GEMEENTEBLAD
Officiële uitgave van de gemeente Ede
Nr. 143126
27 maart
2026

Privacybeleid AVG & Wpg gemeente Ede 2026 - 2030

Burgemeester en wethouders

Gelezen het voorstel van burgemeester en wethouders d.d. 17 maart 2026, met nr. 507843, overwegende vaststellen privacybeleid AVG & Wpg gemeente Ede 2026 - 2030.

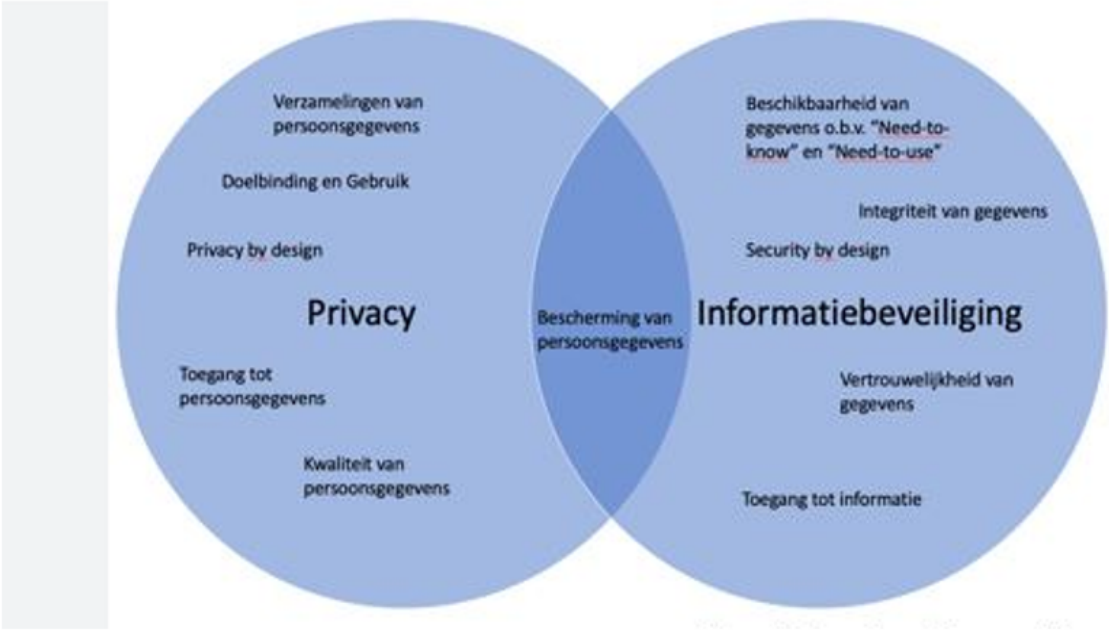
Besluit
Het privacybeleid AVG & Wpg gemeente Ede 2026 - 2030 vast te stellen.

Inleiding
Voor u ligt het privacybeleid Algemene verordening gegevensbescherming & Wet politiegegevens van de gemeente Ede (hierna: de gemeente). Dit document vervangt het privacybeleid uit 2021 en het addendum privacybeleid Wpg uit 2024.

De gemeente werkt met persoonsgegevens van inwoners, medewerkers en (keten)partners. Deze persoonsgegevens verzamelt de gemeente om de gemeentelijke, wettelijke taken goed uit te voeren. Inwoners, medewerkers en (keten)partners moeten erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met deze persoonsgegevens omgaat.

Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds digitaler wordende overheid maakt het zorgvuldig omgaan met persoonsgegevens steeds ingewikkelder en noodzakelijker. De gemeente is zich hiervan bewust en wil daarom met dit beleid aangeven hoe zij in algemene zin invulling geeft aan nationale en Europese wet- en regelgeving op het gebied van privacy, waaronder de Algemene verordening gegevensbescherming (hierna te noemen: AVG).

Samenhang privacy en informatiebeveiliging
Er is een nauwe samenhang tussen privacy en informatiebeveiliging. Binnen de gemeente werken privacy, informatiebeveiliging en de functionaris gegevensbescherming daarom samen in een driehoek. Zowel privacy als informatiebeveiliging gaan over de bescherming van persoonsgegevens. Het privacybeleid wordt door deze samenhang niet los gezien van het informatiebeveiligingsbeleid.



Geldigheidsduur
De gemeente beoordeelt het beleid tenminste een keer per vier jaar en past het waar nodig aan. Als daar aanleiding voor is (bijvoorbeeld in geval van grote organisatorische veranderingen, wetswijzigingen, uitkomsten van DPIA's) kan het college besluiten tot een tussentijdse aanpassing.

Begrippen

De definities van artikel 4 AVG hebben in dit beleidsdocument dezelfde betekenis.

Visie
Inwoners, medewerkers en (keten)partners van de gemeente moeten erop kunnen vertrouwen dat de gemeente hun privacy respecteert en zorgvuldig omgaat met hun persoonsgegevens. Een goede privacy boekhouding is noodzakelijk voor het goed functioneren van de gemeente en de basis voor het beschermen van rechten van inwoners, medewerkers en (keten)partners. Dit vereist een integrale aanpak, goed eigenaarschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken. Daarbij is verantwoord en bewust gedrag van medewerkers essentieel voor privacy binnen de gemeente.

Om deze visie in de praktijk te brengen zet de gemeente daarom in op het verhogen van de privacy bewustwording en verdere professionalisering van de privacyfunctie in de organisatie.

Hoofdstuk 1: Doel en reikwijdte

1.1 Doel

Met dit privacybeleid geeft de gemeente een kader voor het verantwoord omgaan met persoonsgegevens en het waarborgen van de persoonlijke levenssfeer van de personen waarvan de gemeente persoonsgegevens verwerkt (of laat verwerken). Daarnaast is dit privacybeleid bedoeld om taken en verantwoordelijkheden op het gebied van de bescherming van persoonsgegevens helder af te bakenen.

De verdere uitwerking van dit beleid is - waar relevant - vastgelegd in de operationele documenten binnen de gemeente. Denk hierbij aan handreikingen of werkafspraken voor algemene onderwerpen, zoals datalekken. Maar ook concrete werkprocessen en domeinspecifieke onderwerpen, zoals gegevensdeling voor de uitvoering van de Jeugdwet of de Wet maatschappelijke ondersteuning, kunnen een verdere uitwerking van het privacybeleid bevatten.

Verantwoordelijkheid van iedere werknemer
Iedereen werkzaam binnen de gemeente is verantwoordelijk voor het verantwoord omgaan met persoonsgegevens. De gemeente verlangt van al haar medewerkers en alle personen die werkzaam zijn voor de gemeente dat zij de voorschriften van dit privacybeleid opvolgen en actief uitdragen.

1.2 Reikwijdte

De gemeente verzamelt en gebruikt persoonsgegevens van inwoners, medewerkers en (keten)partners.

Dit privacybeleid is van toepassing op alle verwerkingen van persoonsgegevens door of namens de gemeente, waaronder:
1. De verwerking van persoonsgegevens binnen de bedrijfsprocessen van de gemeente;
2. De verwerking van persoonsgegevens die is uitbesteed. Of op een andere manier is georganiseerd, zoals deelname van de gemeente aan een rechtspersoon die voor de gemeente bepaalde diensten verricht;
3. De gegevensuitwisseling met derde partijen zoals bij samenwerkingsverbanden of leveranciers.

Hoofdstuk 2: Uitgangspunten en beleid

2.1 Wettelijk kader voor de omgang met persoonsgegevens

Voor de omgang met persoonsgegevens gelden onder andere de volgende wettelijke kaders:
- Europese Verordening; de Algemene verordening gegevensbescherming (AVG);
- Uitvoeringswet Algemene verordening gegevensbescherming (UAVG);
- Artikel 8 Europees Verdrag voor de Rechten van de mens en de fundamentele vrijheden (EVRM);
- Artikelen 10 en 13 Grondwet (persoonlijke levenssfeer en briefgeheim);
- Sectorale wetgeving;
- Archiefwet;
- Wet politiegegevens (Wpg).

Interne kaders:
- Integriteitsbeleid;
- Informatiebeveiligingsbeleid.

2.2 Uitgangspunten voor de verwerking van persoonsgegevens

De AVG is gebaseerd op een aantal principes voor de verwerking van persoonsgegevens. De gemeente stelt zich tot doel persoonsgegevens alleen te verwerken in overeenstemming met deze principes.

Rechtmatige grondslag
Persoonsgegevens worden door de gemeente alleen verwerkt in overeenstemming met de wet en op een behoorlijke en zorgvuldige manier. Dit betekent onder meer dat verwerkingen alleen plaatsvinden

als hiervoor een rechtmatige verwerkingsgrondslag bestaat. Veelal vloeit de grondslag (reden) voor een verwerking bij een gemeente voort uit een bevoegdheid vanuit het recht (algemeen belang/openbaar gezag) of een wettelijke verplichting.

Welbepaalde doeleinden
De gemeente verwerkt persoonsgegevens voor zeer uiteenlopende doeleinden. Zonder doel mag de gemeente geen persoonsgegevens verwerken. De verwerking van persoonsgegevens vindt plaats op een manier die noodzakelijk is om de doeleinden te bereiken waarvoor de gegevens zijn verkregen. Dit betekent dat de gemeente alleen die persoonsgegevens verwerkt die noodzakelijk zijn om het doel te bereiken (ter zake dienend). De gemeente ziet af van de verwerking als het doel op een andere – minder ingrijpende – manier kan worden bereikt. Bijvoorbeeld door minder of geen persoonsgegevens te verwerken.

Verdere verwerking
De gemeente kan persoonsgegevens in bepaalde gevallen verwerken voor andere doelen dan waarvoor ze in eerste instantie zijn verzameld. Daarbij geldt onder andere dat de twee doelen met elkaar te maken moeten hebben, er geen nadelige effecten zijn voor de betrokkenen, of dat hiervoor extra waarborgen zijn getroffen. De gemeente voert, voordat de verwerking start, een toets uit om te bepalen of de gegevens voor andere doelen mogen worden gebruikt op grond van de wet- en regelgeving.

Minimale gegevensverwerking
De gemeente mag alleen gegevens verwerken als dit in verhouding staat tot het doel. Als het doel (waarvoor persoonsgegevens worden verwerkt) zonder of met minder persoonsgegevens kan worden bereikt, dan kiest de gemeente bij voorkeur voor die mogelijkheid. Ook als het doel waarvoor persoonsgegevens worden verwerkt op een manier kan worden bereikt die minder inbreuk maakt op de privacy van de betrokkene, dan kiest de gemeente voor die mogelijkheid.

Juiste en actuele gegevens
De gemeente zorgt ervoor dat alleen persoonsgegevens worden verwerkt die juist en actueel zijn. Gelet op het doel waarvoor zij verzameld zijn of vervolgens worden verwerkt. De gemeente neemt redelijke maatregelen om persoonsgegevens juist en actueel te houden, onjuiste persoonsgegevens te actualiseren, te rectificeren en/of te wissen.

Gegevens worden op tijd vernietigd
De gemeente stelt de bewaartermijn van een verwerking vast aan de hand van wettelijke bepalingen en de selectielijsten. Gemeenten hebben op grond van de Archiefwet onder andere de plicht om zogenaamde selectielijsten op te stellen. Deze selectielijsten bepalen voor een selectie van documenten hoelang deze moeten worden bewaard. Alleen als de bewaartermijn niet op basis van wettelijke bepalingen of de selectielijsten kan worden vastgesteld, stelt de gemeente de bewaartermijn vast op basis van noodzakelijkheid. Persoonsgegevens mogen dan niet langer worden bewaard dan noodzakelijk. De gemeente bewaart gegevens alleen langer als deze geanonimiseerd worden, zodat directe of indirecte identificatie van een persoon niet meer mogelijk is.

Integriteit en vertrouwelijkheid
De gemeente neemt passende, technische en organisatorische maatregelen om de persoonsgegevens te beschermen tegen misbruik en onrechtmatige of ongeautoriseerde verwerking. De gemeente handelt hierbij volgens het informatiebeveiligingsbeleid. Het informatiebeveiligingsbeleid verplicht de gemeente om informatie te beveiligen tegen ongeautoriseerd gebruik, vernietiging (per ongeluk of onrechtmatig), verlies of vervalsing, onbevoegde bekendmaking of toegang en alle andere onrechtmatige manieren van verwerking.

Privacy by Default en Privacy by Design
De gemeente houdt bij de ontwikkeling van nieuwe diensten, systemen of processen rekening met aspecten van privacy en gegevensbescherming om zo te komen tot een zo optimaal mogelijke bescherming van persoonsgegevens. Dit uitgangspunt wordt Privacy by Design genoemd. De gemeente zorgt ervoor dat concrete maatregelen zoveel mogelijk doorgevoerd worden in het ontwerp. Daarbij neemt de gemeente Privacy by Default als uitgangspunt: de standaardinstellingen zijn altijd zo privacy-vriendelijk mogelijk.

Toegang tot gegevens
Alleen geautoriseerde gebruikers zijn bevoegd om persoonsgegevens in te voeren, rechtstreeks te raadplegen, wijzigen en verwijderen. Deze bevoegdheden worden verleend op grond van het binnen de gemeente geldend beleid voor toegang tot gegevens, waaronder het informatiebeveiligingsbeleid. Het beheer van bevoegdheden wordt regelmatig gecontroleerd. De gemeente hanteert daarnaast specifieke oplossingen en toepassingen, waaronder het bijhouden van loggegevens, om ongeautoriseerde

toegang tot en niet toegestane verwerkingen van persoonsgegevens zo veel mogelijk te voorkomen en aan te pakken.

Inbreuk in verband met persoonsgegevens
Bij toegang tot, verlies of wijziging van persoonsgegevens bij de gemeente, zonder dat dit de bedoeling is, is er sprake van een datalek. De gemeente moet een datalek, afhankelijk van het risico, melden bij de toezichthouder (de Autoriteit Persoonsgegevens: AP) en soms bij de getroffen betrokkenen.

De gemeente heeft een proces "behandelen melding (potentieel) datalek". Dit om ervoor te zorgen dat de gemeente bij het behandelen van datalekken aan alle vereisten van de AVG voldoet. In dit proces is beschreven op welke manier de gemeente datalekken afhandelt, wie daarbij welke verantwoordelijkheid heeft en hoe datalekken worden geregistreerd. De gemeente houdt medewerkers alert door bewustwordingsacties te organiseren.

De gemeente houdt zich verder aan de AVG-eisen voor datalekken en beveiligingsincidenten door een register bij te houden van alle beveiligingsincidenten. In dit register is vastgelegd of een beveiligingsincident heeft geleid tot een datalek en, als dat het geval is, of het datalek is gemeld en welke maatregelen er zijn getroffen om de risico's van het datalek te verminderen.

Op basis van de meldplicht datalekken, meldt de gemeente datalekken bij de AP wanneer de inbreuk waarschijnlijk een (hoog) risico vormt voor de rechten en vrijheden van de betrokkene. Een datalek moet onmiddellijk worden gemeld bij de AP, maar uiterlijk binnen 72 uur nadat een datalek bekend is geworden. Wanneer vaststaat dat het datalek een hoog risico heeft voor betrokkene, dan meldt de gemeente het datalek ook aan betrokkene. Het komt vaak voor dat de gemeente het datalek aan betrokkene meldt vanuit het oogpunt van transparantie, betrouwbare overheid en dienstverlening. Ook als er geen meldplicht is.

Samenwerking
Verwerkers
De gemeente schakelt soms derden in om persoonsgegevens in opdracht van haar te verwerken. Deze derden worden verwerkers genoemd. Ook een verwerker moet zich houden aan de privacyregelgeving en aan het privacybeleid van de gemeente. De AVG verplicht gemeenten tot het maken van contractuele afspraken met verwerkers. Deze afspraken staan in zogenaamde verwerkersovereenkomsten.

Samenwerkingsverbanden
Verder kan het voorkomen dat de gemeente samenwerkt met andere (overheids)organisaties om een taak van algemeen belang uit te voeren. In die gevallen kan sprake zijn van meerdere verwerkersverantwoordelijken (gezamenlijk of individueel). De gemeente maakt met deze organisaties afspraken over de wijze waarop persoonsgegevens worden verwerkt. Derden waarborgen een beschermingsniveau dat minimaal gelijkwaardig is aan dat van de gemeente.

Doorgifte buiten de EER
Doorgifte van persoonsgegevens aan landen buiten de Europese Economische Ruimte (EER) of een internationale organisatie, gebeurt alleen in overeenstemming met de relevante bepalingen in toepasselijke wet- en regelgeving en dit privacybeleid.

Transparantie
De gemeente informeert de betrokkenen tijdig, op een zo eenvoudig mogelijke en toegankelijke manier over het feit dat zij persoonsgegevens verwerkt, op welke wijze en voor welke doeleinden. De betrokkene wordt op heldere en laagdrempelige manier geïnformeerd over zijn/haar rechten en de manier waarop hij/zij deze kan uitoefenen. Alleen wanneer de wet hier ruimte voor biedt, wijkt de gemeente van deze informatieplicht af.

Rechten van betrokkenen
Iedereen heeft het recht om te weten welke persoonsgegevens de gemeente over hem/haar heeft verzameld en waarvoor deze worden gebruikt. Een betrokkene heeft dan ook de mogelijkheid om de rechten uit hoofdstuk III van de AVG uit te oefenen. Te weten: het recht van inzage, recht op rectificatie, recht op verwijdering, recht op bezwaar, recht op beperking en recht op overdraagbaarheid. Betrokkenen kunnen via de website van de gemeente een "verzoek privacyrechten" doen. De gemeente behandelt deze "verzoeken privacyrechten" aan de hand van een vastgesteld werkproces.

Klachten
Indien een betrokkene van mening is dat de gemeente niet op een juiste wijze met zijn/haar persoonsgegevens is omgegaan, kan hij/zij een klacht indienen via de reguliere klachtenprocedure van de ge-

meente. De betrokkene heeft ook het recht om een klacht in te dienen bij de Autoriteit Persoonsgegevens, over de naleving van wet- en regelgeving op het gebied van de bescherming van persoonsgegevens.

Verantwoording
Onder de verantwoordelijkheid van zowel het college van B&W als de gemeenteraad vindt een groot aantal verwerkingen van persoonsgegevens plaats. Daar vindt extern en intern toezicht op plaats. De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de privacyregels in Nederland. Daarnaast heeft de gemeente een interne toezichthouder: de functionaris Gegevensbescherming (FG). De FG ziet erop toe dat de AVG intern wordt nageleefd. De gemeente stelt voldoende middelen ter beschikking aan de FG om het toezicht goed uit te kunnen voeren.

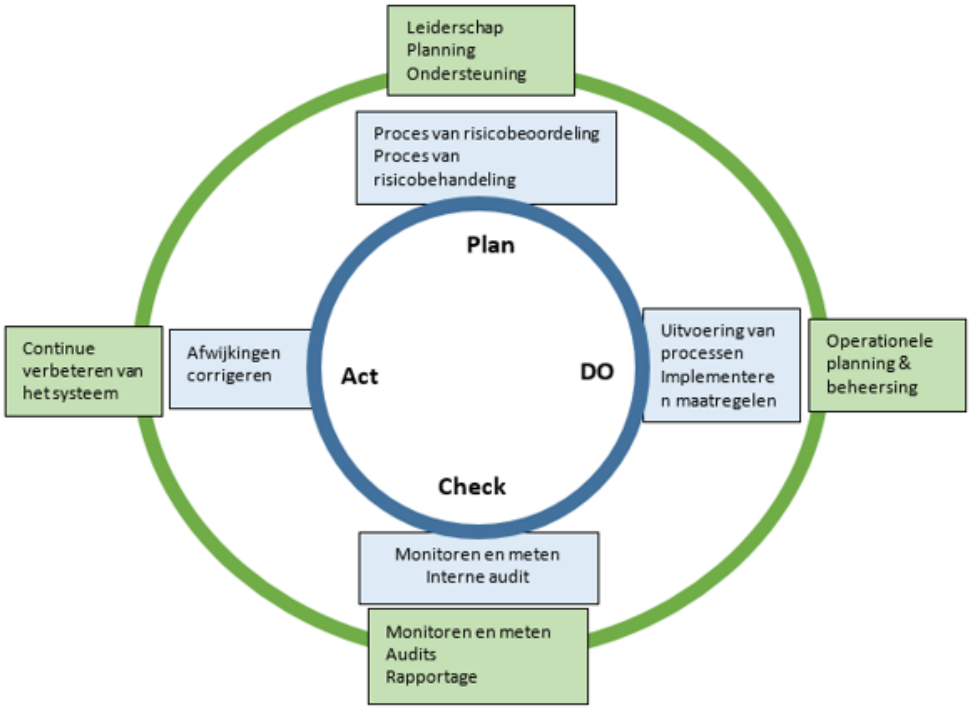
Verwerkingsregister
De gemeente heeft een verwerkingsregister waarin alle bedrijfsprocessen staan waarin persoonsgegevens worden verwerkt. Het verwerkingsregister wordt bijgehouden met behulp van een vastgesteld werkproces "bijhouden verwerkingsregister". De afdelingsmanagers zijn inhoudelijk verantwoordelijk voor de registratie van hun processen in het verwerkingsregister. Ook voor het melden van eventuele veranderingen binnen de processen. Administratief wordt het register bijgehouden door een juridisch adviseur privacy, met de FG als achtervang.

Data protection impact assessment (DPIA)
Als een verwerking mogelijk een hoog risico heeft voor de betrokkene, moet de gemeente een beoordeling uitvoeren van het effect van een verwerking van persoonsgegevens. De gemeente voert in dat geval een risicoanalyse uit op de verwerking van persoonsgegevens (ook wel DPIA genoemd). Als uit de DPIA blijkt dat er inderdaad hoge risico's zijn verbonden aan de verwerking, moet de gemeente voldoende maatregelen nemen om de risico's te verminderen. Als het niet lukt om (voldoende) maatregelen te nemen om dit risico te verminderen, dan moet de gemeente met de AP overleggen, voordat zij met de verwerking start. Dit wordt een voorafgaande raadpleging genoemd. De DPIA's worden begeleid door een juridisch adviseur privacy. De afdelingsmanager blijft verantwoordelijk voor de keuze voor welke verwerking een DPIA wordt uitgevoerd en voor het uitvoeren van de maatregelen die (mogelijk) uit de DPIA komen.

Functionaris gegevensbescherming (FG)
De gemeente is een overheidsinstantie die structureel en op grote schaal persoonsgegevens verwerkt, waaronder bijzondere persoonsgegevens. De gemeente is daarom verplicht een FG aan te stellen. De FG is de onafhankelijke intern toezichthouder en heeft een adviserende, informerende en toezichthoudende taak. Dit betekent dat de FG toeziet op alle verwerkingen van persoonsgegevens. De FG informeert de gemeenteraad en het college van burgemeester en wethouders.

PDCA Cyclus
De gemeente streeft ernaar om rondom de verwerking van persoonsgegevens in control te zijn en daarover op professionele wijze verantwoording af te leggen. In control betekent in dit verband dat de gemeente weet welke maatregelen genomen zijn ten aanzien van de verwerking van persoonsgegevens, dat er een planning is van de maatregelen die nog niet genomen zijn en dat dit geheel verankerd is in een Plan-Do-Check-Act-cyclus.

De PDCA-cyclus wordt dubbelzijdig doorlopen waarbij de uitvoering (blauwe cirkel) zich bevindt in de dagelijkse operationele werkzaamheden binnen de werkprocessen en de governance (groene cirkel) zorgt voor de strategische (bij)sturing. De omloopsnelheid van de 2 cirkels kan onderling verschillen, maar de beide cirkels vormen samen één geheel en hebben onderling afstemming nodig.



Bewustwording
Beleid en maatregelen zijn niet voldoende om risico's op het terrein van het verwerken van persoonsgegevens uit te sluiten. Het is noodzakelijk om het bewustzijn in de gemeentelijke organisatie voortdurend aan te scherpen, zodat kennis van risico's wordt verhoogd en (veilig en verantwoord) gedrag om persoonsgegevens zorgvuldig te verwerken wordt aangemoedigd. Iedere medewerker wordt geïnformeerd over het zorgvuldig omgaan met persoonsgegevens, bijvoorbeeld via de eigen werkprocessen, werkinstructies en protocollen. Dit gebeurt passend binnen de context van en bij het domein waarbinnen die worden verwerkt.

Triage
Aparte aandacht wordt besteed aan het proces rond de triage. Triage speelt op casusniveau en vraagt van de medewerker om een professionele inschatting te maken wat de ernst van de problematiek is en welke verwerking van persoonsgegevens daarbij wenselijk is. Vooral bij multi-probleemsituaties in het sociaal domein kan er opschaling nodig zijn waardoor meer persoonsgegevens worden verwerkt of persoonsgegevens met anderen worden gedeeld. Deze werkwijze is gerechtvaardigd omdat de verwerking van persoonsgegevens noodzakelijk is voor het uitvoeren van wettelijke taken binnen het sociaal domein en plaatsvindt binnen de kaders van de AVG, waaronder de beginselen van proportionaliteit en subsidiariteit.

Medewerkers bepalen per casus het doel waarvoor de gegevensverwerking noodzakelijk is. Daarnaast bepalen zij of er niet bovenmatig gegevens worden verwerkt of dat gegevens niet op een andere, minder ingrijpende manier, kunnen worden verwerkt. Van belang is dat deze afweging door de medewerker wordt vastgelegd. Triagemomenten worden benoemd in het werkproces. De grondslag voor triage is voor de gemeente het algemeen belang/openbaar gezag. Dit betekent concreet dat het toepassen van triage beperkt is tot die werkprocessen waarbij het uitwisselen van persoonsgegevens binnen en buiten de eigen organisatie terug te voeren is op een wettelijke bevoegdheid/taak.

Geautomatiseerde verwerkingen
Onder geautomatiseerde verwerkingen verstaat de gemeente het gebruik van elektronische middelen om gegevens te verwerken. voorbeelden zijn profilering en algoritmen. Als de gemeente hier gebruik van wil maken, wordt vooraf bepaald of dit volgens de AVG kan plaatsvinden en wordt de verwerking opgenomen in het verwerkingsregister.

Voor onderzoeken zal de gemeente, als dat in het kader van het onderzoek gewenst is, gebruik maken van Big data en tracking wanneer de zo verzamelde gegevens niet te herleiden zijn tot een natuurlijke persoon. In die gevallen waarin de gemeente gebruik maakt van Big data onderzoeken en tracking, dan

verstrekt de gemeente vooraf informatie op de gemeentelijke website. Data-analyse (zoals voor beleidsinformatie) is een onderwerp dat in opkomst is, ook bij de gemeente. De gemeente zorgt ervoor dat dergelijk gebruik van data wordt afgewogen en volgens de AVG plaatsvindt.

Opslag van persoonsgegevens
Persoonsgegevens worden binnen de gemeente (vrijwel) altijd digitaal opgeslagen. Voor opslag van gegevens heeft de gemeente een eigen, afgeschermd netwerk. Via sommige applicaties werken we (gedeeltelijk) in de cloud. De manier waarop de gemeente haar netwerk en gegevens beveiligd is in overeenstemming met de gemeentelijke beveiligingsnormen (BIO)

Hoofdstuk 3: Wet politiegegevens (Wpg) beleid

3.1 Inleiding

Net als bij de verwerking van persoonsgegevens onder de AVG, verwerkt de gemeente ook politiegegevens in het kader van haar handhavings- en opsporingstaken. Deze gegevens worden voornamelijk verwerkt door buitengewoon opsporingsambtenaren (boa's).

De gemeente vindt het belangrijk dat ook binnen dit specifieke domein zorgvuldig, rechtmatig en transparant met persoonsgegevens wordt omgegaan. Inwoners moeten erop kunnen vertrouwen dat hun gegevens veilig worden verwerkt, ongeacht of dit gebeurt in het kader van dienstverlening of opsporing.

De verwerking van politiegegevens valt onder de Wet politiegegevens (Wpg) en de daarbij behorende regelgeving, waaronder het Besluit politiegegevens (Bpg), het Besluit politiegegevens buitengewoon opsporingsambtenaren en de Regeling periodieke audit politiegegevens.

Deze wetgeving kent deels andere en meer specifieke verplichtingen dan de AVG. Zo gelden binnen de Wpg bijvoorbeeld specifieke regels over bewaartermijnen, logging, de rechten van betrokkenen en verplichte interne en externe audits. Met dit hoofdstuk geeft de gemeente aan hoe zij invulling geeft aan deze aanvullende verplichtingen binnen het bredere gemeentelijke kader van privacy, informatiebeveiliging en integriteit. De uitgangspunten uit hoofdstuk 2 van dit beleid (zoals rechtmatigheid, transparantie en doelbinding) zijn hierbij onverkort van toepassing.

3.2 Doel

Met dit hoofdstuk geeft de gemeente richting aan de manier waarop zij binnen het kader van de Wpg omgaat met politiegegevens. Het doel is dat deze gegevens op een zorgvuldige, rechtmatige en veilige manier worden verwerkt, overeenkomstig met de gemeentelijke visie op privacy zoals beschreven in hoofdstuk 2.

Doel van het privacybeleid Wpg is onder andere dat de boa's:
- Zich ten volle bewust zijn van de noodzaak om zorgvuldig en op rechtmatige wijze om te gaan met politiegegevens.
- De rechten van betrokkenen respecteren en werken volgens de vastgestelde procedures.
- Het vertrouwen van betrokkenen in de overheid niet beschamen.
- Gedrag vertonen dat past bij goed werknemerschap.
- De kans op financiële- en imagoschade minimaliseren.

Hiermee vormt de uitvoering van de Wpg een integraal onderdeel van het gemeentelijke privacybeleid.

3.3 Wpg kader en verplichtingen

De Wpg kent grotendeels dezelfde uitgangspunten als de AVG, maar stelt op onderdelen aanvullende en specifiekere eisen. De gemeente zorgt ervoor dat ook deze verplichtingen structureel zijn ingebed in het privacy- en informatiebeveiligingsbeleid.

Toepassingsgebied
Boa's van de gemeente kunnen bij het uitvoeren van hun taken te maken hebben met zowel de AVG als de Wpg. Bij iedere verwerking wordt vastgesteld onder welk wettelijk kader de gegevens vallen. Deze scheiding wordt geborgd in de processen en systemen die de gemeente gebruikt, zodat de verwerking zowel praktisch als juridisch correct plaatsvindt.

Scheiding en documentatie van gegevens
Binnen Wpg-verwerkingen wordt onderscheid gemaakt tussen:
- gegevens die op feiten zijn gebaseerd en gegevens die op persoonlijk onderdeel berusten;
- betrokkene zoals verdachten, slachtoffers, derden en veroordeelden.

Feiten	Persoonlijk oordeel	Betrokkenen
•Objectieve informatie over een gebeurtenis •Bijv. datum, locatie, type incident	•Interpretatie of subjectieve beoordeling •Bijv. beoordeling van gedrag/intentie	•Type personen op wie gegevens betrekking hebben •Bijv. verdachten, slachtoffers, derden, veroordeelden

De doelen van onderzoeken, verstrekking of doorgifte, afwijzing van inzageverzoeken, meldingen van inbreuken en doorgiften aan derden worden zorgvuldig gedocumenteerd, inclusief datum en tijd, ontvanger, reden(en) en doorgegeven gegevens. Ook wordt melding gedaan van gemeenschappelijke verwerkingen aan de Autoriteit Persoonsgegevens (AP). Hiermee voldoet de gemeente aan de wettelijke documentatieplicht en aan haar eigen transparantieverplichting.

Specifieke Wpg-verplichtingen
Naast de uitgangspunten van de AVG gelden voor boa's de volgende aanvullende verplichtingen:
- Het delen van politiegegevens met andere opsporingsambtenaren die deze nodig hebben voor hun werk.
- Logging van invoer, raadpleging, wijziging, verstrekking, combineren en vernietiging van politiegegevens in geautomatiseerde systemen.
- Specifieke eisen aan informatiebeveiliging volgens het Bpg.
- Periodieke interne en externe audits om naleving van de wet te waarborgen.

Door deze verplichtingen te borgen in applicaties en systemen wordt gegarandeerd dat de Wpg-voorschriften consequent worden toegepast en dat boa's kunnen werken binnen een gecontroleerd en transparant kader.

Verwerkingsregister
Net als de AVG verplicht de Wpg tot het bijhouden van een verwerkingsregister. Wel zijn er enkele verschillen die hierna met een (*) zijn aangeduid. Het verwerkingsregister in het kader van de Wpg moet het volgende bevatten:
- De naam en de contactgegevens van de verwerkingsverantwoordelijke, de gezamenlijk verwerkingsverantwoordelijken en de functionaris voor gegevensbescherming;
- De doelen van de verwerking;
- De categorieën van ontvangers aan wie politiegegevens zijn of zullen worden verstrekt, met inbegrip van ontvangers in derde landen of internationale organisaties;
- Een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
- In voorkomend geval: het gebruik van profilering. (*)
- In voorkomend geval: de categorieën van doorgiften van politiegegevens aan een derde land of een internationale organisatie.
- Een aanwijzing van de rechtsgrondslag van de verwerking, met inbegrip van doorgiften, waarvoor de politiegegevens bedoeld zijn. (*)
- Zo mogelijk: de beoogde termijnen waarbinnen de verschillende categorieën van gegevens worden verwijderd of vernietigd.
- Zo mogelijk: een algemene beschrijving van de technische en organisatorische maatregelen ter beveiliging.
- De toekenning van de autorisaties. (*)

Informatiebeveiligingsbeleid
Voor alle Wpg-activiteiten gelden dezelfde beveiligingsprincipes als voor andere gemeentelijke verwerkingen. De gemeente handelt daarbij volgens het Informatiebeveiligingsbeleid en de Baseline Informatiebeveiliging Overheid (BIO). Daarbij worden aanvullende beveiligingseisen uit het Bpg toegepast, zoals strengere toegangsbeperkingen en periodieke controles van autorisaties.

Toezicht en audit
De Wpg verplicht gemeenten tot periodieke controle op de naleving van de wet.
- Jaarlijks voert de gemeente interne audits uit;
- Eens per vier jaar wordt een externe audit uitgevoerd, waarvan de resultaten worden gerapporteerd aan de AP.

Bij geconstateerde tekortkomingen stelt de gemeente binnen drie maanden een verbeterplan op, waarna binnen een jaar een hercontrole plaatsvindt. Dit sluit aan op de gemeentelijke PDCA-cyclus (Plan-Do-Check-Act) zoals beschreven in hoofdstuk 2.

FG en bevoegd functionaris

Net als de AVG verplicht artikel 36 van de Wpg tot het aanstellen van de FG. Het is mogelijk dat meerdere organisaties samen één FG aanwijzen. De FG wordt door de verwerkingsverantwoordelijke tijdig en naar behoren betrokken bij alle aangelegenheden die verband houden met de bescherming van politiegegevens. De FG stelt jaarlijks een verslag op van zijn bevindingen.

De bevoegd functionaris
De boa's die opgeleid zijn voor het uitvoeren van de taak bevoegd functionaris zijn verantwoordelijk voor het uitvoeren van deze taak. Zij zijn de 'hoeder' van de gegevens die onder artikel 9 Wpg worden verwerkt. Deze functionaris is beschreven in artikel 2:10, eerste lid, van het Besluit politiegegevens (Bpg). Het moet een persoon zijn met voldoende kennis en vaardigheden over dit type gegevens. Deze functionaris beslist bijvoorbeeld wie er toegang mag hebben tot deze gegevens en of ze verstrekt kunnen worden aan een samenwerkingspartner. Iedere artikel 9-verwerking dient een bevoegd functionaris (BF) te hebben. De bevoegd functionaris heeft onder andere de volgende taken:
- het doel van de artikel 9-verwerking omschrijven en vastleggen;
- het autoriseren van personen voor de betreffende verwerking;
- bepalen of gegevens voor andere doeleinden mogen worden gebruikt;
- zorgen dat voor alle gegevens de herkomst en wijze van verkrijgen wordt vastgelegd;
- bewaken dat gegevensrechtmatig worden verkregen en verwerkt.

Rechten van betrokkenen
De rechten van betrokkenen onder de AVG staan beschreven onder hoofdstuk 2 van dit beleid. Op hoofdlijnen zijn deze rechten op grond van de Wpg gelijkluidend. Het proces "verzoek privacyrechten" op grond waarvan betrokkenen verzoeken kunnen indienen om rechten uit te oefenen is ook van toepassing op de Wpg.

Het bewaren van politiegegevens
Ook politiegegevens worden niet langer bewaard dan de minimale tijd die nodig is, zoals vereist door de toepasselijke wet- en regelgeving, of voor de doeleinden waarvoor deze zijn verwerkt. Politiegegevens dienen na verwijdering nog maximaal vijf jaar te worden bewaard. Daarna, of binnen deze periode van vijf jaar (afhankelijk van welke bewaartermijn geldt) dient definitieve vernietiging plaats te vinden. Indien van cultureel of historisch belang kan worden afgezien van vernietiging van de gegevens. Er wordt dan aan de bewaareisen als genoemd in de Archiefwet voldaan.

Alle politiegegevens worden gelabeld in artikel 8, 9 en 13 informatie. Voor elk label is de bewaartermijn conform de wettelijke bepaling geconfigureerd, zodat geborgd wordt dat deze politiegegevens niet langer worden bewaard dan de minimale tijd die nodig is, zoals vereist door de toepasselijke wet- en regelgeving, of voor de doeleinden waarvoor deze zijn verwerkt.

Het ter beschikking stellen en verstrekken van politiegegevens
De Wpg maakt een onderscheid tussen het ter beschikking stellen van politiegegevens en het verstrekken ervan. Het ter beschikking stellen van politiegegevens houdt in dat deze in principe worden gedeeld met eenieder die de gegevens nodig heeft voor de uitoefening van zijn taak. Bij dit 'need to know'-principe dient altijd een noodzakelijkheids-, proportionaliteits- en subsidiariteitsafweging te worden gemaakt. Het ter beschikking stellen voltrekt zich dus binnen het Wpg-domein.

Bij het verstrekken van politiegegevens gaat het om het delen van gegevens buiten het Wpg-domein. In dat geval moet zijn geborgd dat politiegegevens alleen worden verstrekt aan personen of instanties buiten het Wpg-domein, voor zover dit noodzakelijk is voor de doeleinden zoals deze in de Wpg en het Bpg zijn genoemd. Geborgd moet ook zijn dat wanneer gegevens verstrekt worden, er wordt voldaan aan de documentatieplicht en dat de verstrekking alleen plaatsvindt in overeenstemming met het bevoegd gezag indien dit vereist is in de wet. Het gaat dan bijvoorbeeld om verstrekkingen aan de burgemeester, een toezichthouder, een advocaat of een functionaris in het kader van de Wet Bibob.

Het melden van datalekken
De datalekprocedure onder de AVG staan beschreven in hoofdstuk 2 van dit beleid. Deze procedure is ook van toepassing op de Wpg. Op hoofdlijnen zijn deze rechten op grond van de Wpg gelijkluidend. Specifiek voor de Wpg geldt nog het volgende:
Op deze mededelingsplicht zijn enkele uitzonderingen van toepassing, onder andere als de mededeling achterwege moet blijven ter vermijding van belemmering van de gerechtelijke onderzoeken of procedures en ter vermijding van nadelige gevolgen voor de voorkoming, de opsporing, het onderzoek en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen.

Training en bewustwording
Het zorgvuldig omgaan met persoonsgegevens is enerzijds een kwestie van het organiseren van een goede informatieveiligheid en het zorgvuldig inrichten van werkprocessen, anderzijds is het een zaak

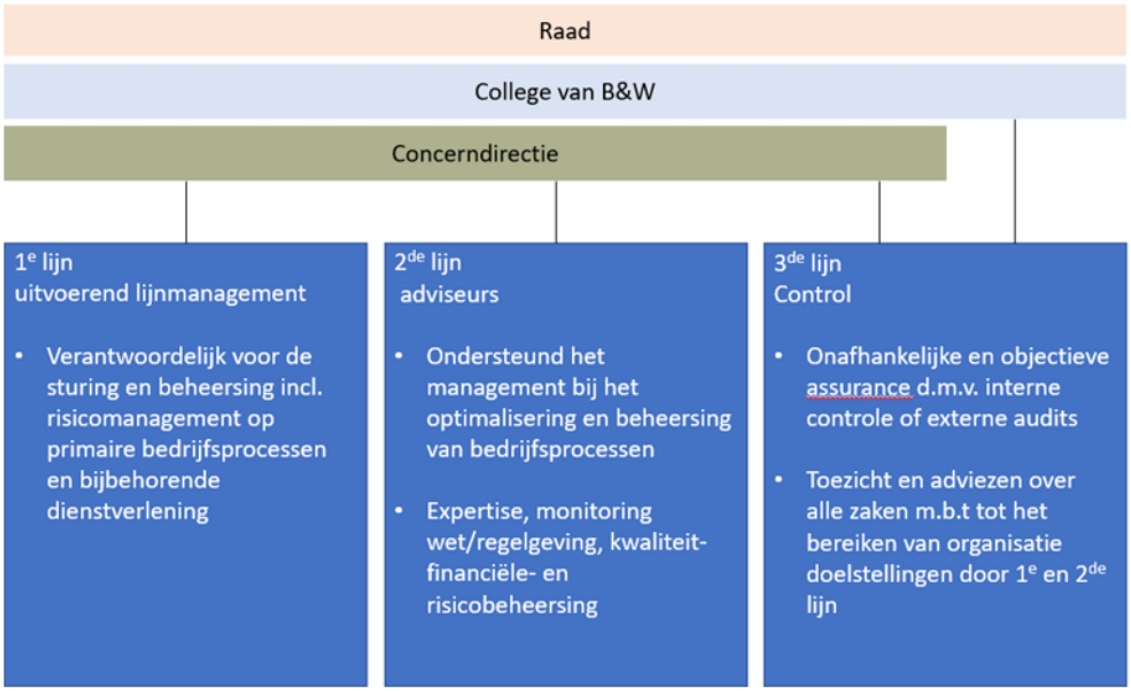
van bewustwording bij de boa's. Het bewustzijn wordt voortdurend aangescherpt, zodat kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd.

Elke nieuwe medewerker met Boa bevoegdheid moet daarom verplicht een Wpg training doorlopen. Daarvan wordt een notitie vastgelegd in het personeelsdossier. Boa's die al in dienst zijn en deze training nog niet hebben doorlopen, doorlopen deze training alsnog. Daarnaast is er in ieder geval jaarlijks aanvullend aandacht voor bewustwording rondom de omgang met politiegegevens. Dit kan bijvoorbeeld in de vorm van een aanvullende training, een bijeenkomst over een specifiek Wpg-onderwerp of in de vorm van een toets. Ook van deelname aan deze initiatieven wordt een notitie in het personeelsdossier gemaakt.

Hoofdstuk 4: Taken en Verantwoordelijkheden

Het Three Lines model
Het Three lines model is een generiek model voor organisaties wat helpt bij de governance op verantwoordelijkheden en rollen. Vanwege de herkomst van risicomanagement is het ook geschikt voor de benodigde organisatie op privacy. Het brengt bewust een scheiding van taken en verantwoordelijkheden om duidelijkheid te creëren en de kans op conflicterende taken en daarmee onbevoegd/onbedoeld wijziging van bedrijfsmiddelen te voorkomen.

Het lijnmanagement is verantwoordelijk voor privacy binnen de eigen processen. De tweede lijn van adviseurs ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel door een Functionaris Gegevensbescherming van een objectief en onafhankelijk oordeel voorzien met mogelijkheden tot verbetering in de 1e en 2de lijn.



4.1 Verdeling van verantwoordelijkheden
De verdeling van verantwoordelijkheden en de daaruit voortvloeiende taken wordt per 'Line' beschreven.

4.2 De eerste lijn: verantwoordelijkheid en uitvoering
De afdelingsmanagers zijn eindverantwoordelijk voor de naleving van de privacywetgeving binnen de afdeling. En ook voor de uitvoering van het privacybeleid. De directie stuurt dit aan. Het College is eindverantwoordelijk voor privacy en informatiebeveiliging en legt hierover verantwoording af aan de raad.

Afdelingsmanagers
De afdelingsmanagers hebben de volgende taken en verantwoordelijkheden:

- Actueel houden van de verwerkingen van persoonsgegevens zoals opgenomen in het verwerkingsregister;
- Betrekken van de juridisch adviseur privacy bij nieuwe of gewijzigde verwerkingen;
- Toetsen bij een nieuwe verwerking of wijziging in een bestaande verwerking of een Data Protection Impact Assessement (DPIA) verplicht is, aanwezig zijn bij de DPIA en opvolging geven aan de resultaten van de DPIA;
- Afsluiten, beheren en actualiseren van verwerkersovereenkomsten;
- Verantwoordelijk voor autorisatie en intrekken van de autorisatie van medewerkers die persoonsgegevens verwerken;
- Verantwoordelijk voor bewustwording voor privacy bij medewerkers binnen de eigen afdeling;
- Het belang van informatieveiligheid en privacy (periodiek) onder de aandacht brengen van de afdeling;
- Uitvoeren van het beleid ten aanzien van de verwerking van persoonsgegevens die onder zijn of haar verantwoordelijkheid vallen;
- Archivering;
- Melden incidenten met betrekking tot de veiligheid van informatie en/of persoonsgegevens.

Een deel van de bevoegdheden en verantwoordelijkheden op het terrein van de privacy die ligt bij het college van B&W is gemandateerd naar de afdelingsmanagers.

College van B&W
Het college van B&W heeft de volgende taken en verantwoordelijkheden:

- Stelt het privacybeleid vast;
- Geeft sturing aan privacy beleidsvoering en legt verantwoording af over privacy beleidsvoering aan de FG;
- Evalueert de toepassing en werking van het privacybeleid op basis van de rapportage van de FG;
- Een van de wethouders heeft privacy in zijn of haar portefeuille, is daar verantwoordelijk voor en fungeert als vast aanspreekpunt voor privacy-problemen.

4.3 De tweede lijn: Advisering
De tweede lijn is het eerste aanspreekpunt voor de organisatie rondom privacy gerelateerde vraagstukken en heeft een monitorende en ondersteunende functie rondom het naleven en uitvoeren van het privacybeleid.

Juridisch adviseur privacy
De juridisch adviseur privacy heeft de volgende taken en verantwoordelijkheden:
- Opstellen privacybeleid, modellen, formats en standaard-overeenkomsten. Waaronder onder andere de verwerkersovereenkomst en de overeenkomst voor uitwisseling van persoonsgegevens;
- Monitort en ondersteunt het (laten) registreren van verwerkingen in het verwerkingsregister en het (laten) registreren van relevante wijzigingen;
- Het beoordelen van de verwerking van persoonsgegevens tegen de achtergrond van de kaders van de (Europese)privacywetgeving. Adviseren bij wijzigingen in procesuitvoering en bedrijfsvoering en de toepassing van een privacy impact assessment (DPIA);
- Adviseren bij programma's en projecten waarvan het resultaat gevolgen kan hebben voor de wijze van verwerking van persoonsgegevens;
- Adviseren over verwerkersovereenkomsten en privacybepalingen in overige documenten;
- Coördineren van verzoeken over verwerking van persoonsgegevens (zogenaamde AVG-verzoeken/verzoeken met betrekking tot de rechten van betrokkenen) en behandelen van concernbrede verzoeken;
- Zorgen voor processen voor de behandeling van AVG-verzoeken, datalekken, het begeleiden van DPIA's en bijhouden van het register van verwerkingsactiviteiten;
- Bijdragen aan privacybewustzijn;
- Adviseren met betrekking tot vraagstukken over de verwerking van persoonsgegevens;
- Beheren en onderhouden van de standaarddocumenten voor verwerkersovereenkomsten, convenanten en reglementen;
- Adviseren en ondersteunen bij het besluitvormingsproces en het afsluiten van verwerkersovereenkomsten, convenanten en de vaststelling van reglementen;
- Het afhandelen van datalekken.

4.4 De derde lijn: Controle
Op basis van de AVG is het aanstellen van een FG verplicht voor de gemeente. De FG is verantwoordelijk voor het toezicht op de naleving van de AVG. De FG heeft een onafhankelijke adviserende en toezichthoudende positie in de organisatie.

Functionaris voor Gegevensbescherming
De FG heeft de volgende taken en verantwoordelijkheden in de gehele organisatie van de gemeente:

- Informeren en adviseren van de gemeente over de verplichtingen volgens de AVG;
- Toezien op naleving van AVG en andere EU wet- en regelgeving en nationale bepalingen over gegevensbescherming;
- Toezien op naleving van het gemeentelijke beleid over de verwerking van persoonsgegevens;
- Eerste aanspreekpunt voor de Autoriteit Persoonsgegevens (AP) en kan afstemmen met de AP;
- Toezien op toewijzing van verantwoordelijkheden, bewustmaking en opleiding van medewerkers;
- Adviseren over vraagstukken over de verwerking van persoonsgegevens;
- Adviseren over veiligheidsincidenten met persoonsgegevens;
- Adviseren over de DPIA en het toezien of de uitvoering daarvan in overeenstemming is met de AVG. Toezien op de opvolging van maatregelen en acties uit DPIA's.
- Toezien op en adviseren over de afhandeling van vragen en klachten over het gebruik van persoonsgegevens;
- Adviseren en ondersteunen bij het opstellen van privacynormen, procedure-, -beleid, -regelingen of –gedragscodes;
- Rechtstreeks aan de directie, het college van B&W en de raad rapporteren.

Burgemeester en wethouders voornoemd,

Maartje Schlebusch
de secretaris,

René Verhulst
de burgemeester,