2023

PRIVACYBELEID

gemeente
Zoetermeer

Inhoudsopgave

1. Inleiding 3
2. Visie 4
3. Doelen van verwerking en soorten gegevens 4
4. Uitgangspunten 4
4.1 Werkbaar en zorgvuldig 4
4.2 Privacy heeft een vaste plek op de werkvloer 5
4.3 Privacy vanaf de start 5
4.4 Transparantie staat voorop 5
5. Verantwoording en toezicht 6
5.1 Verantwoordelijkheid 6
5.2 Verantwoordelijkheid afleggen 6
5.3 Toezicht 6
6. Samenwerking 7
7. Informatieveiligheid 7
8. Gegevensuitwisseling 7
9. Positie en rechten van betrokkenen 8
10. Politiegegevens 9
10.1 Wpg kader 9
10.2 Register van verwerkingen 10
10.3 FG en bevoegd functionaris 10
10.4 Het bewaren van politiegegevens 10
10.5 Het ter beschikking stellen en verstrekken van politiegegevens 10
10.6 Bewustwording 11
11. Bereikbaarheid 11

1. Inleiding

Privacy

Privacy is het recht om jezelf af te schermen ofwel het recht op bescherming van de persoonlijke levenssfeer. Privacy kun je in meerdere soorten onderverdelen, denk met name aan: het huisrecht waaruit volgt dat iemand niet zomaar jouw woning in mag, het recht op lichamelijke integriteit en het recht op bescherming van persoonsgegevens die zijn vastgelegd. Dit beleid gaat over persoonsgegevens die door de gemeente Zoetermeer worden vastgelegd en verwerkt voor de uitvoering van haar taken.

De gemeente verwerkt veel persoonsgegevens. De meest herkenbare persoonsgegevens zijn een naam, adres of e-mailadres. Maar ook indirecte gegevens kunnen persoonsgegevens zijn. Denk daarbij aan een kenteken of een geboortedatum in combinatie met een adres of gegevens over iemands gedrag. Voor alle persoonsgegevens die de gemeente verwerkt, is zij gebonden aan de Algemene Verordening Gegevensbescherming. Dit is de Europese privacywet, ook wel de AVG genoemd. Met dit beleid geeft de gemeente invulling aan haar verplichtingen uit de AVG. Ook uit andere wetten dan de AVG kunnen verplichtingen ten aanzien van privacy volgen, denk aan de Wet maatschappelijke ondersteuning, de Jeugdwet en Wet gemeentelijke schuldhulpverlening.

In sommige gevallen verwerkt de gemeente ook politiegegevens. Bijvoorbeeld bij bepaalde taken die door buitengewoon opsporingsambtenaren worden uitgevoerd. Voor deze gegevens is niet de AVG maar de Wet politiegegevens het kader. Dit beleid geldt ook voor de verwerking van politiegegevens. Voor de uitvoering van deze wet is in dit stuk een apart hoofdstuk opgezet. Dit privacybeleid is een kader voor het college van burgemeester en wethouders (het college), de burgemeester en de overige onderdelen van de organisatie. De in dit beleid genoemde uitgangspunten zorgen ervoor dat we als gemeente op eenduidige wijze persoonsgegevens verwerken.

Het beleid is van toepassing bij alle verwerkingen van persoonsgegevens en op de uitwisseling van persoonsgegevens:
- Tussen verschillende afdelingen;
- Met andere gemeenten;
- Met andere (publiekrechtelijke) organisaties; en
- Bij de uitbesteding van publieke taken.

Het privacybeleid wordt vastgesteld voor de duur van drie jaar en wordt daarna geëvalueerd.

Betrokkene

De natuurlijke persoon over wie een persoonsgegeven gaat. Bijvoorbeeld een aanvrager, medewerker of uitkeringsgerechtigde.

Verwerken

Iedere handeling die met een persoonsgegeven wordt verricht. Bijvoorbeeld vastleggen, delen, verwijderen of raadplegen.

Persoonsgegeven

Ieder gegeven dat iets zegt over een persoon van wie de identiteit bekend of makkelijk te achterhalen is.

2. Visie

Als gemeente doen wij wat nodig is om inwoners zo goed mogelijk van dienst te zijn. Vaak zijn daar persoonsgegevens voor nodig. We gebruiken alleen die gegevens die we nodig hebben. En met die gegevens gaan we uiterst zorgvuldig en integer om. De bescherming van persoonsgegevens mag echter niet zo ver gaan dat het de uitvoering van wettelijke taken in de weg staat of dat andere grondrechten in het geding komen zoals het recht op veiligheid, het recht op onderwijs of het recht op menselijke waardigheid. Bij strijdige belangen maken wij, zoveel mogelijk samen met betrokken partijen, een zorgvuldige afweging. We leggen onze afwegingen goed vast en zijn transparant over de keuzes die we maken.

3. Doelen van verwerking en soorten gegevens

Als gemeente verwerken wij veel soorten persoonsgegevens voor veel verschillende doeleinden. Zo verstrekt de gemeente onder meer identiteitsbewijzen, bouwvergunningen, sociale voorzieningen en andere diensten. Elke soort voorziening of dienst, vraagt deels om andere (persoons)gegevens. De gemeente weegt steeds zorgvuldig af welke gegevens voor welk doeleinden nodig zijn. Daarbij maken we zoveel mogelijk gebruik van authentieke bronnen, zodat inwoners niet steeds opnieuw dezelfde gegevens hoeven te verstrekken.

In het verwerkingsregister wordt voor alle gemeentelijke taken bijgehouden welke persoonsgegevens worden verwerkt. In dit register is ook te zien welke afdeling verantwoordelijk is voor welke verwerkingen en hoe lang gegevens bewaard mogen worden.

4. Uitgangspunten

Als gemeente volgen we een aantal uitganspunten:
- De verwerking van persoonsgegevens moet werkbaar en zorgvuldig zijn;
- Privacy heeft een vaste plek op de werkvloer;
- Privacy wordt vanaf de start meegenomen in alles wat wij doen;
- Transparantie staat voorop.

In dit hoofdstuk lichten we deze uitgangspunten toe.

4.1 Werkbaar en zorgvuldig

De gemeente Zoetermeer verwerkt persoonsgegevens zorgvuldig en binnen de kaders van de AVG:
- Gegevens worden alleen verwerkt als daarvoor een wettelijke grondslag bestaat;
- Er worden niet meer of minder gegevens verwerkt dan noodzakelijk om onze taken goed uit te voeren;
- Persoonsgegevens worden niet zomaar voor nieuwe doelen gebruikt;
- We zorgen dat gegevens juist en actueel zijn;
- De gegevens die in authentieke bronnen beschikbaar zijn, vragen we niet meer uit bij de betrokkene;
- We volgen de wettelijke bewaartermijnen en zorgen dat gegevens tijdig worden verwijderd;
- Als de wet geen bewaartermijn noemt, stellen we een redelijke termijn vast.

Het management stimuleert dat voor veel voorkomende of intensief gebruikte processen werkprocessen worden opgesteld. Daarin moet duidelijk zijn opgenomen hoe voor dat proces wordt omgegaan met (gevoelige) persoonsgegevens.

De gemeente moet kunnen aantonen dat zij aan de regels voldoet. Dit kan op verschillende manieren, onder meer door het aanwezig hebben van duidelijk beleid en door een actueel verwerkingsregister.

4.2 Privacy heeft een vaste plek op de werkvloer

De medewerker is één van de belangrijkste spelers als het gaat om zorgvuldige omgang met persoonsgegevens. Alle nieuwe medewerkers zijn daarom verplicht om de Workshop Informatiebeveiliging, privacy en informatiebeheer te volgen. Daarnaast wordt door middel van trainingen en andere bewustwordingsacties aandacht besteed aan het belang van privacy. Het gemeentelijke intranet dient als kennisbron voor medewerkers.

Er is een netwerk van privacyambassadeurs actief in de organisatie. Zo signaleren we sneller gezamenlijke aandachtspunten en kunnen we effectief informatie delen.

Het belang van privacy is onderdeel van het DNA van de gemeentelijke organisatie en haar medewerkers

Ook is Privacy onderdeel van het integriteitsbeleid van de gemeente Zoetermeer. Wanneer een medewerker in strijd handelt met privacywetgeving handelt zij niet zoals van een goed ambtenaar mag worden verwacht. Dit wordt gezien als plichtsverzuim waartegen een passende maatregel zal worden opgelegd.

4.3 Privacy vanaf de start

Bij de invoering van nieuwe regelgeving of nieuw beleid en bij de ontwikkeling van nieuwe applicaties of systemen, weegt de gemeente Zoetermeer de bescherming van persoonsgegevens vanaf de eerste fase mee. We richten systemen en processen zo in dat alleen de noodzakelijke gegevens worden verwerkt. Daarmee voldoen we aan het beginsel van privacy door ontwerp en door standaardinstellingen. Door de beginselen uit de AVG mee te nemen in inkoop- en aanbestedingstrajecten, zetten we ook opdrachtnemers aan om hiermee rekening te houden.

Wanneer er een hoog risico is voor een verwerking, bijvoorbeeld omdat we veel gevoelige gegevens van kwetsbare inwoners verwerken, dan voeren we een Dataprotection impact assessment (DPIA) uit. Hiermee worden de (privacy- en beveiligings)risico's in kaart gebracht en worden passende maatregelen genomen om die risico's zo goed als mogelijk te beperken. Om te bepalen of een DPIA noodzakelijk is, volgt de gemeente Zoetermeer de Europese richtlijnen.

4.4 Transparantie staat voorop

We zijn transparant over de persoonsgegevens die wij verwerken. We informeren betrokkenen via de privacyverklaring op onze website. Ook is daar dit privacybeleid te lezen. Waar nodig verstrekken we inwoners meer specifieke informatie over de gegevens die we verwerken.

Transparantie staat voorop maar is niet absoluut. In bijzondere gevallen kan informatie (tijdelijk) worden achtergehouden. Bijvoorbeeld bij kwesties van openbare orde en veiligheid of als de belangen van derden in het geding komen.

5. Verantwoording en toezicht

5.1 Verantwoordelijkheid

De eindverantwoordelijkheid voor de verwerking van persoonsgegevens rust in de publieke sector meestal bij het bevoegde bestuursorgaan. Dat kan onder meer zijn:

- De gemeenteraad;
- Het college van burgemeester en wethouders;
- De burgemeester.

Het bestuursorgaan dat eindverantwoordelijk is, noemen we ook wel de verwerkingsverantwoordelijke. De verwerkingsverantwoordelijke is de partij die volgens de AVG verantwoording af moet leggen over de naleving van wet- en regelgeving op gebied van gegevensbescherming.
Binnen de gemeentelijk organisatie zijn de verantwoordelijkheden voor privacy belegd volgens het 'Three lines of defence-model'.

De eerste lijn is de afdeling zelf. Het afdelingshoofd is intern de verantwoordelijke voor de verwerking van persoonsgegevens op de eigen afdeling. Dit houdt onder meer in dat basiskennis over persoonsgegevens die in de processen worden gebruikt op de afdeling zelf aanwezig is. Het verwerkingsregister moet actueel en volledig zijn en wordt door de afdeling bijgehouden. Inzageverzoeken kunnen zelfstandig worden afgehandeld. Ook bij het uitvoeren van DPIA's is de afdeling zelf de eerstverantwoordelijke.
Het afdelingshoofd kan de invulling van deze taak verder in de afdeling beleggen. Wanneer een verwerking een afdelingsoverstijgend karakter heeft of op twee of meer afdelingen ziet, ligt de interne verantwoordelijkheid bij de proceseigenaar.

De tweede lijn is belegd bij de gespecialiseerde adviseurs, in dit geval de senior privacyjuristen. De privacyjuristen adviseren op ingewikkelde of afdelingsoverstijgende vraagstukken. Daarnaast zijn de privacyjuristen verantwoordelijk voor kwaliteitsbewaking van standaardproducten, het opstellen en bijhouden van privacybeleid en het adviseren over de afhandeling van datalekken en DPIA's. De privacyjuristen zijn bevoegd om ernstige datalekken aan de Autoriteit Persoonsgegevens te melden.
De derde lijn ziet toe op de naleving van de AVG en de daarover gemaakte afspraken. Voor de verwerking van persoonsgegevens is dat de Functionaris voor de Gegevensbescherming (de FG).

5.2 Verantwoordelijkheid afleggen

Het college legt verantwoording af over de realisatie en toepassing van het privacybeleid. In het jaarverslag wordt in samenwerking met de onderdelen informatiebeveiliging en informatiebeheer (IPI) verantwoording afgelegd.

Het college meldt bijzonderheden ten aanzien van de bescherming van persoonsgegevens aan de raad. Daarbij valt te denken aan een ernstige inbreuk op de beveiliging van persoonsgegevens of het verlies van persoonsgegevens.

5.3 Toezicht

De FG is de interne onafhankelijke toezichthouder. De FG houdt toezicht op de naleving van de AVG en de toepassing van het privacybeleid. Wanneer dat nodig is, rapporteert de FG rechtstreeks aan het college. Bij calamiteiten kan de FG maatregelen nemen ten aanzien van de bescherming van persoonsgegevens. Om de taken goed uit te kunnen voeren, moet de FG door de verwerkingsverantwoordelijke worden ondersteund. De FG moet tijdig betrokken worden bij aangelegenheden die verband houden met de verwerking van persoonsgegevens en moet toegang krijgen tot de verwerkingsactiviteiten die worden uitgevoerd. Jaarlijks wordt in IPI-verband verslag gedaan van de bevindingen van de interne toezichthouders.

6. Samenwerking

Privacy staat niet op zichzelf, het is onlosmakelijk verbonden met de onderwerpen informatiebeheer en informatiebeveiliging. Zonder degelijk informatiebeheer kan de gemeente bijvoorbeeld niet voldoende reageren op inzageverzoeken van inwoners en kunnen bewaartermijnen niet worden nageleefd. Zonder goede informatiebeveiliging, zou persoonlijke informatie van inwoners op straat kunnen komen te liggen. Samenwerking op deze onderwerpen wordt met de steeds verder toenemende digitalisering steeds meer van belang. Binnen de gemeente is daarom IPI opgericht. IPI staat voor Informatiebeveiliging, Privacy en Informatiebeheer. IPI is een netwerksamenwerking tussen de tweedelijns adviseurs op deze onderwerpen en de drie toezichthouders:

- De Chief Informatie Security Officier (CISO, toezichthouder voor informatiebeveiliging);
- De Gemeentearchivaris (toezichthouder voor informatiebeheer);
- De Functionaris voor de Gegevensbescherming (FG, toezichthouder privacy).

7. Informatieveiligheid

De gemeente Zoetermeer treft passende technische en organisatorische maatregelen om de aanwezige persoonsgegevens te beschermen. Deze maatregelen moeten in verhouding staat tot het risico van de verwerking en de aard van de gegevens die worden verwerkt. Met het informatiebeveiligingsbeleid wordt hier vorm aan gegeven.

Wanneer zich onverhoopt een incident voordoet met persoonsgegevens, heeft de gemeente procedures ingericht om de gevolgen van zo'n incident zo goed als mogelijk te beperken en om herhaling te voorkomen. Meldingen van incidenten en (vermoedens van) datalekken worden via Topdesk gedaan. Indien nodig doen de privacyjuristen of FG melding van een datalek aan de Autoriteit Persoonsgegevens. De senior privacyjuristen of FG bepalen in overleg met de betrokken manager of ook aan de gedupeerde van het datalek melding moet worden gedaan. De gemeente volgt hierbij de Europese richtlijnen, zowel voor meldingen op grond van de AVG als voor meldingen die binnen de Wet politiegegevens vallen. Bij zeer ernstige of zeer omvangrijke datalekken informeert het college de raad.

Datalek

Een datalek is een incident waarbij persoonsgegevens kwijt raken of toegankelijk worden voor personen die daar geen toegang tot zouden mogen hebben.

8. Gegevensuitwisseling

Indien er sprake is van samenwerking waarbij persoonsgegevens (structureel) worden uitgewisseld met externe partijen, maakt de gemeente hierover vooraf passende afspraken. Met deze afspraken worden ieders verantwoordelijkheden op de juiste wijze vastgelegd. Afhankelijk van de omstandigheden kan dat een verwerkersovereenkomst, een gegevensuitwisselingsovereenkomst of een andere vorm van een samenwerkingsovereenkomst zijn. Hierbij wordt waar mogelijk gebruik gemaakt van de door de VNG beschikbaar gestelde modelovereenkomsten. Het verantwoordelijke afdelingshoofd ziet toe op de totstandkoming, bewaring en naleving van deze overeenkomsten. De senior privacyjuristen adviseren over de inhoud van dergelijke overeenkomsten en stellen waar nodig standaarddocumenten op.
Bij gegevensuitwisseling zoekt de gemeente altijd naar een veilige manier om dit te doen. Bij voorkeur gebeurt dit via de daarvoor aangewezen applicaties. Voor de uitwisseling van gegevens over zorg, maken we gebruik van de zogenoemde NTA 7516 standaard. Deze standaard zorgt ervoor dat verschillende partijen op een veilige manier per e-mail gegevens met elkaar kunnen uitwisselen.

9. Positie en rechten van betrokkenen

De gemeente Zoetermeer vindt het belangrijk dat inwoners en andere betrokkenen eenvoudig een vraag kunnen stellen over privacygerelateerde onderwerpen. Ook moet een betrokkene eenvoudig zijn rechten kunnen uitoefenen. Via de website maken we algemene informatie toegankelijk voor inwoners. Een betrokkene kan zowel digitaal als via telefoon of brief om meer informatie vragen. Waar dat nodig is, kan een inwoner een afspraak maken om vragen te bespreken.
Iedere betrokkene heeft recht om zijn eigen gegevens in te zien. Daarbij informeren we de betrokkene ook over het doel van de verwerking en hoe lang we gegevens bewaren. Als gegevens niet juist, onvolledig of niet relevant zijn, kan een betrokkene vragen de gegevens aan te passen of te verwijderen. Tenzij er sprake is van een wettelijke uitzondering, geven we gehoor aan dergelijke verzoeken. Voor de Wet politiegegevens gelden enkele aanvullende uitzonderingen op het recht op inzage dat een betrokkene heeft. We communiceren hierover duidelijk naar de inwoners.
Als iemand meent dat de gemeente onzorgvuldig met zijn gegevens omgaat, kan hierover een klacht worden ingediend. Mocht de klacht intern niet naar genoegen van de klager zijn afgehandeld, kan de klacht bij de Autoriteit Persoonsgegevens worden ingediend.

10. Politiegegevens

Naast persoonsgegevens die onder de AVG vallen, verwerkt de gemeente ook politiegegevens. Deze gegevens worden binnen de gemeente verwerkt door buitengewoon opsporingsambtenaren (boa's). Leerplichtambtenaren, sociaal rechercheurs en handhavers zijn medewerkers die ook boa zijn. Voor hen geldt dat persoonsgegevens die zij verwerken politiegegevens kunnen zijn.
Voor de verwerking van politiegegevens is een andere wet van toepassing: de Wet politiegegevens (de Wpg). Deze wet komt op veel punten overeen met de AVG, maar wijkt soms ook af. Zo stelt de Wpg andere eisen aan het delen van gegevens, moet onderscheid worden gemaakt tussen verschillende soorten betrokkenen en is bepaalde documentatie vereist.

Politiegegevens

Gegevens die worden verwerkt in het kader van opsporing van strafbare feiten. Hieronder valt onderzoek naar uitkeringsfraude en onderzoek naar naleving van de Leerplichtwet. Maar ook een aantal taken van de gemeentelijke handhavers, zoals optreden tegen wildplassen en onderzoek naar milieudelicten.

Profilering

*Wanneer aan de hand van persoonsgegevens bepaalde persoonlijke aspecten worden geëvalueerd om bepaalde zaken over een persoon te voorspellen, noemen we dit profilering. Profilering zonder menselijke tussenkomst (volledig geautomatiseerd) is slechts beperkt toegestaan in de AVG en Wpg. De gemeente Zoetermeer maakt **geen** gebruik van profilering zonder menselijke tussenkomst.*

In dit hoofdstuk gaan we in op de aanvullende eisen die gelden voor de verwerking van persoonsgegevens op grond van de Wpg.

10.1 Wpg kader

Het normenkader van de Wpg is grotendeels gelijkluidend 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 verschillende soorten 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 Besluit politiegegevens.
- Jaarlijks wordt een interne audit uitgevoerd op de verwerking van politiegegevens bij de gemeenten.
- Elke vier jaar wordt er door een externe auditor een audit gedaan op de verwerking van politiegegevens bij de gemeenten. De rapportage van deze audit wordt aan de Autoriteit Persoonsgegevens verstrekt.

10.2 Register van verwerkingen

Om te voldoen aan de AVG houdt de gemeente een verwerkingsregister bij. Deze verplichting geldt ook op grond van de Wpg. De Wpg stelt echter enkele aanvullende eisen aan het verwerkingsregister, deze zijn hieronder met een * aangeduid. Naast de gegevens die al in het verwerkingsregister zijn opgenomen, moet voor de Wpg ook in het verwerkingsregister worden aangegeven:

- Of er gebruikt wordt gemaakt van profilering;
- Een aanwijzing van de rechtsgrondslag van de verwerking, met inbegrip van doorgiften, waarvoor de politiegegevens bedoeld zijn. (*)
- De toekenning van de autorisaties. (*)

10.3 FG en bevoegd functionaris

De FG is tevens de toezichthouder ten aanzien van de verwerking van politiegegevens. Daarnaast is bevoegd functionaris aangewezen.

De bevoegd functionaris beslist over de zogeheten artikel 9 verwerkingen. Zo legt deze rol de doelen van de verwerking vast en bepaalt hij over het al dan verstrekken en ter inzage geven van politiegegevens. Binnen de gemeente Zoetermeer is de senior sociaal rechercheur aangewezen als bevoegd functionaris.

10.4 Het bewaren van politiegegevens

Politiegegevens worden niet langer bewaard dan noodzakelijk is, zoals vereist door de toepasselijke wet- en regelgeving, of voor de doeleinden waarvoor deze zijn verwerkt.
Politiegegevens moeten na verwijdering nog maximaal vijf jaar in een archief 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 vastgesteld, zodat geborgd wordt dat deze politiegegevens niet langer worden bewaard dan noodzakelijk is, zoals vereist door de toepasselijke wet- en regelgeving, of voor de doeleinden waarvoor deze zijn verwerkt.

Artikel 8, 9 en 13 informatie

Persoonsgegevens die worden verwerkt op grond van artikel 8, 9 of 13 van de Wet politiegegevens.
Artikel 8 gaat over gegevens die worden gebruikt bij de uitvoering van de dagelijkse politietaak.
Artikel 9 betreft zogenoemde 'gerichte verwerkingen' en gaat over gegevens die worden verwerkt in het kader van een onderzoek waarbij bijzondere opsporingsbevoegdheden worden ingezet.
Artikel 13 gaat over de verdere verwerking van gegevens die onder artikel 8 of 9 zijn verzameld. Dit komt binnen de gemeente niet voor.

10.5 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 kunnen worden gedeeld met iedereen die de gegevens nodig heeft voor de uitoefening van zijn taak. Het ter beschikking stellen gebeurt altijd alleen maar aan andere boa's, ofwel: binnen het Wpg domein. Bij dit 'need to know'-principe

dient altijd afgewogen te worden of het delen noodzakelijk, proportioneel en passend is.

Bij het verstrekken van politiegegevens gaat het om het delen van gegevens met personen die geen boa zijn: verstrekking 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 Besluit politiegegevens zijn genoemd.

Geborgd moet ook zijn dat wanneer gegevens verstrekt worden, er wordt voldaan aan de documentatieplicht. Ook moet worden geborgd 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.

10.6 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.

11. Bereikbaarheid

Telefoon : **14 079**
Webformulier website : **www.zoetermeer.nl/privacy**
E-mailadres : **privacy@zoetermeer.nl**