Gemeente Amstelveen

GEMEENTEBLAD

Officiële uitgave van de gemeente Amstelveen

Nr. 100362

17 april

2020

Besluit van burgemeester en wethouders van de gemeente Amstelveen tot vaststelling van het Privacybeleid

Zaaknummer: Z20-024757

Burgemeester en wethouders van de gemeente Amstelveen;
gelezen het advies van afdeling Juridische Zaken, team Privacy van eind februari 2020;
gelet op de Algemene verordening gegevensbescherming;
besluiten vast te stellen het:
Privacybeleid

Aanleiding

Digitalisering en privacy, inmiddels kunnen we geen krant of digitale nieuwsbron meer raadplegen zonder deze begrippen tegen te komen. We zitten midden in de digitale revolutie. Deze revolutie heeft ingrijpende gevolgen voor onze maatschappij. Technologische ontwikkelingen zorgen voor nieuwe kansen, bijvoorbeeld in de zorg, veiligheid en in het openbaar vervoer. Maar naast kansen, brengen de ontwikkelingen ook uitdagingen met zich mee. Inwoners hebben andere verwachtingen van onze dienstverlening en de wijze waarop we met hen communiceren. Hierdoor worden er hogere eisen aan onze organisatie gesteld op het gebied van het gebruik, de opslag en uitwisseling van (persoons)gegevens.

Snelheid, Bereikbaarheid en Samenhang

De AA-organisatie (te weten gemeente Amstelveen en Aalsmeer) bevindt zich in een snel veranderende omgeving. Gemeenten krijgen nieuwe taken, meer en andere samenwerkingspartners, de digitalisering zet zich voort en de rol van de gemeente in de lokale samenleving is in beweging. De AA-organisatie ziet dat de verwachtingen bij inwoners, ondernemers en andere betrokkenen, in de kern, op drie fronten aan het schuiven zijn en wil daarom de dienstverlening Sneller, meer Bereikbaar en in Samenhang aanbieden. Wij doen er alles aan om in deze behoefte te voorzien met het grootste respect voor de naleving van de Algemene Verordening Gegevensbescherming (hierna: AVG). [1]

Snelheid: De behoefte van de betrokkene om wanneer het hem schikt snel zaken met de gemeente te kunnen regelen. De factor tijd brengt met zich mee dat men steeds meer gewend is om snel bediend te worden. Deze snelheid mag u ook van ons verwachten binnen de taken waarin dat mogelijk is.

Bereikbaarheid: De tweede ontwikkeling gaat over de manier waarop u bij ons terecht kunt. Het 24/7 kunnen indienen van aanvragen via webformulieren is hiervan een voorbeeld. Van het aanvragen van een paspoort of vergunning tot het melden van een kapotte lantaarnpaal. De AA-organisatie blijft werken aan een veiliger, toegankelijker en uitgebreidere digitale dienstverlening.

Samenhang: De maatschappij wordt steeds complexer en ons werk dus ook. Het komt steeds vaker voor dat een opgave, een dossier of een vraag het werkterrein van meerdere afdelingen raakt. Betrokkenen verwachten van ons onveranderd (en misschien wel steeds meer) dat ze samenhang zien in het antwoord waarmee we komen.

Digitale ambitie

Om deze veranderende verwachtingen voor alle betrokkenen waar te maken heeft de AA-organisatie een digitale ambitie. Deze ambitie is gegoten in het project digitale transformatie welke voor de periode 2019 – 2022 is opgesteld. De digitale ambitie ziet toe op een verbeterde dienstverlening, het zo efficiënt mogelijk werken en het voldoen aan wet- en regelgeving. Zo ook aan de AVG. Er worden hierdoor ook hogere eisen aan onze organisatie gesteld op het gebied van het gebruik, de opslag en uitwisseling (hierna: de verwerking) van de (persoons) gegevens van o.a. onze inwoners.

Iedereen moet erop kunnen vertrouwen dat de AA-organisatie privacy respecteert en zorgvuldig omgaat met persoonsgegevens. Dit privacybeleid laat zien op welke manier dit gebeurt. De bescherming van persoonsgegevens passen wij toe in onze dienstverlening en in de beleidskeuzes die wij mede maken conform dit privacybeleid. In onze afwegingen is wetgeving leidend, maar verliezen wij de menselijke maat en het belang van dienstverlening niet uit het oog.

"Uiteindelijk is het privacybeleid ook een hulpmiddel om mensen in bescherming te nemen, dus ter voorkoming dat een ander met jouw data doet wat hij wil. Dat is een belangrijk doel. Tegelijkertijd is veiligheid of zorg voor mensen die dat n odig hebben ook erg belangrijk"
Tjapko Poppens , burgemeester Amstelveen

1) In de hele Europese Unie geldt vanaf mei 2018 de Algemene Verordening Gegevensbescherming (AVG). De AVG vervangt de Wet bescherming persoonsgegevens. Door de komst van de AVG geldt er nog maar één privacywet in de hele Europese Unie in plaats van 28 verschillende nationale wetten.

Scope privacybeleid
In dit privacybeleid wordt op strategisch en tactisch niveau beschreven welke uitgangspunten gelden ten aanzien van privacy binnen de AA-organisatie. De naleving hiervan biedt, samen met het informatieveiligheidsbeleid, een adequaat beveiligingsniveau voor de persoonsgegevens van alle betrokkenen. De AA-organisatie geeft met dit beleid duidelijk richting aan hoe om moet worden gegaan met privacy en laat zien dat zij de privacy waarborgt, beschermt en handhaaft. Dit beleid is van toepassing op onze gehele organisatie en op alle processen, onderdelen, objecten en gegevensverzamelingen van de gemeente waarin persoonsgegevens worden verwerkt.

Hoofdstuk 1 Persoonsgegevens en de verwerking daarvan

De AVG is van toepassing op 'de geheel of gedeeltelijke geautomatiseerde verwerking, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen'[2] . Dit betekent kort gezegd dat bijna iedere verwerking van persoonsgegevens, zowel op de computer als op papier, onder de AVG valt. Hieronder vallen dus ook voor een dossier bestemde op papier gestelde gespreksnotities wanneer hierop persoonsgegevens zijn opgenomen. De woorden "(bijzondere) persoonsgegevens" en "verwerken" komt men veel tegen wanneer onderwerpen als privacy en de bescherming daarvan worden behandeld. Het is echter van belang om te weten wat met deze definities wordt bedoelt. Om die reden is hier in het kort aandacht aan besteed.

Paragraaf 1.1 Persoonsgegevens
Een persoonsgegeven is informatie die direct over iemand gaat of informatie die naar deze persoon te herleiden is.
Deze persoon wordt aangeduid als 'de betrokkene'. Dit zijn gegevens als de naam, het adres, e-mailadres en het Burgerservicenummer (BSN).

Paragraaf 1.2 Bijzondere persoonsgegevens
Sommige persoonsgegevens zijn extra gevoelig, omdat de verwerking ervan veel impact kan hebben op iemands leven. Bijzondere persoonsgegevens zijn gegevens die iets zeggen over iemands ras of etniciteit, politieke opvattingen, religie/levensbeschouwing, vakbondslidmaatschap, genetische gegevens, biometrische gegevens, gezondheid of seksualiteit.
Deze gegevens zijn extra beschermd door de wet. De AVG en de Uitvoeringswet AVG bepaalt in welke gevallen bijzondere of gevoelige gegevens verwerkt mogen worden. Een voorbeeld hiervan is de WMO 2015. Persoonsgegevens van kinderen zijn altijd gevoelig en krijgen daarom altijd extra bescherming. De gemeente gaat uiterst zorgvuldig om met bijzondere persoonsgegevens.

Paragraaf 1.3 Wat houdt verwerken in?
Tot de verwerking van persoonsgegevens behoren alle handelingen die gedaan worden met deze gegevens; bijvoorbeeld het verzamelen, vastleggen, ordenen, structureren, bijwerken, opvragen, raadplegen, verstrekken door middel van doorzending, verspreiden, combineren, afschermen, en vernietigen van gegevens.

Hoofdstuk 2 Uitgangspunten en grondslagen

Paragraaf 2.1 Uitgangspunten
De gemeente gaat op een veilige manier met persoonsgegevens om en respecteert de privacy van betrokkenen. De gemeente houdt zich hierbij aan de volgende uitgangspunten die uit de geldende wetgeving voortvloeien:

- Rechtmatigheid, behoorlijkheid en transparantie

Persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt. Deze beginselen brengen met zich mee dat de betrokkene zoveel mogelijk moeten worden geïnformeerd over de verwerking van zijn persoonsgegevens. Voor de informatie en communicatie over deze verwerking moet duidelijke en eenvoudige taal worden gebruikt. Ook moet op transparante wijze aan de betrokkene duidelijk gemaakt worden welke risico's, regels, waarborgen en rechten hij heeft en hoe hij deze rechten kan uitoefenen.

- Grondslag en doelbinding

De gemeente zorgt ervoor dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen worden verzameld en verwerkt. Persoonsgegevens worden alleen met een rechtmatige grondslag verwerkt.
Voorbeeld: Bij het aanvragen van een paspoort vraagt de mede werker van de afdeling Publiekszaken van de gemeente Amstelveen niet aan de inwoner wat zijn/haar inkomen of zijn hoogst genoten opleiding is. Deze gegevens zijn namelijk helemaal niet nodig om een paspoortaanvraag te kunnen behandelen.

- Dataminimalisatie

2) Artikel 2, eerste lid, AVG.

De gemeente verwerkt alleen de persoonsgegevens die noodzakelijk zijn voor het vooraf bepaalde doel. De gemeente streeft naar minimale gegevensverwerking. Waar mogelijk worden minder of geen persoonsgegevens verwerkt.

- Bewaartermijn

Persoonsgegevens worden niet langer bewaard dan nodig is of dan wettelijk is toegestaan. Het bewaren van persoonsgegevens kan nodig zijn om de gemeentelijke taken goed te kunnen uitoefenen of om wettelijke verplichtingen te kunnen naleven.
Voorbeeld: Een medewerker van de afdeling HRM van de gemeente Amstelveen vernietigt/verwijdert de sollicitatiebrief en CV van een sollicitant, vier weken nadat de sollicitatieprocedure is geëindigd. Hiermee handelt de gemeente in overeenstemming met 'het niet langer dan noodzakelijk bewaren van persoonsgegevens'.

- Subsidiariteit

Wanneer een doel ook op een andere, meer privacyvriendelijke, wijze kan worden bereikt dan heeft dat de voorkeur (subsidiariteit). De gedachte hierachter is dat bij de verwerking van persoonsgegevens de privacy van de betrokkene en derden zo min mogelijk geschaad mag worden.
Voorbeeld: Kan het doel dat de gemeente voor ogen heeft, name lijk het informeren van inwoners u it een bepaald straat over over lastgevende wegwerkzaamheden, worden bereikt zonder dat daar verwerking van persoonsgegevens voor nodig is? In dit geval is het niet nodig om de inwoners van de straat bij naam en toenaam te noemen. De brieven kunnen worden gericht "aan de inwoner van…". Op deze manier hoeven geen namen te worden verwerkt.

- Proportionaliteit

Het doel van de verwerking van de persoonsgegevens moet in verhouding staan tot de inbreuk op de privacy van de betrokkene (proportioneel). Dit betekent dat niet meer persoonsgegevens worden verwerkt dan nodig.

Paragraaf 2.2 Grondslagen

Eén van de eisen die de AVG stelt is dat persoonsgegevens rechtmatig worden verwerkt. Artikel 6 AVG geeft in dat kader de grondslagen voor verwerking. De AVG kent de volgende zes gronden op basis waarvan persoonsgegeven mogen worden verwerkt:

1. Toestemming van de betrokken persoon;
Voorbeeld: Een bet rokkene gaat akkoord met de ver werking van zijn e-mailadres voor het ontvangen van een nieuwsbrief.
2. De gegevensverwerking is noodzakelijk voor de uitvoering van een overeenkomst;
Voorbeeld: De gemeente verkoopt een kavel waar een particulier interesse in heeft. Voor het toezenden van aanvullende informatie mogen de persoonsgegevens van deze geïnteresseerde persoon gebruikt worden.
3. De gegevensverwerking is noodzakelijk voor het nakomen van een wettelijke verplichting;
Voorbeeld: Op grond van fiscale wetgeving is de gemeente verplicht om een kopie van het identiteitsbewijs van haar werknemers te bewaren.
4. De gegevensverwerking is noodzakelijk ter bescherming van de vitale belangen;
Voorbeeld: Wanneer er acuut gevaar dreigt maar iemand bewusteloos is of mentaal niet in staat is om toestemming te geven en hulp essentieel is voor de gezondheid.
5. De gegevensverwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of uitoefening van openbaar gezag;
Voorbeeld: De gemeente heeft vele wettelijke taken uit te voeren zoals het in behandeling nemen van vergunningaanvragen, handhaving parkeerbeleid en uitvoeren Participatiewet.
6. De gegevensverwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen. Hier komt het neer op het maken van een belangenafweging. Deze grondslag wordt soms door de gemeente gebruikt voor de uitvoering van andere dan haar wettelijke taken.
Voorbeeld: De gemeente wil haar (telefonische) dienstverlening verbeteren en analyseert hiervoor de telefoongesprekken. In dit geval wordt afgewogen of de verwerking noodzakelijk is voor de gerechtvaardigde belangen en of deze in verhouding staat tot de privacybelangen van betrokkenen (burgers, ondernemers en andere partijen die bellen met de gemeente).

Hoofdstuk 3 Governance

Paragraaf 3.1 Organisatie van privacy

De verantwoordelijkheid voor de zorgvuldige omgang met persoonsgegevens ligt bij de afdelingen die in het kader van hun werkzaamheden werken met persoonsgegevens. Dit betekent dat de lijn binnen de afdelingen zelf wordt aangesproken op het nakomen van de uit het privacybeleid voortvloeiende eisen. Privacy is immers niet een op zichzelf staand iets, maar onlosmakelijk verbonden met de gemeentelijke dienstverlening.
De gemeente heeft een 'Privacy governance-document' opgesteld waarin de onderstaande verantwoordelijkheids- en taakniveaus aangaande privacy zijn opgenomen.

Paragraaf 3.1.1 Proceseigenaar (lijnmanagement)
De verwerkingen van persoongegevens vinden operationeel voornamelijk plaats binnen de afdelingen (zoals Burgerzaken, Sociale Voorzieningen, Veiligheid en Handhaving) van de AA-organisatie. Om die reden staat de proceseigenaar dicht op het vuur. De proceseigenaar (verantwoordelijke) van de betreffende persoonsgegevens binnen de betreffende afdeling is verantwoordelijk voor een adequate bescherming van de persoonsgegevens. De proceseigenaar is het afdelingshoofd van de afdeling die de betreffende persoonsgegevens verwerkt. De proces-eigenaar legt verantwoording af aan de directie.
Paragraaf 3.1.2. College van burgemeester en wethouders en de burgemeester als verwerkingsverantwoordelijke
Het college van burgemeester en wethouders (hierna: college van B&W) en de burgemeester zijn de verantwoordelijke bestuursorganen die, ieder voor zover het hun taakuitoefening betreft, invulling geven aan de taken en verantwoordelijkheden die door de AVG zijn toebedeeld aan de verwerkingsverantwoordelijke.
De verwerkingsverantwoordelijken zijn verantwoordelijk voor:

- De naleving van de beginselen voor de verwerking van persoonsgegevens;
- De maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met deze verordening wordt uitgeoefend.

Het college heeft zijn verantwoordelijkheden gemandateerd aan de algemeen directeur.
Paragraaf 3.1.3 Gemeentesecretaris (Algemeen directeur)
De gemeentesecretaris is de algemeen directeur, de hoogste ambtenaar binnen de ambtelijke organisatie en de eerste adviseur van het college. Hij vormt dus de schakel tussen het bestuur en de medewerkers. Hij is verantwoordelijk voor de juiste en volledige implementatie van de wet- en regelgeving. Hij stelt samen met het managementteam het gewenste niveau van in-formatieveiligheid en privacy vast voor de gemeente. Dit krijgt vorm in het door het college vastgestelde informatieveiligheidsbeleid.
Paragraaf 3.1.4 Chief Information Officer, lid directie (CIO)
De CIO is eindverantwoordelijk voor de dagelijkse ICT-ondersteuning en de werking van alle ICT-onderdelen. Ook de strategische visie en kaderstelling op het terrein van (technologische) innovatie, informatievoorziening, ICT en privacy komen voor zijn rekening. Daarnaast voorziet hij in het goed aansluiten van de informatievoorziening op de doelstellingen van de organisatie.
Paragraaf 3.1.5 Chief Information Security Officer (CISO)
De CISO is op organisatieniveau verantwoordelijk voor het actueel houden van het informatie-veiligheids- en privacybeleid, het coördineren van de uitvoering van het beleid, het adviseren bij projecten, het beheersen van risico's, evenals het opstellen van rapportages.
De CISO rapporteert rechtstreeks aan de directie.
Paragraaf 3.1.6 Functionaris Gegevensbescherming (FG)
De AVG stelt het aanstellen van een Functionaris Gegevensbescherming (hierna: FG) verplicht voor overheidsinstanties en publieke organisaties. De FG is verantwoordelijk voor het intern onafhankelijk toezicht op de naleving van de wettelijke verplichtingen bij het verwerken van persoonsgegevens. Daarnaast adviseert de FG de organisatie over de juiste en zorgvuldige omgang met persoonsgegevens en onderhoudt hij contact met de Autoriteit Persoonsgegevens.
Paragraaf 3.1.7 Privacybeheerder
De privacybeheerder richt zich op de uitvoering en de naleving van de privacywetgeving. Hij adviseert de organisatie over alle onderdelen op het gebied van de (mogelijke) verwerking van persoonsgegevens. In het bijzonder ziet de privacybeheerder toe op het doorlopen van de Privacy Impact Assessments, het privacyvriendelijk ontwerpen van werkprocessen en het maken en beoordelen van afspraken met ketenpartners over gegevensdeling Daarnaast adviseert hij de organisatie hoe conform het privacybeleid gewerkt kan worden.
Paragraaf 3.1.8 Contactpersonen Informatieveiligheid & Privacy
De AA-organisatie voert uiteenlopende taken uit welke zijn verdeeld over verschillende afdelingen. Door iedere afdelingsmanager is er een contactpersoon (plus achtervang) aangewezen die zich bezig houdt met de uitvoering van het informatieveiligheids-en privacybeleid. Tot de taken van de contactpersoon behoren bijvoorbeeld:

- Actueel houden van het register van verwerkingsactiviteiten met alle verwerkingen die binnen de afdeling zijn geïnventariseerd;
- Het creëren van bewustwording binnen de afdeling;
- Betrokkenen de mogelijkheid bieden om hun rechten uit te oefenen;
- Onderhouden en beheren van verwerkersovereenkomsten.

Het privacyteam en de contactpersonen komen regelmatig samen om actuele vraagstukken op het gebied van informatieveiligheid en privacy te bespreken. Tijdens deze vergaderingen vindt er uitwisseling van verschillende casussen plaats. Dit brengt met zich mee dat snel op de actuele thema's kan worden ingespeeld en zo oplossingen kunnen worden bedacht voor dilemma's die zich kunnen aandienen.

Hoofdstuk 4 Informatieveiligheid als randvoorwaarde

In het gemeentebrede Informatieveiligheidsbeleid wordt op strategisch en tactisch niveau beschreven welke uitgangspunten gelden ten aanzien van de informatieveiligheid van de AA-organisatie. Informatieveiligheid en de bescherming van persoonsgegevens zijn onlosmakelijk met elkaar verbonden. Informatieveiligheid is een randvoorwaarde voor de borging van privacy bij de verwerking van persoonsgegevens. In het vastgestelde Informatieveiligheidsbeleid van de AA-organisatie zijn maatregelen genoemd om (persoons)gegevens te beschermen.
Deze maatregelen dienen om misbruik, verlies, onbevoegde toegang en andere ongewenste handelingen met (persoons)gegevens tegen te gaan. Denk hierbij onder andere aan het inregelen van autorisaties, het hebben van een betrouwbare back-up en een goede firewall om beschermd te zijn tegen hackers.
Het informatieveiligheidsbeleid is gebaseerd op de geldende gemeentelijke beveiligingsnormen zoals vastgelegd in de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG en met ingang van 1-1-2020 BIO) en voldoet aan de laatste standaarden. De naleving van dit beleid levert samen met de technische beveiligingsmaatregelen en de procedures een adequaat niveau van beveiliging voor de organisatie op. Dit maakt dat de kwaliteitskenmerken van informatie, te weten: de beschikbaarheid, de integriteit, de vertrouwelijkheid en de controleerbaarheid van de informatie binnen alle domeinen van de organisatie zijn gewaarborgd.

Hoofdstuk 5 Instrumenten

Het garanderen van privacybescherming en het houden van een hoog niveau van informatieveiligheid is een continu doorlopend proces. De in dit hoofdstuk besproken instrumenten zetten wij hiervoor in.

Paragraaf 5.1 Bewustwording

De AA-organisatie ziet in dat haar medewerkers de belangrijkste schakel zijn in het ten uitvoer brengen van haar ambities. Bewustzijn op het gebied van privacy en informatieveiligheid is dan ook essentieel voor het verwezenlijken van de ambities. Medewerkers moeten inzicht hebben in wat de impact van de AVG is op de verwerking van persoonsgegevens, processen en beleid. De AA-organisatie investeert daarom in persoonlijke privacytrainingen voor haar medewerkers,. Dit begint al in de eerste werkweek waarin nieuwe medewerkers tijdens de ‘onboarding’ een inleiding privacy en informatieveiligheid krijgen. Kort daaropvolgend wordt een uitgebreidere workshop over dit onderwerp aangeboden. Ook andere vormen van voorlichting vinden continu plaats.
Bewustwording wordt daarnaast gerealiseerd door middel van het jaarlijks organiseren van verschillende evenementen en trainingen. Wekelijks is er een laagdrempelig inloopspreekuur, waar iedereen binnen de organisatie terecht kan met vragen die gerelateerd zijn aan privacy- en in-formatieveiligheid. Verder wordt er zorg gedragen voor het actueel houden van beleid en procedures.

Paragraaf 5.2 Register van verwerkingen

De AA-organisatie wil betrokkenen inzicht geven in de wijze waarop hun persoonsgegevens worden verwerkt en beheerd binnen de organisatie.
De gemeente Amstelveen en Aalsmeer hebben daarom een openbaar register waarin alle verwerkingen van persoonsgegevens staan waarvoor de betreffende gemeente verantwoordelijk is. In het register zijn minimaal de volgende gegevens opgenomen:

1. De naam en contactgegevens van de verwerkingsverantwoordelijke en (indien van toepassing) de gezamenlijke verwerkingsverantwoordelijken;
2. Het doel of de doelen van de verwerking;
3. Een beschrijving van de soort persoonsgegevens en de categorieën van betrokkenen;
4. Een beschrijving van de ontvangers van de persoonsgegevens;
5. Een beschrijving van (indien van toepassing) het delen van persoonsgegevens aan een derde land of internationale organisatie;
6. De bewaartermijn van de gegevens;
7. Een algemene beschrijving van de beveiligingsmaatregelen.

Paragraaf 5.3 Procedure datalekken

Indien zich een veiligheidsincident voordoet, handelt de AA-organisatie in overeenstemming met de vastgestelde werkwijze in de Procedure: melden en afhandelen van veiligheidsincidenten. Deze procedure bevat een vastgesteld proces van de te nemen stappen om de (kans op) eventuele schade bij een datalek te beperken en de getroffen betrokkenen te beschermen en te informeren.
Er is sprake van een datalek wanneer persoonsgegevens zijn vernietigd of verloren, gewijzigd, verstrekt of toegankelijk gemaakt op een manier die in strijd is met de AVG. Indien er sprake is van een datalek, dient de AA-organisatie, als verwerkingsverantwoordelijke, dit in voorkomende gevallen zo spoedig mogelijk te melden bij de toezichthouder – de Autoriteit Persoonsgegevens - zo mogelijk binnen 72 uur. Wanneer er een grote kans bestaat dat het datalek negatieve gevolgen heeft voor betrokkenen, moeten deze ook worden gewaarschuwd.
De AA-organisatie houdt een register van veiligheidsincidenten bij waarin is terug te zien waar het incident betrekking op heeft gehad, of sprake was van een datalek, welke beheersmaatregelen zijn getroffen

en of de Autoriteit Persoonsgegevens en/of betrokkene(n) op de hoogte zijn gesteld. Het register wordt jaarlijks geëvalueerd met als doel om met de verworven inzichten beheersmaatregelen te treffen die de kans op veiligheidsincidenten verkleinen.

Paragraaf 5.4 Risicobeheersing

De AA-organisatie neemt verschillende maatregelen om de risico's bij de verwerking van persoonsgegevens in kaart te brengen en zo veel mogelijk te verminderen.

Data Protection Impact Assessment (DPIA)

Privacy begint aan de voorkant. Voorafgaand aan de verwerking van persoonsgegevens, en soms bij bestaande verwerkingen, voert de AA-organisatie een risico-inventarisatie uit, ook wel een PIA genoemd. Op basis van de PIA wordt inzicht verworven in de verwerking van persoonsgegevens en in welke mate dit noodzakelijk en veilig is. Vervolgens neemt de AA-organisatie maatregelen om de risico's zo veel mogelijk weg te nemen of te beperken. Pas nadat de PIA is uitgevoerd en de maatregelen zijn getroffen die nodig zijn om de risico's weg te nemen of te beperken, verwerkt de AA-organisatie de persoonsgegevens.

Privacy door ontwerp

Privacy door ontwerp houdt in dat er bij de ontwikkeling van nieuwe processen, diensten en producten al aan de ontwerptafel wordt nagedacht over de bescherming van de persoonsgegevens.
Door het borgen van de privacyaspecten aan het begin van het inkoop-, ontwikkel- en inrichtingsproces wordt ervoor gezorgd dat risico's zo veel mogelijk worden beperkt. Onder privacy door ontwerpmaatregelen wordt onder meer het afsluiten van verwerkersovereenkomsten, toegangsbeveiliging, encryptie, verwijderen van persoonsgegevens, dataminimalisatie en het houden van een PIA verstaan.

Privacy door standaardinstellingen

Privacy door standaardinstellingen wordt vaak in verband gebracht met Privacy door ontwerp. Hiervan is sprake als de standaardinstellingen van een programma, app, website, dienst of apparaat zodanig zijn ingesteld dat maximale privacy wordt nagestreefd. Bijvoorbeeld door een app niet de locatie van gebruikers te laten registreren als dat niet nodig is.

Verwerkersovereenkomsten/privacyconvenanten

De AA-organisatie verstrekt persoonsgegevens uitsluitend aan andere organisaties indien dat noodzakelijk is voor de uitvoering van onze dienstverlening of om te voldoen aan een wettelijke verplichting. Met deze organisaties maken wij concrete afspraken over de beveiliging van die persoonsgegevens, de afhandeling van datalekken en de rechten van betrokkenen.
Wanneer de gemeente een partij inschakelt om ten behoeve van de gemeente persoonsgegevens te verwerken en het verwerken van de persoonsgegevens de primaire taak is van deze partij, kan deze partij worden beschouwd als verwerker. Hier kan bijvoorbeeld worden gedacht aan een leverancier van software of een drukkerij. De gemeente schakelt enkel verwerkers in die afdoende garanties bieden met betrekking tot het toepassen van passende technische, procesmatige, communicatieve en organisatorische maatregelen.
De afspraken omtrent de verwerking door de verwerker worden schriftelijk vastgelegd in een verwerkersovereenkomst en worden voordat de dienstverlening aanvangt en daarna periodiek of steekproefsgewijs getoetst. Een verwerker heeft geen zeggenschap over de wijze van verwerken, en werkt strikt onder instructies en in opdracht van de verwerkingsverantwoordelijke. Een verwerker neemt geen beslissingen over het gebruik van de gegevens, verstrekking aan derden en andere ontvangers, de duur van de opslag van de gegevens etc.
Verder kan het voorkomen dat de AA-organisatie een andere partij inschakelt, die geen verwerker is, maar waarmee wel persoonsgegevens worden uitgewisseld. Ook dan maakt de gemeente passende afspraken. In dat geval zal de AA-organisatie een privacy-convenant afsluiten waarin de verantwoordelijkheden worden vastgelegd. Hierbij kan bijvoorbeeld gedacht worden aan zorgaanbieders en de politie.
De AA-organisatie controleert periodiek de naleving van deze afspraken. Op deze manier wordt de veilige verwerking van de persoonsgegevens zo goed mogelijk geborgd en behoudt de gemeente de regie bij contracten met deze derden.

Hoofdstuk 6 Verwerkingen door middel van camera's, Big data en tracking

Ook het opnemen van camerabeelden staat gelijk aan het verwerken van persoonsgegevens, de persoon zichtbaar op camerabeeld is immers te herleiden op grond van zijn voorkomen. Verwerking van persoonsgegevens kan ook van toepassing wanneer grote hoeveelheden data worden gebruikt om analyses op los te laten, in het bijzonder wanneer het gaat om data die tot een persoon terug te leiden is. Ten aanzien van het gebruik van tracking technologieën zoals cookies of wifi-tracking is terughoudendheid geboden. De AA-organisatie is van mening dat een bezoeker van haar website zich onbespied mag wanen.

Paragraaf 6.1 Inzet van camera's

Binnen de AA-organisatie 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 en in het kader van de openbare orde. De gemeente maakt gebruik van cameratoezicht op openbare plaatsen. Persoonsgegevens die in dat kader verwerkt worden vallen onder

de Wet politiegegevens, ze worden namelijk verwerkt met als doel het handhaven van de openbare orde. De AVG is niet van toepassing op politiegegevens.
Verder gebruikt de gemeente camera's in bijvoorbeeld de publiekshal van het stadskantoor, af-valbrengstation Legmeer en de gemeentewerf ter beveiliging van hen die zich daar bevinden. De camerabeelden worden slechts ter beveiligingsdoeleinden gebruikt en binnen 28 dagen vernietigd.

Paragraaf 6.2 Big data en tracking

Gegevens in big data en tracking mogen alleen worden verzameld, opgeslagen en gedeeld, als ze niet herleidbaar zijn tot een persoon en worden alleen verzameld voor onderzoek dat door of namens de AA-organisatie wordt uitgevoerd;
Voor big data en tracking wordt uitsluitend gebruik gemaakt van brongegevens die door daartoe geautoriseerde personen zijn verzameld;
Er worden geen tracking links in door of namens de AA-organisatie verzonden mails verwerkt. Evenmin worden er tracking cookies gebruikt op de websites amstelveen.nl en aalsmeer.nl;
Brongegevens die gebruikt worden voor big datatoepassingen worden omgezet tot een dataset die geen persoonsgegevens bevat en dus geanonimiseerd is;
Indien anonimiseren niet mogelijk is, wordt vooraf toestemming aangevraagd aan de FG.
Deze zal de aanvraag beoordelen in het kader van de wet- en doelmatigheid. Alleen bij een goedgekeurde aanvraag mogen de gegevens gepseudonimiseerd in plaats van geanonimiseerd worden;
Onderzoek aan de hand van de dataset mag niet door dezelfde medewerkers worden uitgevoerd die de gegevens hebben verzameld;
Voorafgaand aan het samenstellen van datasets in het kader van business intelligence vindt er, indien hierbij een relatie is met persoonskenmerken, overeenkomstig de "procedure verzoek informatie rondom personen", een toetsing plaats ten aanzien van de borging van de privacy-rechten. Gegevens worden enkel geaggregeerd aangeleverd met een minimum resultaatregels zodat de gegevens niet tot een persoon herleidbaar zijn.

Hoofdstuk 7 Rechten van betrokkenen

Met de invoering van de AVG krijgen betrokkenen meer mogelijkheden om voor zichzelf op te komen bij de verwerking van hun gegevens. Hun rechten en plichten worden namelijk versterkt en uitgebreid in de artikelen 13 t/m 22 AVG. De betrokkene kan zich voor het inroepen van zijn rechten wenden tot de verwerkingsverantwoordelijke, in de meeste gevallen het college van burgemeester en wethouders. De rechten en plichten gelden voor een ieder waarvan persoonsgegevens worden verwerkt door de gemeente. Het gaat dus niet alleen om de rechten en plichten van de inwoners van Amstelveen en Aalsmeer. De AVG spreekt daarom over de rechten van betrokkenen. Hieronder worden de verschillende rechten uiteengezet.

Paragraaf 7.1 Rechten en plichten

Informatieplicht

De gemeente informeert betrokkenen over welke persoonsgegevens waar verwerkt worden. Voor de gemeente is het heel belangrijk dat betrokkenen erop kunnen vertrouwen dat de gemeente hun persoonsgegevens zorgvuldig verwerkt. Dat vertrouwen wordt gecreëerd door inzichtelijk te maken op welke wijze persoonsgegevens worden verwerkt en beheerd.
Voorbeeld: Op verschillende manieren informeert de gemeente de be trokkene over voor welke doeleinde de persoonsgegevens worden verzamelt zoals via het register van verwerkingen, het privacystatement op de gemeentelijke website en de aanvraagformulieren in het sociaal d o mein.

Recht tot inzage en correctie van persoonsgegevens

Betrokkenen hebben de mogelijkheid om te controleren of en op welke manier hun gegevens worden verzameld en verwerkt. Dit met inachtneming van de beperkingen zoals neergelegd in wet- en regelgeving. Iedere betrokkene kan daarom de gemeente verzoeken om zijn persoonsgegevens in te zien, te wijzigen, te verbeteren, aan te vullen, te verwijderen of af te schermen. Dit verzoek kan digitaal via het webportaal, via het algemene mailadres (gemeen-te@amstelveen.nl) mail of schriftelijk (postbus 4, 1180 BA Amstelveen) worden ingediend. De gemeente deelt, na vaststelling van de identiteit, binnen een maand na ontvangst van het verzoek schriftelijk aan de betrokkene mede hoe het verzoek wordt afgehandeld.

Recht van bezwaar

De gemeente voert publiekrechtelijke taken uit, dit is doorgaans de grondslag voor gegevensverwerking. Ondanks dat heeft iedere betrokkene het recht om, vanwege bijzondere persoonlijke omstandigheden, te vragen zijn of haar persoonsgegevens niet meer te gebruiken. Dit heet het recht van bezwaar. De gemeente zal bij dit verzoek beoordelen of de gegevensverwerking gerechtvaardigd is of dat de bijzondere omstandigheden van de betrokkene dusdanig zijn, dat het verzoek moet worden ingewilligd.

Recht op menselijke blik bij besluiten

Wanneer er een geautomatiseerde verwerking van persoonsgegevens plaatsvindt waarbij aan de hand van persoonsgegevens naar bepaalde persoonlijke aspecten (zoals de financiële situatie, interesses en gedrag) van een persoon wordt gekeken om deze persoon te categoriseren en te analyseren, is er sprake van profilering. Het nemen van geautomatiseerde besluiten op basis van profilering is niet toe-

gestaan, tenzij er een (expliciete) wettelijke basis voor bestaat. Bij dit recht kan gedacht worden aan de verwerking van persoonsgegevens via internet zonder menselijke tussenkomst.

Uitoefening van rechten

Om gebruik te kunnen maken van de bovenstaande rechten kunnen de betrokkenen een verzoek indienen. Dit verzoek kan zowel schriftelijk als via de elektronische weg ingediend worden. Er zal, waar mogelijk, gebruik worden gemaakt van een formulier dat de betrokkene helpt om zijn recht(en) uit te oefenen. Deze formulieren zullen op de website van de gemeente beschikbaar komen.

Paragraaf 7.2 Besluitvorming verzoeken

Indien een betrokkene een recht gaat uitoefenen zal dat vooral zijn door middel van een gericht verzoek aan de gemeente. De beslissing van de gemeente op dit verzoek valt onder de Algemene wet bestuursrecht (hierna: Awb). Dat betekent dat de beslissing op het verzoek een besluit is in de zin van de Awb waartegen bezwaar en beroep kan worden ingediend. De wettelijke beslistermijn is één maand en bij een complex verzoek kan deze termijn verlengd worden met twee maanden.

Paragraaf 7.3 Klachtrecht

Indien een betrokkene van mening is dat de gemeente privacyregels ten opzichte van hem overtreedt, kan betrokkene hierover een schriftelijke klacht indienen via de centrale klachtenregeling bij de AA-organisatie. In de afhandeling van de klacht vervult de FG een centrale rol.
De betrokkene kan zijn of haar klacht of een verzoek tot bemiddeling ook indienen bij de Autoriteit Persoonsgegevens.

Hoofdstuk 8 Inwerkingtreding, evaluatie en herziening

De AVG verplicht de AA-organisatie om steeds te kijken of het beleid nog voldoet en of het eventueel aangepast moet worden. Technologische en maatschappelijke ontwikkelingen volgen elkaar snel op. Dit kan reden zijn om het beleid aan te passen. Omdat daarnaast nog niet geheel duidelijk is hoe de toezichthouder (de Autoriteit Persoonsgegevens) zijn taak zal opvatten, is het noodzakelijk om het privacybeleid periodiek te evalueren. Er is immers sprake van nieuwe wetgeving die volop in beweging is en waar door de rechtspraak en de toezichthouder nog nader invulling aan zal worden gegeven.
Dit privacybeleid treedt in werking na vaststelling door het college van B&W. Het beleid wordt iedere drie jaar geëvalueerd en indien nodig herzien. Indien zich eerder grote wijzigingen voordoen vindt actualisatie eerder plaats. Aanpassingen van dit beleid worden aangekondigd via overheid.nl, Amstelveen.nl en Aalsmeer.nl.

Aldus vastgesteld in de vergadering van 31 maart 2020.
De secretaris,
Bert Winthorst
De voorzitter,
Tjapko Poppens

Bijlage 1 Wettelijke kaders voor de omgang met persoonsgegevens

De gemeente is verantwoordelijk voor het opstellen, uitvoeren en handhaven van het beleid. Hiervoor gelden onder andere de volgende (wettelijke) kaders:

Wettelijke kaders

- De Algemene verordening gegevensbescherming;
- De Uitvoeringswet Algemene verordening gegevensbescherming;
- Artikel 8 Europees Verdrag voor de Rechten van de Mens;
- Artikel 10 t/m 13 Nederlandse Grondwet;
- Artikel 272 Wetboek van Strafrecht;
- Wet maatschappelijke ondersteuning 2015;
- Jeugdwet;
- Participatiewet;
- Archiefwet.

Interne kaders

- Privacybeleid;
- Het privacyverklaring op de site van de gemeente Amstelveen en de gemeente Aalsmeer;
- Informatieveiligheidsbeleid;Code voor Informatiebeveiliging (NEN/ISO 27002);
- Baseline Informatiebeveliging Gemeenten (BIG) / Overheid (BIO).

De kaders vormen het uitgangspunt voor nader uit te werken gedragsrichtlijnen en protocollen of om deze te actualiseren. Deze gedragsrichtlijnen en protocollen geven richting aan de uitvoering in de dagelijkse praktijk. Het gaat in ieder geval om de volgende protocollen (niet limitatief):

- GIR Privacy-protocol registratie agressie- en geweldsincidenten
- Monitor top 1000
- Interne Privacyverklaring ten aanzien van verwerking persoonsgegevens van medewerkers en sollicitanten (wordt binnenkort opgesteld),
- E-mail-protocol,
- Privacyreglement Stichting Wijkteams,
- Verordening gegevensverstrekking basisregistratie personen Amstelveen,
- Procedures en richtlijnen WBP GBA (verstrekkingenreglement verordening/beleidsregels),
- Protocol: Afhandeling Datalekken,
- Protocol gebruik thuiswerkplek / thuiscomputer (wordt binnenkort opgesteld),

Naast bovengenoemde kunnen in de toekomst nog meer richtlijnen en protocollen worden opgesteld. Hiermee kunnen we snel en flexibel inspelen op nieuwe ontwikkelingen.