BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 1384

15 juni 2026

Officiële uitgave van de gemeenschappelijke regeling ABG-organisatie

Privacybeleid AVG en Wpg 2026-2029 ABG-organisatie

Besluit:
Het Privacybeleid ABG 2026-2029 vast te stellen.

1. Inleiding

1.1 Algemeen

De gemeente werkt met (persoons)gegevens van burgers, ondernemers, medewerkers en (keten)partners. Deze gegevens verzamelt de gemeente voor het goed kunnen uitvoeren van de gemeentelijke wettelijke taken. Denk hierbij onder andere aan taken in het sociaal domein, openbare orde en veiligheidsdomein of voor burgerzaken. Of wanneer we bezig zijn met onze interne bedrijfsvoering of de veiligheid van onze organisatie en onze medewerkers. Om deze taken goed te volbrengen is het noodzakelijk dat de gemeente persoonsgegevens verwerkt. De burgers 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 complexer en noodzakelijker. De ABG-organisatie 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)[1] en de Wet Politie Gegevens (hierna te noemen: Wpg).

1.2 Doel, ambitie en visie

Het doel van de gemeente is om compliant aan privacywetgeving te worden en blijven, het verhogen van de privacy bewustwording en verdere professionalisering van de privacy-organisatie binnen de gemeente.

Met dit beleid wordt de ambitie gesteld om binnen 4 jaar op “volwassenheidsniveau 3” te komen: het aantoonbaar voldoen aan privacywetgeving[2] . Om dit goed te borgen en vast te kunnen stellen wordt er een inventarisatie gemaakt[3]. Na het eerste jaar zal worden geëvalueerd wat de impact is van de privacywetgeving op het takenpakket van de organisatie.

Goed privacymanagement is risicogestuurd en is noodzakelijk voor het goed functioneren van de gemeente en is de basis voor het beschermen van rechten van burgers en bedrijven. 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. Zowel medewerkers als management worden door middel van voorlichting geïnformeerd.

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 beoogt dit privacybeleid taken en verantwoordelijkheden op het gebied van de bescherming van persoonsgegevens helder af te bakenen. Een derde doel van dit beleidsstuk is dat dit kader de basis vormt voor nadere uitwerkingen zoals operationeel privacybeleid, procedures en werkinstructies.

Verantwoordelijkheid van iedere werknemer

Iedereen werkzaam binnen de gemeente[4] 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 de voorschriften van dit privacybeleid worden opgevolgd en actief worden uitgedragen.

1) *Gebruikte definities van art. 4 AVG hebben in dit beleidsdocument dezelfde betekenis.*
2) *Methodiek van Centrum Informatiebeveiliging en Privacybescherming (CIP)*
3) *Bijvoorbeeld https://www.cip-overheid.nl/producten-en-diensten/privacyselfassessmenttool*
4) *Hiermee worden ook de werknemers van de ABG-organisatie bedoeld.*

1.3 Reikwijdte en plaats in het gemeentelijk kader

Dit beleid is van toepassing op alle gemeentelijke processen waarin persoonsgegevens worden verwerkt, met uitzondering van de werkzaamheden van de raad en griffie[5]. Het beleid is voor alle 3 ABG-gemeenten gelijk en zo ook voor de ABG-organisatie (zie ook paragraaf 1.4).

Het beleid betreft zowel digitale informatie als fysieke documenten, en geldt voor alle medewerkers, externe partijen en systemen die betrokken zijn bij de verwerking van gemeentelijke gegevens.

De gemeente verzamelt en gebruikt persoonsgegevens van inwoners, ondernemers, leveranciers, medewerkers en andere natuurlijke personen (hierna te noemen: betrokkenen).

Dit privacybeleid is van toepassing op:
1. Alle gemeentelijke afdelingen en diensten en de ABG-organisatie die namens de gemeente(n) handelt;
2. Verwerkers en leveranciers die namens de gemeente en de ABG-organisatie gegevens verwerken;
3. Persoonsgegevens die zijn opgeslagen in computersystemen en in papieren dossiers of archieven.

1.4 Relatie tot ander beleid

Dit strategisch en tactische beleid wordt verder uitgewerkt in een *operationeel* privacybeleid voor zowel de AVG als separaat voor de Wpg. Het operationele beleid richt zich op de dagelijkse praktijk en werkprocessen.

Naast dit door het college vastgestelde privacybeleid is een informatiebeveiligingsbeleid vastgesteld. Hierin zijn maatregelen opgenomen om de beschikbaarheid, integriteit en vertrouwelijkheid van (persoons)gegevens te garanderen. Informatiebeveiliging is een randvoorwaarde voor de bescherming van persoonsgegevens. Het gemeentelijke privacybeleid kan daarom niet los worden gezien van het gemeentelijke informatiebeveiligingsbeleid.

1.5 Vaststelling, inwerkingtreding en evaluatie

Het beleid is voor alle ABG-gemeenten gelijk. Vanwege wetgeving moet dit beleid worden vastgesteld door de verwerkingsverantwoordelijke(n). In het geval van de ABG-organisatie zijn dit de 3 colleges[6] en het ABG-bestuur[7].

Dit privacybeleid is vastgesteld op 4 mei 2026 door het bestuur van de ABG-organisatie.

Het beleid wordt (minimaal) iedere 2 jaar geëvalueerd en waar nodig geactualiseerd op basis van:
- Wijzigingen in wet- en regelgeving (zoals AVG en Wpg);
- Nieuwe dreigingen en risico's;
- Bevindingen uit audits, incidenten en evaluaties;
- Technologische ontwikkelingen;

De herziening wordt gecoördineerd door de Privacy Officer, in samenwerking met de Functionaris Gegevensbescherming, Chief Information Security Officer en relevante beleidsafdelingen.

2. Principes voor de verwerking van persoonsgegevens

De AVG en Wpg zijn gebaseerd op een aantal overeenkomstige principes voor de verwerking[8] van persoonsgegevens. De gemeente onderschrijft deze principes en stelt zich ten doel persoonsgegevens slechts te verwerken in overeenstemming met deze principes.[9]

2.1 Rechtmatige grondslag

Persoonsgegevens worden door de gemeente slechts in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze verwerkt. Dit betekent onder meer dat verwerkingen slechts plaatsvinden indien hiervoor een rechtmatige verwerkingsgrondslag bestaat. Veelal vloeit de grondslag voor een verwerking bij een gemeente voort uit een wet (wettelijke verplichting) of een publiekrechtelijke taak.

5) *Dit beleid wordt separaat uitgewerkt.*
6) *Voor zowel de taken die namens het college worden uitgevoerd, alsook de taken onder verantwoordelijkheid van de burgemeester op gebied van veiligheid en openbare orde.*
7) *Als verwerkingsverantwoordelijke voor bedrijfsvoering en HR.*
8) *Zie art. 4 AVG of https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/privacy-en-persoonsgegevens/verwerken-van-persoonsgegevens*
9) *Waar in dit privacybeleid "persoonsgegevens" is geschreven, kunnen ook politiegegevens onder worden verstaan.*

2.2 Doelbinding
De gemeente verwerkt persoonsgegevens voor zeer uiteenlopende doeleinden. Zonder doel mogen persoonsgegevens niet worden verwerkt. De verwerking van persoonsgegevens vindt plaats op een wijze 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).

Verdere verwerking
Persoonsgegevens kunnen in bepaalde gevallen worden verwerkt voor andere doelen dan waarvoor deze persoonsgegevens in eerste instantie zijn verzameld. Daarbij geldt onder andere dat de twee doelen aan elkaar verwant (verenigbaar) moeten zijn, er zich geen nadelige effecten voor de betrokkenen voordoen, dan wel 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.
De Wpg maakt onderscheid tussen ter beschikking stellen en het verstrekken van politiegegevens. Dit wordt nader uitgewerkt in het operationeel Wpg-beleid.

2.3 Minimale gegevensverwerking
Gegevens mogen alleen worden verwerkt als dit noodzakelijk is om het doel te bereiken. Als dit 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 voor de betrokkene *minder inbreukmakende wijze* kan worden verwezenlijkt dan kiest de gemeente bij voorkeur voor die mogelijkheid. Dit laatste wordt het subsidiariteit genoemd.

Het verwerken van politiegegevens vallen met de Wpg onder een ander regime dan de gegevens die onder de AVG vallen. In het kader van minimale gegevensverwerking en subsidiariteit zal de gemeente dan er ook voor kiezen om standaard het AVG-regime te hanteren en alleen op te schalen naar het Wpg-regime wanneer dat wettelijk is verplicht of noodzakelijk om het doel te behalen. In welke gevallen er wordt opgeschaald naar Wpg is uitgewerkt in nadere instructies.

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 draagt er zorg voor 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.

2.4 Juiste en actuele gegevens
De gemeente zorgt ervoor dat alleen persoonsgegevens worden verwerkt die accuraat, toereikend, ter zake dienend en niet bovenmatig 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.

2.5 Gegevens worden niet langer bewaard dan nodig
De gemeente is een overheidsdienst. De overheid moet documenten archiveren, onder andere in het kader van historisch belang en rechtszekerheid. Deze verplichting is vastgelegd in de Archiefwet en nader uitgewerkt in de gemeentelijke selectielijsten die de Vereniging van Nederlandse Gemeenten voor de gemeente opstelt en herziet. Voor de Wpg gelden bewaartermijnen die voortvloeien uit de Wpg.

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.

2.6 Integriteit en vertrouwelijkheid
Zoals omschreven in paragraaf 1.4 neemt de gemeente passende technische en organisatorische maatregelen om persoonsgegevens, waaronder bijzondere categorieën van persoonsgegevens, te beschermen tegen verlies, ongeoorloofde toegang, ongeautoriseerde wijziging of andere vormen van onrechtmatige verwerking. De gemeente handelt daarbij in overeenstemming met het geldende informatiebeveiligingsbeleid.

Veilig omgaan met persoonsgegevens vereist een integere houding zoals ook van medewerkers verwacht wordt. Iedere (nieuwe) medewerker wordt geïnformeerd over het zorgvuldig omgaan met persoonsgegevens, bijvoorbeeld via instructies. Daarnaast legt iedere ambtenaar een ambtseed af. Integriteit, zoals verwoord in de gedragscode voor ambtenaren, is hiervan een onderdeel. Ook voor andere medewerkers dan de ambtenaren binnen de gemeente geldt de geheimhoudingsplicht. Daarnaast geldt dat elke nieuwe medewerker dat zij een Verklaring Omtrent Gedrag (VOG) moeten overleggen voorafgaand aan de start van de werkzaamheden.

Vanuit de Wpg worden er een aantal extra eisen aan gegevens gesteld, welke worden opgenomen in het operationeel Wpg-beleid. Voorbeelden hiervan zijn maatregelen rondom het loggen van de politiegegevens en het aanstellen van een Bevoegd Functionaris voor bepaalde verwerkingen.

3. Waarborgen voor gegevensbescherming

3.1 Verantwoordingsplicht

De AVG en Wpg bevatten beide een verantwoordingsplicht, dat inhoudt dat de gemeente actief aan de toezichthouder moeten kunnen aantonen dat zij voldoet aan de gestelde privacyregels. Dit vereist documentatie, zoals privacybeleid, verwerkersovereenkomsten en een verwerkingsregister, evenals het nemen van passende technische en organisatorische beveiligingsmaatregelen.

De Autoriteit Persoonsgegevens houdt toezicht op de naleving van de privacyregels in Nederland. Daarnaast beschikt de gemeente over een interne toezichthouder: de Functionaris Gegevensbescherming. De Functionaris Gegevensbescherming ziet erop toe dat de AVG en de Wpg intern wordt nageleefd. De gemeente stelt voldoende middelen ter beschikking aan de Functionaris Gegevensbescherming om het toezicht adequaat uit te kunnen voeren.

3.2 Verwerkingsregister

De gemeente beschikt over een verwerkingsregister, waarin alle verwerkingen van persoonsgegevens gedocumenteerd zijn en inzichtelijk zijn gemaakt, zowel voor de AVG als de Wpg. Wanneer een gegevensverwerking binnen een proces structureel wijzigt, wordt het verwerkingsregister zo snel mogelijk bijgewerkt.

3.3 Risicoanalyses en DPIA's

Als een verwerking mogelijk een hoog risico inhoudt voor een betrokkene, moet de gemeente een beoordeling uitvoeren van het effect van een verwerking van persoonsgegevens op de grondrechten van betrokkenen. De gemeente voert in dat geval een gegevensbeschermingseffectbeoordeling uit, een zogenaamde Data Processing Impact Assessment (DPIA). 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 beperken, dan kan ervoor gekozen worden het risico te accepteren door de proceseigenaar. De Functionaris Gegevensbescherming geeft advies over de scope van de DPIA en op de uitgevoerde DPIA zelf, in het bijzonder op de risico's die uit de DPIA voortvloeien.

3.4 Toegang tot gegevens

Alleen daartoe geautoriseerde gebruikers hebben toegang tot het invoeren, raadplegen, wijzigen en verwijderen van persoonsgegevens. Toegang en bevoegdheden worden toegekend conform het gemeentelijke beleid voor gegevenstoegang, waaronder het informatiebeveiligingsbeleid, en periodiek gecontroleerd. De gemeente maakt daarnaast gebruik van technische en organisatorische maatregelen, zoals logging, om ongeautoriseerde toegang en onrechtmatige verwerkingen te voorkomen en te signaleren.

3.5 Inbreuk in verband met persoonsgegevens

Bij onbedoelde toegang tot, verlies of wijziging van persoonsgegevens bij de gemeente is er sprake van een datalek. Dat wordt gemeld bij de Autoriteit Persoonsgegevens en wanneer er sprake is van een hoog risico, ook bij de getroffen betrokkene(n). De gemeente noteert datalekken in een register, zet de bevindingen om in verbeterpunten en ziet toe op de opvolging hiervan. Nadere regels ten aanzien van het vaststellen, melden en afhandelen van datalekken zijn opgenomen in de procedure meldplicht datalekken.

3.6 Samenwerking

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

Verder kan het voorkomen dat de gemeente met andere (overheids-)organisaties samenwerkt om een taak van algemeen belang uit te voeren. In die gevallen kan sprake zijn van meerdere verwerkersverantwoordelijken (gezamenlijk of zelfstandig). De gemeente maakt met deze organisaties afspraken over de wijze waarop persoonsgegevens worden verwerkt. Met derden wordt afgesproken dat zij een beschermingsniveau dat gelijk is aan dat van de gemeente moeten waarborgen.

De gemeente stelt de politiegegevens conform de Wpg ter beschikking wanneer dit noodzakelijk is voor de uitoefening van de taken binnen het Wpg-domein. Daarbij wijst de gemeente de ontvangende partij op de plicht tot geheimhouding die op de versterkte gegevens van toepassing is.

3.7 Doorgifte buiten de EER

In principe geven we geen persoonsgegevens door aan landen buiten de Europese Economische Ruimte (EER) of een internationale organisatie. Bij eventuele uitzonderingen volgen we de wetgeving hierop en wordt de Functionaris Gegevensbescherming hierbij betrokken.

3.8 Bewustwording

Beleid en maatregelen alleen 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 aantoonbaar geïnformeerd over het zorgvuldig omgaan met persoonsgegevens, bijvoorbeeld via de gedragscode en informatie over onderwerp (via intranet en voorlichting aan de medewerkers).

3.9 PDCA Cyclus

De gemeente streeft ernaar om rondom de verwerkingen 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. Daarnaast worden vanuit de Wpg jaarlijks een interne privacy audit uitgevoerd. In opdracht van de gemeente wordt tenminste eenmaal per 4 jaar een externe audit uitgevoerd op de Wpg.

3.10 Transparantie

De gemeente informeert de betrokkenen tijdig, op een zo eenvoudig mogelijke, begrijpelijke en toegankelijke wijze over het feit dat zij persoonsgegevens verwerkt, op welke wijze en voor welke doeleinden. De betrokkene wordt op heldere en laagdrempelige wijze geïnformeerd over zijn rechten en de wijze waarop hij deze kan uitoefenen. Alleen indien de wet anders bepaalt, wijkt de gemeente van deze informatieplicht af.

3.11 Rechten van betrokkenen

Iedereen heeft het recht om te vernemen welke persoonsgegevens de gemeente over hem/haar heeft verzameld en waarvoor deze worden gebruikt. Naast dit zogenaamde recht op inzage hebben betrokkenen nog andere rechten, zoals het recht op verwijdering, rectificatie en het recht op beperking van de verwerking. Nadere regels ten aanzien van deze rechten van betrokkenen worden uitgewerkt in de interne procedure rechten van betrokkenen AVG en Wpg. Nadere informatie is ook opgenomen op de website van de gemeente en ABG-organisatie (privacyverklaring en webpagina over rechten van betrokkenen).

3.12 Geschillenbeslechting

Indien de betrokkene van mening is dat de gemeente niet op een juiste wijze met zijn persoonsgegevens is omgegaan, kan hij of zij contact opnemen met de Functionaris Gegevensbescherming van de gemeente of een klacht indienen middels de van toepassing zijnde klachtenprocedure van de gemeente. De betrokkene heeft ook het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens, met betrekking tot de naleving van wet- en regelgeving op het gebied van de bescherming van persoonsgegevens.

4. Rollen en verantwoordelijkheden

4.1 Three Lines model

Het Three Lines model helpt de gemeente om duidelijk te maken wie waarvoor verantwoordelijk is bij het omgaan met risico's omtrent privacy en andere vormen van risicobeheersing. Het model verdeelt de taken binnen de organisatie in drie lijnen. Hoewel het Three Lines model duidelijke rolverdelingen kent, werkt het niet met harde scheidslijnen

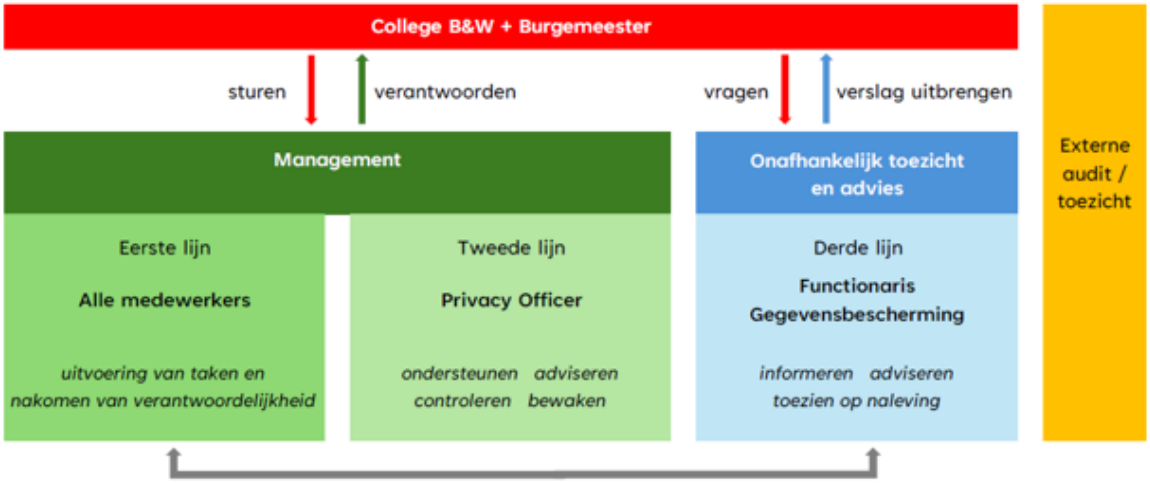
Elke lijn kijkt vanuit een eigen perspectief naar risico's, maar door actief samen te werken ontstaat een samenhangende aanpak. Zo wordt risicobeheersing niet iets van één onderdeel, maar een gezamenlijke verantwoordelijkheid van de hele organisatie.

Het College van Burgemeester en Wethouders (B&W) en de burgemeester hebben hierin een sturende rol. Zij stellen het beleid vast, bewaken de voortgang en ontvangen verantwoording van de organisatie. Zo blijft de gemeentelijke organisatie werken volgens de wet en de afgesproken normen.

Naast drie interne lijnen is er ook externe controle. Externe auditors en toezichthouders kijken onafhankelijk mee. Zij controleren of de gemeente haar werk goed, veilig en volgens de regels uitvoert. Dit zorgt voor extra zekerheid dat de gemeente betrouwbaar handelt.

Samen zorgen deze drie lijnen, aangevuld met extern toezicht, voor een heldere structuur waarin risico's worden beheerst, verantwoordelijkheden duidelijk zijn en de gemeente haar taken op een veilige en verantwoorde manier kan uitvoeren.

Schematisch ziet het Three lines model voor het privacybeleid er als volgt uit:



<u>Eerste lijn – Management en medewerkers</u>
De eerste lijn vormt de basis van het model en omvat het management en alle medewerkers binnen de organisatie. Zij zijn primair verantwoordelijk voor de uitvoering van taken en het naleven van de eigen verantwoordelijkheden op het gebied van privacy en informatiebeveiliging.

Kernverantwoordelijkheden van de eerste lijn:
- Toepassen van vastgesteld beleid en richtlijnen in de dagelijkse werkzaamheden;
- Zorgdragen voor correcte verwerking van persoonsgegevens en vertrouwelijke informatie;
- Zorgdragen voor procesbeschrijvingen, instructies en aanwijzingsbesluiten;
- Signaleren van risico's, incidenten of afwijkingen en deze tijdig melden;
- Naleven van procedures en beveiligingsmaatregelen zoals vastgesteld door de tweede lijn.

De eerste lijn voert uit en verantwoordt zich over de naleving van beleid richting het management en de tweede lijn. Hiermee vormt zij het fundament van een veilige en betrouwbare informatiehuishouding.

<u>Tweede lijn – Bedrijfsvoering Control</u>
De tweede lijn bestaat uit de functies die toezien op de uitvoering en de naleving van beleid binnen de organisatie. Binnen de gemeenten betreft dit de Privacy Officer(s). Deze functies hebben een ondersteunende, adviserende en controlerende rol. Het management organiseert dat de eerste en tweede lijn samenwerken en hun rol (kunnen) pakken.

Kernverantwoordelijkheden tweede lijn:
- Ondersteunen van de organisatie bij de implementatie van beleid en maatregelen op het gebied van privacy;
- Bieden van expertise en richtlijnen over risicobeheersing en privacywetgeving (zoals de AVG en Wpg);
- Controleren en bewaken van naleving van beleid, risico's en verbetermaatregelen;

De tweede lijn stuurt en bewaakt de naleving van kaders, maar is niet verantwoordelijk voor de feitelijke uitvoering van maatregelen, dat blijft bij de eerste lijn.

<u>Derde lijn – Onafhankelijk toezicht en advies (Functionaris Gegevensbescherming)</u>

De derde lijn wordt gevormd door de Functionaris Gegevensbescherming. Deze lijn vervult een onafhankelijke rol binnen de organisatie en heeft tot taak om toezicht te houden op de naleving van privacywetgeving en de effectiviteit van de genomen maatregelen.

Kernverantwoordelijkheden derde lijn:
- Toezien op de naleving van de AVG, Wpg en intern beleid;
- Adviseren van directie en indien noodzakelijk bestuur over privacyvraagstukken en naleving;
- Informeren van de organisatie over verplichtingen en verbeterpunten op het gebied van gegevensbescherming;
- Rapporteren aan het College van B&W, burgemeester en de gemeentesecretaris over de bevindingen en de naleving binnen de organisatie.
- Rapporteren aan het management en het college over de status van privacybescherming.

College van Burgemeester en Wethouders + Burgemeester
Het College en de burgemeester hebben de eindverantwoordelijkheid voor een zorgvuldig en rechtmatig privacybeleid. Het College is de verwerkingsverantwoordelijke voor bijna alle gemeentelijke taken; zij stelt kaders vast, faciliteert de noodzakelijke middelen en ziet erop toe dat de organisatie voldoet aan wettelijke verplichtingen. De burgemeester heeft aanvullende taken en verantwoordelijkheden op het gebied van openbare orde en veiligheid [10].

Het college stuurt op basis van rapportages uit de tweede [11] en derde lijn [12] en ontvangen verantwoording van het management over de uitvoering van beleid en maatregelen.

Externe audit en toezicht
Naast de drie interne lijnen vindt er ook externe toetsing plaats. Deze externe audit of toezicht (bijvoorbeeld door de Autoriteit Persoonsgegevens of een onafhankelijke auditor) biedt een aanvullende borging op de kwaliteit van het interne toezicht en de naleving van wet- en regelgeving. Hiermee wordt de transparantie en betrouwbaarheid van de organisatie verder versterkt.

4.2 Rollen en verantwoordelijkheden
Binnen de drie lijnen horen verschillende rollen met daarbij behorende taken en verantwoordelijkheden. Elke rol draagt op een eigen manier bij aan het veilig en zorgvuldig omgaan met informatie binnen de gemeente. In onderstaande paragrafen worden deze rollen nader toegelicht, zodat duidelijk wordt wie waarvoor verantwoordelijk is en hoe de samenwerking tussen de lijnen is georganiseerd.

R	Responsible/ Feitelijk verantwoordelijk	• Afdelingshoofden en Directeuren • De medewerkers (inclusief inhuur/externen) die persoonsgegevens verwerken
A	Accountable/ Eindverantwoordelijk	• Het College van B&W
C	Consulted/ Adviserend	• Privacy Officer • Functionaris Gegevensbescherming
I	Informed/ Geïnformeerd	• Gemeenteraad (privacy rechtelijk geen controlerende taak, maar op basis van de Gemeentewet en de decentralisatiewetgeving een bestuurlijke toezichttaak) • Functionaris Gegevensbescherming • Belanghebbende(n)/Betrokkene(n)

College van B&W en burgemeester
Het College is eindverantwoordelijk voor de naleving van de privacywetgeving binnen de gemeente.

Het College heeft de volgende rollen en verantwoordelijkheden [13]:
- Eindverantwoordelijk voor de naleving van de privacywetgeving binnen de gemeente;
- Stelt het (strategisch-tactisch) privacybeleid en de FG-regeling vast;

10)*Het bestuur van de ABG-organisatie is verwerkingsverantwoordelijke binnen het domein bedrijfsvoering en personeelszaken.*
11)*Door middel van documenten van de planning & control-cyclus, paragraaf Bedrijfsvoering.*
12)*Biijvoorbeeld jaarverslag van de Functionaris Gegevensbescherming*
13)*Deze rollen en verantwoordelijkheden gelden voor de burgemeester voor diens taken binnen het domein openbare orde en veiligheid.*

- Geeft sturing aan privacybeleidsvoering en legt rekenschap af over privacybeleidsvoering aan de raad en inwoners;
- Evalueert de toepassing en werking van het privacybeleid en privacybeleidsvoering/privacymanagement op basis van de rapportage van de Functionaris Gegevensbescherming.

Gemeentesecretaris (directeur), bestuur ABG-organisatie
- Eindverantwoordelijk voor de naleving van de privacywetgeving binnen de gemeente/gemeenschappelijke regeling binnen het domein bedrijfsvoering en personeelszaken;
- Verantwoordelijk voor implementatie en uitvoering van het privacybeleid binnen de gemeente/gemeenschappelijke regeling binnen het domein bedrijfsvoering en personeelszaken;
- Bevordert een duurzame, organisatiebrede privacycultuur.

Afdelingshoofden
De afdelingshoofden zijn eindverantwoordelijk voor de naleving van de privacywetgeving binnen de afdeling, alsmede voor de uitvoering van het privacybeleid. De afdelingshoofden hebben de volgende rollen en verantwoordelijkheden:
- Eindverantwoordelijk voor de naleving van de privacywetgeving binnen de eigen afdeling, voor zowel medewerkers als voor eigen afdelingscomputersystemen en -archieven (digitaal en fysiek);
- Verantwoordelijk voor implementatie en uitvoering van het privacybeleid binnen de eigen afdeling;
- Informeert de Functionaris Gegevensbescherming op welke manier de eigen afdeling compliant is aan de privacywetgeving;
- Verantwoordelijk voor (laten) volgen van trainingen door werknemers binnen de eigen afdeling;
- Verantwoordelijk voor het actueel houden van het verwerkingsregister voor zover dit betrekking heeft op de eigen afdeling;
- Verantwoordelijk voor het hebben van een DPIA voor de relevante processen en het uitvoeren van eventuele risicomitigerende maatregelen die hieruit voortvloeien;
- Verantwoordelijk voor autorisatie en intrekken van de autorisatie van medewerkers die persoonsgegevens verwerken;
- Aansturen van de Privacy & Security Officers, voor zover benoemd binnen de eigen afdeling;
- Bevordert een duurzame privacycultuur binnen de eigen afdeling;
- Betrekt Privacy Officers en/of Functionaris Gegevensbescherming in een vroeg stadium bij nieuwe of gewijzigde verwerkingen van persoonsgegevens.

Privacy Officer
De Privacy Officer (PO) ondersteunt de gemeente bij het toepassen van de privacywetgeving in de dagelijkse praktijk. De PO helpt afdelingen en medewerkers bij het zorgvuldig omgaan met persoonsgegevens, het uitvoeren van privacy analyses en het naleven van het gemeentelijk privacybeleid. De PO heeft een adviserende en begeleidende rol. De PO werkt nauw samen met de FG, het management en medewerkers, en draagt bij aan het vergroten van privacybewustzijn binnen de hele organisatie.

Onderdeel	**Verantwoordelijkheid**
Coördineren	• Coördineert de uitvoering van (meer)(jaren)plannen. • Coördineert de afhandeling van (domeinoverstijgende) datalekken. • Coördineert de afhandeling van (domeinoverstijgende) rechtenverzoeken. • Coördineert de uitvoering van DPIA's. • Onderhoudt een overlegstructuur met de verschillende organisatieonderdelen ter bevordering van kennis en kwaliteit ten aanzien van privacy.
Beleid / planvorming	• Formuleert, beheert, evalueert en monitort privacybeleid en procedures. • Stelt (meer)(jaren)plannen op, waaronder voor de bewustwording en opleiding van management en medewerkers en voor communicatie naar betrokkenen. • Monitort en evalueert de uitvoering van (meer)(jaren)plannen.
Adviseren	• Adviseert bestuur en de ambtelijke organisatie over privacybeleid en -ontwikkelingen. • Geeft advies aan management, teamleiders en medewerkers over de toepassing van privacygerelateerde wet- en regelgeving. • Toetst en geeft advies over afdelingsspecifieke privacygerelateerde reglementen, beleid en werkinstructies en over de positionering van privacy in werkprocessen.

	• Adviseert en ondersteunt bij het sluiten van (verwerkers)overeenkomsten, regelingen, reglementen en convenanten. • Adviseert over organisatorische maatregelen onder andere n.a.v. datalekken en risicoanalyses.
Uitvoeren	• Beheren van privacyregisters, zoals verwerkingsregisters, datalekregisters. • Is eerste aanspreekpunt voor privacygerelateerde onderwerpen binnen de organisatie. • Participeert in projectgroepen. • Werkt nauw samen met de FG, security officer(s) en adviseur(s) informatiebeheer. • Inventariseert en analyseert meldingen van inbreuken in verband met persoonsgegevens (datalekken). • Organiseert bewustwordings- en trainingsactiviteiten. • Houdt interne controles bij diverse afdelingen.
Ondersteunen	• Ondersteunt bij de afhandeling van datalekken. • Ondersteunt bij de afhandeling van rechtenverzoeken. • Ondersteunt bij implementatie en de uitvoering van het privacybeleid.
Rapporteren	• Legt verantwoording af in het kader van de planning en control cyclus.

Functionaris Gegevensbescherming

De gemeente is op grond van de AVG verplicht een Functionaris voor Gegevensbescherming (FG) aan te stellen. De FG heeft een onafhankelijke rol binnen de organisatie. De FG houdt toezicht op de naleving van de privacywetgeving, geeft advies en ondersteunt de gemeente bij het beschermen van persoonsgegevens. De FG werkt zonder invloed van bestuur of management en rapporteert rechtstreeks aan de gemeentesecretaris, griffier en het bestuur.

De FG heeft de volgende taken en verantwoordelijkheden binnen de gehele organisatie:

Onderdeel	Verantwoordelijkheid
Toezicht houden	• Ziet toe op de toepassing en naleving van verplichtingen van de organisatie t.a.v. gegevensbescherming. Er wordt toezicht gehouden op: de verplichting om medewerkers bewust te maken en op te leiden, verantwoordelijkheden toe te wijzen, DPIA's en audits uit te voeren, risicomaatregelen te implementeren en de afhandeling van verzoeken en klachten van betrokkenen. • Ziet toe op de toepassing en naleving van verplichtingen van de organisatie t.a.v. gegevensbescherming bij samenwerkingen met anderen waarin de organisatie (gezamenlijk) verwerkingsverantwoordelijk blijft. • Ziet toe op de toepassing en naleving van het gegevensbeschermingsbeleid van de organisatie. • Treedt op als contactpunt voor en pleegt overleg met de Autoriteit Persoonsgegevens over aangelegenheden t.a.v. gegevensbescherming, en werkt in die hoedanigheid met haar samen ten behoeve van de versterking van haar systeemtoezicht. • Treedt op als contactpunt voor burgers aangaande aangelegenheden t.a.v. gegevensbescherming, en ziet in die hoedanigheid toe op de afhandeling door de organisatie van klachten en andere knelpunten die de burger signaleert.
Informeren	• Informeert bestuur, management en medewerkers over hun plichten op het gebied van gegevensbescherming.
Adviseren	• Geeft gevraagd en ongevraagd advies aan bestuur en management over privacyrisico's, beleid, strategische keuzes en passende maatregelen. • Adviseert over het uitvoeren en verbeteren van DPIA's en andere risicoanalyses. • Adviseert over de afhandeling van klachten en verzoeken van inwoners. • Adviseert over het omgaan met datalekken, volgens de geldende procedures.

Onafhankelijke positie	• Voert geen taken uit die in strijd zijn met zijn onafhankelijke toezichthoudende rol. • Heeft toegang tot alle informatie, systemen en processen die nodig zijn voor het uitvoeren van toezicht. • Wordt tijdig betrokken bij nieuwe plannen, projecten en wijzigingen die gevolgen hebben voor de bescherming van persoonsgegevens.
Rapporteren	• Rapporteert rechtstreeks aan het College van B&W en, waar relevant, andere bestuursorganen over bevindingen, risico's en aanbevelingen.

Andere rollen en verantwoordelijkheden

Naast de eerder beschreven functies zijn er binnen de gemeente nog andere rollen die bijdragen aan een goede bescherming van informatie en persoonsgegevens. Deze rollen hebben aanvullende taken en ondersteunen de organisatie bij het veilig en zorgvuldig omgaan met gegevens.

Afdeling	**Betrokkenheid**
IT	Beheert informatiesystemen en zorgt voor datakwaliteit, dataveiligheid, archivering en toegankelijkheid.
Information Security Officer (ISO)	ISO is het dagelijks aanspreekpunt voor collega's binnen zijn/haar domein als het gaat om vragen over informatiebeveiliging en het melden van beveiligingsincidenten. Bijdragen aan het opstellen, implementeren, bijstellen, vernieuwen en herzien van (operationele) plannen die voortvloeien uit het organisatie brede informatiebeveiligingsbeleid. Samen met de CISO optreden als informatiebeveiligingsadviseur voor de proceseigenaar waarbij hij adviseert en ondersteunt over de uitwerking van het informatiebeveiligingsbeleid in plannen voor gebieden waar zij verantwoordelijk voor zijn, alsook de implementatie van deze plannen; Het samen met de CISO ondersteunen bij de uitvoering van risicoanalyses, adviseren bij verwekersovereenkomsten en opzetten en initiëren van bewustwordingsprogramma's en voorlichtingsbijeenkomsten op afdelingsniveau
Chief Information Security Officer (CISO)	Verantwoordelijk voor het sturen en coördineren van het informatiebeveiligingsbeleid binnen de gemeente. De CISO bewaakt de strategische koers en zorgt ervoor dat informatiebeveiliging goed is ingebed in de gehele organisatie. De CISO adviseert het bestuur en het management over risico's, prioriteiten en noodzakelijke beveiligingsmaatregelen. Daarnaast houdt de CISO toezicht op de uitvoering van het beleid en ondersteunt de organisatie bij het verbeteren van de digitale weerbaarheid. De CISO werkt nauw samen met de ISO, informatiemanagement, de PO, en de FG.
Juridische Zaken	Ondersteunen van de PO ten aanzien van privacyvraagstukken en adviseren over privacy-gerelateerde bepalingen in overeenkomsten en interne maatregelen.
Communicatie	In alle gevallen waarbij communicatie (intern en extern) een rol speelt worden medewerkers van communicatie betrokken. Adviseren van de organisatie over de communicatie bij datalekken (volgens de meldprocedure). Zorgt voor interne en externe communicatie bij incidenten en bewustwordingscampagnes.
Audit / Concern Control	Toetst het goed en betrouwbaar functioneren van de gehele interne organisatie.