

Beleid bescherming persoonsgegevens gemeente Waalwijk

Versie:	2.3
Versiedatum:	2-12-2022
Gemaakt door:	
Goedgekeurd door:	College
V-Classificatie:	Openbaar

Inhoudsopgave

1. Inleiding. 3
2. Begripsbepalingen. 3
3. Visie. 3
4. Doel 3
5. Reikwijdte. 4
6. Principes voor de verwerking van persoonsgegevens 4
7. Rollen en Verantwoordelijken. 10

1. Inleiding

De gemeente Waalwijk werkt met (persoons)gegevens van burgers, ondernemers, medewerkers en (keten)partners. Deze gegevens verzamelt de gemeente om de gemeentelijke wettelijke taken goed uit te kunnen voeren van. Denk hierbij aan taken in het sociaal domein, openbare orde en veiligheidsdomein of voor burgerzaken. Om deze taken goed te volbrengen is het noodzakelijk dat de gemeente persoonsgegevens verwerkt. De burger moet erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met deze persoonsgegevens omgaat.

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

Geldigheidsduur

Dit beleid is vastgesteld door het college van B&W als eindverantwoordelijke voor de gemeentelijke gegevensverwerking. Het beleid wordt tenminste eens per drie jaar beoordeeld en zo nodig herzien. Indien daar aanleiding toe is (bijvoorbeeld bij grote organisatorische veranderingen, wetswijzigingen, uitkomsten van DPIA's/GEB's) kan het college besluiten tot een tussentijdse herziening.

2. Begripsbepalingen

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

3. Visie

De komende jaren zet de gemeente in op het verhogen van de privacy bewustwording en verdere professionalisering van de privacy functie in de organisatie. Een goede privacy boekhouding is noodzakelijk voor het goed functioneren van de gemeente en de basis voor het beschermen van rechten van burgers en bedrijven. Dit vereist een integrale aanpak, goed eigenaarschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken. Daarbij is verantwoord en bewust gedrag van alle medewerkers essentieel voor privacy binnen de gemeente.

4. Doel

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

De verdere uitwerking van dit beleid is - waar relevant - vastgelegd in de operationele documenten binnen de gemeente, zoals handreikingen, concrete werkprocedures of werkafspraken voor algemene onderwerpen zoals datalekken, maar ook domeinspecifieke onderwerpen als gegevensdeling voor de uitvoering van de Jeugdwet of de Wet Maatschappelijke Ondersteuning.

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

Verantwoordelijkheid van iedere werknemer

Iedereen werkzaam binnen de gemeente is verantwoordelijk voor het verantwoord omgaan met persoonsgegevens. De gemeente verlangt van al haar medewerkers en alle personen die werkzaam zijn voor de gemeente dat de voorschriften van dit privacybeleid worden opgevolgd en actief worden uitgedragen.

5. Reikwijdte

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

Dit privacybeleid is van toepassing op alle verwerkingen van persoonsgegevens door of namens de gemeente, waaronder:

1. De verwerking van persoonsgegevens binnen de bedrijfsprocessen van de gemeente;
2. De verwerking van persoonsgegevens die is uitbesteed, of op een andere manier is georganiseerd, zoals deelname van de gemeente aan een rechtspersoon die voor de gemeente bepaalde diensten verricht;
3. De gegevensuitwisseling met derde partijen zoals bij samenwerkingsverbanden of leveranciers.

6. Principes voor de verwerking van persoonsgegevens

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

Rechtmatige grondslag

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

Welbepaalde doeleinden

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

Verdere verwerking

Persoonsgegevens kunnen in bepaalde gevallen worden verwerkt voor andere doelen dan waarvoor ze in eerste instantie zijn verzameld. Daarbij geldt onder andere dat de twee doelen aan elkaar verwant moeten zijn, er zich geen nadelige effecten voor de betrokkenen voordoen, dan wel dat hiervoor extra waarborgen zijn getroffen. De gemeente voert, voordat de verwerking start, een toets uit om te bepalen of de gegevens voor andere doelen mogen worden gebruikt op grond van de wet- en regelgeving.

Minimale gegevensverwerking

Gegevens mogen alleen worden verwerkt als dit in verhouding staat tot het doel. Als het doel waarvoor persoonsgegevens worden verwerkt, zonder of met minder persoonsgegevens kan worden bereikt, dan kiest de gemeente bij voorkeur voor die mogelijkheid. Ook als het doel waarvoor persoonsgegevens worden verwerkt op een wijze kan worden verwezenlijkt die minder inbreuk maakt op de privacy van de betrokkene, dan kiest de gemeente bij voorkeur voor die mogelijkheid.

Juiste en actuele gegevens

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

Gegevens worden op tijd vernietigd

De gemeente stelt de bewaartermijn van een verwerking vast aan de hand van wettelijke bepalingen en de selectielijsten. Gemeenten hebben op grond van de Archiefwet 1995 onder andere de plicht om zogenaamde selectielijsten op te stellen. Deze selectielijsten bepalen voor een selectie van documenten hoelang deze moeten worden bewaard.

Alleen als de bewaartermijn niet op basis van wettelijke bepalingen of de selectielijsten kan worden vastgesteld, stelt de gemeente de bewaartermijn vast op basis van noodzakelijkheid. Persoonsgegevens mogen dan niet langer worden bewaard dan noodzakelijk. De gemeente bewaart gegevens alleen langer als deze geanonimiseerd worden, zodat directe of indirecte identificatie van een persoon niet meer mogelijk is.

Integriteit en vertrouwelijkheid

De gemeente neemt passende technische en organisatorische maatregelen om de persoonsgegevens, met name bijzondere persoonsgegevens, te beschermen tegen misbruik en onrechtmatige of ongeautoriseerde verwerking. De gemeente handelt hierbij in overeenstemming met het informatiebeveiligings-

beleid. Het informatiebeveiligingsbeleid verplicht de gemeente om informatie te beveiligen tegen ongeautoriseerd gebruik, vernietiging (per ongeluk of onrechtmatig), verlies of vervalsing, onbevoegde bekendmaking of toegang en alle andere onrechtmatige manieren van verwerking.

Privacy by Default en Privacy by Design

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

Toegang tot gegevens

Uitsluitend geautoriseerde gebruikers zijn bevoegd tot onder meer het invoeren, rechtstreeks raadplegen, wijzigen en verwijderen van persoonsgegevens voor zover aan hen hiervoor bevoegdheden zijn toegekend. Deze bevoegdheden worden verleend op grond van het binnen de gemeente geldend beleid voor toegang tot gegevens, waaronder het informatiebeveiligingsbeleid. Het beheer van bevoegdheden wordt periodiek gecontroleerd. De gemeente hanteert daarnaast specifieke oplossingen en toepassingen, waaronder het bijhouden van loggegevens, om ongeautoriseerde toegang tot en niet toegestane verwerkingen van persoonsgegevens zo veel mogelijk te voorkomen en aan te pakken.

Inbreuk in verband met persoonsgegevens

Bij toegang tot, verlies of wijziging van persoonsgegevens bij de gemeente, zonder dat dit de bedoeling is, is er sprake van een datalek. Dat moet, afhankelijk van het risico, worden gemeld bij de toezichthouder (de Autoriteit Persoonsgegevens) en soms bij de getroffen betrokkenen. De gemeente registreert datalekken, zet de bevindingen om in verbeterpunten en ziet toe op de opvolging hiervan. Nadere regels ten aanzien van het vaststellen, melden en afhandelen van datalekken zijn opgenomen in een vastgestelde procedure.

Samenwerking

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

Samenwerkingsverbanden

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

Doorgifte buiten de EER

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

Transparantie

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

Rechten van betrokkenen

Iedereen heeft het recht om te vernemen welke persoonsgegevens de gemeente over hem/haar heeft verzameld en waarvoor deze worden gebruikt. Betrokkenen hebben de mogelijkheid om hun rechten uit hoofdstuk III van de AVG uit te oefenen, te weten het recht van inzage, recht op rectificatie, recht op verwijdering, recht op bezwaar, recht op beperking en recht op overdraagbaarheid. Nadere regels ten aanzien van de rechten van betrokkenen zijn opgenomen in de een vastgestelde procedure rechten van betrokkenen.

Geschillenbeslechting

Indien de betrokkene van mening is dat de gemeente niet op een juiste wijze met zijn persoonsgegevens is omgegaan, kan hij een klacht indienen middels de van toepassing zijnde klachtenprocedure zoals opgenomen in de privacyverklaring op de website[1]. De betrokkene heeft ook het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens, met betrekking tot de naleving van wet- en regelgeving op het gebied van de bescherming van persoonsgegevens.

Verantwoording

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

Verwerkingsregister

De gemeente beschikt over een verwerkingsregister, waarin alle verwerkingen van persoonsgegevens gedocumenteerd zijn en inzichtelijk zijn gemaakt.

Gegevenseffectbeoordeling (GEB)

Als een verwerking mogelijk een hoog risico inhoudt voor de betrokkene, moet de gemeente een beoordeling uitvoeren van het effect van een verwerking van persoonsgegevens. De gemeente voert in dat geval een gegevenseffectbeoordeling (ook wel Data Processing Impact Assessment of DPIA genoemd). Als uit de GEB blijkt dat er inderdaad hoge risico's zijn verbonden aan de verwerking, moet de gemeente voldoende maatregelen nemen om de risico's te verminderen. Als het niet lukt om (voldoende) maatregelen te nemen om dit risico te beperken, dan moet de gemeente met de AP overleggen, voordat zij met de verwerking start. Dit wordt een voorafgaande raadpleging[2] genoemd.

Functionaris gegevensbescherming (FG)

De gemeente is een overheidsinstantie die structureel en op grote schaal persoonsgegevens verwerkt, waaronder bijzondere persoonsgegevens. De gemeente is daarom verplicht een FG aan te stellen. De FG is de onafhankelijke intern toezichthouder en heeft een adviserende, informerende en toezichthoudende taak. Dit betekent dat de FG toeziet op alle verwerkingen van persoonsgegevens. De FG brengt jaarlijks een verslag uit aan de gemeenteraad en het College van B&W van zijn werkzaamheden, bevindingen en aanbevelingen.

PDCA Cyclus

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

Daarnaast gebruikt de gemeente het borgingsproduct van de VNG als het beoordelingskader voor het waarborgen van privacy compliance binnen de gemeente. Het borgingsproduct is een normenkader wat door de gemeente gebruikt wordt voor het duiden van privacy risico's en de daarbij behorende beheersmaatregelen binnen de gemeente.

Bewustwording

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

[1] <https://www.waalwijk.nl/privacy>

[2] <https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/voorafgaande-raadpleging>

7. Rollen en Verantwoordelijken

Het governancemodel van de gemeente biedt een overkoepelende visie en strategie hoe de bescherming van persoonsgegevens effectief belegd wordt binnen de organisatie. Daartoe bevat het een beschrijving van de taken en verantwoordelijkheden van het College van B&W, het managementteam en medewerkers, de Functionaris voor de Gegevensbescherming (FG), de Security & Privacy Officer en de CISO.

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

Rollen en verantwoordelijkheden

College van B&W

Het College is eindverantwoordelijk voor de naleving van de privacywetgeving binnen de gemeente. Het College heeft de volgende rollen en verantwoordelijkheden:

- Eindverantwoordelijk voor de naleving van de privacywetgeving binnen de gemeente;
- Stelt het privacybeleid vast;
- Geeft sturing aan privacy beleidsvoering en legt rekenschap af over privacy beleidsvoering aan de FG;
- Evalueert de toepassing en werking van het privacybeleid op basis van de rapportage van de FG;
- Bevordert duurzame privacycultuur.

Teammanagers en directeuren

De teammanagers en directeuren zijn eindverantwoordelijk voor de naleving van de privacywetgeving binnen de afdeling, alsmede voor de uitvoering van het privacybeleid.

De teammanagers en directeuren hebben de volgende rollen en verantwoordelijkheden:

- Eindverantwoordelijk voor de naleving van de privacywetgeving binnen de eigen afdeling;
- Verantwoordelijk voor implementatie en uitvoering van het privacybeleid binnen de eigen afdeling;
- Informeert de FG op welke manier het eigen team compliant is aan de privacywetgeving;
- Verantwoordelijk voor (laten) volgen van trainingen door werknemers binnen het eigen team;
- Verantwoordelijk voor registreren van de gegevensverwerkingen in het verwerkingenregister voor zover dit betrekking heeft op de eigen afdeling;
- Verantwoordelijk voor autorisatie en intrekken van de autorisatie van medewerkers die persoonsgegevens verwerken;
- Aansturen van de team-security & privacy officers, voor zover benoemd binnen het eigen team;
- Bevordert duurzame privacycultuur;
- Betrekt SPO en/of FG in een vroeg stadium bij nieuwe of gewijzigde verwerkingen van persoonsgegevens.

Functionaris Gegevensbescherming (FG)

Op basis van de AVG is het aanstellen van een FG verplicht voor de gemeente. De FG is verantwoordelijk voor het toezicht op de naleving van de AVG. De FG heeft een onafhankelijke adviserende en toezicht houdende positie in de organisatie. De FG heeft de volgende rollen en verantwoordelijkheden in de gehele organisatie van de gemeente:

- Interne toezichthouder op de naleving van de AVG namens de Autoriteit Persoonsgegevens;
- Monitort veranderingen in wetgeving en stelt de impact van deze wijzigingen vast en adviseert de organisatie bij de implementatie hiervan;
- Neemt de leiding bij het interpreteren van (nieuwe) wetgeving op het gebied van privacy en gegevensbescherming;
- Draagt privacybeleid actief uit binnen de gehele gemeente en bevordert een cultuur van duurzame gegevensbescherming;
- Adviseert verwerkingsverantwoordelijken bij privacyklachten en verzoeken van betrokkenen (ombudsfunctie);
- Adviseert verwerkingsverantwoordelijken ten aanzien van het mitigeren van privacy risico's, bijvoorbeeld bij het uitvoeren van DPIA's en hoog-risico dossiers;
- Adviseert de verwerkingsverantwoordelijke bij datalekken (volgens de meldprocedure);
- Beschikt over controle- en monitoringbevoegdheden[3] (het recht om interne onderzoeken te laten uitvoeren met toegang tot informatie);
- Rapporteert aan het College van B&W.

Security & Privacy Officer

De Security & Privacy Officer (SPO) is het eerste aanspreekpunt voor de gemeente rondom privacygerelateerde vraagstukken, en heeft een monitorende en ondersteunende functie rondom het naleven en uitvoeren van het privacybeleid. De SPO heeft de volgende rollen en verantwoordelijkheden:

- Adviseert en faciliteert de verwerkingsverantwoordelijken ten aanzien van het naleven en de uitvoering van het privacybeleid;
- Opstellen privacybeleid en modellen, formats en standaard-overeenkomsten, waaronder o.a. de verwerkersovereenkomst en de overeenkomst voor uitwisseling van persoonsgegevens;
- Monitort en ondersteunt verwerkingsverantwoordelijken bij toepassing, opvolging en uitvoering van het privacybeleid;
- Monitort en ondersteunt het (laten) registreren van verwerkingen in het verwerkingsregister door de verwerkingsverantwoordelijke en het (laten) registreren van relevante wijzigingen;
- Adviseert de verwerkingsverantwoordelijke bij het uitvoeren van gegevenseffectbeoordeling (GEB) en de daaruit voortvloeiende risico's alsmede de organisatorische en technische maatregelen om deze te mitigeren;
- Adviseert over de bepalingen in verwerkersovereenkomsten en faciliteert bij het opstellen, aanpassen en uitonderhandelen daarvan;
- Adviseert over mechanismen voor internationale uitwisseling van persoonsgegevens naar landen buiten de EU/EER;

- Adviseert over privacy-gerelateerde bepalingen in overeenkomsten met derden waarbij persoonsgegevens worden uitgewisseld;
 - Adviseert over de verwerkingsgrondslag (en adviseert, indien van toepassing, over de informed consent);
 - Ontwikkelt de bewustmakingsprogramma's- en privacytrainingen voor medewerkers, organiseert deze en voert deze trainingen uit;
 - Adviseert de verwerkingsverantwoordelijke over Privacy by Design & Default bij ontwikkeling van nieuwe systemen in samenwerking met de CISO en ondersteunt en faciliteert bij het opstellen en uitwerken daarvan;
 - Ondersteunt en faciliteert verwerkingsverantwoordelijke bij het afhandelen van datalekken (volgens de meldprocedure).
- [3] Zie hiervoor het Reglement FG

Andere rollen en verantwoordelijkheden

Afdeling	Betrokkenheid
CISO	Toezicht op de toepassing en implementatie van technische en organisatorische maatregelen in het kader van de bescherming van persoonsgegevens. Adviseren van de organisatie bij datalekken (volgens de meldprocedure). Tijdig melden van Informatiebeveiligingsincidenten bij PO/FG als er mogelijk sprake is van betrokkenheid van persoonsgegevens bij het incident.
Communicatie	In alle gevallen waarbij communicatie (intern en extern) een rol speelt worden medewerkers van communicatie betrokken. Adviseren van de organisatie over de communicatie bij datalekken (volgens de meldprocedure)
Interne Controle / Auditors	Toetst het goed en betrouwbaar functioneren van de gehele interne organisatie.
CIO-Office / Informatiemanagement	Inrichten van de informatievoorziening (de beoordeling van welke functionaliteit en welke data in op welke wijze / in welk systeem verwerkt kan / moet worden). Bijhouden verwerkingsregister. Uitvoeren van risico-analyses en advisering.
Team Security Privacy officers / ambassadeurs/contactpersonen	De team security & privacy officer is het eerste aanspreekpunt binnen het team voor de SPO en heeft een moniterende en ondersteunende functie rondom het naleven en uitvoeren van het privacybeleid.

Overlegstructuur

De stuurgroep AVG & Informatiebeveiliging monitort de doelen uit het jaarplan en de doelen voor de middellange termijn op het gebied van privacy en security. Hierin nemen deel: de directeur bedrijfsvoering en dienstverlening, de teammanagers ICT en IBF, de SPO en de FG. In het CIO-office / werkgroep AVG worden acties belegd om verbeterpunten uit het jaarplan te realiseren. Zij rapporteren hierover aan de stuurgroep AVG & IB.

Addendum Beleid bescherming persoonsgegevens gemeente Waalwijk - Wet Politiegegevens

Inleiding

Vanaf 25 mei 2018 geldt de Algemene Verordening Gegevensbescherming (AVG). De gemeente heeft in haar privacybeleid en informatiebeveiligingsbeleid vastgelegd hoe zij omgaat met de bescherming van persoonsgegevens.

De verwerking van persoonsgegevens door buitengewoon opsporingsambtenaren (boa's) valt niet alleen onder de AVG maar ook onder de Wet politiegegevens (Wpg). Daarnaast is een aantal andere regelingen van toepassing op de verwerking van politiegegevens. Zoals het Besluit politiegegevens (Bpg), het Besluit politiegegevens buitengewoon opsporingsambtenaren en de Regeling periodieke audit politiegegevens. Deze wetten en regelgevingen kennen op enkele gebieden wat onderlinge verschillen. Zo kent de Wpg bijvoorbeeld specifieke bewaartermijnen voor de opslag van politiegegevens, terwijl de AVG geen concrete bewaartermijnen voorschrijft. Ook stelt de Wpg andere eisen bij het delen van politiegegevens tussen verschillende partijen, is er een verplichting tot logging en zijn er in de Wpg aanvullende beperkingen en uitzonderingen op de in de AVG geldende privacyrechten van betrokkenen. Andere verplichtingen zijn vergelijkbaar maar kennen verschillen in de concrete uitwerking, zoals de verplichting voor de verwerkingsverantwoordelijke om passende technische en organisatorische maatregelen te treffen ter bescherming en beveiliging van de gegevens. In het kader van de Wpg is bijvoorbeeld ook eens per 4 jaar een externe audit verplicht en moeten elk jaar interne audits worden gehouden.

Het huidige privacybeleid van de gemeente gaat alleen uit van de AVG. Het is daarom wenselijk er de verplichtingen uit de Wpg aan toe te voegen.

Doelstellingen van het privacybeleid

Het privacybeleid van de gemeente beschrijft hoe we verantwoordelijk en binnen wettelijke kaders met persoonsgegevens omgaan. Voor de reikwijdte van dit addendum bestaat het wettelijk kader voor bescherming van persoonsgegevens uit de Wpg en de genoemde regelingen. De gemeente wil met dit addendum op het privacybeleid onder andere bereiken dat de boa's:

- Zich ten volle bewust zijn van de noodzaak om zorgvuldig en op rechtmatige wijze om te gaan met politiegegevens;
- De rechten van betrokkenen respecteren en werken volgens de vastgestelde procedures;
- Het vertrouwen van betrokkenen in de overheid niet beschamen.
- Gedrag vertonen dat past bij goed werknemerschap.
- De kans op financiële en imagoschade minimaliseren.

Wpg kader

Het normenkader van de Wpg is grotendeels gelijklopend aan dat van de AVG. Op hoofdlijnen geldt aanvullend nog het volgende:

- De boa's van de gemeente kunnen naast hun opsporingstaken ook bestuursrechtelijke toezichts- en handhavingstaken hebben. Zij krijgen dan bij het verwerken van persoonsgegevens te maken zowel met de AVG te maken als met de Wpg;
- In de verwerking van gegevens moet duidelijk zijn welke gegevens er worden verwerkt onder de AVG en welke onder de Wpg. De Wpg stelt andere eisen aan de verwerking van persoonsgegevens dan de AVG. Zo geldt onder andere de plicht tot delen met ieder andere opsporingsambtenaar die deze gegevens nodig heeft voor zijn werk.

De hierna genoemde verplichtingen uit de Wpg zijn veelal geborgd binnen onze applicaties:

- Er moet een scheiding worden aangebracht tussen gegevens die op feiten zijn gebaseerd en feiten die op een persoonlijk oordeel zijn gebaseerd;
- Er moet onderscheid worden gemaakt tussen betrokkenen, zoals verdachten, slachtoffers, derden en veroordeelden;
- Documentatie is vereist van de doelen van onderzoeken, verstrekking of doorgifte, afwijzing van verzoeken om inzage, inbreuk op de beveiliging, doorgifte buiten de EU met datum en tijd, ontvanger, redenen en doorgegeven gegevens en melding van gemeenschappelijke verwerkingen aan de Autoriteit Persoonsgegevens (AP).
- Er vindt logging plaats in geautomatiseerde systemen van de invoer van gegevens in systemen en op termijn ook van het verzamelen, wijzigen, raadplegen, verstrekken (o.a. in de vorm van doorgifte), combineren of vernietigen van politiegegevens.
- Er worden specifieke eisen gesteld aan de informatiebeveiliging uit het Bpg.

Er geldt met ingang van 2021 een verplichting tot het uitvoeren van een externe privacyaudits. De rapportage die hieruit voortvloeit moet worden verstrekt aan de AP. Als er tekortkomingen zijn geconstateerd moet 3 maanden na het uitvoeren van de audit een verbeterrapport worden opgesteld, waarop binnen een jaar een hercontrole plaatsvindt. De hercontrole geldt alleen voor die onderdelen van de wet waar de tekortkomingen geconstateerd worden. De resultaten van de hercontrole worden vastgelegd in een rapportage en eveneens verstrekt aan de AP, uiterlijk 1 jaar na het uitvoeren van de externe audit.

Register van verwerkingen

Net als de AVG verplicht de Wpg tot het bijhouden van een register van verwerkingen. Wel zijn er enkele verschillen die hierna met een (*) zijn aangeduid. Het register van verwerkingen in het kader van de Wpg moet het volgende bevatten:

- De naam en de contactgegevens van de verwerkingsverantwoordelijke, de gezamenlijk verwerkingsverantwoordelijken en de functionaris voor gegevensbescherming;
- De doelen van de verwerking;
- De categorieën van ontvangers aan wie politiegegevens zijn of zullen worden verstrekt, met inbegrip van ontvangers in derde landen of internationale organisaties;
- Een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
- In voorkomend geval: het gebruik van profilering. (*)
- In voorkomend geval: de categorieën van doorgiften van politiegegevens aan een derde land of een internationale organisatie.
- Een aanwijzing van de rechtsgrondslag van de verwerking, met inbegrip van doorgiften, waarvoor de politiegegevens bedoeld zijn. (*)
- Zo mogelijk: de beoogde termijnen waarbinnen de verschillende categorieën van gegevens worden verwijderd of vernietigd.
- Zo mogelijk: een algemene beschrijving van de technische en organisatorische maatregelen ter beveiliging.
- De toekenning van de autorisaties. (*)

Informatiebeveiligingsbeleid

Het informatiebeveiligingsbeleid is een richtinggevend en kaderstellend beleidsdocument. De gemeente vult het aan met beleid voor informatiebeveiliging op tactisch en operationeel niveau met specifieke (beleids-) documenten.

Het informatiebeveiligingsbeleid geldt voor alle activiteiten van de gemeente. Ook voor de activiteiten die vallen onder de Wpg geldt dat passende technische en organisatorische maatregelen moeten zijn genomen en geïmplementeerd, op basis van een risicoanalyse waaruit het risiconiveau blijkt met betrekking tot ongeoorloofde of onrechtmatige verwerking en tegen opzettelijk verlies, vernietiging of beschadiging. Deze maatregelen moeten bovendien periodiek worden geëvalueerd en zo nodig geactualiseerd.

FG en bevoegd functionaris

De Functionaris Gegevensbescherming (FG)

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

De bevoegd functionaris

De senior medewerker handhaving BOA is verantwoordelijk voor het uitvoeren van de taak bevoegd functionaris. Dit is de 'hoeder' van de gegevens die onder artikel 9 Wpg worden verwerkt. Deze functionaris is beschreven in artikel 2:10, eerste lid, van het Besluit politiegegevens (Bpg). Het moet een persoon zijn met voldoende kennis en vaardigheden over dit type gegevens. Deze functionaris beslist bijvoorbeeld wie er toegang mag hebben tot deze gegevens en of ze verstrekt kunnen worden aan een samenwerkingspartner. Iedere artikel 9-verwerking dient een bevoegd functionaris (BF) te hebben. De bevoegd functionaris heeft onder andere de volgende taken:

- het doel van de artikel 9-verwerking omschrijven en vastleggen;
- het autoriseren van personen voor de betreffende verwerking;
- bepalen of gegevens voor andere doeleinden mogen worden gebruikt;
- zorgen dat voor alle gegevens de herkomst en wijze van verkrijgen wordt vastgelegd;
- bewaken dat gegevensrechtmatig worden verkregen en verwerkt.

Rechten van betrokkenen

De rechten van betrokkenen onder de AVG staan uitgebreid beschreven in het privacybeleid van de gemeente. Op hoofdlijnen zijn deze rechten op grond van de Wpg gelijklopend. Specifiek voor de Wpg is er een addendum opgesteld.

Het bewaren van politiegegevens

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

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

Het ter beschikking stellen en verstrekken van politiegegevens

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

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

Het melden van datalekken

De datalek procedure onder de AVG staan uitgebreid beschreven in het privacybeleid van de gemeente. Op hoofdlijnen zijn deze rechten op grond van de Wpg gelijkloidend. Specifiek voor de Wpg geldt nog het volgende:

Op deze mededelingsplicht zijn enkele uitzonderingen van toepassing, onder andere als de mededeling achterwege moet blijven ter vermijding van belemmering van de gerechtelijke onderzoeken of procedures en ter vermijding van nadelige gevolgen voor de voorkoming, de opsporing, het onderzoek en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen.

Bewustwording

Het zorgvuldig omgaan met persoonsgegevens is enerzijds een kwestie van het organiseren van een goede informatieveiligheid en het zorgvuldig inrichten van werkprocessen, anderzijds is het een zaak van bewustwording bij de boa's. Het bewustzijn wordt voortdurend aangescherpt, zodat kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd.

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

Open communicatie

Betrokkenen moeten erop kunnen vertrouwen dat hun persoonsgegevens zorgvuldig worden verwerkt. De gemeente creëert dat vertrouwen door inzichtelijk te maken, door middel van verschillende communicatiekanalen, op welke wijze zij persoonsgegevens verwerkt en beheert. Dit staat in de privacyverklaring die op de website is te vinden.

Aldus vastgesteld in de collegevergadering van 31 januari 2023.

Het College van Waalwijk,

*de secretaris, de burgemeester,
Michel Tromp, Sacha C.A.M. Ausems*