gegevensbescherming

Vanuit het algemene behoorlijkheids-, -integriteits en -vertrouwelijksheidsbeginsel is het essentieel dat de gemeente passende technische en organisatorische maatregelen neemt ter beveiliging van persoonsgegevens. Het is belangrijk dat bij nieuwe projecten of verwerkingen aan de voorkant over privacybeschermende maatregelen wordt nagedacht (Privacy by Design). Dit om achteraf ingewikkelde en/of dure aanpassingen te voorkomen.
Daarnaast geldt onder de AVG een meldplicht voor datalekken. Dit houdt in dat beveiligingsincidenten met persoonsgegevens onder omstandigheden gemeld dienen te worden aan de AP en/of de betrokkene(n) (zie ook de bijlage met kengetallen).

Bevindingen FG

- De praktijk laat een mooie ontwikkeling zien dat I-adviseurs veelal aan de voorkant bij nieuwe initiatieven worden betrokken (Privacy by Design). Aan de andere kant gebeurt het ook nog dat er nieuwe verwerkingen worden gestart, zonder dat de afstemming over informatiebeveiliging en privacy heeft plaatsgevonden. Een voorbeeld hiervan is de anonimiseringssoftware van Datamask.
  Inmiddels is in Q4 2024 het onderdeel Privacy en Informatiebeveiliging toegevoegd aan het format projecten-formulier, waardoor wordt beoogd te voorkomen dat er geen aandacht is voor gegevensbescherming.
- Er zijn in de organisatie voor de hoog risico AVG-verwerkingen geen controle-processen ingericht.
- Cybercriminaliteit is aan de orde van dag. Het bewustzijn binnen de organisatie over de eventuele gevolgen van een cyberaanval is groot. Er is een Cyber- en IT-crisisplan ontwikkeld om na een cyberaanval of IT crisis (een hack of soortgelijks) zo snel mogelijk weer door te kunnen met de kernprocessen van de organisatie.
- Vanuit de Privacy Office is er aandacht voor de mogelijke effecten op de bescherming van persoonsgegevens door de ontwikkeling van Artificial Intelligence (AI). Daarom zijn er vuistregels opgesteld voor het gebruik van chatbot GPT.
- Er is nog geen organisatie brede visie of beleid voor Artificial Intelligence (AI) als leidraad in de inkoopprocessen. Zonder een duidelijke AI-visie kan de gemeente risico’s lopen op het gebied van gegevensbescherming bij het gebruik van nieuwe AI-technologieën.
- Uit eigen waarnemingen en gesprekken met jeugd -en WMO-professionals, constateert de FG dat na herinrichting van het Stadshuis, er voor professionals van Geynwijs onvoldoende fysieke randvoorwaarden zijn om op de 5e etage persoonsgegevens goed te kunnen beschermen bij de uitvoering van hun werk. Het werken in een kantoortuin (en dan meer specifiek de 5e etage) maakt dat collega’s van andere afdelingen onbevoegd kennis (kunnen) nemen van (doorgaans) gevoelige persoonsgegevens. Bijvoorbeeld bij collegiaal overleg of bij telefoongesprekken met inwoners, ook omdat de belhokjes vaak bezet zijn. Daar staat tegenover dat de professionals ook aangeven dat na de herinrichting de lijnen naar de eigen beleidsafdeling, JZ en communicatie veel korter zijn geworden, wat beter werkt.

FG-aanbeveling voor het DT en de Privacy Office:

- Borg dat bij de start van initiatieven/projecten/beleidsontwikkeling er een privacy toets plaatsvindt.
- De FG geeft als suggestie mee om het Cyber- en IT Crisisplan te gaan beoefenen.

FG-aanbeveling voor DT:

- Beleg het onderwerp AI in de organisatie.
- Ontwikkel een visie/beleid op het gebruik van AI.

- Ga na of aan de professionals van Geynwijs betere randvoorwaarden kunnen worden geboden voor het vereiste beschermingsniveau van persoonsgegevens, waarbij toch de samenwerking met beleid, JZ en communicatie bevorderd kan blijven.

10. Verantwoording

De AVG legt de verantwoordelijkheid bij de organisatie zelf om aantoonbaar te maken dat deze voldoet aan de privacyregels. Dit betekent dat de gemeente aan moet kunnen tonen dat de verwerkingen van persoonsgegevens voldoen aan de beginselen van de AVG en aan de relevante wet- en regelgeving. De verantwoordingsplicht komt voornamelijk tot uiting in het jaarplan de PO, het gepubliceerde register van verwerkingen en de openheid die met dit jaarverslag wordt gegeven in uitgevoerde DPIA's en (gemelde) datalekken.

Bevindingen FG

- Er worden tal van goede initiatieven genomen en acties in de organisatie uitgezet. Alleen ontbreekt het hierin vaak aan een juiste opvolging binnen de teams en organisatie of worden acties onvoldoende gedocumenteerd en beslissingen vaak onvoldoende vastgelegd. Daardoor heeft de organisatie nog geen goed overzicht en is de gewenste informatie slechts gefragmenteerd en maar bij bepaalde personen geconcentreerd. Hierdoor is het lastig om aantoonbaar in control te zijn. De huidige PDCA-cyclus is vooral gericht op de ondersteunende en adviserende rol van de Privacy Office. Voor een organisatiebrede verantwoording is het gewenst dat ook de afdelingen en de teams zich verantwoorden over hun uitgevoerde taken voor Privacy en Informatieveiligheid. Hiermee zou een belangrijke stap voorwaarts gezet kunnen worden in het privacy volwassenheidsniveau.
  Dit was ook al een FG-aanbeveling in vorige jaarverslag.
- Binnen de organisatie worden op verschillende manieren risico's waargenomen en/of geregistreerd. Ook wordt daarover verschillend gerapporteerd. Om aantoonbaar in control te zijn volgens de AVG, is het gewenst dat er voor gegevensbescherming een adequaat verantwoordingssysteem is. Omdat er in de organisatie meer risicogebieden zijn wordt in overleg met Concerncontrol gekeken hoe gemeentebreed risicomanagement kan worden ingericht, zodat de kwaliteit van de dienstverlening kan worden gewaarborgd of verbeterd.
- Voor dit moment wordt vooral ingezet op een goed relatiemanagement met de proceseigenaren, onder meer door de IB&P talks. De FG raadt aan om deze werkwijze een stap verder te brengen door afspraken vast te gaan leggen en hierover periodiek te rapporteren.
  Een daaropvolgende stap zou kunnen zijn dat de afspraken en de opvolging daarvan worden opgenomen in een gemeente breed verantwoordingssysteem (tool).

FG-aanbeveling voor het DT, Afdelingshoofden, Teamleiders en de Privacy Office:

- Leg aan de hand van de MT-actielijst afspraken met proceseigenaren over gegevensbescherming vast en rapporteer daarover periodiek aan de directie en MT.
- Onderzoek de mogelijkheden voor de implementatie van een adequaat verantwoordingssysteem.

Deel B: WPG

1. Inleiding

De FG ziet er in brede zin op toe dat de Wet politiegegevens wordt nageleefd. De FG rapporteert jaarlijks de bevindingen aan de hand van een jaarverslag. In dit jaarverslag staan bevindingen beschreven over acties en maatregelen die in 2024 zijn genomen om de doelstellingen en beginselen uit de Wet politiegegevens (Wpg) te behalen en te waarborgen. Voor zijn bevindingen steunt de FG ook op de interne controle 2024 die is uitgevoerd door Concerncontrol over het wettelijk verplichte Wpg-normenkader. De scores hieronder zijn geven een algemeen inzicht. Voor een nadere duiding verwijst de FG naar de interne controle 2024 uitgevoerd door Concerncontrol.

WPG-dashboard	2024	2023	2022
Beleid Domein I			
Beleid Domein II			
Beleid Domein III			
Bewustwording Domein I, en II			
Bewustwording Domein III			
Autorisatieproces Domein I, II en III			
Bewaartermijnen Domein I, II en III			
Bewaartermijnen Domein III			
Verstrekken van persoonsgegevens Domein I, II en III			
Domein III			
DPIA Domein I, II en III			
Register van verwerkingen Domein I, II			
Register van verwerkingen Domein III			
Auditplanning Domein I, II en III			
Controle proces Domein I, II en III			
Documentatie Domein I en II			
Documentatie Domein III			

Legenda:

- AANDACHT VEREIST VAN MANAGEMENT
- IN TE HALEN ACHTERSTAND
- OPGEPAKT
- BIJNA OP SCHEMA
- OP SCHEMA

2. Taak van de FG

De taken van de FG (artikel 36 van de Wet politiegegevens) voor de Wpg kunnen als volgt worden samengevat:

De FG houdt toezicht op:

1. het hebben van een beleid aangaande de uitvoering van de Wpg en de bewustwordingsverplichting;
2. het autorisatieproces met betrekking tot het vastleggen van politiegegevens;
3. de kwaliteit en waarborging van de juistheid van de nauwkeurigheid van politiegegevens;
4. het verwerken van politiegegevens en de bewaartermijnen;
5. het ter beschikking stellen en verstrekken van politiegegevens;
6. de controle op de informatiebeveiliging en de controle op het uitvoeren van een risicoanalyse;
7. het register voor verwerkingen;
8. de verplichtingen ten aanzien van de audit.

3. Bevindingen 2024 en aanbevelingen voor alle domeinen

Onderwerp	Bevindingen	Aanbeveling
Beleid	Er is nog geen vastgesteld Wpg beleid.	Ontwikkel een Wpg-beleidskader
Bewustwording	Bewustwording rondom Wpg is momenteel onderdeel van de centrale bewustwordingssessies	Maak een concreet bewustwordingsplan en leg vervolgens de bewustwordings-activiteiten vast (ook die in teamoverleggen).
Transparantie	Er zijn geen procedures ingericht over het informeren van betrokkenen.	Maak een procedure voor het informeren van betrokkenen over het gebruik van persoonsgegevens.
Autorisatieproces	Het autorisatieproces is afgestemd met en ingericht in de applicaties, maar er ontbreken hiervoor een autorisatiematrix. Bij het onderdeel Leerplicht is hiervoor wel een instructie gemaakt.	Maak een autorisatiematrix.
Bewaartermijnen	De bewaartermijnen zijn ingericht.	Zorg voor adequate archivering en verwijdering van gegevens en richt een controleproces in voor de bewaartermijnen.
Verstrekken van politiegegevens	De Boa's zijn zich goed bewust van het verstrekkingenregister, maar er ontbreken afspraken en instructies voor verstrekkingen buiten het politiedomein.	Richt een proces in voor het verstrekken van politiegegevens, inclusief duidelijke afspraken/instructies. Voor leerplicht is dit al opgenomen in werkinstructies.
DPIA	Er is nog geen DPIA uitgevoerd.	Voer een DPIA uit.
Register van verwerkingen	Het register van verwerkingen is nog niet aangepast op de Wpg	Controleer periodiek of het register nog klopt. Pas het register aan voor de Wpg
Auditverplichting	• In 2024 heeft de hercontrole plaatsgevonden van de verbeterpunten. • Eind 2024 is ook de Wpg-rapportage over 2022 opgeleverd door de externe auditor. • De interne audit voor de Wpg zal voortaan worden uitgevoerd door het team Concerncontrol. Inmiddels is de interne audit 2024 uitgevoerd	• Faciliteer de medewerkers die de interne audit uitvoeren met de volgens de wet verplichte Wpg-audittraining.
Verbeterplan	Er is een verbeterplan opgesteld.	Zorg dat het verbeterplan wordt uitgevoerd aan de hand van te stellen prioriteiten.

Onderwerp	Bevindingen	Aanbeveling
Controleproces	Er is nog geen controleproces.	Richt een adequaat eerstelijns controleproces in en zorg ervoor dat Concerncontrol en de FG de juiste controle-informatie krijgen.

Groeimodel volwassenheid totale gegevensbescherming AVG en Wpg

In het kader van het privacy volwassenheidsniveau wordt doorgaans uitgegaan van het volgende groeimodel.

(1) Initieel	• Minimale vereisten van de AVG zijn aanwezig • Succes afhankelijk van inzet van individuen • Ad hoc herhaling van activiteiten privacy bewustzijn
(2) Beheerst	• Verwerkingen in het register zijn actueel • Risicobesef aanwezig bij sleutelfiguren • Succes door teaminzet • Periodieke herhaling activiteiten privacy bewustzijn
(3) Vastgesteld (Basis op orde)	• Verwerkingen worden cyclisch actueel gehouden • Alle medewerkers worden standaard meegenomen
(4) Voorspelbaar (Integraal)	• Gegevensbescherming vanzelfsprekend onderdeel elk proces • Interne discipline organisatie
(5) Geoptimaliseerd (Optimaal)	• Focus op systematische verbetering alle organisatieonderdelen • Aanpassing mogelijk na verandering externe factoren

De FG concludeert dat de gemeente Nieuwegein zich over het geheel genomen bevindt op volwassenheidsniveau “beheerst” (2), maar dicht ligt tegen het niveau “vastgesteld” (3). De FG gaat er nog steeds vanuit dat als voor de AVG/Wpg een adequaat verantwoordingssysteem wordt ingericht, er een belangrijke stap kan worden gezet in de privacy volwassenheid.

FG-aanbeveling voor de directie:

- Formuleer een haalbare ambitie voor het volwassenheidsniveau en koppel hieraan de juiste middelen.

BIJLAGE KENGETALLEN 2024