EINDHOVEN
GEMEENTEBLAD
Officiële uitgave van de gemeente Eindhoven
Nr. 417737
26 september
2025

Privacybeleid AVG Gemeente Eindhoven

Beleidskader gegevensbescherming

Uitgave
gemeente Eindhoven

1. Inleiding

1.1 Algemeen

Als gemeente verwerken we grote hoeveelheden persoonsgegevens van onze inwoners, collega's en andere personen. Dit doen we onder meer om onze publieke taken te vervullen, om onze bedrijfsvoering aan te sturen of om onze processen te verbeteren.

Maatschappelijk verantwoorde, kwalitatief goede en daarnaast ook veilige gegevensverwerking is randvoorwaardelijk om onze taken en plannen uit te voeren en vraagt om duidelijke kaders. In dit privacybeleid worden deze kaders beschreven. Deze kaders zijn tot stand gekomen op basis van de kernwaarden van onze organisatie, maar ook uit de normen en principes van onder andere het Handvest van de grondrechten van de Europese Unie en de Algemene Verordening Gegevensbescherming. Dit beleid dient als fundament voor alles wat we als gemeente Eindhoven doen rondom gegevensbescherming. Onderdelen van dit privacybeleid zijn verder uitgewerkt in onder meer jaarplannen, werkinstructies, reglementen en protocollen.

1.2 Visie, ambitie en doel

Met dit beleid streven we naar een volwassen gegevensbeschermingsaanpak en willen door ontwikkelen naar een risicogebaseerde aanpak. Dit betekent dat:
- we ons inzetten om in overeenstemming met de AVG te handelen. Daarbij realiseren wij ons dat we nooit helemaal kunnen uitsluiten dat het misgaat, maar dat we vooral inzetten op veerkracht, oftewel: in staat zijn om dit zo snel mogelijk te herstellen.
- we willen omgaan met persoonsgegevens op een manier die wij als mens zelf ook prettig zouden vinden;
- we de kansen die digitalisering biedt graag benutten op een verantwoorde manier;
- we willen dat maatregelen een op het risico afgestemd beveiligingsniveau waarborgen voor inwoners en medewerkers.
- we ervoor zorgdragen dat dit beleid binnen de gemeentelijke organisatie bekend is en wordt toegepast en
- we een aanpak hanteren die niet alleen leidt tot vertrouwen bij inwoners en ketenpartners maar ook leidt tot vertrouwen binnen onze organisatie.

1.3 Reikwijdte en plaats in het gemeentelijke beleidskader

Dit beleid is van toepassing op alle verwerkingen van persoonsgegevens onder de bestuurlijke verantwoordelijkheid van het College van B&W en de Burgemeester.

Het beleid is van toepassing vanaf het moment van verzameling van de persoonsgegevens tot het moment van vernietiging daarvan. Het maakt daarbij niet uit of de gegevens digitaal, op papier of mondeling worden verwerkt. Het beleid is ook van toepassing op de gegevensverwerkingen die we uitbesteden aan een zogeheten 'verwerker' (een dienstverlener of samenwerkingspartner die in opdracht van ons de persoonsgegevens verwerkt).

Het privacybeleid legt de uitgangspunten van ons gedrag vast als we met persoonsgegevens werken. Het wordt aangevuld met deelbeleid voor specifieke onderwerpen, zoals het melden van (vermoedelijke) datalekken. Daarnaast zijn er aanvullend andere regels binnen onze gemeente, zoals de Gedragscode Ambtenaren, en meer in het bijzonder de omgang met informatie, het Organisatiehandboek 'Zo werkt Eindhoven' en het strategisch informatiebeveiligingsbeleid.

1.4 Vaststelling, inwerkingtreding, publicatie en evaluatie

Dit privacybeleid is vastgesteld door het college van B&W. Na vaststelling treedt het privacybeleid in werking en vervangt daarmee de eerder vastgestelde versie(s).
Het beleid wordt ter kennisname aan de gemeenteraad aangeboden. Het wordt ook gepubliceerd op het gemeentelijke intranet, de gemeentelijke website en overheid.nl.

De werking van dit beleid wordt jaarlijks geëvalueerd in samenspraak met ambtelijk privacy overleg en met consultatie van de FG. Als daar aanleiding toe is, wordt het privacybeleid geactualiseerd. Wijzigingen worden ter vaststelling voorgelegd aan het College van B&W.

2. Onze privacyprincipes

Als gemeente nemen we de verantwoordelijkheid om verantwoord met persoonsgegevens om te gaan. Dit doen wij aan de hand van de volgende uitgangspunten.

NB. Onderstaande principes zijn uitgangspunten van ons handelen. Voorbeelden en toelichtingen zijn slechts illustratief bedoeld. De wet is leidend en vult deze principes aan. Voor zover de Wet politiegegevens van toepassing is op de persoonsgegevens, kunnen aanvullende of andere eisen van toepassing zijn (zie Addendum Wpg-beleid).

2.1 Dit doen wij altijd

• Wij gaan respectvol en zorgvuldig om met persoonsgegevens
Wij begrijpen dat het uitoefenen van openbaar gezag (zoals bescherming van de openbare orde en het beslissen op vergunningaanvragen) en het handelen in het algemeen belang leidt tot het verzamelen en uitwisselen van persoonsgegevens. Dit vraagt van ons dat wij respectvol met deze persoonsgegevens omgaan. Dit doen wij door bij het uitvoeren van de wettelijke taak of plicht af te vragen of de verwerking van persoonsgegevens noodzakelijk is en de verwerking veilig is.

• Wij tonen eigenaarschap
We werken aan een volwassen, gegevensbeschermingscultuur, waarin de fundamentele rechten en vrijheden van mensen optimaal gerespecteerd worden. Wij zijn en voelen ons verantwoordelijk om ons beleid en relevante wet- en regelgeving na te leven, ons gedrag bij te sturen en elkaar hierop aan te spreken. Wij nemen de zwaarwegende adviezen van de Functionaris Gegevensbescherming in acht. In voorkomend geval wijken wij daar alleen gemotiveerd van af.

• Wij verwerken alleen persoonsgegevens als dat is toegestaan
Wij verwerken alleen als er een rechtsgrondslag voor is. In onze praktijk betekent dit dat we bevoegd zijn om persoonsgegevens te verwerken:
o als we onze gemeentelijke taken uitvoeren,
o als we een wettelijk verplichting of overeenkomst uitvoeren,
o in noodsituaties waarin het leven of de gezondheid van een persoon ernstig wordt bedreigd en acuut handelen geboden is, of
o als de betrokkene toestemming heeft gegeven voor de gegevensverwerking (Deze situatie is enkel van toepassing als het wettelijk verplicht is om toestemming te vragen).
o als we bezig zijn met onze interne bedrijfsvoering of de beveiliging/veiligheid van onze organisatie of onze medewerkers,
Of in het kader van een gerechtvaardigd belang, maar op die rechtsgrond kan alleen een beroep worden gedaan als het gaat om verwerkingen die los staan van de gemeentelijke taken, zoals de interne bedrijfsvoering en de beveiliging, veiligheid van onze organisatie en medewerkers.

• We verwerken alleen de persoonsgegevens die noodzakelijk zijn voor het doel
We verwerken alle persoonsgegevens die noodzakelijk zijn om onze taken of verplichtingen goed uit te voeren, maar ook niet meer dan nodig. Wij stellen ons steeds de vraag of het doel ook met minder gegevens kan worden bereikt (dataminimalisatie) en of het doel ook op een andere manier kan worden bereikt die minder ingrijpend is voor de privacy van de betrokken persoon (subsidiariteit). We stellen ons ook de vraag of de gegevens geschikt zijn om het gestelde doel te bereiken (effectiviteit). Voorts nemen we maatregelen om de ongewenste gevolgen van de gegevensverwerking voor de betrokkene(n) te beperken (evenredigheid).

• We spannen ons in om te zorgen dat persoonsgegevens inhoudelijk kloppen en up-to-date zijn.
Onjuiste informatie kan leiden tot onjuiste beslissingen, waar voor de inwoner of medewerker (grote) gevolgen aan verbonden kunnen zijn. Wij zijn ons ervan bewust dat de situatie zich voor kan doen dat persoonsgegevens in dossiers niet kloppen. Daarom nemen wij passende maatregelen om (periodiek) de actualiteit en de juistheid van de gegevens te controleren.

• We bewaren persoonsgegevens alleen zolang als dat noodzakelijk is.
We bewaren persoonsgegevens zolang als noodzakelijk is voor het doel van de gegevensverwerking of zolang de wet voorschrijft. We slaan persoonsgegevens alleen op in de daarvoor aangewezen systemen en apparatuur van de gemeente. Wij houden ons aan de regels van de Archiefwet.

• Wij slaan persoonsgegevens bij voorkeur op in de Europese Economische Ruimte
Als hoofdregel selecteren wij dienstverleners die die garanderen dat de persoonsgegevens in de Europese Economische Ruimte (EER) worden opgeslagen. Indien dit niet mogelijk is, mogen persoonsgegevens alleen worden opgeslagen in een derde land als dat land een passend beschermingsniveau biedt.

• Wij zijn dienstverlenend
Als we over persoonsgegevens van een inwoner beschikken, bekijken we of we deze kunnen hergebruiken. We gebruiken de gegevens echter niet zomaar voor andere doeleinden. Wij toetsen eerst of dit wel mag ('verdere verwerking'). Daarbij nemen we de grenzen van de wet in acht. Het doeleinde waarvoor we de gegevens hergebruiken moet verenigbaar zijn (eenvoudiger gezegd: niet te ver afwijken van) met het doel waarvoor we het persoonsgegeven hebben verzameld of verkregen (doelbindingsbeginsel).

• We zijn transparant
Wij geven tijdig volledige, begrijpelijke en makkelijk toegankelijke informatie over waarom en hoe wij persoonsgegevens verwerken bij de uitoefening van onze taken en bevoegdheden. We communiceren met betrokkenen over de verwerking van hun persoonsgegevens in begrijpelijk Nederlands of in een andere taal als dat doelmatiger is. Waar mogelijk of verplicht stemmen wij het doel van de gegevensverwerking af met vertegenwoordigers van betrokkenen.

• Wij respecteren de rechten van betrokkenen
Wij geven tijdig en volledig antwoord op een verzoek van een betrokkene of diens (wettelijke) vertegenwoordiger of advocaat, zoals inzage in diens persoonsgegevens, correctie, afscherming of verwijdering van persoonsgegevens, of bezwaar tegen de gegevensverwerking. Alleen als daar een zwaarwegende reden voor is, zoals de opsporing, vervolging of voorkoming van strafbare feiten, de bescherming van de openbare veiligheid of volksgezondheid of bescherming van anderen, doen we dat niet. Dit is uitgewerkt in procedure 'rechten van betrokkenen'.

• Wij nemen passende maatregelen om privacyvriendelijk te werken
We hebben inzicht in de processen waarin persoonsgegevens worden verwerkt en nemen deze op in ons verwerkingenregister. We houden al tijdens de ontwikkeling van processen en systemen rekening met de wettelijke voorwaarden en onze privacyprincipes. Dit wordt uitgewerkt in een protocol… waarin in het bijzonder aandacht wordt besteed aan de toepassing van deze principes bij het extern inkopen van systemen of diensten en het uitwisselen van persoonsgegevens met derden.

• Wij houden persoonsgegevens veilig
Wij nemen passende maatregelen om te zorgen dat persoonsgegevens beschikbaar, integer en vertrouwelijk zijn (informatiebeveiliging), in overeenstemming met het strategisch informatiebeveiligingsbeleid. Dit betekent onder meer dat:
o we de persoonsgegevens veilig opslaan. Indien daar toe noodzaak bestaat versleutelen we de persoonsgegevens.
o we zorgen dat de persoonsgegevens binnen en buiten de gemeentelijke organisatie alleen toegankelijk zijn voor mensen die vanwege hun rol toegang tot die gegevens mogen hebben ('need to know') en controleren dat ook (logging);
o we persoonsgegevens veilig delen met anderen op een wijze die past bij de gevoeligheid ervan; en
o we een vermoedelijk datalek zo snel mogelijk melden volgens de daarvoor bestemde procedure.

In Bijlage 1 staat een checklist die kan worden gebruikt om af te wegen of een gegevensverwerking in overeenstemming is met de wet- en regelgeving en dit privacybeleid.

2.2 Dit doen we in beginsel niet
• Wij vragen in beginsel geen toestemming voor de verwerking van persoonsgegevens. Als gemeente oefenen wij openbaar gezag uit. Daarnaast zijn inwoners vaak ook afhankelijk van de gemeente. Ook met onze medewerkers hebben we een gezagsrelatie. In deze situaties voelen mensen zich niet altijd vrij om toestemming te weigeren. Daarom is toestemming vragen in deze situaties ongepast. Toestemming vragen we alleen als de wet ons daartoe verplicht.

• We verwerken geen bijzondere gegevens of strafrechtelijke persoonsgegevens, tenzij dit moet of mag van de wet. Wij begrijpen dat sommige persoonsgegevens extra risico's voor de betrokkene met zich meebrengen, met name risico's op discriminatie. Het gaat met name om:
o informatie waaruit iemands ras of etniciteit, geloofsovertuiging, politieke overtuigingen of vakbondslidmaatschap blijkt,
o biometrische gegevens om iemand te identificeren (bijv. gezichtsherkenning),
o gezondheidsgegevens (waaronder ziekte, handicap, zwangerschap of behandelingen),

o gegevens betreffende iemands seksuele gerichtheid of seksuele leven, en
o gegevens met betrekking tot veroordelingen, het plegen van strafbare feiten, en gedragingen waarvoor door de rechter een verbod is opgelegd.
Wij verzamelen deze gegevens alleen als het absoluut noodzakelijk is en voor zover dit wettelijk is toegestaan.

• Wij nemen geen volledig geautomatiseerde beslissingen en doen ook niet aan volledig geautomatiseerde (risico)profilering die mensen ernstig in hun rechten aantasten, tenzij in overeenstemming met de wet.
Wij doen niet aan geheel geautomatiseerde besluitvorming. Dat is een besluit zonder dat een ambtenaar dit heeft beoordeeld. Wel gebruikt de gemeente algoritmes die ondersteunend zijn aan de besluitvorming. Alvorens een dergelijk algoritme in gebruik te nemen, overtuigen wij ons ervan dat het algoritme geen ingebouwde voorkeur (bias) heeft die leidt tot directe of indirecte discriminatie of uitsluiting van mensen. Wij bewaken dit zolang we het algoritme gebruiken. Zo nodig sturen we het algoritme bij of stoppen we met het gebruik ervan. Impactvolle algoritmes die persoonsgegevens gebruiken registreren wij in het landelijke Algoritmeregister.

• Wij verstrekken geen persoonsgegevens aan een ontvanger in een land buiten de Europese Economische Ruimte of aan een internationale organisatie, tenzij dit is toegestaan door de wet
Wij begrijpen dat de bescherming van persoonsgegevens in andere landen of internationale organisaties vaak niet op hetzelfde niveau is als in de Europese Economische Ruimte (EU-landen plus Noorwegen, IJsland en Liechtenstein). Daarom zijn wij terughoudend in de verstrekking van persoonsgegevens aan derden in landen buiten Europa of internationale organisaties. Als voor het realiseren van een publieke opgave het noodzakelijk is en er geen reëel alternatief is om de persoonsgegevens te verstrekken, treffen wij waar mogelijk passende waarborgen om de belangen van de betrokkenen te beschermen, zoals het afsluiten van een Europees erkend modelcontract met de ontvanger. Alleen in uitzonderlijke, door de wet erkende gevallen mogen de waarborgen achterwege blijven.

3. Waarborgen voor gegevensbescherming

3.1 Volwassen organisatie

Als gemeente zijn wij verantwoordelijk voor de bescherming van persoonsgegevens. Daarvoor moeten wij ons huiswerk doen en waar nodig juridische, technische en organisatorische waarborgen inbouwen in onze processen en systemen. Wij streven als organisatie ten minste naar volwassenheidsniveau Gedefinieerd (3 van 5). Dat wil zeggen dat wij de basis van gegevensbescherming op orde hebben. Ook hebben wij risico's voor onze inwoners en medewerkers in zicht en onder controle.

3.2 Risicoanalyses en DPIA's

Voor elk nieuw of gewijzigd 'geheel van verwerkingen' (bijv. omgevingsvergunningen, cameratoezicht op straat, of de personeelsadministratie), voeren wij een risicoanalyse ('quickscan') uit. Als uit deze analyse blijkt dat het proces mogelijk een hoog risico kan inhouden voor de grondrechten van betrokkenen, voeren we voorafgaand aan de verwerking een data protection impact assessment (DPIA) uit. Periodiek herijken we de DPIA's volgens het schema dat we in onze DPIA-procedure hebben vastgesteld. Waar mogelijk bespreken we de conclusies van de DPIA met de doelgroep of hun vertegenwoordigers.

3.3 Informatiebeveiliging

Informatiebeveiliging is de verzamelnaam voor de processen, die de gemeente inricht om de betrouwbaarheid van informatie te beschermen, ook als die zich in gemeentelijke processen of in informatiesystemen bevinden. Het begrip 'informatiebeveiliging' heeft betrekking op:
- Beschikbaarheid: het zorg dragen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers;
- Vertrouwelijkheid: het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn;
- Integriteit: het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking.

Wij beveiligen persoonsgegevens met passende technische en organisatorische maatregelen. Dit hebben wij verder uitgewerkt in ons strategisch informatiebeveiligingsbeleid.

Indien zich een informatiebeveiligingsincident voordoet, waarbij bijvoorbeeld gegevens van personen in verkeerde handen kunnen komen of zijn gekomen, handelt de gemeente in overeenstemming met de vastgestelde werkwijze in de datalekkenprocedure. Deze procedure bevat een vastgesteld proces van te doorlopen stappen om de eventuele schade voor betrokkenen (of de kans hierop) bij een datalek te beperken en er als organisatie van te leren.

3.4 Verwerkingsregister
Alle gegevensverwerkingen moeten worden geregistreerd in het 'verwerkingsregister'. In dit register houden we onder andere bij welke persoonsgegevens waar worden opgeslagen, met welke partijen we gegevens uitwisselen en hoelang deze informatie bewaard moet worden. Als een gegevensverwerking structureel wijzigt, wordt het verwerkingsregister zo snel mogelijk daarop aangepast. Hierbij houden we ons aan onze interne procedure voor het bijhouden van het verwerkingsregister. We publiceren het verwerkingsregister met de wettelijk verplichte onderdelen op de website. Dit wordt dagelijks ververst naar de laatste versie.

3.5 Transparantie
Iedere inwoner heeft het recht om geïnformeerd te worden over de verwerkingen van zijn persoonsgegevens.

We leggen in onze regelgeving en beleidsregels uit wanneer de verwerking van bijzondere of strafrechtelijke persoonsgegevens wettelijk is toegestaan. In die gevallen geven wij dit duidelijk aan.

Als we persoonsgegevens verwerken, leggen we uit waarom we persoonsgegevens verwerken, welke persoonsgegevens we verwerken, met welke partijen we persoonsgegevens (kunnen) delen, en hoelang we de gegevens bewaren. Als we een algoritme inzetten in een proces wat ernstige gevolgen kan hebben voor mensen, leggen we de werking van het algoritme uit. Dit doen wij in privacyverklaringen op onze website, maar ook in aanvraagformulieren en informatiebrieven en -brochures. We communiceren beknopt, transparant en begrijpelijk over privacy en gegevensbescherming en bij voorkeur schriftelijk en/of met gebruik van beelden. Als de betrokkene daarom vraagt of als we denken dat de betrokkene daar behoefte aan heeft, geven we de informatie mondeling of via een andere geschikte methode.

Soms hebben we een zwaarwegende reden om een gegevensverwerking geheim te houden, bijvoorbeeld als:
• dat nodig is voor de opsporing, vervolging of voorkoming van strafbare feiten, de bescherming van de openbare veiligheid of de bescherming van anderen.
• als het geven van de informatie in praktijk onmogelijk is of gelet op de belangen van de betrokkene een onevenredige inspanning van de gemeente zou vergen, of
• het geven van de informatie wettelijk verboden is of het doel van de gegevensverwerking zou doorkruisen.

Als een uitzondering op de informatieplicht van toepassing is op een bepaald type gegevensverwerking, leggen we vast waarom we vinden dat die uitzondering van toepassing is.

3.6 Rechten van betrokkenen
Betrokkenen hebben verschillende rechten om invloed uit te oefenen op de verwerking van hun persoonsgegevens, waaronder het recht om hun persoonsgegevens in te zien, te corrigeren, te laten verwijderen of bezwaar te maken tegen de gegevensverwerking.
We hebben een loket ingericht waar betrokkenen op verschillende manieren hun verzoeken kunnen doen om hun rechten uit te oefenen. We gaan alleen over tot uitvoering van een verzoek als we zeker weten dat de verzoeker de betrokkene (of diens vertegenwoordiger) is. Wij bieden onder andere de mogelijkheid om via DigiD de identiteit van de verzoeker vast te stellen. Bij het afhandelen van deze verzoeken, houden wij ons aan onze procedure voor het afhandelen van verzoeken van betrokkenen. We streven ernaar om zo snel mogelijk, maar in ieder geval binnen de wettelijke termijn van een maand, op een verzoek te reageren.

3.7 Grip op gegevensuitwisseling met externe partijen
Als we processen uitbesteden aan externe partijen en diensten inkopen, moeten onze inwoners en medewerkers ervan kunnen uitgaan dat die leveranciers óók verantwoord en netjes met hun persoonsgegevens omgaan. Daarom moeten we op voorhand afspraken maken met deze leveranciers.
• Met partijen die verwerker zijn, sluiten we een zogeheten 'verwerkersovereenkomst'.
• Met partijen met wie we gezamenlijk verwerkingsverantwoordelijke zijn, maken we afspraken over hoe wij samen de wettelijke regels naleven.
• Met partijen die zelf verwerkingsverantwoordelijke zijn maken we – indien nodig – afspraken over de bescherming van persoonsgegevens.

Wij controleren steekproefsgewijs of leveranciers zich aan de afspraken houden. Daarvoor hebben we een interne procedure waarin de frequentie, het toetsingskader en de opvolging is vastgelegd.

Voor het aanpakken van sociale, maatschappelijke en veiligheidsvraagstukken werken we vaak samen met ander overheidsorganisaties en sociale partners. In deze zogenoemde samenwerkingsverbanden

kan het noodzakelijk zijn om persoonsgegevens te delen met een of meer van de samenwerkingspartners. Voor de Zorg- en Veiligheidshuizen en de RIEC's zijn de regels daarvoor opgenomen in de Wet gegevensverwerking door samenwerkingsverbanden. Er kan echter ook binnen de gemeente worden samengewerkt met andere afdelingen, waarbij er sprake is van structurele gegevensuitwisseling, bijvoorbeeld bij thema's als bestaanszekerheid en ondermijning.

Bij de uitvoering van zulke interne en externe samenwerkingsverbanden houden we rekening met de wettelijke privacyvoorschriften die van toepassing zijn op onszelf en op onze samenwerkingspartners. Als de wet hierin geen duidelijke werkwijze voorschrijft (denk daarbij bijvoorbeeld aan verplichte gegevenslevering of juist een geheimhoudingsplicht), hanteren we de volgende werkwijze als uitgangspunt:
• Mochten de wetten niet in de uitwisseling van gegevens voorzien, dan onderzoeken we of het verwerkingsdoel 'verenigbaar' is met het oorspronkelijke doel waarvoor de gegevens zijn verzameld (doelbinding).
• Voor gezamenlijke verwerkingen die mogelijk een hoog risico voor betrokkenen inhouden, voeren we een (gezamenlijke) DPIA uit.

Als de wijze van samenwerking ertoe leidt dat we samen met een of meer partijen verwerkingsverantwoordelijke zijn (gezamenlijke verwerkingsverantwoordelijke), maken we, indien de wet daarin niet voorziet, afspraken over de verdeling van de wettelijke verplichtingen, zoals het melden van een datalek of het faciliteren van de rechten van betrokkenen. De afspraken leggen we in dat geval vast in onderlinge regeling. De gemaakte afspraken worden geïntegreerd in de werkprocessen.

3.8 Bewustwording en opleiding
Vanuit meerdere invalshoeken proberen we onze collega's bewust te maken over het belang van privacy en de manier waarop zij hieraan bijdragen. Medewerkers die met persoonsgegevens gaan werken, krijgen na indiensttreding uitgebreide informatie en/of training over het belang van privacy en gegevensbescherming. Ook beloven zij bij aanvang van hun dienstverband dat zij zich zullen houden aan de gedragscode waarin meerdere normen zijn opgenomen over gegevensbescherming en de toepassing van de principes uit dit privacybeleid.

Naast het verhogen van de bewustwording, leiden we intern ook privacyambassadeurs op. Zij hebben een bovengemiddelde affiniteit met het onderwerp privacy. Zij worden geschoold zodat zij een behoorlijke kennis hebben, waarmee zij op basaal niveau privacyvragen van collega's kunnen beantwoorden en de privacy officer daarin kunnen ondersteunen. Zij hebben een essentiële rol bij de cultuurverandering die nodig is om een volwassen organisatie te worden en te blijven.

3.9 Bewaren en archiveren
Persoonsgegevens die niet langer nodig zijn voor het bereiken van het doel worden zo snel mogelijk verwijderd. Dit betekent dat deze gegevens vernietigd worden of zó worden aangepast dat de informatie redelijkerwijs niet meer herleidbaar is tot een specifieke persoon. Hierbij houden we rekening met andere zwaarwichtige belangen, zoals archivering voor historisch onderzoek of geschillenbeslechting, wetenschappelijk onderzoek en statistisch onderzoek. De Archiefwet en de vertaling ervan naar de VNG selectielijst is voor ons leidend als het gaat om het archiveren van persoonsgegevens.

We werken dit nader uit in onze bewaarstrategie. Deze strategie beschrijft welke technische en organisatorische maatregelen we nemen om ervoor te zorgen dat informatie niet langer wordt bewaard dan noodzakelijk. De bewaarstrategie wordt verder uitgewerkt in ons- bewaar en vernietigingsbeleid. De archiefinspecteur houdt hier toezicht op.

3.10 Monitoring en audit
Een periodieke toets op het onderdeel privacy vindt plaats aan de hand van onze PDCA-cyclus. In de eerste plaats controleren we hoeverre de feitelijke situatie in overeenstemming is met de toepassing van het privacybeleid. Daarnaast houdt de Functionaris Gegevensbescherming (FG) toezicht op de naleving van ons beleid en de wet- en regelgeving.
Verder wordt elk jaar per sector een interne review uitgevoerd op het beleid, procedures en maatregelen. Elke vier jaar wordt hierop een externe audit uitgevoerd (i.c.m. de wettelijke verplichte externe audit Wpg). In hoofdstuk 4 staat verder beschreven hoe de taken en verantwoordelijkheden binnen onze organisatie zijn ingericht.

3.11 Non-compliance en klachten
We moedigen iedereen aan om elkaar aan te spreken op (vermoedelijke) gevallen van non-compliance met de wet- en regelgeving. Denk bijvoorbeeld aan het in strijd met de wet gegevens verzamelen of verstrekken, gegevens te lang bewaren, en het niet of te laat antwoorden op verzoeken van betrokkenen. Als dit niet leidt tot verbeteringen in het gedrag, kan eenieder een signaal afgeven in de betreffende

lijn (afdelingsmanager of sectorhoofd onder wiens verantwoordelijkheid de gegevensverwerking plaatsvindt).

Een formele klacht over de verwerking van persoonsgegevens door de gemeente kan worden ingediend via de daarvoor bestemde kanalen, zoals het formulier Privacyrechten verzoek of klacht over verwerking of privacy@eindhoven.nl.

Een vraag of klacht wordt in beginsel behandeld door de eerste lijn (met ondersteuning van de tweede lijn), maar indien iemand niet tevreden is over de afhandeling kan diegene zich wenden tot de FG (via fg@eindhoven.nl). De FG is tevens een aanspreekpunt voor vragen en klachten over privacy en gegevensverwerking. De FG is onafhankelijk en heeft een wettelijke geheimhoudingsplicht.

4. Privacygovernance: Taken, rollen en verantwoordelijkheden

In dit hoofdstuk beschrijven we wie binnen de gemeente Eindhoven de verantwoordelijkheid heeft voor de naleving van de wet- en regelgeving op het gebied van privacy en gegevensbescherming en welke taken eenieder heeft oftewel privacy governance.

4.1 Three lines model

De borging van de naleving van de AVG, Uitvoeringswet AVG en relevante materiewetten is afhankelijk van goede afspraken in de organisatie, zoals over de toebedeling van verantwoordelijkheden en afgestemde werkprocessen. Het is dan ook noodzakelijk dat de gemeente een organisatiestructuur vaststelt waarin privacy van de inwoners en medewerkers is ingebed. Dit vraagt om een duidelijke, eenduidige toebedeling van verantwoordelijkheden, taken en bevoegdheden tussen bestuur en uitvoering. Het three lines of defence-model is gericht op de beheersing van de risico's in de naleving van deze wet- en regelgeving.

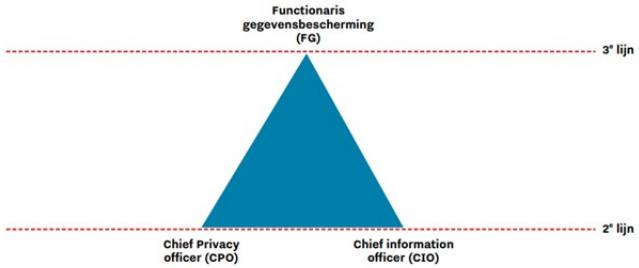
De eerste lijn: de gegevensverwerking voor de gemeentelijke taken gebeurt onder verantwoordelijkheid van de burgemeester respectievelijk het college van burgemeester en wethouders. Zij leggen daarover verantwoording af aan de gemeenteraad. Op de burgemeester respectievelijk het college van burgemeester en wethouders rust daarnaast de verantwoordingsplicht als bedoeld in de AVG.
De feitelijke verantwoordelijkheid ligt in de lijnorganisatie. Het is dan ook van belang dat er op alle niveaus aandacht is voor het onderwerp en dat bekend is welke taken, bevoegdheden en verantwoordelijkheden daar belegd zijn.
De eerste lijn neemt verantwoordelijkheid voor risico's die ontstaan bij de uitvoering van de gemeentelijke taken en bevoegdheden en de verwerking van persoonsgegevens die daaraan ten grondslag ligt. Daartoe behoort de verantwoordelijkheid om maatregelen te treffen om tot een aanvaardbaar risico te komen en restrisico te accepteren en ook daar verantwoordelijkheid voor te nemen.

De tweede lijn: De verantwoordelijkheid tot naleving van het gegevensbeschermingsrecht ligt bij de eerste lijn. De eerste lijn wordt daarbij ondersteund, geadviseerd en gecontroleerd door de tweede lijn. De tweede lijn staat onder aansturing van het management behorende tot de eerste lijn. De tweede lijn bestaat in beginsel uit privacy officers en -juristen en specialisten op het gebied van informatiebeveiliging.

De tweede lijn ondersteunt de eerste lijn met specialistische kennis en vaardigheden. Zij voeren daarom taken uit waarvoor specialistische kennis of vaardigheden nodig zijn, zonder de verantwoordelijkheid van de eerste lijn over te nemen. De taken zijn samen te vatten als: ondersteunen, expertise bieden, controleren en bewaken.
• Met ondersteunende taken wordt onder meer bedoeld: het verzorgen van activiteiten ter bewustwording van de eerste lijn, de begeleiding van de uitvoering en afronding van DPIA's, de begeleiding en coördinatie bij datalekken, het voorstellen van algemeen en specifiek privacybeleid, coördineren en begeleiden bij het inzichtelijk en overzichtelijk maken van de verwerkingen binnen de organisatie, het signaleren en voorstellen van noodzakelijke wijzigingen in de privacyverklaring en het bieden van juridische ondersteuning van de afhandeling van verzoeken tot het uitoefenen van de rechten van betrokkenen.
• Het bieden van expertise is een integraal onderdeel van de ondersteuning, maar omvat ook privacyjuridische expertise waar het gaat om de rechtmatigheid van en de te nemen maatregelen bij verwerkingen van persoonsgegevens. Het kan daarbij ook gaan om expertise op het gebied van informatiebeveiliging.
• De controlerende taak omvat periodieke en incidentele controles op de rechtmatigheid van verwerkingen, de effectiviteit van vastgestelde maatregelen, autorisaties en logging, het naleven van vastgestelde bewaartermijnen en de juistheid, volledigheid en actualiteit van gegevens.
• Het bewaken omvat het nemen van maatregelen op grond van beleid of bijvoorbeeld in het kader van DPIA's en in hoeverre geïdentificeerde risico's zich ontwikkelen. Bij de bewakende taak gaat het met name om het houden van overzicht van en inzicht in de status van alle afspraken en de nakoming van afspraken.

Derde lijn: De verwerkingsverantwoordelijke heeft de verplichting om een FG aan te stellen als interne toezichthouder. De FG moet betrokken worden bij 'alle aangelegenheden die verband houden met de bescherming van persoonsgegevens' (zie artikel 38, eerste lid, AVG). De FG wordt benoemd op grond van zijn professionele kwaliteiten, deskundigheid op het gebied van de wetgeving en de (gemeentelijke) praktijk.
De FG werkt autonoom en voert zijn werkzaamheden onafhankelijk uit en ontvangt daarbij geen instructies vanuit de gemeentelijke organisatie en verwerkers. De FG rapporteert rechtstreeks aan het college van burgemeester en wethouders en de gemeentesecretaris. Er is overleg mogelijk met de Autoriteit Persoonsgegevens (AP) waarbij de FG als liaison kan optreden, maar er is geen meldingsplicht van de FG aan de AP bij onregelmatigheden. De FG kan niet tevens een functie vervullen in de eerste en/of tweede lijn.

RELATIE CPO, CIO EN FG



4.2 Eerste lijn: bestuurlijke en ambtelijke verantwoordelijkheid
Verwerkingsverantwoordelijkheid
De wetgeving legt de verantwoordelijkheid voor de gegevensverwerking door de overheid neer bij het bestuursorgaan. Binnen de gemeente kennen we dus meerdere verwerkingsverantwoordelijken, ieder voor de gegevensverwerkingen in het kader van de aan hen door het publiekrecht opdragen taken en toegekende bevoegdheden. In het kader van dit beleid zijn dat:
• **De burgemeester:** verwerkingsverantwoordelijke voor verwerkingen van persoonsgegevens in het kader van de handhaving van de openbare orde;
• **Het college van burgemeester en wethouders:** verwerkingsverantwoordelijke voor verwerkingen van persoonsgegevens in het kader van alle andere gemeentelijke taken;
Voor wat betreft de verwerking van persoonsgegevens in het kader van de uitoefening van privaatrechtelijke bevoegdheden, is de publiekrechtelijke rechtspersoon, **de gemeente Eindhoven**, de verwerkingsverantwoordelijke.

De uitoefening van de taken en bevoegdheden wordt neergelegd bij de aangewezen leidinggevenden en ambtenaren van de gemeente. Zij nemen dus de beslissingen rondom de doelen en middelen van de gegevensverwerkingen. Daar waar nodig is via het Mandaatbesluit en de Budgethoudersregeling voorzien in de specifieke bevoegdheden en taken. Dat betekent dat zij functioneel verantwoordelijk zijn voor de naleving van de wet- en regelgeving op het gebied van privacy en bescherming van persoonsgegevens. De formele verantwoordelijkheid blijft echter liggen bij de bovengenoemde verwerkingsverantwoordelijken. Zie voor een actuele inrichting van de functionele verantwoordelijkheid de mandaat- en bevoegdhedenregeling van de gemeente Eindhoven.

Bestuurlijk
Bij de meeste verwerkingsprocessen is, zoals hiervoor is weergegeven, de burgemeester dan wel het college van burgemeester en wethouders op bestuurlijk niveau eindverantwoordelijk voor het aantoonbaar naleven van de AVG en dit privacybeleid.

De wethouder met dienstverlening in de portefeuille is voor de gegevensverwerkingen onder de verantwoordelijkheid van het college coördinerend portefeuillehouder, en is verantwoordelijk voor het gemeentebreed voldoen aan de AVG en de Uitvoeringswet AVG. De burgemeester is coördinerend portefeuillehouder voor het toezicht op de AVG en Uitvoeringswet AVG. De burgemeester en iedere wethouder is bestuurlijk verantwoordelijk voor het voldoen aan AVG, de Uitvoeringswet AVG en de relevante materiewetten binnen de eigen portefeuille. Het college van burgemeester en wethouders heeft een bestuurlijke visie en aandacht voor het belang van de naleving van het gegevensbeschermingsrecht, stelt het privacybeleid vast, stelt de benodigde mensen en middelen beschikbaar om de werkprocessen van de gemeente privacybestendig te houden volgens dit privacybeleid en ziet toe op de inbedding van de privacy governance binnen de lijnorganisatie en verantwoordingsstructuur.

Ambtelijk
De Directieraad
De Directieraad (DR) is op ambtelijk niveau eindverantwoordelijk voor naleving van de AVG en het privacybeleid. De directeur algemene dienstverlening is binnen de DR de portefeuillehouder voor de AVG. De taken van de DR op het gebied van bescherming van persoonsgegevens zijn:
• Het adviseren van het College van B&W over de risico's van de verwerking van persoonsgegevens en de naleving van het privacybeleid;
• Het behandelen van voorstellen tot vaststellen van privacybeleid en behandelen van de resultaten van evaluatie van het privacybeleid;
• Het alloceren van financiële middelen om het privacybeleid uit te voeren;
• Het bewaken van de naleving van het privacybeleid, waaronder het opdracht geven tot het uitvoeren van audits.
In het kader van de uitvoering van deze taken, laat de DR zich informeren, waaronder in de vorm van (periodieke) rapportages, door: de sectorhoofden, de Chief Privacy Officer en de Chief Information Officer en de FG volgens de Regeling FG.

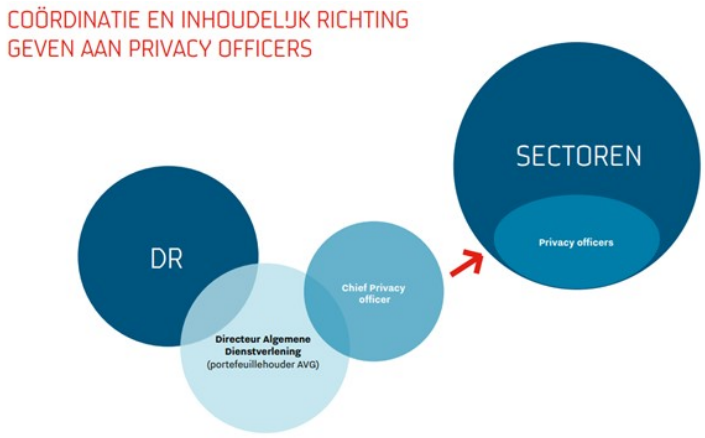
Afwijking van dit privacybeleid, mits dit incidenteel en tijdelijk is, behoeft de uitdrukkelijke instemming van de DR, gehoord hebbende het verantwoordelijke sectorhoofd. Het sectorhoofd kan zich hierbij laten ondersteunen door de (Chief) Privacy Officer. De DR vraagt daarbij advies aan de FG. De DR stemt de voorgenomen afwijking zo nodig af met de burgemeester dan wel het college van burgemeester en wethouders.
Beslissingen om af te wijken worden schriftelijk vastgelegd met de reden waarom wordt afgeweken en de overwegingen die daaraan ten grondslag lagen en welke risico's hierbij aan de orde zijn. Dit gebeurt in een directieraaddossier of, indien nodig, in een collegedossier.
Sectorhoofden
Elk Sectorhoofd is eindverantwoordelijk voor de implementatie en naleving van de wet- en regelgeving betreffende privacy en bescherming van persoonsgegevens en het privacybeleid in zijn of haar sector. Dit doet hij samen met de medewerkers binnen zijn sector. Zie in dat licht de Mandaat- en bevoegdhedenregeling van de gemeente Eindhoven. Het Sectorhoofd legt over zijn handelen en dat van zijn medewerkers verantwoording af aan de DR. De taken van het Sectorhoofd hierbij zijn:
• het (laten) uitvoeren van risicoanalyses (DPIA's) op gegevensverwerkingen, waaronder het, indien mogelijk, consulteren van (vertegenwoordigers van) betrokkenen en het inwinnen van het advies van de Functionaris Gegevensbescherming en, zo nodig, de Ethische Commissie.
• Het, in overleg met de directeur, de (Chief) Privacy Officer en de juristen, zo nodig verzoeken middels een DR-dossier om een voorafgaande raadpleging bij de Autoriteit Persoonsgegevens;
• in een voorkomend geval met ondersteuning van de (Chief) Privacy Officer onderbouwen waarom van een advies van de Functionaris Gegevensbescherming en/of van de Ethische Commissie wordt afgeweken en dit documenteren;
• het (laten) implementeren van passende juridische, technische en/of organisatorische maatregelen in de (gegevensverwerkings)processen om de geïdentificeerde risico's te mitigeren, inclusief:

o het – verplicht – sluiten van verwerkersovereenkomsten met dienstverleners die verwerker zijn voor de verwerkte persoonsgegevens;
o het – verplicht – maken van schriftelijke afspraken met gezamenlijke verwerkingsverantwoordelijken over de verdeling van taken rondom de naleving van de wet- en regelgeving op het gebied van de bescherming van persoonsgegevens;
o het – optioneel – sluiten van overeenkomsten met dienstverleners die zelfstandig verwerkingsverantwoordelijke zijn voor de verwerking van persoonsgegevens die zij ontvangen van de gemeente Eindhoven met daarin passende waarborgen voor de bescherming van persoonsgegevens;
o het sluiten van convenanten met samenwerkingspartners met daarin passende waarborgen voor de bescherming van persoonsgegevens waarvoor de gemeente Eindhoven verantwoordelijk is,
o het nemen van passende maatregelen om de persoonsgegevens te beveiligen, een en ander conform het informatiebeveiligingsbeleid van de gemeente Eindhoven;
o het zorgdragen dat de gegevensverwerking plaatsvindt volgens de beginselen van privacy-by-design & default.
o het organiseren van betekenisvolle menselijke tussenkomst in geval van de inzet van een algoritme dat leidt tot volledig geautomatiseerde besluitvorming, inclusief profilering, waaraan voor de betrokkene(n) rechtsgevolgen zijn verbonden of dat de betrokkene(n) anderszins in aanmerkelijke mate treft.
• het accepteren, documenteren en periodiek evalueren van eventuele restrisico's in de gegevensverwerking;
• het monitoren van de geïdentificeerde risico's, waaronder het periodiek evalueren van reeds uitgevoerde DPIA's, en het waar nodig implementeren van aanvullende maatregelen dan wel besluiten de gegevensverwerking te beëindigen;
• het monitoren van de naleving van de wet- en regelgeving en het privacybeleid;
• het (laten) behandelen van verzoeken van betrokkenen onder de AVG of Wpg, zoals inzage, correctie of verwijdering van persoonsgegevens, dan wel bezwaar tegen de (voorgenomen) verwerking van persoonsgegevens;
• het tijdig en op passende wijze (laten) onderzoeken van signalen en klachten met betrekking tot compliance-incidenten en het nemen van herstelmaatregelen, waaronder het (laten) nemen van passende maatregelen na een geconstateerd datalek en het (laten) melden van een datalek bij de Autoriteit Persoonsgegevens en de betrokkene(n);
• het, in overleg met de DR en Juridische Zaken, beslissen op een verzoek tot schadevergoeding als een betrokkene stelt schade te hebben geleden als gevolg van een gegevensverwerking in strijd met de toepasselijke wet- en regelgeving;
• het (laten) bijhouden van het (deel)register van verwerkingen in de sector en het (deel)register van geconstateerde datalekken;
• het zo nodig nemen van disciplinaire maatregelen jegens medewerkers en leveranciers die zich niet houden aan het privacybeleid en de daarbij behorende procedures, afspraken en instructies.

Waar een Sectorhoofd een taak kan laten uitvoeren, kan die taak worden uitgevoerd door het betreffende Afdelingshoofd in de betreffende sector. Het Sectorhoofd monitort de uitvoering van deze taken. Het Sectorhoofd c.q. het Afdelingshoofd kan zich daarbij laten bijstaan door een Privacy Officer en de juristen. Daarnaast wijst het Sectorhoofd een medewerker aan die de rol van Privacy Ambassadeur vervult. Deze Privacy Ambassadeur biedt eerstelijnsondersteuning bij het naleven van de wet- en regelgeving en het privacybeleid, zoals, het afhandelen van verzoeken van de uitoefening van de rechten van betrokkenen, het creëren van bewustwording onder collega's en het beantwoorden van hun vragen en het vanuit de eerste lijn helpen bij het afhandelen van een datalek.

Conform de regeling FG wordt de FG bij alle genoemde taken tijdig en naar behoren betrokken.

4.3 Tweede lijn: inhoudelijke en functionele ondersteuning



Inhoudelijke ondersteuning

De Chief Privacy Officer (CPO)

De Chief Privacy Officer is de schakel naar directie en sectoren en verantwoordelijk voor organisatiebrede privacyvraagstukken. De Chief Privacy Officer en het team die hij coördineert zijn verantwoordelijk voor de algemene kennisoverdracht met betrekking tot gegevensbescherming en het signaleren en oppakken van organisatiebrede vraagstukken op dat vlak. Eveneens coördineert hij de controlerende en bewakende taak van en het inhoudelijk richting geven aan de tweede lijn.

Deze functie omvat het zorgdragen voor coördinatie van en inhoudelijk richting geven aan de Privacy Officiers (PO's) en directie aan de hand van het vormen van beleid, preventie, voorlichting, scholing, incidentenaanpak en onderzoek. Ook is hij de noodzakelijke luis in de pels van de organisatie. De Chief Privacy Officer is namens de portefeuillehouder in de DR belast met de uitrol van het privacybeleid in de gemeentelijke organisatie, het bewaken van de naleving daarvan en het borgen van het vertrouwen van inwoners en medewerkers in de gemeente Eindhoven. De Chief Privacy Officer heeft de volgende taken:

- het signaleren en oppakken van organisatiebrede gegevensbeschermingsrechtelijke vraagstukken;
- het coördineren van het verhogen van de bewustwording bij de eerste lijn;
- het opstellen, beheren en uitdragen van ethische richtlijnen voor het gebruik van (digitale) informatie, waaronder privacy en AI;
- het opstellen van een compliance programma;
- het beheren van het privacybeleid en waar nodig doen van wijzigingsvoorstellen aan de DR;
- het opstellen van deelbeleid en procedures ter ondersteuning van de hierboven beschreven taken van het Sectorhoofd;
- het controleren en bewaken van de naleving van de toepasselijke wet- en regelgeving op het gebied van bescherming van persoonsgegevens en het privacybeleid door de gemeentelijke organisatie, onder meer door het opstellen en meten van key performance indicators (KPI's) en het rapporteren daarover aan de DR;
- het voorzitten van de het privacy overleg, en het afstemmen van het (deel)beleid en procedures met andere gemeentelijke functies, waarbij het gaat om het afwegen van de noodzaak, haalbaarheid en uitvoerbaarheid van de voorstellen van de Chief Privacy Officer;
- het coördineren van en het inhoudelijk richting geven aan de Privacy Officer(s).
- het onderhouden van contacten met relevante organisaties buiten de gemeentelijke organisatie, zoals de Chief Privacy Officers van samenwerkingspartners/-verbanden, de VNG, de verantwoordelijke ministeries en de Europese Commissie, het (Europees) parlement, vaktechnische organisaties en belangengroepen namens betrokkenen.

De Chief Privacy Officer rapporteert rechtstreeks aan de Directeur Algemene Dienstverlening. De rol van Chief Privacy Officer wordt vervuld vanuit de tweede lijn. Deze rol kan niet vervuld worden door een medewerker die ook een rol in de eerste of derde lijn vervult.

De Strategisch Privacy Adviseur

De Strategisch Privacy Adviseur maakt onderdeel uit van het team van de Chief Privacy Officer en is verantwoordelijk voor het opstellen, het beheer en de werking van het privacybeleid en het borgen van het vertrouwen van inwoners en medewerkers in de gemeente Eindhoven. Hij of zij voert voor de Chief Privacy Officer de volgende taken uit:

- het adviseren van de Chief Privacy Officer over het verhogen van de bewustwording bij de eerste lijn;
- het opstellen, beheren en uitdragen van ethische richtlijnen voor het gebruik van (digitale) informatie, waaronder privacy en AI.
- het beheren van het privacybeleid en waar nodig doen van wijzigingsvoorstellen

• het doen van voorstellen voor beleid en procedures ter ondersteuning van de hierboven beschreven taken van het Sectorhoofd;
• het bewaken en verbeteren van de kwaliteit van organisatiebrede privacybeheersmaatregelen en -procedures, waaronder risicomanagement, privacytraining, incidentmanagement, en de inzet van deskundige adviseurs (intern/extern).
• het controleren en bewaken van de naleving van de toepasselijke wet- en regelgeving op het gebied van bescherming van persoonsgegevens en het privacybeleid door de gemeentelijke organisatie, onder meer door het opstellen en meten van key performance indicators (KPI's) en het rapporteren daarover aan de Chief Privacy Officer;
• het in afstemming met de Chief Privacy Officer onderhouden van contacten met relevante organisaties buiten de gemeentelijke organisatie.

De Privacy officer
De Privacy Officer ondersteunt het Sectorhoofd (c.q. het Afdelingshoofd) bij de uitvoering van diens taken met betrekking tot de bescherming van persoonsgegevens, het privacybeleid, het eventuele deelbeleid en de procedures.
De aanvullende taken van de Privacy Officer zijn:
• het verhogen van de bewustwording bij de eerste lijn in de vorm van het geven van voorlichting over privacy en bescherming van persoonsgegevens aan de sectoren en afdelingen;
• het gevraagd en ongevraagd geven van deskundig advies met betrekking tot de toepassing van wet- en regelgeving, het privacybeleid, het eventuele deelbeleid en de relevante procedures;
• het begeleiden van de uitvoering en afronding van DPIA's en het geven van deskundig advies met betrekking tot de risico's en maatregelen;
• het opstellen van sector-/afdelingsspecifieke regels en procedures; en
• het signaleren van nalevingsproblemen richting het Sectorhoofd en de Chief Privacy Officer.

De Privacy Officer maakt net als de Strategische Privacy Adviseur deel uit van het team wat de Chief Privacy Officer coördineert. De Chief Privacy Officer stemt de toewijzing van privacy officier aan één of meerdere sectoren c.q. afdelingen af met de betrokken directeur en/of sectorhoofden. De Privacy Officer heeft een functionele rapportagelijn met het betreffende Sectorhoofd c.q. Afdelingshoofd.

Juridische Zaken
De Afdeling Juridische Zaken biedt met behulp van gespecialiseerde privacy juristen ondersteuning aan de eerste lijn zoals bij:
• het opstellen van standaard(verwerkers)overeenkomsten en convenanten organisatie breed inzake de verwerking van persoonsgegevens (het sluiten van verwerkersovereenkomsten niet, dat gebeurt door eerste lijn);
• het voeren van bezwaar- en beroepsprocedures met betrekking tot de verwerking van persoonsgegevens dan wel de uitoefening van de rechten van betrokkenen.

De Afdeling Juridische Zaken biedt ook ondersteuning aan de tweede lijn zoals bij:
• de uitleg van wet- en regelgeving, relevante jurisprudentie en de richtlijnen en uitspraken van de Autoriteit Persoonsgegevens;
• het adviseren van de Chief Privacy Officer bij de beantwoording van complexe privacyvraagstukken.

CIO Office
Vanuit de systeemverantwoordelijkheid zorgt CIO Office voor het organiseren van de infrastructuur en het actueel houden van de benodigde randvoorwaarden (systeem, proces, beleid, tooling, etc.) zodat de uitvoerend verantwoordelijken de resultaten keer op keer kunnen realiseren.

Het ambtelijk privacy overleg
De Chief Privacy Officer is verantwoordelijk voor het organiseren en voorzitten van het ambtelijk privacy overleg. Het overleg heeft tot doel om voorstellen van de Chief Privacy Officier (bijvoorbeeld beleid, plannen, compliance programma, e.d.) te bespreken op noodzaak, uitvoerbaarheid en haalbaarheid.Het overleg neemt geen beslissingen, besluiten worden voorgelegd aan directieraad of college van B&W. Bij deze besluitvorming wordt de FG conform de FG regeling betrokken. In het overleg wordt de jaaragenda van activiteiten ter verbetering van het compliance programma opgesteld en bewaakt, waarbij eveneens wordt stilgestaan bij de uitvoerbaarheid van die activiteiten, en zet het overleg zich in voor het bevorderen van het algemene volwassenheidsniveau binnen de gemeente.

In dit overleg hebben in ieder geval zitting:
• De Sectorhoofden die het meest aangaat, waaronder:
o het Sectorhoofd Veiligheid en Handhaving
o het Sectorhoofd Sociaal Maatschappelijke Ondersteuning
o het Sectorhoofd Publiekscontacten
o het Sectorhoofd Intake, Vergunningen, Toezicht en Handhaving

• de Strategisch Privacy Adviseur
• het afdelingshoofd Juridische zaken
• de Chief Information Officer (CIO)
• de Chief Procurement Officer

De ambtelijk privacy overleg komt in ieder geval 2x per jaar bijeen, of zoveel vaker als nodig is.

Functionele ondersteuning
Inkoop en Contractmanagement
De sector CPO Office (Inkoop en Contractmanagement) biedt ondersteuning bij de inkoop van producten en diensten die relevant zijn voor de verwerking c.q. de bescherming van persoonsgegevens waarvoor de gemeente Eindhoven verantwoordelijk is. Meer in het bijzonder ondersteunt Inkoop en Contractmanagement bij:
• de naleving van de eisen van privacy-by-design & default;
• de naleving van het informatiebeveiligingsbeleid;
• het sluiten van de (verwerkers)overeenkomsten; en
• de (periodieke) controle van de naleving van de gemaakte afspraken inzake privacy en de bescherming van persoonsgegevens;

Personeel & Organisatie
De sector Personeel & Organisatie (P&O) biedt ondersteuning voor wat de naleving van de wet- en regelgeving, het privacybeleid en het eventuele deelbeleid door de medewerkers van de gemeente Eindhoven. Meer in het bijzonder adviseert P&O bij het vaststellen en de uitvoering van het beleid op het gebied van het niet-naleven van wet- en regelgeving, het privacybeleid en het eventuele deelbeleid door de medewerkers van de gemeente Eindhoven, waaronder het opleggen van disciplinaire maatregelen. Daarnaast registreert P&O de trainingen en opleidingen rondom privacy.

Communicatie
De sector Communicatie biedt deskundige ondersteuning bij de communicatie rondom de bescherming van privacy en persoonsgegevens. Meer in het bijzonder ondersteunt de sector Communicatie bij:
• het opstellen van privacyverklaringen;
• het opstellen van meldingen van datalekken aan betrokkenen;
• het opstellen van persberichten met betrekking tot privacy en bescherming van persoonsgegevens; en
• het vormgeven van bewustzijnscampagnes op het gebied van privacy en bescherming van persoonsgegevens.

Conform de regeling FG wordt de FG bij alle genoemde taken tijdig en naar behoren betrokken.

4.4 Derde lijn: de Functionaris voor Gegevensbescherming (FG)
Het oordeel of advies van de FG is ‘zwaarwegend’, dat wil zeggen dat daar alleen schriftelijk en gemotiveerd van het oordeel of advies kan worden afgeweken. Het oordeel van de FG is daarmee niet bindend

De gemeente dient ervoor te zorgen dat de FG tijdig en naar behoren wordt betrokken. De Regeling FG is hiervoor een hulpmiddel. De situaties die in de regeling zijn beschreven, waarin de FG moet worden geraadpleegd, betreft geen limitatieve opsomming. Het blijft dus van belang dat de organisatie ook buiten de situaties die zijn opgenomen in deze regeling, blijft beoordelen of de FG dient te worden betrokken.

Versiebeheer

Versie	Status	Door	Datum	Beschrijving
1.00	Concept	Gemeente Eindhoven	21-05-2025	Conceptversie Privacybeleid AVG: Beleidskader gegevensbescherming 1.00

Bijlage 1: Afwegingskader voor gegevensverwerkingen
Onderstaande vragen helpen om te bepalen of een gegevensverwerking is toegestaan en welke risico's daarmee gemoeid zijn. Daarbij moeten we eerst kijken naar onze bevoegdheden en pas daarna naar de verwerking van persoonsgegevens. Als het proces an sich problematisch is, is de bijbehorende gegevensverwerking immers ook problematisch.

I. Belangenafweging rondom de inzet van bevoegdheden of uitvoering van taken

1. Zijn wij bevoegd om het proces uit te voeren waar we de persoonsgegevens voor willen verwerken?
Als gemeente mogen wij alleen belangen behartigen waartoe we wettelijk bevoegd zijn. Onze taken en bevoegdheden staan in materiewetten, zoals de Gemeentewet, de Participatiewet of de Wet basisregistratie personen. Als werkgever mogen wij arbeidsovereenkomsten uitvoeren en alle redelijke maatregelen nemen ter bevordering van de goede orde in onze organisatie (waaronder het nemen beveiligingsmaatregelen of het aanbieden faciliteiten aan onze medewerkers). En als verkoper of inkoper van goederen en diensten mogen wij onze belangen behartigen die gemoeid zijn met die verkoop of inkoop.

2. Dient de inzet van de bevoegdheden een legitiem doel?
Een veelheid aan belangen waarvoor wij als gemeente aan de lat staan, dienen als legitiem doel. Denk bijvoorbeeld aan de bescherming van de openbare orde of de volksgezondheid, belastingheffing, de bescherming van de betrokkene of anderen, en dergelijke.

3. Is het noodzakelijk om in deze situatie onze bevoegdheden in te zetten?
Of het noodzakelijk is om onze bevoegdheden in te zetten, is vaak afhankelijk van de omstandigheden van het geval. Daarbij moeten we letten op de volgende aandachtspunten:
a. Kunnen we uitleggen wat we doen en waarom? En doen we wat we zeggen?
b. Leidt wat we willen doen tot een verregaande inperking van grondrechten en vrijheden van mensen?
c. Draagt het proces effectief bij aan het verwezenlijken van het doel?
d. Kunnen we dit doel wellicht ook bereiken met minder vergaande middelen?
e. Zijn er, zo nodig, effectieve waarborgen aanwezig om de gevolgen voor mensen tot een minimum te beperken?

4. Is het maatschappelijk aanvaardbaar of ethisch dat wij die bevoegdheid in deze situatie(s) inzetten?
Het feit dat we van de wet iets mogen, wil niet zeggen dat we het ook moeten doen. Het inzetten van bevoegdheden vereist een belangenafweging, vaak door het management (DR, Sectorhoofd, afdelingshoofd) in mandaat van het College. Bij alles wat we doen, moeten we ons de vraag stellen of het ook moreel verantwoord is wat we doen en of we het ook willen. Een goede lakmoesproef is: "wie wordt er boos als wij dit doen, en hebben we dan een goed verhaal"?

Belangenafweging rondom de gegevensverwerking

5. Identificeer de belangen die zijn gemoeid met de gegevensverwerking
De gegevensverwerking kan meerdere belanghebbenden hebben, zoals de betrokkene zelf, de gemeente en/of derden. Breng alle betrokken belangen en bijbehorende belanghebbenden in kaart.

6. Breng in kaart hoe zwaar elk belang weegt
Hoe groter een belang, hoe waarschijnlijker het is dat de gegevensverwerking wel of juist niet is toegestaan. Of wellicht alleen onder voorwaarden. Dit noemen we ook wel de proportionaliteitstoets.

7. Breng in kaart welke soort(en) persoonsgegevens we willen verwerken?
a. Gewone persoonsgegevens.
b. Een wettelijk identificerend nummer (zoals BSN).
c. Politiegegevens (ga naar Addendum Wpg-gegevens).
d. Bijzondere persoonsgegevens (verboden, tenzij).
e. Strafrechtelijke persoonsgegevens (verboden, tenzij).

8. Breng van elk gegeven de noodzaak in beeld.
Het principe van dataminimalisatie vereist dat we niet meer gegevens verwerken dan nodig. Een gegeven is noodzakelijk als het 'objectief onmisbaar' is voor het doel. Met andere woorden: wat gaat er fout als dit specifieke gegeven niet zou worden verwerkt, en is dat voor ons of een ander onaanvaardbaar? Daarnaast moet het gegevens geschikt zijn om het doel te bereiken (effectiiteit). Als dat niet zo is, is een gegeven niet noodzakelijk.

9. Beoordeel de risico's van de (voorgenomen) gegevensverwerking voor de betrokkene
Privacyrisico's (kans x impact) kunnen als volgt worden geclassificeerd:

i. Een privacyrisico is laag/verwaarloosbaar als de gevolgen waarschijnlijk herstelbaar zijn (zoals terugdraaien van de gevolgen of de schade snel en makkelijk compenseren), zodat de gevolgen en de daaruit voortvloeiende schade niet blijvend zijn.
ii. Een privacyrisico is gemiddeld als de kans op bepaalde gevolgen fifty-fifty is en die gevolgen waarschijnlijk (voorlopig) onherstelbaar zijn.
iii. Een privacyrisico is hoog als de kans op bepaalde gevolgen groot is en de gevolgen vermoedelijk onherstelbaar zijn.

We kijken naar de risico's van de gegevensverwerking zoals die is voorgenomen (op de tekentafel ligt); dat wil zeggen de risico's zonder de aanvullende maatregelen en waarborgen die we eventueel naar aanleiding van de DPIA nemen (oftewel het brutorisico). Als blijkt dat die risico's disproportioneel zijn, dan moeten we passende maatregelen treffen of waarborgen inbouwen die de gevonden risico's tot een aanvaardbaar niveau terugbrengen (oftewel het nettorisico). Risico's die we niet hoeven terug te brengen, noemen we de restrisico's. Die moeten we accepteren (en periodiek evalueren).

10. Weeg de betrokken belangen tegen elkaar af
Als een DPIA is uitgevoerd, leggen we in de DPIA de belangenafweging vast. Als geen DPIA is uitgevoerd, bijvoorbeeld omdat de risico's waarschijnlijk laag/verwaarloosbaar waren, dan is de vastlegging van de belangenafweging niet vereist. Als er echter bezwaar tegen wordt gemaakt of als de FG of de AP er vragen over stelt, moet de belangenafweging wel gereproduceerd kunnen worden!