EINDHOVEN
GEMEENTEBLAD
Officiële uitgave van de gemeente Eindhoven
Nr. 417575
26 september
2025

Strategisch privacybeleid Gemeente Eindhoven

Uitvoering AVG en Wpg

Uitgave
Gemeente Eindhoven
CIO Office

Datum
Februari 2023

Grondslag van dit document
De Algemene Verordening Gegevensbescherming (AVG), inwerking getreden op 25 mei 2018 en de Wet politiegegevens (Wpg), geïmplementeerd op 1 januari 2019, zijn het raamwerk dat is gebruikt voor de uitwerking van het beleid in dit document.

Inwerkingtreding
Dit beleid treedt in werking na vaststelling en bekendmaking door het college van burgemeester en wethouders (college van B&W).

Begrippen en afkortingen

Elk begrip dat hier niet is gedefinieerd, maar dat wel is gedefinieerd in de AVG, UAVG of de Wpg (zoals 'persoonsgegeven', 'verwerken', 'Inbreuk', etc.), heeft in het privacybeleid dezelfde betekenis als voornoemde wetgeving. Om deze reden worden deze begrippen hier niet opgesomd.

AP	Autoriteit Persoonsgegevens
AVG	Algemene Verordening Gegevensbescherming
Awb	Algemene wet bestuursrecht
Bureau FG	Ter ondersteuning van de taken en werkzaamheden van de FG zijn een adviseur gegevensbescherming/plaatsvervangend FG en een medewerker gegevensbescherming aangesteld. Samen met de FG vormen zij 'bureau FG', toezichthouder op het gebied van naleving van de AVG en Wpg.
CIO	Chief Information Officer (sectorhoofd Informatievoorziening (IV))
CIO Office	Het CIO Office is verantwoordelijk en kaderstellend voor strategie op het gebied van informatievoorziening (IV).
CISO	Chief Information and Security Officer
College van B&W	College van burgemeester en wethouders gemeente Eindhoven
DPIA	Data Protection Impact Assessment (gegevensbeschermingseffectbeoordeling)
DR	Directieraad gemeente Eindhoven
FG	Functionaris Gegevensbescherming. De FG AVG is de interne toezichthouder op de naleving van de AVG/Wpg.
Gemeente	Gemeente Eindhoven en in elk geval ook bestuurders en medewerkers van de gemeente Eindhoven.
Governance	Implementatie van richtlijnen, strategie en verantwoordelijkheden en het uitvoeren van beleid.
Medewerkers	Eigen personeel, inhuur uitzendkrachten en stagiaires

Persoonsgegevens	Een persoonsgegeven is alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Het betreft gegevens waardoor een persoon direct of indirect herleidbaar is.
PO	Privacy Officer (hieronder valt ook de functie Adviseur privacy, AVG en procesmanagement).
Privacy Team	De SIA Privacy en de Privacy Officers
Raad	Gemeenteraad gemeente Eindhoven
Risico	Kans x impact
SIA	Strategisch informatieadviseur
SIA Privacy	Strategisch Informatieadviseur privacy (deze functionaris wordt intern ook Centrale Privacy Officer of Chief Privacy Officer genoemd)
UAVG	Uitvoeringswet Algemene Verordening Gegevensbescherming
Wpg	Wet politiegegevens

Inleiding

De gemeente als overheidsorganisatie verricht wettelijke en bestuurlijke taken voor inwoners en bedrijven. Voor veel van deze taken is het noodzakelijk om persoonsgegevens van betrokkenen te verwerken. Betrokkenen hebben recht op correcte, veilige en betrouwbare informatieverwerking en moeten erop kunnen vertrouwen dat de gemeente zorgvuldig met deze gegevens omgaat. Zeker omdat zij niet altijd de keuze hebben om hun (soms zeer privacy gevoelige) gegevens aan de gemeente toe te vertrouwen. Het doel van dit strategische privacybeleid is om de belangen van betrokken van wie de gemeente persoonsgegevens verwerkt centraal te stellen.

De AVG en de Wpg zijn de wettelijke kaders voor de wijze waarop de gemeente omgaat met persoonsgegevens. Dit strategische privacybeleid is de uitwerking van deze centrale kaders voor de gemeentelijke bedrijfsvoering (voor zover hierbij sprake is van de verwerking van persoonsgegevens).

De AVG geldt niet voor gegevens die worden verwerkt voor de opsporing of vervolging van strafbare feiten. Voor dat soort gegevens geldt de Europese Richtlijn gegevensverwerking opsporing en vervolging. In Nederland is deze richtlijn geïmplementeerd in de Wpg per 1 januari 2019.

Dit strategisch privacybeleid vormt het kaderstellende en richtinggevende ‘kapstokbeleid’ voor de gemeente bij het voldoen aan de verplichtingen van de AVG en de Wpg. Het maakt deel uit van het pakket aan documenten, processen en beheersmaatregelen waarmee de gemeente voldoet aan haar verantwoordingsplicht. Het helpt de gemeente zelf om te zien of er voldoende maatregelen zijn genomen door de borging van privacy.
Uit dit strategische ‘kapstokbeleid’ vloeien interne tactische uitvoeringsregels, processen, handreikingen en standaarden voort over onder andere:

- Privacy risicomanagement
- DPIA
- Meldplicht datalekken
- Rechten van betrokkenen
- Inkoop- en contractmanagement
- Datastrategie

In de operationele processen zijn de taken, rollen en verantwoordelijkheden expliciet belegd. Dit draagt bij aan het daadwerkelijk en structureel uniform uitvoeren en borgen van de beheersmaatregelen. Indien nodig worden specifieke privacy beleidsregels opgesteld voor een specifieke toepassing of sector.

Dit strategische beleid is bestemd voor alle medewerkers van de gemeente. Het geeft aan waar de gemeente voor staat en wat zij wil uitdragen.

1 Algemeen

1.1 Doel

Doel van dit strategisch privacy beleid is ervoor zorgen dat er op strategisch niveau binnen de gemeente afdoende randvoorwaarden en condities aanwezig zijn om persoonsgegevens in overeenstemming met de toepasselijke wet- en regelgeving te verwerken.

1.2 Visie

- Een goed geïmplementeerd privacybeleid, waarbij alle medewerkers zich ten volle bewust zijn van de noodzakelijkheid van een goede omgang met persoonsgegevens én van de ruimte die de wet- en regelgeving biedt om persoonsgegevens te verwerken.
- De gemeente past de wettelijke eisen toe en gaat respectvol om met de persoonsgegevens van betrokkenen van wie persoonsgegevens worden verwerkt.
- De rechten van betrokkenen worden gerespecteerd en zijn in de gemeentelijke processen verankerd.
- Bij verwerking van persoonsgegevens worden alle relevante wettelijke grondslagen die verwerking mogelijk maken in de afweging betrokken en wordt gezocht naar de ruimte die de wet biedt.
- Afwijking van wet- en regelgeving vraagt om expliciete besluitvorming. Een besluit hiertoe moet gemotiveerd en met een risicoanalyse aan de DR worden voorgelegd waarna besluitvorming door portefeuillehouder of college van B&W volgt. De FG wordt betrokken en geïnformeerd.
- Het vertrouwen van inwoners in de overheid wordt niet beschaamd.
- Het vertrouwen van de medewerkers in de gemeente als werkgever wordt niet beschaamd.
- De risico's bij het verwijtbaar en onvoldoende beschermen van persoonsgegevens en het niet naleven van privacywet- en regelgeving worden zo veel mogelijk beperkt.

1.3 Ambitie

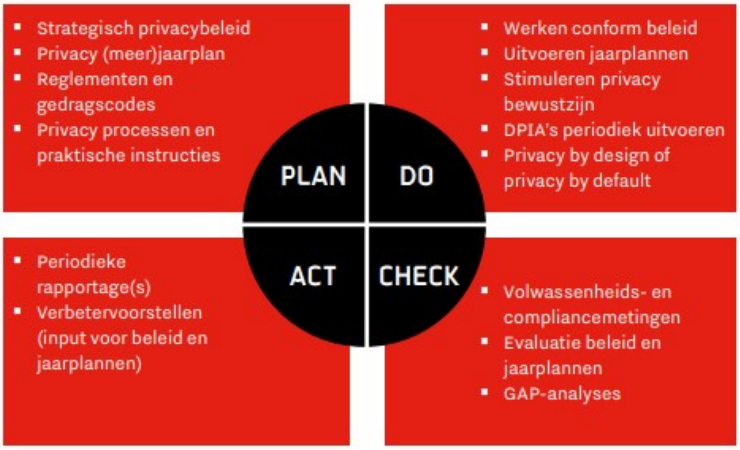
De ambitie gaat over de gewenste richting waarop geanticipeerd wordt in dit strategisch privacybeleid. Door het adviesbureau PMP is een privacy kompas ontwikkeld als middel om de privacy ambitie te formuleren. Het kompas helpt, adviseert en geeft richting aan de naleving van de AVG en de Wpg alsook aan sturing hierop. Dit kompas gebruikt de gemeente om haar privacy ambitie te bepalen.

De 4 kwadranten staan voor de compliance niveaus van privacy:
- Kwadrant rechtsboven: de AVG en Wpg wordt goed toegepast volgens de principes van privacy by design (voorzien waar dat werkelijk nodig is).
- Kwadrant rechtsonder: roekeloos gedrag waarbij geen aandacht wordt besteed aan de AVG en/of Wpg.
- Kwadrant linksonder: ontoereikend werken binnen een afvinkcultuur.
- Kwadrant linksboven: bureaucratische werkwijze met een contra productieve uitwerking op het efficiënt en effectief uitvoeren van de AVG en Wpg.

De gemeente voldoet aan de minimale eisen van de AVG. De ambitie van de gemeente is stapsgewijs professionaliseren tot het compliance niveau naar de bedoeling van de AVG en de Wpg (kwadrant rechtsboven: evenwichtig en duurzaam).

1.4 PDCA

Het geambieerde ambitieniveau bereikt de gemeente stapsgewijs met de Plan-Do-Check-Act (PDCA methode) en door een positieve en actieve betrokkenheid van iedereen. Deze methode is bedoeld als verbeterproces.



De PDCA vormt het privacy managementsysteem om compliance blijvend te beheersen en waarbij elke verbeterstap wordt geborgd.

1.5 Cultuur en gedrag

Privacy moet in de bedrijfsvoering van de organisatie worden ingebed en alle medewerkers moeten zich er continu van bewust zijn. Met beleid alleen wordt niet geborgd dat persoonsgegevens rechtmatig worden verwerkt. Ook de cultuur van de gemeente en het gedrag van medewerkers waarbij continu aandacht voor privacy is, zijn nodig om te kunnen voldoen aan wet- en regelgeving.

Het belang van privacy moet sterk uitgedragen worden door bestuur en management omdat dit mede-bepalend is voor het positief beïnvloeden van gedrag en cultuur in de organisatie. Daarom ligt de focus op zowel processen en methodes, alsook op doel en mensen inclusief het verbreden en verdiepen van het kennisniveau organisatie breed.
Bij alle zaken die over persoonsgegevens gaan, wordt tijdig en naar behoren advies van de FG ingewonnen. Om voornoemde goed te laten werken, wordt het besef breed uitgedragen dat privacy van belang is. Op deze manier zijn de verantwoordelijkheden van medewerkers op alle niveaus duidelijk en is duidelijk wie wanneer en waarvoor aan zet is.

Iedere (nieuwe) medewerker wordt door de gemeente geïnformeerd over het zorgvuldig omgaan met persoonsgegevens, bijvoorbeeld via instructies. Daarnaast legt iedere ambtenaar een ambtseed af. Integriteit, zoals verwoord in de Gedragscode Ambtenaren 2020, is hiervan een onderdeel. De overige principes uit de 'gedragscode voor ambtenaren' gelden ook bij de bescherming van persoonsgegevens. Handelen naar deze principes zorgt ervoor dat de medewerkers van de gemeente op gebied van persoonsgegevensbescherming een cultuur creëren waar privacy onderdeel is van de processen die de gemeente uit voert. Die cultuur zorgt ervoor dat het gemak en de veiligheid voor de betrokkenen, waarvan de gemeente persoonsgegevens verwerkt, niet vergeten wordt.

Daarnaast zijn de 3 centrale kernwaarden uit de gemeentelijke organisatievisie van belang:

1. Samenwerking binnen de gemeente en met organisaties buiten de gemeente is van essentieel belang voor een optimale dienstverlening. Vanuit die samenwerking oog hebben voor privacy en de bescherming van persoonsgegevens betekent dat de gemeente betrokkenen direct en in begrijpelijke taal meldt voor welke rechtmatige, gerechtvaardigde doelen zij hun persoonsgegevens registreren en met elkaar uitwisselen (als dit het geval is).
2. Vertrouwen (integer, vriendelijk, eerlijk en open). De diensten die de gemeente levert, komen voort uit wat betrokkenen nodig hebben. Betrokkenen kunnen er ook op rekenen dat de gemeente zorgt voor correcte en consequente handhaving. Betrokkenen moeten er altijd op kunnen vertrouwen dat hun gegevens in veilige handen zijn. Vertrouwelijkheid en integriteit zijn hierbij de sleutelwoorden. Daarnaast betekent dit dat de gemeente passende organisatorische en technische maatregelen neemt om risico's te vermijden en daarmee de privacy te waarborgen.
3. Eigenaarschap ("we zijn ervan"). Duidelijkheid en verantwoordelijkheid ('ervan zijn') zijn nodig om het beste resultaat te boeken voor de stad. Dit betekent verantwoordelijkheid nemen om de privacy te waarborgen van betrokkenen, door zorgvuldig om te gaan met de persoonsgegevens van de betrokkenen en zo nodig anderen erop aan te spreken als zij de vereiste zorgvuldigheid niet voldoende in acht nemen. Door als gemeente voor deze betrokkenen altijd goed bereikbaar en aanspreekbaar te zijn als deze een beroep doen op hun privacy rechten. Maar ook door het direct melden van datalekken, mocht er onverhoopt toch iets zijn misgegaan.

1.6 Reikwijdte (scope)

Het strategisch privacybeleid is van toepassing op:
- alle persoonsgegevens die door de gemeente verwerkt worden van inwoners, medewerkers van (en voor) de gemeente en medewerkers van bedrijven;
- alle processen van de gemeente waarbinnen persoonsgegevens worden verwerkt;
- de onderliggende voorzieningen voor informatieverwerking en gegevensopslag (zowel papier als digitaal);
- alle ruimten en devices die door medewerkers worden gebruikt waar(op) persoonsgegevens worden verwerkt;
- de verwerking van statistische en/of geaggregeerde gegevens, voor zover niet kan worden uitgesloten dat personen kunnen worden geïdentificeerd of geprofileerd.

2 Juridische uitgangspunten

2.1 Doelbinding

De gemeente verwerkt alleen persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Voor de uitvoering van een aantal sectorspecifieke wetten zijn de doelen al in de wet vastgelegd evenals de persoonsgegevens die gevraagd en verwerkt mogen worden. Bij verzameling of gebruik van grote aantallen gegevens (open/big data) is er extra aandacht als er verwerking van persoonsgegeven plaatsvindt.

Gegevens mogen niet voor andere doelen verwerkt worden. Verdere verwerking kan alleen plaatsvinden wanneer dit verenigbaar is met het oorspronkelijke doel. Als de gegevens gebruikt worden voor een ander doel, doet de gemeente dit alleen als het past binnen de wettelijke kaders. Als deze beoordeling positief is dan verwerkt de gemeente de gegevens ook voor het andere doel.

Voor al haar verwerkingen specifieert, omschrijft en legitimeert de gemeente het doel. Zolang de gemeente de persoonsgegevens verwerkt, is er doelbinding. Dit betekent dat periodiek opnieuw wordt getoetst wat het doel is, hoe dit omschreven moet worden en wat de legitimiteit van de verwerking is. Specificering (welbepaald), omschrijving (uitdrukkelijk omschreven) en legitimatie (gerechtvaardigd) zijn voorwaardelijk voor de doelbinding.

Voor meer informatie over de doeleinden van de verwerking van persoonsgegevens door de gemeente wordt verwezen naar de specifieke privacyverklaringen, zoals gepubliceerd op de gemeentelijke website, en het verwerkingsregister.

2.2 Rechtmatigheid en behoorlijkheid

Persoonsgegevens worden in overeenstemming met wet- en regelgeving en op behoorlijke en zorgvuldige wijze verwerkt. De verwerking van persoonsgegevens door de gemeente is gebaseerd op een of meer van de wettelijke grondslagen uit de AVG of Wpg. De grondslag m.b.t. gerechtvaardigde belangen mag niet worden gebruikt voor de uitoefening van de gemeentelijk taak.

De gemeente heeft te maken met de verwerking van reguliere en gevoelige persoonsgegevens alsook bijzondere persoonsgegevens. Vanuit de wetgeving geldt nadrukkelijk het verbod om bijzondere persoonsgegevens te verwerken. Onder bepaalde voorwaarden, uitgewerkt in de UAVG, zijn verwerkingen van deze gegevens wél toegestaan. Daar waar de gemeente bijzondere categorieën persoonsgegevens verwerkt, is aan deze voorwaarden voldaan.

2.3 Transparantie

Het transparantiebeginsel vereist dat betrokkenen kunnen achterhalen dat, hoe en waarom hun persoonsgegevens worden verwerkt. Tenzij er belangen zijn, genoemd in wet- of regelgeving, die zich daartegen verzetten.
De gemeente informeert betrokkenen over het verwerken van persoonsgegevens op of voor het moment dat betrokkene ze beschikbaar stelt. Worden de gegevens buiten de betrokkene om verkregen, dan wordt de betrokkene op het moment dat ze voor de eerste keer worden verwerkt hierover geïnformeerd. Tenzij er een grond is om achteraf te informeren.

2.4 Dataminimalisatie (subsidiariteit en proportionaliteit)

Het verwerken van persoonsgegevens dient te voldoen aan het vereiste van dataminimalisatie. Dit beginsel brengt met zich mee dat niet meer persoonsgegevens mogen worden verwerkt dan strikt noodzakelijk is voor het doel. Ook vloeit uit dit beginsel voort dat persoonsgegevens alleen mogen worden verwerkt indien het doel van de verwerking niet redelijkerwijs op een andere wijze kan worden verwezenlijkt.
Waar mogelijk worden minder of geen persoonsgegevens verwerkt.
De gemeente beperkt inbreuk op de persoonlijke levenssfeer van de betrokkene zoveel mogelijk en zoekt altijd de minst belastende manier. Inbreuk op de belangen van de betrokkene mag niet onevenredig zijn in verhouding tot het doel. Hoofdregel is dat het alleen toegestaan is in overeenstemming met de wet en op een zorgvuldige wijze. Persoonsgegevens worden zoveel mogelijk verzameld bij de betrokkene zelf. De wet gaat uit van subsidiariteit: verwerking is alleen toegestaan als het doel niet op een andere manier kan worden bereikt. In de wet wordt ook gesproken over proportionaliteit: gegevens mogen alleen worden verwerkt als dit in verhouding staat tot het doel. Kan zonder of met minder (belastende) persoonsgegevens hetzelfde doel worden bereikt, kiest de gemeente daar altijd voor.

2.5 Juistheid

De gemeente draagt zorg voor de juistheid van persoonsgegevens en actualiseert deze gegevens. De gemeente neemt alle redelijke maatregelen om persoonsgegevens onverwijld te wissen of te rectificeren indien deze onjuist zijn.

2.6 Opslagbeperking en bewaartermijnen

Het bewaren kan nodig zijn om de gemeentelijke taken goed uit te oefenen of om wettelijke verplichtingen na te leven. De gemeente bewaart persoonsgegevens niet langer dan noodzakelijk voor het doel van de verwerking en/of voor een gedegen uitvoering van de gemeentelijke taak en de naleving van haar wettelijke verplichtingen. Er zijn uitzonderingen voor archivering, algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden. Persoonsgegevens die niet langer nodig zijn voor het bereiken van het doel worden zo snel mogelijk verwijderd. Dit houdt in dat deze gegevens vernietigd worden of zó worden aangepast dat de informatie niet meer gebruikt kan worden om iemand te identificeren.
Hierbij worden de archiefverordening, het besluit informatiebeheer, het beheerplan en de selectool gevolgd. Bij de verwerking wordt vastgelegd welke bewaartermijn wordt gehanteerd. Er moet binnen elk gegevensverwerkend proces gezocht worden naar de minimale set van gegevens die voor de kortst mogelijke tijd wordt bewaard. Vragen ter bepaling van de bewaartermijn zijn:

- Wanneer is het procesdoel behaald?
- Kan ik gegevens gedurende de bewaartermijn actueel, juist en volledig houden?
- Kunnen als het doel is behaald de gegevens worden vernietigd zonder afbreuk te doen aan het proces?
- Is het langer bewaren van de gegevens een grotere inbreuk op de persoonlijke levenssfeer van de betrokkenen?
- Zijn de risico's op ongewenste verspreiding ook bij langer bewaren klein (de kans wordt tenslotte groter als er meer tijd is)?
- Is er een wettelijke plicht de gegevens te bewaren?
- Kunnen de gegevens ook geanonimiseerd worden?
- Kan ik een betrokkene tijdens de hele bewaartermijn toegang tot de gegevens geven?

Een vastgestelde bewaartermijn wordt in het kader van transparantie voor zover mogelijk gemeld aan de betrokkenen.

E.e.a. staat los van hetgeen in de Archiefwet is bepaald. Doelstelling van de Archiefwet is zorgdragen voor het gedurende een vastgestelde termijn bewaren van geselecteerde informatie ten behoeve van geheugen en kennisbehoud aan de hand van vooraf vastgestelde selectiecriteria.

2.7 Integriteit en vertrouwelijkheid

De gemeente past adequate beveiligingsmaatregelen toe met het doel persoonsgegevens optimaal te beveiligen zodat gegevens niet door onbevoegden kunnen worden ingezien of gewijzigd. De technische en organisatorische maatregelen zijn vastgelegd in het Informatiebeveiligingsbeleid van de gemeente. De passende beveiliging en vertrouwelijkheid betreft ook fysieke waarborgen ter voorkoming van ongeoorloofde toegang of gebruik van persoonsgegevens en/of apparatuur. Dit is eveneens toepasselijk op de toegang en het gebruik door medewerkers.

Veilig omgaan met persoonsgegevens vereist een integere houding zoals ook van medewerkers verwacht wordt. Iedere (nieuwe) medewerker wordt door de verwerkingsverantwoordelijke aantoonbaar 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 inhuur dat zij een Verklaring Omtrent Gedrag (VOG) moeten overleggen voorafgaand aan de start van de werkzaamheden.

2.8 Verantwoording (accountability)

Het college van B&W is eindverantwoordelijk voor het vaststellen van het strategisch privacybeleid van de gemeente. Zij moet de naleving van de toepassing van de wet- en regelgeving inzake verwerking van persoonsgegevens kunnen aantonen (accountability).
Sectorhoofden zorgen voor een gedegen uitvoering van het strategisch beleid. Zij worden daarbij ondersteund door het privacy team. Het toezicht op de naleving van de privacy wetgeving (waaronder naleving van het strategisch privacy beleid) is belegd bij bureau FG. Het opstellen, evalueren, actualiseren en (indien nodig) tussentijds herzien van het strategisch privacybeleid vindt plaats onder coördinatie van de SIA Privacy.

In dit kader neemt de gemeente onder andere de volgende maatregelen:
• Het strategisch privacybeleid openbaar maken;
• Een actueel en volledig verwerkingsregister bijhouden;
• Waar nodig een DPIA uitvoeren;
• Een register van datalekken bijhouden.

3 Processen en maatregelen

In dit hoofdstuk komen de belangrijkste processen en maatregelen aan bod. Dit betreft geen uitputtende lijst van processen en maatregelen.

3.1 Privacy by design en privacy by default

Het uitgangspunt van privacy by design zorgt ervoor dat tijdig de benodigde technische en organisatorische maatregelen kunnen worden getroffen zodat aan de voorkant voor gezorgd dat bepaalde privacy problemen zich niet kunnen voordoen. Privacy by default kan gezien worden als een onderdeel van privacy by design. Privacy by default vereist dat de standaardinstellingen altijd zo privacy-vriendelijk mogelijk zijn.
Privacy by design wordt binnen de gemeente geborgd door bijvoorbeeld bij aanbestedingsprocedures en projecten in een vroeg stadium de privacy vereisten voor de aanbesteding kenbaar te maken. Door het voor aanvang van risicovolle verwerkingen uitvoeren van DPIA's worden tijdig de risico's en daarop te nemen mitigerende maatregelen in kaart gebracht. Dit geldt ook voor andere zaken zoals low code apps, robotisering, proces automatisering, etc.
Privacy by default past de gemeente toe door bijvoorbeeld aan te geven dat in bestaande verwerkingen de privacy automatisch is geborgd.

3.2 Verwerkingsregister

Het is de verantwoordelijkheid van de gemeente om een verwerkingsregister bij te houden. Het verwerkingsregister wordt gevuld met informatie afkomstig van verschillende sectoren (afdelingen) binnen de gemeente die persoonsgegevens verwerken. Dit is een middel om de conformiteit aan de AVG en de Wpg te monitoren en dient tevens als basis bij het adviseren van de gemeente door het privacy team. Daarnaast biedt het een overzicht van alle persoonsgegevens die worden verwerkt door de gemeente.

Bij de registratie worden in ieder geval de volgende gegevens vermeld voor zowel de AVG als de Wpg:
- de naam van de verwerking;
- verantwoordelijke sector(en) van de verwerking;
- het doel van de verwerking;
- de groep(en) van personen van wie persoonsgegevens worden verwerkt (betrokkenen);
- de categorieën persoonsgegevens die worden verwerkt;
- de (eventuele) ontvangers van de gegevens;
- de grondslag voor de verwerking;
- locatie van de verwerking;

- de bewaartermijn(en) van de verwerking;
- een algemene beschrijving van de technische en organisatorische maatregelen;
- een registratie van eventueel gebruikte algoritmes en/of AI binnen de verwerking
Voor de Wpg is hieraan toegevoegd:
- politiegegevens die vallen onder het strafrecht

Voor het beheren van het verwerkingsregister zijn op operationeel niveau voor intern gebruik (deel)processen met onder andere taken, rollen en verantwoordelijkheden vastgesteld met werkinstructies voor medewerkers. Deze zijn voor medewerkers van de gemeente terug te vinden in het (interne) processenhuis van de gemeente.

3.3 Delen met derden

Om de wettelijke taken te kunnen uitvoeren, kan het nodig zijn om gegevens te delen met derden. Dit doet de gemeente alleen als dat volgens de wet mag.
Ook bij het verstrekken van gegevens aan andere organisaties moet de gemeente voldoen aan regels over bescherming en beveiliging van persoonsgegevens. Daarom maakt de gemeente afspraken met de partijen waaraan gegevens worden verstrekt. Die afspraken gaan onder andere over de te volgen procedures bij de verstrekking van de gegevens en de informatiebeveiliging. Die afspraken worden vastgelegd in samenwerkingsovereenkomsten of -verbanden.

Wanneer bedrijven in opdracht van de gemeente werk verrichten waarbij persoonsgegevens worden verwerkt, dan sluit de gemeente een verwerkersovereenkomst af met deze bedrijven. Daarin worden afspraken gemaakt om te zorgen dat de gegevens net zo goed beschermd worden als bij verwerking door de gemeente zelf. De gemeente bepaalt als verwerkingsverantwoordelijke het doel en de middelen voor de verwerking van persoonsgegevens onder zowel de AVG als de Wpg. De gemeente moet er dus voor zorgen dat de systemen worden aangepast, dat de autorisaties goed geregeld zijn, dat de beveiliging en toegang tot gegevens op orde is en dat gegevens verwijderd, gedeeld en verder worden verwerkt conform de regels uit de AVG en de Wpg. In de relatie verwerkingsverantwoordelijke – verwerker wordt vastgelegd op welke manier wordt voldaan aan de eisen die de wet en de AP hieraan stelt.

Indien er bij een verwerking sprake is van gezamenlijke verwerkingsverantwoordelijkheid worden de onderlinge rechten en plichten conform de wet vastgelegd. Van gezamenlijke verwerkingsverantwoordelijkheid is sprake als twee of meerdere verwerkingsverantwoordelijken gezamenlijk de doelen en middelen van de verwerking bepalen.
Het bestaan van een gezamenlijke verantwoordelijkheid betekent niet noodzakelijkerwijs dat de verwerkingsverantwoordelijken een gelijke verantwoordelijkheid hebben ten aanzien van de verschillende verwerkingen van persoonsgegevens. Het niveau van verantwoordelijkheid van elk van hen moet worden beoordeeld in het licht van alle relevante omstandigheden van de verwerking. Hierbij is het uitgangspunt dat verantwoordelijkheid niet verder gaat dan de bevoegdheid van de verwerkingsverantwoordelijke.

Als de gemeente persoonsgegevens verwerkt voor haar eigen doeleinden en deze gegevens deelt met een andere organisatie die de persoonsgegevens voor haar eigen doelen gebruikt, dan is sprake van twee zelfstandige verwerkingsverantwoordelijken. Zelfstandige verwerkingsverantwoordelijken hoeven geen overeenkomst te sluiten ten aanzien van hun verantwoordelijkheden binnen dezelfde verwerking. Hier is namelijk geen sprake van gezamenlijke verwerkingsverantwoordelijkheid. Iedere zelfstandige verantwoordelijke is ten slotte zelf verantwoordelijk voor de eigen gegevensverwerking.

Voor het afsluiten en beheren van privacy overeenkomsten zijn op operationeel niveau voor intern gebruik (deel)processen met onder andere taken, rollen en verantwoordelijkheden vastgesteld met werkinstructies voor medewerkers. Deze zijn voor medewerkers van de gemeente terug te vinden in het (interne) processenhuis van de gemeente.

3.4 Data Protection Impact Assessment (DPIA)

Wanneer een verwerking van persoonsgegevens waarschijnlijk een hoog privacy risico oplevert, dient voorafgaand aan de start van deze verwerking een DPIA uitgevoerd te worden. Hiermee worden de privacyrisico's vooraf in kaart gebracht. Op basis van deze risicoanalyse kunnen relevante maatregelen worden genomen om de onderkende risico's terug te brengen naar een acceptabel niveau.

De gemeente is verplicht om een DPIA uit te voeren indien het gaat om een hoog risicoverwerking. De AVG geeft globaal aan wanneer daar sprake van is. De gezamenlijke Europese toezichthouders hebben aanvullende richtsnoeren met 9 criteria opgesteld om te bepalen of sprake is van een hoog risico. Vuistregel is dat een DPIA moet worden uitgevoerd als aan minimaal 2 van deze 9 criteria wordt voldaan.

De richtsnoer geldt als verduidelijking van de AVG. De door de Europese toezichthouder geformuleerde negen criteria of voor een verwerking een DPIA uitgevoerd moet worden bieden goede uitgangspunten bij de inhoudelijke beoordeling van de verwerking.

De gemeente categoriseert de DPIA's op onderwerp of type verwerking, zoals bijvoorbeeld cameratoezicht of (marketing) onderzoek. Voor verwerkingen die 'gebundeld' kunnen worden, kan een overkoepelende DPIA worden uitgevoerd. Hiervoor geldt wel dat de overkoepelende DPIA uitgebreider is dan voor risicovolle verwerkingen die niet gecategoriseerd kunnen worden. In overkoepelende DPIA's zal namelijk met meer factoren rekening moeten worden gehouden.

Er is tactisch uitvoeringsbeleid over het uitvoeren van een DPIA opgesteld. Dit beleid is voor intern gebruik en is voor de medewerkers van de gemeente terug te vinden op het (interne) intranet. Daarnaast zijn op operationeel niveau (deel)processen met onder andere taken, rollen en verantwoordelijkheden vastgesteld met werkinstructies voor medewerkers. Deze zijn voor de medewerkers van de gemeente terug te vinden in het (interne) processenhuis van de gemeente.

3.5 Datalekken

Wanneer sprake is van een inbreuk in verband met persoonsgegevens, is er sprake van een datalek. De gemeente heeft als verwerkingsverantwoordelijke verschillende wettelijke plichten wanneer het gaat om de behandeling van datalekken. Zo is de gemeente verplicht een datalekkenregistratie bij te houden en kan de gemeente verplicht zijn het datalek te melden aan de AP en/of de betrokkenen op wie de inbreuk betrekking heeft.

Indien blijkt dat het datalek voor de betrokkene een risico vormt, moet het datalek zonder onredelijke vertraging en, indien mogelijk, uiterlijk 72 uur nadat de gemeente er kennis van heeft genomen, bij de AP worden gemeld. Hierbij gelden twee aandachtspunten:
1. De 72 uur gaat lopen vanaf het moment dat de gemeente kennis heeft genomen van het datalek, oftewel bekend is geworden met het datalek. Dit hoeft dus niet het moment te zijn dat het datalek heeft plaatsgevonden.
2. Een datalek moet binnen 72 uur gemeld worden voor zover dat mogelijk is. De enkele omstandigheid dat een melding na 72 uur wordt gedaan, leidt niet per definitie tot een schending van de AVG. Tegelijkertijd dient wel alles in werk te worden gezet om een melding binnen 72 uur te doen. Ook is het meldformulier zo ingesteld dat gemotiveerd moet worden waarom een melding (pas) na 72 uur is gedaan.
3. De (C)ISO wordt ook geïnformeerd om z.s.m. de technische, organisatorische of personele mitigerende maatregelen te kunnen adviseren om het lek te dichten.

Tot slot geldt dat de betrokkenen over het datalek geïnformeerd moeten worden, indien de inbreuk waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van betrokkenen. Dit risico bestaat als de inbreuk kan leiden tot lichamelijke, materiële of immateriële schade voor de personen wier gegevens het voorwerp van de inbreuk zijn. Voorbeelden van dergelijke schade zijn discriminatie, identiteitsdiefstal of -fraude, financieel verlies en reputatieschade.
De betrokkenen hoeven niet te worden geïnformeerd indien (1) voorafgaand aan de inbreuk passende technische en organisatorische beschermingsmaatregelen waren genomen, bijvoorbeeld versleuteling van de gegevens, (2) na de inbreuk maatregelen zijn getroffen waardoor het hoge risico zich waarschijnlijk niet meer zal voordoen of (3) indien de melding aan de betrokkenen onevenredige inspanningen vergt

Voor de beantwoording van de vraag in hoeverre sprake is van een (hoog) risico voor de betrokkenen, moeten verschillende factoren tegen elkaar moeten worden afgewogen, zoals de aard van de inbreuk, de aard van de gegevens, de ernst van de gevolgen voor de betrokkenen en het aantal betrokkenen. Er dient daarbij rekening te worden gehouden met de enerzijds waarschijnlijkheid dat het risico zich zal verwezenlijken en anderzijds ernst van de potentiële gevolgen voor de betrokkenen.

De gemeente heeft een registratieplicht. Dit houdt in dat meldingen van (mogelijke) datalekken worden bijgehouden in een register. Hierin zijn de details van de datalekken vastgelegd.

Er is tactisch uitvoeringsbeleid opgesteld over de meldplicht datalekken. Dit is voor intern gebruik en is voor de medewerkers van de gemeente terug te vinden op het (interne) intranet van de gemeente. Daarnaast zijn op operationeel niveau voor intern gebruik (deel)processen met onder andere taken, rollen en verantwoordelijkheden vastgesteld met werkinstructies voor medewerkers. Deze zijn voor de medewerkers van de gemeente terug te vinden in het (interne) processenhuis van de gemeente.

3.6 Rechten van betrokkenen

De gemeente verwerkt een grote hoeveelheid persoonsgegevens van burgers en werknemers en moet een voorbeeldrol vervullen als het gaat om zorgvuldig en veilig gebruik van persoonsgegevens. Als de gemeente de privacy niet voldoende beschermt, gaat dat ten koste van het vertrouwen in de gemeentelijke dienstverlening, idem als werkgever.
De bescherming van persoonsgegevens is een verantwoordelijkheid van iedereen die bij de gemeente werkt. Iedere medewerker gebruikt dagelijks persoonsgegevens bij het uitvoeren van zijn of haar werkzaamheden. Degenen van wie de persoonsgegevens worden verwerkt, noemen we 'betrokkenen'.

Betrokkenen hebben onder de AVG en Wpg de volgende rechten:
1. Recht om geïnformeerd te worden (art. 12, 13 en 14 AVG en art. 24a,b Wpg);
2. Recht van inzage (art. 15 AVG en art. 25 Wpg);
3. Recht op rectificatie (art. 16 AVG en art. 28 Wpg);
4. Recht op vergetelheid (gegevenswissing) (art. 17 AVG);
5. Recht op beperking van de verwerking (art. 18 AVG);
6. Kennisgevingsplicht bij rectificatie, wissing of verwerkingsbeperking. (art. 19 AVG en art. 28 lid 4 & 5 Wpg).
7. Recht op dataportabiliteit (overdraagbaarheid gegevens) (art. 20 AVG);
8. Recht van bezwaar tegen verwerking (art. 21 AVG);
9. Recht niet te worden onderworpen aan uitsluitend geautomatiseerde individuele besluitvorming/profileren (art. 22 AVG en art. 7a Wpg);
10. Recht om een klacht in te dienen bij de AP (art. 77 AVG en art. 31a Wpg)

De informatieplicht hangt nauw samen met de rechten van betrokkenen: aan de ene kant is er de verplichting voor de gemeente om betrokkenen actief, tijdig en adequaat te informeren over verwerkingen van persoonsgegevens. Denk bijvoorbeeld aan het publiceren van specifieke privacyverklaringen op de gemeentelijke website.
Aan de andere kant kunnen betrokkenen hun rechten uitoefenen richting de gemeente.

Om gebruik te maken van zijn/haar rechten kan de betrokkene een verzoek indienen bij de gemeente. De gemeente heeft vanaf ontvangst van het verzoek een maand de tijd om een besluit te nemen op het verzoek. Onder omstandigheden kan deze termijn met twee maanden worden verlengd. Wordt de termijn overschreden, dan kan betrokkene de gemeente in gebreke stellen.
Voordat een verzoek in behandeling kan worden genomen, dient de identiteit van betrokkene vastgesteld te worden. Dit om fraude te voorkomen. De gemeente voldoet aan het verzoek, tenzij er gerechtvaardigde gronden zijn om een verzoek af te wijzen. Een betrokkene heeft het recht om bezwaar te maken tegen de beslissing.

Betrokkenen kunnen met de FG contact opnemen over alle aangelegenheden die verband houden met de verwerking van hun persoonsgegevens.

Er is tactisch uitvoeringsbeleid over rechten van betrokkenen opgesteld. Dit beleid is voor intern gebruik en is voor de medewerkers van de gemeente terug te vinden op het (interne) intranet van de gemeente. Daarnaast zijn op operationeel niveau voor intern gebruik (deel)processen met onder andere taken, rollen en verantwoordelijkheden vastgesteld met werkinstructies voor medewerkers. Dit is terug te vinden in het interne processenhuis van de gemeente.

4 Advisering

4.1 FG advisering

De gemeente heeft een FG aangesteld die intern toezicht houdt op de toepassing en naleving van de AVG en Wpg. De taken van de FG zijn in de wet opgenomen (artikel 39 AVG en artikel 36 Wpg). Dit betreft onder andere het informeren en adviseren van (medewerkers van) de gemeente en haar verwerkers over hun verplichtingen uit hoofde van de AVG, de Wpg en andere gegevensbeschermingsbepalingen. De FG adviezen moeten goed onderbouwd zijn.

De adviezen van de FG zijn zwaarwegend. Afwijking van een FG advies is mogelijk als dat gemotiveerd wordt vastgelegd door de verwerkingsverantwoordelijke. De FG wordt hierbij tijdig en naar behoren betrokken.

4.2 Ethische advisering

Het beschermen van persoonlijke gegevens wordt door de nieuwe technologische ontwikkelingen steeds belangrijker. Onzorgvuldige omgang met persoonlijke gegevens kan tot schade leiden voor individuen, maar ook tot sociale ongelijkheid, onrechtvaardigheid en discriminatie. Een voorgestelde innovatie kan onbedoeld impact hebben op een ingewikkeld speelveld met interne en externe actoren. Er zullen in dat geval genuanceerde afwegingen moeten worden gemaakt tussen de verschillende belangen.

Het college van B&W heeft daartoe een ethisch waardenkader, een ethische commissie en een werkwijze vastgesteld die samen kunnen helpen om deze afwegingen expliciet te maken. In het waardenkader worden de publieke waarden, zoals autonomie, mens centraal, privacy, veiligheid, controle over technologie, rechtvaardigheid en duurzaamheid als uitgangspunt voor het gesprek benoemd. Zodat niet alleen de interne waarden (bijv. doelmatigheid, uitvoerbaarheid, rechtmatigheid) maar ook de externe waarden (m.n. morele autoriteit, sociale effecten, participatie, afruil) worden besproken. Hierdoor is de gemeente beter in staat om te anticiperen op belangenconflicten en afwegingen te motiveren.

Voor de medewerkers van de gemeente is de werkwijze over ethische advisering terug te vinden op het (interne) intranet van de gemeente.

5 Verantwoordelijkheden en rollen

5.1 RASCI

Het RASCI-model is een hulpmiddel om verantwoordelijkheden en bevoegdheden op een zeer eenvoudige manier in kaart te brengen. Dit zijn de rollen binnen de RASCI-matrix:
- Responsible (verantwoordelijk): verantwoordelijk voor de uitvoering van een proces of activiteit. Deze persoon legt verantwoording af aan de persoon die accountable is.
- Accountable (eindverantwoordelijk): de eindverantwoordelijke die ook goedkeuring moet geven aan het resultaat.
- Supporting (ondersteunend): de persoon die ondersteuning verleent aan het proces of project en de werkzaamheden uitvoert.
- Consulted (geraadpleegd): de persoon die moet worden geraadpleegd, goedkeuring verleent of input levert aan de 'responsible' persoon, voorafgaand aan een stap in het proces.
- Informed (geïnformeerd): degene die geïnformeerd wordt over de beslissingen, de voortgang en de bereikte resultaten, zodat er een volgende stap kan worden gezet.

De verantwoordelijkheden t.a.v. de naleving van de AVG beginselen en de uitgangspunten van het privacybeleid zijn aan de hand van het RASCI-model vastgesteld.

	R	A	S	C	I
College van B&W		✓			✓
DR	✓				✓
Sectorhoofden (op sectorniveau)	✓				✓
Afdelingshoofden / projectleiders	✓				✓
CIO	✓				✓
SIA Privacy (sectoroverstijgend)			✓	✓	✓
PO (op sectorniveau)			✓	✓	✓
CISO (sectoroverstijgend)				✓	✓
Medewerkers (incl. inhuur, externen en stagiaires)			✓		✓
Juridische zaken			✓	✓	
Bureau FG				✓	✓
Raad					✓

5.2 Bestuurlijk

Het college van B&W is op bestuurlijk niveau beslissingsverantwoordelijk en daarmee integraal eindverantwoordelijk voor privacy bescherming en het aantoonbaar naleven van de AVG, de Wpg en het strategisch privacybeleid. De wethouder van wonen, wijken, ruimte en dienstverlening is coördinerend portefeuillehouder en verantwoordelijk voor voldoen aan AVG en Wpg gemeentebreed. De burgemeester

is portefeuillehouder voor toezicht AVG en Wpg. Iedere portefeuillehouder is verantwoordelijk voor voldoen aan AVG en Wpg binnen de eigen portefeuille.
Het college van B&W stelt formeel het strategisch privacybeleid vast en stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen privacybestendig te houden volgens dit strategische privacy beleid.

5.3 Ambtelijk

De DR is op ambtelijk niveau verantwoordelijk voor privacy bescherming. De DR heeft een sturende rol is daarmee verantwoordelijk voor kaderstelling en sturing. Verder adviseert de DR formeel aan het college van B&W over vast te stellen strategisch privacybeleid en controleert of de getroffen maatregelen overeenstemmen met het strategisch privacybeleid en of deze voldoende bescherming bieden. De DR evalueert periodiek de beleidskaders en stelt deze waar nodig bij.
De directeur van externe en interne dienstverlening is binnen de DR het aanspreekpunt voor de AVG en Wpg. Ieder DR lid is verantwoordelijk voor voldoen aan AVG en Wpg binnen de eigen sectoren.
De DR heeft de bevoegdheid (op aangeven van een sectorhoofd) om gemotiveerd af te wijken van het strategisch privacybeleid en zal dit voorleggen aan de betreffende portefeuillehouder / het college van B&W.

5.4 Three Lines Model

De uitvoering van het strategisch privacybeleid is onderdeel van de bedrijfsvoering van de ambtelijke organisatie en volgt de verantwoordelijkheidslijnen van de mandaatbesluiten.

Bij het inrichten van de governance in de ambtelijke organisatie maken we onderscheid in drie lijnen volgens het zogenaamde “Three Lines Model” (TLM). Het TLM helpt de gemeente om de specifieke verantwoordelijkheden van de gemeente en haar medewerkers te beschrijven. Het schept ook transparantie voor de interne en externe belanghebbenden.
De 'eerste lijn, 'tweede lijn' en 'derde lijn' dienen om rollen in de ambtelijke organisatie van de gemeente op een zinvolle manier van elkaar te onderscheiden. Dit zorgt voor een zuivere rolverdeling.
Logischerwijs vormt de bestuurlijke organisatie samen met de DR van de gemeente ook een 'lijn', maar die ligt in de breedte boven de ambtelijke organisatie en valt niet binnen het ‘Three Lines Model’. De nummering (eerste, tweede, derde) moet niet worden opgevat als een opeenvolging van activiteiten: alle rollen worden gelijktijdig vervuld.

5.4.1 Eerste lijn (uitvoerend)

De eerste lijn is primair verantwoordelijk voor het uitvoeren van de werkprocessen en gegevensverwerkingen conform de AVG, de Wpg en dit beleid.

De eerste lijn is primair verantwoordelijk voor een goede interne beheersing en ast de door de tweede lijn ontwikkelde methoden en technieken toe.

Sectorhoofden
Sturen op bewustzijn en naleving van regels en richtlijnen (gedrag en risicobewustzijn) over privacy bij de medewerkers binnen de sector. Rapporteren over de naleving van wet- en regelgeving en strategisch privacy beleid binnen de sector in de managementrapportages aan de CIO en de DR. Een deelregister van verwerkingsactiviteiten van de sector bij houden en documenteren (‘de registerplicht’).
Voorafgaand aan risicovolle verwerkingsactiviteiten een DPIA uitvoeren en documenteren. De AP onder bepaalde omstandigheden voorafgaand aan een nieuwe risicovolle verwerkingsactiviteit raadplegen (‘de voorafgaande raadpleging’). Bij het inrichten van verwerkingen rekening houden met het verplichte principe van privacy door ontwerp en standaardinstellingen (‘privacy by design & default’). Passende beveiligingsmaatregelen treffen en documenteren met het oog op de bescherming van persoonsgegevens. In het geval van een datalek melding doen bij de AP en onder bepaalde omstandigheden betrokkenen daarover informeren, een registratie hiervan bij houden en documenteren (‘registerplicht’). Afspraken maken met derden in privacy overeenkomsten conform de eisen uit de AVG voor elke inzet van een derde partij. De rechten van betrokkenen binnen sector uitvoeren en documenteren.
Sectorhoofden zijn 1:1 gehouden aan het uitvoeren van het strategisch privacybeleid. Er is geen eigen ruimte om zelf hiervan af te wijken. Mocht dit wel nodig zijn dan zal de gewenste afwijking worden voorgelegd aan de DR.
De specifieke taken, rollen en verantwoordelijkheden binnen de privacy processen staan expliciet beschreven in het interne processenhuis van de gemeente.

Medewerkers (inclusief inhuur/stagiaires)
Werken volgens de volgende basisregels:

- Verwerk persoonsgegevens alléén als dit nodig is in het kader van de gemeentelijke taken;
- Gebruik alleen die persoonsgegevens die nodig zijn voor het doel;
- Zorg dat de persoonsgegevens die verwerkt worden juist en actueel zijn;
- Sla persoonsgegevens op zo min mogelijk plekken op;
- Deel de persoonsgegevens alleen met collega's die direct betrokken zijn;
- Laat persoonsgegevens niet onbeheerd achter;
- Neem de grootste zorgvuldigheid in acht wanneer je persoonsgegevens verwerkt over iemands ras, religie, gezondheid, strafverleden etc.;
- Verwijder de persoonsgegevens na het verstrijken van de bewaartermijn;
- Neem de grootste zorgvuldigheid en terughoudendheid in acht als het gaat om het verstrekken van persoonsgegevens aan derden;
- Raadpleeg de PO ten dienste van de sector of de SIA Privacy bij bijzondere situaties of voor advies;
- Zijn er mogelijk persoonsgegevens gelekt? Meld dit direct aan meldpuntdatalekken@eindhoven.nl en aan de PO ten dienste van de sector en levert alle benodigde informatie daar over aan ten behoeve van registratie.
- Is op de hoogte van de privacy processen en voert de taken uit die binnen deze processen aan hem/haar zijn toebedeeld.

De specifieke taken, rollen en verantwoordelijkheden binnen de privacy processen staan expliciet beschreven in het interne processenhuis van de gemeente.

Bevoegd Functionaris
Wordt aangewezen door de gemeente en is de 'hoeder' van de gegevens die onder artikel 9 Wpg (onderzoek voor de handhaving van de rechtsorde in een bepaald geval) worden verwerkt. Beslist oa wie er toegang mag hebben tot deze gegevens en of ze verstrekt kunnen worden aan een samenwerkingspartner op basis van de Wpg vereisten. Iedere artikel 9-verwerking dient een bevoegd functionaris (BF) te hebben. Ook als een Buitengewoon opsporingsambtenaar een dergelijke verwerking doet, dient er een BF te worden aangewezen. Omschrijft het doel van de artikel 9-verwerking en legt dit vast. Autoriseert personen voor de betreffende verwerking. Bepaalt of gegevens voor andere doeleinden mogen worden verwerkt. Zorgt dat voor alle gegevens de herkomst en wijze van verkrijgen wordt vastgelegd. Bewaakt dat gegevens rechtmatig worden verkregen en verwerkt. Hierbij moet vooral gelet worden op de termijnen.
Deze rol komt alleen voor in de Wpg en niet in de AVG.

5.4.2 Tweede lijn (ondersteunend)
De bescherming van persoonsgegevens is een inherent onderdeel van ieders functie. Tegelijkertijd is de bescherming van persoonsgegevens niet de core business van de meeste medewerkers. Er zijn daarom medewerkers aangewezen om hen daarbij te ondersteunen en om als vraagbaak te fungeren. De tweede lijn helpt de eerste lijn bij de uitvoering van de normenkaders (wet- en regelgeving en beleidsregels) en de bewaking van de naleving. Ook ondersteunt de tweede lijn bij de monitoring en de verbetering van de uitvoering van de AVG.

CIO
Bereidt in afstemming met de verantwoordelijke sectorhoofden gemeentebrede besluitvorming voor. Is verantwoordelijk voor opstellen cq actualiseren van het privacybeleid.

SIA Privacy (Centrale PO)
Heeft een gemeentebrede coördinerende, (beleids)ontwikkelende en adviserende rol als het gaat om het aantoonbaar kunnen voldoen aan de AVG en Wpg door de gemeente. Stuurt daarnaast de medewerkers binnen het privacy team functioneel en inhoudelijk (operationeel) aan.
De rol/taak van de 'Privacy Functionaris', zoals beschreven in artikel 34 Wpg , is op centraal niveau geborgd binnen deze functie. De specifieke taken, rollen en verantwoordelijkheden binnen de privacy processen staan expliciet beschreven in het interne processenhuis van de gemeente.

Privacy Officer
Heeft ten dienste van de sector een aanjagende, signalerende, coördinerende, faciliterende, adviserende en begeleidende rol als het gaat om de aantoonbaar kunnen voldoen aan de AVG en Wpg.
De rol/taak van de 'Privacy Functionaris', zoals beschreven in artikel 34 Wpg , is gedeconcentreerd geborgd binnen deze functie bij de sectoren Sociaal Domein en Ruimtelijk Domein. De specifieke taken, rollen en verantwoordelijkheden binnen de privacy processen staan expliciet beschreven in het interne processenhuis van de gemeente.

Juridische zaken
Geeft juridisch advies en biedt juridische ondersteuning. Draagt bij aan het opstellen cq updaten van het juridische gedeelte van het privacybeleid.

5.4.3 Derde lijn (toezicht)

De gemeente heeft een FG aangesteld. De FG handelt onafhankelijk van de gemeente en wordt niet aangestuurd door de gemeente. Bij de positionering van de FG binnen de gemeente wordt hiermee rekening gehouden. De gemeente oefent geen invloed uit op hetgeen de FG doet. Alle medewerkers van de gemeente werken volledig mee aan alle verzoeken van de FG.

FG

De FG heeft in artikel 39 AVG en artikel 36 Wpg taken toebedeeld gekregen. Deze taken zijn onder andere informeren en adviseren over verplichtingen die uit de AVG en Wpg voortvloeien en toezien dat de AVG en Wpg worden nageleefd. Ook heeft de FG als taak om met de AP samen te werken. Om deze taken goed uit te kunnen voeren moet de FG deskundig zijn op het gebied van gegevensbescherming en van de verwerkingspraktijken bij de gemeente. Ook moet de FG verslag kunnen uitbrengen bij het hoogste leidinggevende niveau van de gemeente. De FG moet de taken op onafhankelijke wijze uitvoeren. Dat betekent dat de FG door de gemeente in staat moet worden gesteld met voldoende middelen de taak uit te voeren en dat deze geen instructies mag krijgen met betrekking tot de FG taken.
Bij het uitoefenen van haar taak wordt de FG ondersteund door een adviseur AVG/plaatsvervangend FG en een medewerker gegevensbescherming.