Gemeente Waalwijk

GEMEENTEBLAD

Officiële uitgave van de gemeente Waalwijk

Nr. 243515

15 november 2018

Beleid bescherming persoonsgegevens 2018 tot 2021 & Privacycontrol met ingang van 25 mei 2018

Versie: 4.1
Versiedatum: 30-08-2018
Goedgekeurd door: Gemeenteraad
V-Classificatie: Openbaar

Inhoud

1. Noodzaak privacybeleid

1.1 Privacybeleid

In de afgelopen periode heeft de gemeente Waalwijk gewerkt aan het op adequaat niveau brengen van de uitvoering van de privacywetgeving in lijn met de visie van het college (zie bijlage 1: Visie op gegevensbescherming). Er is in kaart gebracht welke processen met persoonsgegevens de gemeente uitvoert en al deze processen zijn beoordeeld tegen de achtergrond van het omvangrijke wettelijk kader op privacygebied.
Het resultaat van die werkzaamheden zal de gemeente Waalwijk voor de komende jaren moeten borgen door maatregelen te treffen in onderhoud, beheer en advisering. Dit betreft voornamelijk werkzaamheden op tactisch en operationeel gebied.

In dit privacybeleid worden daarvoor de kaders aangegeven. Bestuur, management en medewerkers moeten weten op welke wijze de gemeente Waalwijk uitvoering geeft aan de privacywet- en regelgeving en waarmee zij in hun werk rekening moeten houden als het om privacybescherming gaat. Onder privacywetgeving wordt in het algemeen verstaan de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG), privacyvoorschriften in sectorale wet- en regelgeving en de Algemene verordening gegevensbescherming (AVG).

1.2 Noodzaak van beleid

Gevoeligheid gegevens cliënten in het sociaal domein en veiligheid

Met de overdracht van taken in het sociaal domein heeft de gemeente meer en privacygevoeliger gegevens te verwerken gekregen. Door de integrale aanpak van meervoudige problemen worden gegevens uitgewisseld met maatschappelijke en zorgpartners. Daarbij is van belang dat de uitwisseling van die gegevens minimaal binnen de juridische kaders van de privacywetgeving plaatsvindt.
De rol van de gemeente op het gebied van openbare orde en met name veiligheid ondergaat verandering. Veiligheidsinstanties roepen de gemeente op om signalen uit de samenleving over vermoedelijke radicalisering door te geven en of gegevens te verzamelen in het kader van het creëren van een ondermijningsbeeld. De vraag is eigenlijk niet meer of de gemeente Waalwijk daaraan medewerking gaat verlenen, maar eerder onder welke privacybeschermende voorwaarden. Daar is beleid voor nodig en er moet bestuurlijke verantwoordelijkheid voor de privacy van de betrokkenen worden genomen.

Nieuw wettelijk kader

Sinds 25 mei 2016 is de AVG van kracht. De AVG heeft rechtstreekse werking in de lidstaten van de EU. De gemeente Waalwijk moet op 25 mei 2018 aan de AVG voldoen, dat wil zeggen aantoonbaar kunnen maken dat zij in control is op privacygebied.
De AVG is in hoofdlijnen vergelijkbaar met de Wbp. De belangrijkste wijzigingen die het gevolg zijn van de AVG:

- Overheidsorganisaties moeten een functionaris voor de gegevensbescherming aanstellen, die toeziet op de naleving van de AVG.
- De Europese burger moet meer controle over en keuze in de verwerking van persoonsgegevens krijgen. De Europese wetgeving sluit beter aan op de nieuwe technologieën waarmee deze gegevens worden verzameld.
- De verordening brengt grote administratieve lasten met zich mee. Organisaties moeten investeren in het aanpassen van alle systemen die niet aan de AVG voldoen. Daarnaast moeten zij uitgebreide documentatie bijhouden over alle verwerkingen van persoonsgegevens die zij doen en alle verwerkingen die zij uitbesteden aan ‘verwerkers’ (nieuwe begrip voor bewerker, gebaseerd op artikel 4, lid 9 AVG).
- Bij processen waarvoor een hoog privacyrisico wordt voorzien dient de gemeente een gegevensbeschermingseffectbeoordeling (artikel 35 AVG) c.q. een privacy impact assesment (PIA) uit te voeren, voordat de persoonsgegevens worden verwerkt.
- De AVG voorziet ook in een meldplicht. Datalekken dienen te worden gemeld bij de nationale toezichthouder en bij degene wiens gegevens gelekt zijn.

1.3 Samenloop met beveiligingsbeleid

Artikel 24 AVG vormt het algemeen wettelijk kader voor de beveiliging van persoons-gegevens. Volgens dat artikel moet de verantwoordelijke de noodzakelijke beveiligingsmaatregelen treffen om misbruik en verlies van persoonsgegevens te voorkomen.
De ontwikkeling van gemeentebreed veiligheidsbeleid loopt parallel met de ontwikkeling van het privacybeleid. Waar privacybeleid met name gaat over hoe om te gaan met persoonsgegevens, gaat het beveiligingsbeleid over de strategische, tactische en operationele maatregelen die de gemeente treft om de persoonsgegevens te beveiligen. Waalwijk beschikt door de werkzaamheden van de afgelopen periode over een actueel beeld van de persoonsinformatiehuishouding en heeft daarmee inzicht in wat er aan persoonsgegevens moet worden beveiligd. Onderhoud- en beheermaatregelen moeten worden getroffen om dat beeld bij te houden en actueel. Het register van verwerkingen van persoonsgegevens vormt daarmee een substantieel deel van het instrumentarium dat nodig is om de beveiliging te kunnen regelen.

2. Governance en beleid stuk

2.1 Directie en management zijn verantwoordelijk en hebben beleid nodig om hun verantwoordelijkheid te kunnen nemen op privacygebied

De AVG is een kaderwet waaraan publieke en private organisaties zich moeten houden.
De verantwoordelijkheid voor de uitvoering en handhaving ligt bij de verantwoordelijke, in casu de burgemeester, respectievelijk het college van burgemeester en wethouders. Voor gegevensverwerkingen bij de Griffier (bijvoorbeeld over de raadsleden zelf of gegevens over personen in aan de Raad gerichte

post) is de gemeenteraad het verantwoordelijke bestuursorgaan. Daarnaast hebben we de heffingsambtenaar en de invorderingsambtenaar als bestuursorganen.
Ambtelijke verantwoordelijkheid verloopt via de lijnen van het mandaatbesluit, waarbij de uitvoering in de lijn in (sub)mandaat bij de directie en teammanagers in de rol van proceseigenaar ligt. Net zoals een manager zich houdt aan de financiële kaders, moet deze ook de algemene privacykaders van de AVG en de bijzondere regels in de wetgeving die hij/zij uitvoert in acht nemen.
Privacy speelt zich echter niet alleen in de lijn af. Een aantal privacy-issues is teamoverstijgend. De verantwoordelijkheid voor dergelijke issues ligt bij de directie. Bijvoorbeeld voor de keteninformatisering, die optreedt als gevolg van de invoering van de basisregistraties of het brede gebruik van de documentaire informatievoorziening, het thuiswerken of in de Cloud werken.
Het is enerzijds van belang dat directie en teammanagers zich bewust zijn van de rol en de verantwoordelijkheid die daarbij hoort, en anderzijds dat ze daar ook naar kunnen en gaan handelen. Om dat te bewerkstelligen is een beleid en beheerinstrumentarium voor privacy noodzakelijk met bijbehorende besluitvormingsstructuur en –procedure. De Gemeenteraad stelt het beleid vast. Het college (en andere bestuursorganen) is verantwoordelijk voor de uitvoering. Directie en teammanagers voeren namens het college uit en besluiten over de beleidsissues die zij vanuit de organisatie ter besluitvorming krijgen voorgelegd. De hiervoor in te richten governancestructuur komt grotendeels overeen met de structuur op het gebied van de informatiebeveiliging[1]. In bijlage 2 is deze verder uitgewerkt.
[1] DT-besluit dd. 28 januari 2016 Organisatie van informatiebeveiligingsbeleid en bescherming persoonsgegevens

2.2 Grip op privacy via de planning en controlcyclus

Om grip op privacy te krijgen en te houden is het nodig dit onderwerp (meer en integraal) mee te nemen als onderdeel van de bedrijfsvoering. De invulling daarvan ligt bij de proceseigenaren. Elke manager zal uiteindelijk moeten aantonen op privacygebied in control te zijn voor de processen waarvan hij of zij eigenaar is. Een privacymanagementsysteem stelt de organisatie in staat de beheersing van privacy aantoonbaar te maken.

2.3 Privacybeleid vergt kennis, kunde én capaciteit

2.3.1 FG/AVG

De uitvoering en handhaving van de privacywetgeving vergt tamelijk specialistische kennis en kunde, die logischerwijze niet bij directie en management voorhanden is. Een Privacy Officer kan directie en management hierin ondersteunen (zie bijlage 2).
Vanaf 25 mei 2018 stelt de AVG de aanstelling van een functionaris voor de gegevensbescherming (kortweg FG) verplicht voor overheidsorganisaties. Dit is een privacydesdeskundige die naast adviserende en beheertaken ook een toezichthoudende rol heeft. Bijlage 4 bevat een uitgebreide omschrijving van de taken, verantwoordelijkheden en bevoegdheden van de FG in het reglement FG.
Belangrijkste taken FG in het kort

- Adviseren over de mogelijkheden van gebruik van persoonsgegevens en bij datalekken
- Desgevraagd begeleiden van privacy impact assessments
- Aanleg en onderhoud openbaar register met verwerkingen persoonsgegevens
- Toezicht houden op het verwerken van persoonsgegevens in de organisatie
- Rapporteren over de omgang met persoonsgegevens door de organisatie
- Intermediair tussen burger en gemeente bij vragen over de toepassing van de AVG door de organisatie
  Het is uitdrukkelijk niet de bedoeling dat deze functionaris de taken op het gebied van de privacybescherming van de teams overneemt, voorkomen moet worden dat ‘de slager zijn eigen vlees keurt’. De teams hebben hun eigen verantwoordelijkheid in het borgen van het omgaan met privacygevoelige gegevens en worden hierbij ondersteund door de FG en/of de Privacy Officer.

2.3.2 Toetsing en advisering

De vrijwel permanente veranderingen in organisatie en processen als gevolg van nieuwe wetgeving, verbetering van de dienstverlening, samenwerkingen met andere gemeenten en met maatschappelijke partners, moeten worden getoetst aan de kaders van de privacywetgeving. Dat geldt ook voor het koppelen van gegevensbestanden, zoals bijvoorbeeld is gebeurd tussen de Basisregistratie Personen enerzijds en de systemen die de bedrijfsprocessen ondersteunen anderzijds. Daarnaast hebben zich

inmiddels nieuwe privacyvraagstukken aangediend op het gebied van het sociaal domein, moeten er besluiten genomen worden over bijvoorbeeld het thuiswerken met BRP-gegevens, het beschikbaar stellen van persoonsgegevens aan leveranciers voor testdoeleinden, big data en cloudcomputing. De organisatie voert hiervoor risico-analyses uit, die worden gedocumenteerd. De FG kan in voorkomende gevallen om advies worden gevraagd.

2.3.3 Administratieve en beheertaken

Onder de administratieve taken van de FG vallen onder meer het beheer van het register van gegevensverwerkingen en het bijhouden van een register van Datalekken. Het bijhouden van deze registers blijft een verantwoordelijkheid van het verantwoordelijke bestuursorgaan, maar de FG houdt het hem bij. De voornoemde veranderingen kunnen verwerkt worden in een openbaar register.

2.3.4 Capaciteitsinzet

Voor een deugdelijke en adequate uitvoering van de rol van FG is formatieve capaciteit nodig. De omvang van die capaciteitsinzet voor Waalwijk is thans een kwestie van schatten. Ervaring met dit vraagstuk bij andere gemeenten leert dat de capaciteitsinzet zal uitkomen op een hele formatieplaats. In Waalwijk maakt de functie van FG deel uit van die van de CISO[2]. De ervaring over de komende jaren zal uitmaken hoeveel tijd er uiteindelijk aan privacy besteed zal worden en of dat de rol van ook in kwalitatieve zin te verenigen is met die van de CISO.
Zodra besloten wordt tot het inzetten van een Privacy Officer zal hiervoor een nieuwe functie worden opgesteld.
[2] Chief Information Security Officer. Dit is de toezichthouder/adviseur informatiebeveiliging.

3. Privacybeleid is vooral een belangenafweging

De toepassing en uitvoering van de wettelijke privacykaders is in het algemeen gesproken complex van aard. Bovendien is het onderwerp privacy nogal eens onderwerp van discussie en wordt vaak als sta in de weg ervaren voor de verbetering van de dienstverlening en bedrijfsvoering. De vraag die zich dan aandient is op welke manier geeft de organisatie uitvoering aan de privacywetgeving en wie is waarvoor verantwoordelijk. Anders gezegd, wie beslist binnen de organisatie of het belang van de privacy en de daarvoor te treffen maatregelen opwegen tegen ‘het organisatiebelang’. In feite gaat het dan over privacybeleid. Voor dat beleid gelden de volgende uitgangspunten.

3.1 Uitgangspunten van beleid

1. Burgers hebben het recht om de over hen bij de overheid bekende en beschikbare gegevens niet opnieuw te hoeven verstrekken.
2. Burgers beschikken over het grondwettelijk recht op privacy, waaronder het recht op informationele privacy.
3. Waalwijk is voortdurend bezig de dienstverlening en bedrijfsvoering te verbeteren en een deugdelijke persoonsinformatiehuishouding geldt daarvoor als randvoorwaarde.
4. De naleving van wet- en regelgeving op het gebied van de privacybescherming is uitgangspunt van handelen bij de uitvoering van primaire processen en bedrijfsvoering en wordt opgevat als kenmerk van goede dienstverlening / kwaliteit. Dat impliceert dat de wettelijke uitgangspunten in acht moeten worden genomen.
5. Het privacyrecht zal op een efficiënte en effectieve wijze worden toegepast.
6. De AVG gaat uit van zelfregulering en laat ruimte tot interpretatie.
7. Directie, management en medewerkers hebben behoefte aan beleid op het gebied van de toepassing en uitvoering van de privacyregels.
8. Een privacymanagementsysteem stelt het management en de organisatie in staat de beheersing van privacy aantoonbaar te maken. (Zie bijlage 6).

3.2 Beleid ten aanzien van gebruik van persoonsgegevens algemeen

1. Elke medewerker die persoonsgegevens nodig heeft voor de uitvoering van diens taak of taken, moet daarover op zo efficiënt mogelijke wijze kunnen beschikken.
2. Voor zover een algemeen gegeven (basisgegeven) over een persoon beschikbaar is in een van de basisregistraties, gebruikt de medewerker dat gegeven tenzij dat gegeven onjuist is.
3. Het delen van gegevens is gebaseerd op de mogelijkheden die de wet biedt en in die gevallen waarin de wet niet voorziet wordt een noodzakelijkheidstoets uitgevoerd gebaseerd op het triagemodel (opgenomen in bijlage 5).
4. Het takenpakket van een medewerker is bepalend voor de set aan gegevens waarover een medewerker mag beschikken evenals de wijze waarop deze gegevens ter beschikking worden gesteld.

5. De teammanager is uit oogpunt van privacybescherming verantwoordelijk voor en beslist over de vaststelling van de inhoud van de gegevensset behorende bij het takenpakket van een medewerker. De teammanager neemt daarbij de wettelijke uitgangspunten in acht met betrekking tot:
   a. doelbinding: gegevens worden uitsluitend voor een vooraf bepaald gerechtvaardigd doel gebruikt;
   b. proportionaliteit: niet meer gegevens gebruiken, dan toereikend en strikt noodzakelijk is;
   c. subsidiariteit: kan het doel zonder persoonsgegevens worden bereikt, dan heeft dat de voorkeur.

6. Het management is verantwoordelijk voor de gemeentebrede naleving van de AVG en de directie beslist over privacyissues die teamsoverschrijdend zijn.
7. Er is een FG die directie en teammanagers gevraagd en ongevraagd van advies dient met betrekking tot de bescherming van de persoonlijke levenssfeer van degenen over wie in de organisatie van de gemeente Waalwijk persoonsgegevens worden verwerkt.
   Wijzigingen in de wijze waarop uitvoering wordt gegeven aan primaire en bedrijfsvoeringprocessen met al dan niet volledige organisatiebrede consequenties die ook van invloed zijn voor de manier waarop met persoonsgegevens wordt omgegaan, moet worden getoetst aan de privacywetgeving door de FG (bijvoorbeeld thuis werken, uitbesteding van werk aan een derde partij, gegevensdeling in het sociaal domein, verwerking van persoonsgegevens met business intelligencesystemen, systeemkoppelingen). Het informatiebeleid zal in lijn moeten zijn met het privacybeleid.
8. Bij nieuw uit te voeren processen waarbij de verwerking van persoonsgegevens, waaronder bijzondere persoonsgegevens, qua inhoud en omvang complex is en van substantieel belang is voor de uitvoering van het proces, maakt een privacy impact assessment (gegevensbeschermingseffectbeoordeling) deel uit van het implementatieproces.

3.3 Beleid ten aanzievan van gebruik van persoonsgegevens uit de BRP

De verstrekking van persoonsgegevens uit de Basisregistratie Personen (BRP) en de wijze van verstrekking is gebaseerd op de Wet BRP, de Verordening gegevensverstrekking basisregistratie personen Waalwijk 2014 en het Autorisatiebesluit van de Minister van Binnenlandse Zaken d.d. 26 juni 2018, met kenmerk 2018-0000302229, en opvolgende versies van dat besluit.

1. De gegevensuitwisseling tussen de BRP en de gebruikers van de BRP wordt vastgelegd in het register van gegevensverwerkingen. Het register regelt de volgende onderwerpen.
   a. De inhoud van de taak of van de taken;
   b. De set aan gegevens die verstrekt wordt;
   c. De wijze van verstrekking: raadplegen (op persoonsniveau en/of op adresniveau) en/of mutatieberichten en/of selecties en/of koppelingen;
   d. Additionele voorwaarden in het geval de gebruiker werkzaamheden laat uitvoeren door een derde waarbij persoonsgegevens uit de BRP nodig zijn;
   e. De verplichting tot terugmelding bij gerede twijfel over de juistheid van de gegevens uit de BRP.

2. Uitbreiding van de gegevensset van een medewerker, buiten de kaders van de regels als genoemd onder 1 is slechts mogelijk, indien door het ontbreken van een gegeven diens taak niet naar behoren is uit te voeren.
3. Tot het indienen van een gemotiveerd verzoek tot uitbreiding van de gegevensset als bedoeld onder 3 is bevoegd de manager van het team waarbij de medewerker werkzaam is. De teammanager vergewist zich of de uitbreiding van de gegevensset voor de uitvoering van de taak noodzakelijk is en niet in strijd is met de privacywetgeving. De teammanager onder wiens verantwoordelijkheid de BRP wordt bijgehouden beslist over het verzoek.
4. De geautomatiseerde verstrekking van BRP-gegevens door middel van koppeling van systemen dient gebaseerd te zijn op de onder 1 genoemde Verordening en het Autorisatiebesluit van de Minister van Binnenlandse Zaken en Koninkrijksrelaties.
5. Bij onzekerheid over de uitleg van de privacywetgeving of vermoeden van strijd met deze wetgeving, legt de teammanager(s) het verzoek, voorzien van een advies van de FG, ter besluitvorming voor aan de directie. Directie of in voorkomend geval het bestuursorgaan, dat is aan te merken als de verantwoordelijke voor de verwerking van persoonsgegevens, besluiten.

4. Privacybeleid in de praktijk

4.1 Waalwijk heeft zicht op alle processen waarin persoonsgegevens een rol spelen

4.1.1 Primaire processen

De gemeente Waalwijk verwerkt persoonsgegevens op tal van beleidsterreinen. Dat gebeurt zowel binnen het sociaal domein, als op het gebied van openbare orde en veiligheid, fraude-opsporing en handhaving van illegale activiteiten, als voor het uitnodigen van burgers om een zienswijze te geven over een bestemmingsplan.
Alle processen met persoonsgegevens van alle beleidsterreinen zijn in kaart gebracht (zie bijlage 2) en getoetst aan de privacyvoorschriften. Een register met deze processen is beschikbaar en biedt, ook aan burgers, inzicht in:

- Het doel van de verwerking van persoonsgegevens;
- De categorieën van personen over wie gegevens worden verwerkt;
- De gegevens per categorie van personen die worden verwerkt;
- Met wie (delen van de set aan) persoonsgegevens worden gedeeld;
- De rechtmatige grondslag waarop de verwerking is gebaseerd;
- De bewaartermijn die geldt voor de persoonsgegevens;
- Of de gemeente werkzaamheden heeft uitbesteed, waarvoor een bewerkersovereenkomst moet zijn vastgesteld;
- De herkomst van de gegevens, bijvoorbeeld afkomstig van de burger zelf of uit een basisregistratie.
- Wijze van beveiliging (voor zover mogelijk)
  Vanaf 25 mei 2018 meldt de organisatie deze processen aan bij de FG.
  Wijzigingen in wet- en regelgeving, processen, dienstverlening, en andere zaken worden getoetst aan de privacyvoorschriften. De administratieve werkzaamheden van de AVG leiden vervolgens tot een aanpassing of intrekking van een melding, dan wel een nieuwe melding. Daarnaast leiden die werkzaamheden tot aanpassing van het register.

4.1.2 Bedrijfsvoering

Naast gegevens van burgers in primaire processen, verwerkt de gemeente Waalwijk persoonsgegevens van haar medewerkers. Persoonsgegevens van medewerkers zijn te vinden in de personeels- en salarisadministratie, ICT-administratie (ten behoeve van autorisaties en beveiligingsbeheer) en in planningsystemen. Ook worden gegevens van een medewerker geregistreerd als behandelaar van een aanvraag van een burger. De verwerking van persoonsgegevens van personeelsleden is vastgelegd in een privacyreglement, dat driejaarlijks moet worden geactualiseerd. Voor de monitoring van het gebruik van informatiesystemen, telefonie en internet en in planningsystemen zijn door de OR goedgekeurde protocollen beschikbaar.

4.1.3. Communicatie en training medewerkers gemeente

Het Bestuurlijk/juridisch instrumentarium dat de gemeente Waalwijk inzet om privacyproof uitvoering te geven aan haar taken, zal ook in de praktijk van de medewerkers moeten landen.
Medewerkers van de gemeente en van partners moeten kennisnemen van deze regels en geïnstrueerd worden over de manier waarop ze met persoonsgegevens kunnen en moeten omgaan.
Kwaliteits- en beleidsmedewerkers zullen de proceseigenaren moeten ondersteunen bij de handhaving van privacy door de (her) in te richten processen ook te laten voldoen aan de privacyvoorschriften. Voor hen is een uitgebreider leertraject noodzakelijk.
Een en ander zal geborgd moeten worden door middel van een trainings- en communicatieplan.

4.1.4 Communicatie met de burger

Burgers worden op allerlei manieren op de hoogte gehouden van de bestuurlijke en maatschappelijke veranderingen. Voor wat betreft de verwerking van persoonsgegevens is het van belang dat de burger geïnformeerd wordt over het doel van de verwerking van diens gegevens, welke gegevens op welk moment in het proces nodig zijn (ook wel triage genoemd) en met wie welke gegevens noodzakelijkerwijze gedeeld gaan worden. Het moment van informeren is in de meeste gevallen het moment waarop een burger om hulp vraagt. In sommige situaties, bijvoorbeeld in het geval de burger niet zelf om hulp vraagt, kan de burger op een later moment worden geïnformeerd. De informatieplicht jegens de burger is in de procesinrichting van gemeente en partners voorzien.
Het moment van informeren wordt tevens benut om, indien nodig toestemming te vragen om gegevens te mogen verwerken of uit reeds bestaande dossiers bij de gemeente gegevens te hergebruiken en om eventuele bijzondere gegevens omtrent de gezondheid te mogen opvragen bij een medicus.
Buiten de informatieplicht heeft een burger te allen tijde recht op inzage en kan deze het betreffende bestuursorgaan verzoeken foutieve gegevens te corrigeren. De gemeente Waalwijk hanteert hiervoor een eenvoudige en voor ieder toegankelijke procedure.

4.2 Privacybeleid in specifieke beleidsterreinen

4.2.1 Sociaal domein
De nieuwe taken die de gemeente in het sociaal domein sinds 1 januari 2015 in uitvoering heeft genomen gaan gepaard met de verwerking van, veelal bijzondere, persoonsgegevens van nieuwe klantgroepen. In de fase van transformatie worden bestaande processen opnieuw ingericht. De gemeente voert zelf regie op de integrale behandeling van meervoudige problemen in de verschillende overlegstructuren. De verwerking van persoonsgegevens in de nieuwe processen moet voldoen aan de privacywetgeving, waardoor burgers erop kunnen vertrouwen dat de gemeente en haar partners zorgvuldig omgaan met hun persoonsgegevens.

4.3.1.a Overleg over cliënten
Efficiency, effectiviteit en kwaliteit van de dienstverlening zijn er mee gebaat dat daar waar nodig en mogelijk, zowel intern als extern afstemming over een cliënt plaatsvindt tussen de verschillende onderdelen van het sociaal domein. Ondanks dat dit ook een van doelstellingen is van de wetgever, heeft deze het nagelaten om dat te regelen.
Participatiewet, Jeugdwet en Wet maatschappelijke ondersteuning 2015 (WMO 2015) kennen daarvoor ieder hun eigen regels. In die gevallen dat het gewenst is om gegevens uit te wisselen, geldt de wet waarop een verzoek is gebaseerd als uitgangspunt van handelen. Dat betekent in het geval van de WMO 2015 dat de WMO-consulent toestemming van de betrokkene nodig heeft om de reeds bij de gemeente beschikbare gegevens over een uitkering of schuld op te vragen bij de bijstandsconsulent respectievelijk de medewerker schuldhulpverlening (artikel 5.1.1. lid 4 WMO 2015). Bij de inrichting van het overleg dient dit als uitgangspunt te gelden. De gemeente Waalwijk ziet erop toe dat dergelijke uitgangspunten ook worden doorgevoerd bij haar uitvoeringspartners.

4.2.2 Openbare orde en veiligheid
De afgelopen jaren is de gemeente Waalwijk steeds meer persoonsgegevens gaan verwerken van personen die een bedreiging (kunnen) vormen voor de openbare orde en veiligheid. Het oplossen van problemen met (potentiële) overlastgevers is steeds vaker een bestuurlijke, in plaats van een politionele aangelegenheid en gegevens van politie en justitie worden meegenomen in casusoverleggen in het sociaal domein. De uitwisseling van dergelijke gegevens levert in de praktijk de nodige vraagstukken op privacygebied op die (landelijk) moeten worden opgelost.

4.2.3 Openbaarheid van bestuur
Publicatie van persoonsgegevens op internet wordt tot het uiterste beperkt. In de eerste plaats dient te worden afgewogen of aan publicatie van persoonsgegevens (zowel spontaan als op verzoek) niet valt te ontkomen. Als publicatie onontkoombaar is, dan wordt afgewogen of het publicatiemiddel internet het kanaal is waarlangs gepubliceerd wordt. De gemeente Waalwijk hanteert daarbij als uitgangspunt de Richtsnoeren voor actieve openbaarmaking en de Richtsnoeren inzake de publicatie van persoonsgegevens op internet van de Autoriteit Persoonsgegevens. Mocht publicatie van persoonsgegevens op internet noodzakelijk zijn, dan zullen die gegevens worden afgeschermd voor zoekmachines. De gemeenteraad stelt een gedragscode vast voor de publicatie van persoonsgegevens door de Raad.

Aldus vastgesteld in de raadsvergadering van 11 oktober 2018,

Namens deze,

DE RAAD VAN WAALWIJK
de griffier, de voorzitter,
G.H. Kocken, drs. A.M.P. Kleijngeld

Bijlage 1 Visie op gegevensbescherming
Het uitgangspunt van dat beleid[3] is, dat de gemeente respect heeft voor de persoonlijke levenssfeer van haar inwoners en medewerkers. Het verwerken van persoonsgegevens is altijd gebonden aan een specifiek doel en moet bijdragen aan een effectieve en efficiënte dienstverlening. Privacywetgeving is geen 'kan niet/mag niet wetgeving' maar schept juist ruimte. Daarvoor is een aanpak nodig die erg lijkt op integraal risicomanagement, hoewel er ook verschillen zijn omdat privacy uiteindelijk een integriteitsaangelegenheid is (moraliteit).
Privacybeleidsvoering biedt duurzaamheidsvoordelen. De doelen zijn hierbij:
1. beschermt het college haar inwoners tegen de risico's van de informatiemaatschappij;
2. beheerst het college gemeentelijke afbreuk- en aansprakelijkheidsrisico's;
3. bevordert het college de kwaliteit, continuïteit, veiligheid en klantgerichtheid van de gemeentelijke administratieve organisatie;
4. bouwt het college aan maatschappelijk vertrouwen en draagvlak;
5. respecteert Gemeente Waalwijk de privacy;
6. kan het college met vertrouwen verantwoording afleggen aan de raad en, in voorkomende gevallen, de Autoriteit Persoonsgegevens of desnoods de rechter.
7. speelt het college adequaat in op wettelijke ontwikkelingen – met name de komst van de Algemene Verordening Gegevensbescherming.

Voldoen aan wetgeving op privacygebied betekent dat Gemeente Waalwijk structureel de onderstaande privacywaarborgen biedt. De waarborgen zijn tegelijkertijd ook de handvatten (controls) om op privacy te sturen.
Alle hieronder genoemde aandachtpunten moeten op groen staan wil er sprake zijn van behoorlijke en zorgvuldige gegevensverwerking in overeenstemming met de wet.

Beleidsmatige privacywaarborgen
1. Privacy management: pro-actieve sturing door het college om de gegevensprivacy van burgers en medewerkers te waarborgen, onder meer door duidelijke afbakening van rollen en verantwoordelijkheden.
2. Beleid: een goed gedocumenteerd stelsel van afspraken om persoonlijke en gemeentelijke belangen te beschermen.
3. Ketenregie: een goed gedocumenteerd stelsel van afspraken met ketenpartners en uitvoeringsorganisaties – met name bij samenwerking binnen een gemeenschappelijke regeling.
4. Beleidstransparantie: doelgroepgerichte uitleg over het gemeentelijk privacybeleid.
5. Service: klantgericht inspelen op vragen over het privacybeleid, klachten en verzoeken om inzage, correctie en – voor zover de wet daartoe verplicht – stopzetting en verwijdering van gegevens.
6. Toezicht: controle op de privacybestendigheid van de organisatie door een onafhankelijke privacyfunctionaris.

7. Accountability: het vermogen om op ieder gewenst moment verantwoording te kunnen afleggen over de naleving van privacywetgeving.

Bij het beschermen van persoonsgegevens kiest de gemeente Waalwijk voor een risicogerichte benadering. Daar waar er met zeer gevoelige gegevens wordt gewerkt zullen er extra beschermingsmaatregelen genomen worden. Wij zoeken daarbij voortdurend naar de technisch best mogelijke oplossingen, trainen ons personeel en houden contact met onze toezichthouders. Als er met minder gevoelige persoonsgegevens wordt gewerkt dan blijft een verwerking uiteraard ook altijd binnen de grenzen van de wet.
[3] De visie is door het college vastgesteld op 16 februari 2016 en had betrekking op de regeling bescherming persoonsgegevens dat op 1 maart 2016 van kracht werd.
Bijlage 2: Governancestructuur privacy
Verantwoordelijkheden
Het *betreffende bestuursorgaan* is integraal verantwoordelijk voor de uitvoering van de privacywetgeving. De Raad stelt kaders voor privacy op basis van Europese en landelijke wet- en regelgeving en normenkaders.
De *directie* (sturende rol) is verantwoordelijk voor kaderstelling en sturing.
De directieleden binnen het directieoverleg:
- sturen op handhaving van het privacybeleid op concernniveau;
- controleren of de getroffen beleidsmaatregelen in overeenstemming zijn met de wettelijke kaders;
- evalueren periodiek beleidskaders en stellen deze waar nodig bij.
  De *teammanagers* binnen de gemeente zijn verantwoordelijk voor de integrale handhaving van de bescherming van de privacy binnen hun teams.
  De teammanagers:
- sturen op privacybewustzijn en naleving van regels en richtlijnen (gedrag en privacybewustzijn);

- rapporteren over compliance aan wet- en regelgeving en algemeen beleid van de gemeente aan de directie.

De *teams* zijn verantwoordelijk voor:

- de bescherming van de persoonlijke levenssfeer van burgers en medewerkers en de implementatie van privacyvoorwaarden, die voortvloeien uit wet - en regelgeving;
- alle beheeraspecten van privacy;
- het verzorgen van logging, monitoring en rapportage.

Taken en rollen

Het Gemeenteraad stelt formeel het privacybeleid vast. De uitvoering van het beleid moet gecontroleerd worden, zowel het college als de raad kunnen hiervoor opdracht geven om dit te (laten) controleren. De directie adviseert het college een voorstel aan de Raad met betrekking tot het vaststellen van beleid.

Het team Concern en Strategie (CSTR) geeft namens de directie op dagelijkse basis invulling aan de sturende rol door besluitvorming in de directie voor te bereiden, en toe te zien op de uitvoering ervan.

De Functionaris Gegevensbescherming rapporteert eens per jaar aan de bestuursorganen en halfjaarlijks aan de directie. Binnen de Planning & Controlcyclus is de rapportage over privacy opgenomen onder de paragraaf Bedrijfsvoering.

Binnen CSTR kan een privacy officer worden benoemd. Het werkveld van de privacy officer omvat de gehele gemeentelijke organisatie. De privacy officer vormt samen met de Functionaris voor de gegevensbescherming (FG) het centrale privacy onderdeel van de gemeente. De privacy officer is een gesprekspartner voor teammanagers, projectleiders, IT-leveranciers en de privacybeheerders binnen de team. De pivacy officer heeft de volgende taken:

- Het aansturen van specifieke privacyprojecten of –activiteiten in opdracht van de directie;
- Het samenwerken met belanghebbenden aan (de bijstelling van) beleid, procedures en hulpmiddelen;
- Het adviseren over de privacywetgeving, maatregelen ter borging hiervan en de praktische toepassing ervan;
- Het begeleiden van Privacy Impact Analyses (PIA's) en de evaluatie van datalekken;
- Het adviseren over en evalueren van contracten, verwerkersovereenkomsten met derden;
- Het adviseren ten aanzien van privacy borging binnen processen en systemen, onder andere door deelname aan het i-overleg;
- Het coördineren van de afhandeling van datalekken;
- Het opstellen van rapportages en plannen ten aanzien van privacy borging;
- Het uitdragen van het privacy beleid met bijbehorende –formats en –procedures;
- De taken van de privacy officer kunnen ook werkzaamheden in het kader van informatiebeveiliging bevatten.

Op sleutelplekken in de organisatie zijn 'privacybeheerders' benoemd die decentraal bij teams werken. De teamprivacybeheerders rapporteren aan de teammanager en de Privacy Officer.
De privacybeheerders zijn benoemd in het DT-besluit van 28 januari 2016 "Organisatie van informatiebeveiliging en bescherming persoonsgegevens".

De privacybeheerders hebben de volgende taken:

- Uitdragen privacy binnen het team, unit of cluster waarvoor zij verantwoordelijk zijn;
- Nieuwe ontwikkelingen vanuit taakveld en bijbehorende wetgeving inpassen in het privacybeleid;
- Signalering van nieuwe ontwikkelingen, incidenten en knelpunten aan de functionaris gegevensbescherming;
- Toetsing van teamplannen op het gebied van privacybescherming;
- Zorgen voor toepassing van de privacyvoorschriften binnen het team waarvoor zij verantwoordelijk zijn;
- Uitvoeren van privacy impact assessments voor het eigen taakveld waar nodig, ondersteund door de privacy officer;
- Uitvoering werkzaamheden voor de oplossing van privacy-issues of werkzaamheden voor verbetermaatregelen vanuit privacyadviezen, waar nodig ondersteund door de privacy officer.

Bijlage 3: Register verwerkingen persoonsgegevens en het register van datalekken
Het register van verwerkingen is een apart bestand (doc. nr. 18-0079694).
Het register van datalekken is een apart bestand (doc. nr. 18-0003646).

De registers worden continue actueel gehouden. De hiergenoemde documentnummers zijn een momentopname.

Bijlage 4: Functionaris voor de gegevensbescherming (FG) Taken, verantwoordelijkheden en bevoegdheden

Het Reglement Functionaris Gegevensbescherming gemeente Waalwijk is een apart bestand. (doc nr: 18-0065398).

Bijlage 5: Triagemodel gegevensdeling

Dit model geldt voor de professionals van de gemeente Waalwijk en van partners die de gemeentelijke taken uitvoeren als uitgangspunt voor het maken van de afweging of en wanneer persoonsgegevens mogen worden gedeeld met personen of organisaties in het sociaal domein. Het model volgt het afwegingsproces geredeneerd vanuit de professional / hulpverlener.
Er wordt uitgegaan van de wettelijke mogelijkheden tot uitwisseling van gegevens. Dat betekent dat geen toestemming hoeft te worden gevraagd in die situaties waarin de van toepassing zijnde wetgeving mij als professional de bevoegdheid geeft gegevens van een cliënt te verwerken[4]. Is er geen wettelijke bevoegdheid, dan is toestemming vereist. In die gevallen waarbij de toestemming voor het verwerken of delen van gegevens niet kan worden verkregen, weeg ik de gewenste gegevensverwerking/-uitwisseling af tegen de noodzaak van de hulp, zorg of bijsturing die ik wil verlenen. Met wie wil ik welke informatie delen en op welk moment? Is mijn aanpak zuiver gericht op de beoogde doelstellingen?

1. <u>Komen tot een aanpak</u>
   In samenspraak met de cliënt en personen in zijn omgeving kom ik tot een passende aanpak voor de geconstateerde problemen. Ik neem in deze aanpak mee met wie ik wil samenwerken en welke gegevens ik daarvoor wens te verwerken en uit te wisselen. Dit bespreek ik met de cliënt. Mochten de cliënt niet instemmen met mijn aanpak, dan stel ik hem in de gelegenheid zijn bezwaren te uiten.
2. <u>Afwegen gegevensverwerking/-uitwisseling</u>
   Ik stel mijzelf de volgende algemene vragen:

- Noodzaak: welke gegevens zijn noodzakelijk gegeven het gestelde doel?
- Subsidiariteit: is het delen of opvragen van informatie de minst ingrijpende maatregel? (need-to-know)
- Proportionaliteit: staan het delen of opvragen van informatie en het doel met elkaar in verhouding? Kan het ook met minder informatie?
- Kan en mag het: zijn er specifieke privacyregels die gelden voor betrokken partijen?

1. <u>Informeren</u>
   Is het in het belang van de cliënt om hem op de hoogte te stellen van mijn afweging vóórdat ik overga tot het uitwisselen van gegevens of is in het belang van de cliënt om dat op een later tijdstip te doen? In beide gevallen stel ik (uiteindelijk) de cliënt op de hoogte van de gemaakte afweging(en).
2. <u>Documenteren</u>
   Ik motiveer en documenteer kort en krachtig mijn besluit en afwegingen in het informatie- en registratiesysteem.
   [4]Bijvoorbeeld artikel 5.1.1 Wmo: Het college is bevoegd tot het verwerken van persoonsgegevens van de cliënt, waaronder persoonsgegevens betreffende de gezondheid die noodzakelijk zijn voor de beoordeling van diens behoefte aan ondersteuning van zijn participatie of zelfredzaamheid dan wel opvang of beschermd wonen ….etc.

Bijlage 6: Privacymanagementsysteem

Een privacymanagementsysteem stelt de organisatie in staat de beheersing van privacy aantoonbaar te maken.
Een daartoe ingericht informatie privacy managementsysteem (PMS) ondersteunt de organisatie door te voorzien in tijdige stuur- en verantwoordingsinformatie en stelt de organisatie daarmee in staat de beheersing van privacy aantoonbaar te maken voor stakeholders zoals auditors, toezichthouders, management, bestuur en gemeenteraad.
De componenten van het privacymanagementsysteem bestaan uit:

- Het beleid bescherming persoonsgegevens dat driejaarlijks wordt geëvalueerd;
- Specifiek themabeleid voor onder andere het sociaal domein en openbare orde en veiligheid dat jaarlijks geëvalueerd wordt;
- Het vastgestelde informatiebeveiligingsbeleid dat driejaarlijks geëvalueerd wordt;
- Procesplannen met betrekking tot de legitimiteit en uitvoering van processen gelet op de privacywetgeving dat jaarlijks getoetst wordt;
- De toetsing van opzet, bestaan en werking van het proces waarin privacy impact analyses worden uitgevoerd
- De rapportagecyclus naar bestuur en organisatie met betrekking tot de bescherming van persoonsgegevens onder andere bestaande uit relevante kengetallen.

Deze componenten worden vastgelegd in een computerprogramma waarmee het PMS beheerst kan worden. De Functionaris Gegevensbescherming heeft (in ieder geval) toegang tot dit computerprogramma. Daarnaast kunnen op onderdelen taakverantwoordelijken worden aangewezen die toegang kunnen krijgen om te raadplegen of stukken in te kunnen sturen.

Uitgangspunten voor het privacymanagementsysteem is de laatste versie van het normenkader van stichting CIP-Overheid[5] en/of het privacy controlframework van NOREA.
[5] https://www.cip-overheid.nl/wp-content/uploads/2018/03/20171030-Privacy-Baseline-v3_1.pdf

Bijlage 7: Toelichtende tekst op de website[6]

Toelichting privacybeleid Gemeente Waalwijk

In deze toelichting laat gemeente Waalwijk zien op welke manier zij dagelijks omgaat met persoonsgegevens en privacy, en wat er wettelijk wel en niet verantwoord is.
Privacy speelt een belangrijke rol in de relatie tussen de burger en de overheid en staat daarmee hoog op de bestuurlijke agenda. Gemeenten hebben de verantwoordelijkheid over persoonsgegevens en gegevensuitwisseling op alle terreinen waar ze actief zijn. Gemeenten zijn verplicht om zorgvuldig en veilig, proportioneel en vertrouwelijk om te gaan met het verzamelen, bewaren en beheren van persoonsgegevens van burgers. Dat geldt voor taken op het gebied van basisadministraties, openbare orde en veiligheid, en het sociaal domein. Goed en zorgvuldig omgaan met persoonsgegevens is een dagelijkse bezigheid van gemeenten. Het beschermen van de privacy is complex, en wordt steeds complexer door technologische ontwikkelingen, de decentralisaties, grote uitdagingen op het terrein van veiligheid en nieuwe Europese wetgeving. Daarom vinden wij het belangrijk om transparant te zijn over de manier waarop wij met persoonsgegevens omgaan, en de privacy waarborgen.

1. Wetgeving en definities
Op dit moment heeft elke lidstaat van de Europese Unie een eigen privacywet, gebaseerd op de Europese richtlijn van 1995. De Wet bescherming persoonsgegevens (Wbp) regelt het juridische kader voor de omgang met persoonsgegevens in Nederland. Op 25 mei 2018 vervalt de Wbp en treedt de Europese Verordening; de Algemene Verordening Gegevensbescherming (AVG), in werking, samen met de uitvoeringswet. De AVG bouwt voort op de Wbp en zorgt onder andere voor versterking en uitbreiding van de privacyrechten met meer verantwoordelijkheden voor organisaties.
De volgende begrippen worden in de AVG gebruikt (Artikel 4, AVG):

Betrokkene: De persoon op wie de persoonsgegevens betrekking hebben. De betrokkene is degene van wie de gegevens worden verwerkt.
Verwerker: De persoon of organisatie die de persoonsgegevens verwerkt in opdracht van een andere persoon of organisatie.

Persoonsgegevens: Alle gegevens die gaan over mensen en waaraan je een mens als individu kunt herkennen. Het gaat hierbij niet alleen om vertrouwelijke gegevens, zoals over iemands gezondheid, maar om ieder gegeven dat te herleiden is tot een bepaald persoon (bijvoorbeeld; naam, adres, geboortedatum). Naast gewone persoonsgegevens kent de wet ook bijzondere persoonsgegevens. Dit zijn gegevens die gaan over gevoelige onderwerpen, zoals etnische achtergrond, politieke voorkeuren of het Burgerservicenummer (BSN).

Gegevensbeschermingseffectbeoordeling: Met een gegevensbeschermingseffect-beoordeling worden de effecten en risico's van de nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. Dit heet ook wel een Privacy Impact Assessment (PIA).
[6]www.waalwijk.nl/privacy

Verwerkingsverantwoordelijke: Een persoon of instantie die alleen, of samen met een ander, het doel en de middelen voor de verwerking van persoonsgegevens vaststelt.
Verwerking: Een verwerking is alles wat je met een persoonsgegeven doet, zoals: vastleggen, bewaren, verzamelen, bij elkaar voegen, verstrekken aan een ander, en vernietigen.

2. Reikwijdte
Deze toelichting is van toepassing op alle verwerkingen van persoonsgegevens door alle bestuursorganen van de gemeente. Oftewel: voor alle verwerkingen die binnen de gemeente plaatsvinden.

3. Verantwoordelijke
De bestuursorganen van de gemeente zijn allemaal verantwoordelijken voor de verwerkingen die door of namens de gemeente worden uitgevoerd. De bestuursorganen van de gemeente zijn de burgemeester, het college van Burgemeester en Wethouders (het college), de heffingsambtenaar, de invorderingsambtenaar en de Gemeenteraad.

4. Verwerkingen (Artikel 4, AVG)
De verwerking van persoonsgegevens is elke handeling of elk geheel van handelingen met persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde processen. In de AVG valt onder een verwerking:
- Verzamelen, vastleggen en ordenen

- Bewaren, bijwerken en wijzigen
- Opvragen, raadplegen, gebruiken
- Verstrekken door middel van doorzending
- Verspreiding of enige andere vorm van ter beschikkingstellen
- Samenbrengen, met elkaar in verband brengen
- Afschermen, uitwissen of vernietigen van gegevens

Uit deze opsomming blijkt dat alles wat je met een persoonsgegeven doet een verwerking is.

Doeleinden (Artikel 5, AVG)
Volgens de wet mogen persoonsgegevens alleen verzameld worden als daarvoor een doel is vastgesteld. Het doel moet uitdrukkelijk omschreven en gerechtvaardigd zijn. De gegevens mogen niet voor andere doelen verwerkt worden. Voor de uitvoering van sommige wetten, zoals bijvoorbeeld de Jeugdwet, zijn de doelen voor het verwerken in de wet al vastgelegd, net als de persoonsgegevens die gevraagd en verwerkt mogen worden.

Rechtmatige grondslag (Artikel 6, AVG)
De wet zegt dat er voor elke verwerking van persoonsgegevens een rechtmatige grondslag uit de wet van toepassing moet zijn. Dat betekent dat de verwerking alleen mag plaatsvinden:
- Om een verplichting na te komen die in de wet staat
- Voor de uitvoering van een overeenkomst waar de betrokkene onderdeel was
- Om een ernstige bedreiging voor de gezondheid van de betrokkene te bestrijden
- Voor de goede vervulling van de gemeentelijke taak
- Wanneer de betrokkene toestemming heeft gegeven voor de specifieke verwerking
- De gemeente een gerechtvaardigd belang heeft om gegevens te verwerken, als de gemeente als private partij handelt.

Wijze van verwerking
De hoofdregel van de verwerking van persoonsgegevens 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. Dit betekent dat verwerking alleen is toegestaan wanneer het doel niet op een andere manier kan worden bereikt.
In de wet wordt ook gesproken over proportionaliteit. Dit betekent dat persoonsgegevens alleen mogen worden verwerkt als dit in verhouding staat tot het doel. Wanneer met geen, of minder (belastende), persoonsgegevens hetzelfde doel bereikt kan worden moet daar altijd voor gekozen worden.
De gemeente zorgt ervoor dat de persoonsgegevens kloppen en volledig zijn voordat ze verwerkt worden. Deze gegevens worden alleen verwerkt door personen met een geheimhoudingsplicht. Daarnaast beveiligt de gemeente alle persoonsgegevens. Dit moet voorkomen dat de persoonsgegevens kunnen worden ingezien of gewijzigd door iemand die daar geen recht toe heeft. Hoe de gemeente dit doet staat in het informatiebeveiligingsbeleid van de gemeente en in een eventueel aanvullend beveiligingsplan specifiek opgesteld voor een proces of registratie.

Doorgifte (Artikel 44 t/m 50, AVG)
De gemeente geeft alleen persoonsgegevens door aan een land buiten de Europese Economische Ruimte (EER) of een internationale organisatie op grond van goedgekeurde afspraken door de Europese Commissie.

5. Transparantie en communicatie
Wet openbaarheid van bestuur (Wob)
Via de Wob (en straks wellicht de Wet Open Overheid) kun je een verzoek om informatie indienen bij de gemeente. Bij het verzoek bekijkt de gemeente altijd of het antwoord geen inbreuk maakt op de persoonlijke levenssfeer van betrokkenen. In principe worden geen persoonsgegevens verstrekt.

Wet hergebruik van overheidsinformatie
De Wet hergebruik van overheidsinformatie6 regelt het op verzoek verstrekken van overheidsinformatie voor hergebruik. Bij het verzoek bekijkt de gemeente altijd of het antwoord geen inbreuk maakt op de persoonlijke levenssfeer van betrokkenen. In principe worden geen persoonsgegevens verstrekt.

Informatieplicht (Artikel 13,14, AVG)
De gemeente informeert betrokkenen over het verwerken van persoonsgegevens. Wanneer betrokkenen gegevens aan de gemeente geven, worden zij op de hoogte gesteld van de manier waarop de gemeente met persoonsgegevens om zal gaan. Dit kan bijvoorbeeld via een formulier gebeuren. Vaak staat op de aanvraagformulieren vermeld welke gegevens zonder toestemming niet openbaar gemaakt zullen worden. De betrokkene wordt niet nogmaals geïnformeerd als hij/zij al weet dat de gemeente persoonsgegevens van hem/haar verzamelt en verwerkt, en weet waarom en voor welk doel dat gebeurt.

Wanneer de gegevens via een andere weg verkregen worden, dus buiten de betrokkene om, wordt de betrokkene geïnformeerd op het moment dat deze voor de eerste keer worden verwerkt.

Verwijdering
De gemeente bewaart de persoonsgegevens niet langer dan nodig is voor de uitvoering van gemeentelijke taken, of zoals vastgelegd in de Archiefwet. Wanneer er nog persoonsgegevens opgeslagen zijn die niet langer nodig zijn voor het bereiken van het doel worden deze zo snel mogelijk verwijderd. Dit houdt in dat deze gegevens vernietigd worden, of zo worden aangepast dat de informatie niet meer gebruikt kan worden om iemand te identificeren.

Rechten van betrokkenen (Artikel 13 t/m 20, AVG)
De wet bepaalt niet alleen de plichten van degenen die de persoonsgegevens verwerken, maar bepaalt ook de rechten van de personen van wie de gegevens worden verwerkt. Deze rechten worden ook wel de rechten van betrokkenen genoemd, en bestaan uit de volgende rechten:

- Recht op informatie: Betrokkenen hebben het recht om aan de gemeente te vragen of zijn/haar persoonsgegevens worden verwerkt.
- Inzagerecht: Betrokkenen hebben de mogelijkheid om te controleren of, en op welke manier, zijn/haar gegevens worden verwerkt.
- Correctierecht: Als duidelijk wordt dat de gegevens niet kloppen, kan de betrokkene een verzoek indienen bij de gemeente om dit te corrigeren.
- Recht van verzet: Betrokkenen hebben het recht aan de gemeente te vragen om hun persoonsgegevens niet meer te gebruiken.
- Recht om vergeten te worden: In gevallen waar de betrokkene toestemming heeft gegeven om gegevens te verwerken, heeft de betrokkene het recht om de persoonsgegevens te laten verwijderen.
- Recht op bezwaar: Betrokkenen hebben het recht om bezwaar aan te maken tegen de verwerking van zijn/haar persoonsgegevens. De gemeente zal hieraan voldoen, tenzij er gerechtvaardigde gronden zijn voor de verwerking.

Indienen van verzoek
Om gebruik te maken van zijn/haar rechten kan de betrokkene een verzoek indienen. Dit verzoek kan zowel schriftelijk als via de e-mail ingediend worden. De gemeente heeft een maand de tijd, vanaf de ontvangst van het verzoek, om te beoordelen of het verzoek gerechtvaardigd is. Binnen een maand zal de gemeente laten weten wat er met het verzoek gaat gebeuren. Als het verzoek niet wordt opgevolgd is er de mogelijkheid om bezwaar te maken bij de gemeente, of een klacht in te dienen bij de Autoriteit Persoonsgegevens (AP). Aan de hand van een verzoek kan de gemeente aanvullende informatie opvragen om zeker te zijn van de identiteit van de betrokkene.

6. Geautomatiseerde verwerkingen

Profilering (Artikel 22, AVG)
De wet geeft aan dat er geen besluit mag worden genomen op basis van profilering.
Profilering vindt plaats wanneer er een geautomatiseerde verwerking van persoonsgegevens plaatsvindt waarbij aan de hand van persoonsgegevens naar bepaalde persoonlijke aspecten van een persoon wordt gekeken om deze persoon te categoriseren en te analyseren, of om zaken te kunnen voorspellen. Voorbeelden van persoonlijke aspecten kunnen zijn; financiële situatie, interesses, gedrag of locatie. Om profilering wat duidelijker te maken gebruiken we het volgende voorbeeld: Wanneer een bezoeker op de gemeentelijke website naar een bepaalde dienst kijkt, mag de gemeente geen actie ondernemen om de dienst aan te bieden. Gemeenten mogen wel bekijken hoe vaak een bepaalde dienst bekeken is, maar dus niet specifiek gericht adverteren. Dit doen wij niet.

Big data en tracking
Door middel van Big data onderzoek en tracking mogen alleen gegevens verwerkt worden wanneer deze niet herleidbaar zijn tot een natuurlijk persoon. Daarnaast worden ze alleen verzameld voor onderzoek dat door, of namens, de gemeente wordt uitgevoerd. De verzamelde gegevens door Big data onderzoek en tracking zijn alleen de gegevens die door geautoriseerde personen zijn verzameld. Wanneer de gegevens worden omgezet in een dataset zal dataminimalisatie worden toegepast. Dit betekent dat alleen de data die echt nodig is voor het behalen van het doel gebruikt zullen worden. Daarnaast kunnen persoonsgegevens gepseudonimiseerd worden zodat zij niet herleidbaar zijn tot een persoon.

Gemeente Waalwijk maakt geen gebruik van tracking. Het gebruik van Big Data wordt op dit moment niet systematisch toegepast maar wij onderzoeken wel welke voordelen het gebruik van Big Data kan hebben voor onze dienstverlening. Voor beleidsdoeleinden worden regelmatig onderzoeken uitgevoerd.

Persoonsgegevens worden dan geanonimiseerd of ze worden verwerkt na de ondubbelzinnige toestemming van de betrokkene.

Inzet van camera's
Binnen de gemeente wordt onder bepaalde omstandigheden gebruik gemaakt van cameratoezicht, zoals vastgelegd in de Gemeentewet. Cameratoezicht wordt onder andere gebruikt voor het vergroten van de veiligheid op straat. Camera's kunnen een grote inbreuk maken op de privacy van diegene die gefilmd worden. Om de privacy zo goed mogelijk te waarborgen worden camera's alleen ingezet wanneer er geen andere manieren zijn om het doel te bereiken, en worden er eisen gesteld aan de inzet van camera's.

Cameratoezicht Gemeente Waalwijk maakt gebruikt van cameratoezicht. Informatie hierover kunt u lezen op [https://www.waalwijk.nl/inwoners/regelgeving_3809/item/openbare-orde-en-veiligheid_3758.html].

7. Plichten van de gemeente
Register van verwerkingen (Artikel 30, AVG) De gemeente is verantwoordelijk voor het aanleggen van een register van alle verwerkingen waarvan de gemeente de verwerkingsverantwoordelijke is. Elk register bevat een beschrijving van wat er tijdens een verwerking plaatsvindt, en welke gegevens daarvoor worden gebruikt, namelijk:
De naam en contactgegevens van de verwerkingsverantwoordelijke en, mogelijk, de gezamenlijke verwerkingsverantwoordelijke;
- De doelen van de verwerking;
- Een beschrijving van het soort persoonsgegevens en de daarbij horende betrokkenen; Een beschrijving van de ontvangers van de persoonsgegevens;
- Een beschrijving van het delen van persoonsgegevens aan een derde land of internationale organisatie;
- De termijnen waarin de verschillende persoonsgegevens moeten worden gewist;
- Een algemene beschrijving van de beveiligingsmaatregelen.

Gegevensbeschermingseffectbeoordeling (Artikel 35, AVG)
Met een gegevensbeschermingseffectbeoordeling worden de effecten en risico's van nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. De gemeente voert deze uit wanneer er een geautomatiseerde verwerking, een grootschalige verwerking, of wanneer er een grootschalige monitoring van openbare ruimten plaatsvindt. Dit geldt in het bijzonder bij verwerkingen waarbij nieuwe technologieën worden gebruikt.

Aanstellen van een Functionaris voor gegevensbescherming (FG) (Artikel 37 t/m 39, AVG)
De gemeente heeft een FG aangesteld. De FG is betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. De taken van de functionaris zijn informeren, adviseren, toezicht houden, bewustwording creëren, en optreden als contactpersoon van de AP. Het is niet de bedoeling dat de functionaris de taken op het gebied van bescherming van de privacy van de afdelingen overneemt. De afdelingen hebben hun eigen verantwoordelijkheid in het goed omgaan met privacygevoelige gegevens. Een verwerking van persoonsgegevens wordt eerst aan de FG gemeld voordat de verwerking begint. De FG is verantwoordelijk voor het structureel toetsen van de implementatie en de uitvoering van de wettelijke eisen en de gemeentelijke richtlijnen op het gebied van privacy.

Voor vragen over privacy of over deze toelichting kunt u contact opnemen met de functionaris voor gegevensbescherming van gemeente Waalwijk via: fg@waalwijk.nl

Datalekken (Artikel 33,34, AVG)
We spreken van een datalek wanneer persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens mogen hebben. Wanneer er een datalek heeft plaatsgevonden meldt de gemeente dit zonder onredelijke vertraging, uiterlijk 72 uur nadat er kennis van de inbreuk is vernomen, aan de AP. Als dit later dan 72 uur is wordt er een motivering voor de vertraging bij de melding gevoegd. Het kan zijn dat de inbreuk een hoog risico met zich meebrengt voor de rechten en vrijheden van de betrokkenen. In dit geval meldt de gemeente dit aan de betrokkenen in eenvoudige en duidelijke taal. Om toekomstige datalekken te voorkomen worden bestaande datalekken geëvalueerd.

Afsluiting
Als de gemeente een wettelijke verplichting niet nakomt kan de betrokkene een klacht indienen. Deze zal via de klachtenregeling van de gemeente worden behandeld. In gevallen waar het reglement niets over zegt, beslist het verantwoordelijke bestuursorgaan van de gemeente.

Disclaimer: Deze toelichting is een eenvoudige en begrijpbare vertaling van de huidige privacywetgeving en gebaseerd op de AVG. Vanzelfsprekend is de toepasbare wet- en regelgeving altijd leidend en kunnen er geen rechten ontleend worden aan dit document.