Strategisch beleidskader Privacy

Gemeente Veenendaal 2020

Inhoudsopgave

1 Kernpunten ... 3
1.1 Inleiding ... 3
1.2 Leeswijzer ... 3
1.3 Visie ... 3
1.4 Doel ... 4
1.5 Wettelijk kader ... 4
1.6 Uitgangspunten ... 4
1.7 Risico's ... 5
1.8 Scope ... 5

2 Privacybeleid ... 7
2.1 Begrippen ... 7
2.2 Eisen aan gegevensverwerking ... 7
2.3 Gegevensuitwisseling bij samenwerking ... 10
2.4 Risicogestuurde aanpak ... 11

3 Verantwoordelijkheid voor privacy ... 13
3.1 Verantwoordelijkheid voor verwerking ... 13
3.2 Bestuurlijke verantwoordelijkheid ... 13
3.3 Verantwoordelijkheid gemeentelijke organisatie ... 13

4 Toezicht ... 15
4.1 Controle op werking en naleving ... 15
4.2 Functionaris voor gegevensbescherming ... 15

5 Privacy voor betrokkenen ... 16
5.1 Rechten ... 16
5.2 Vragen en klachten ... 16

6 Beleidsevaluatie ... 17

1 Kernpunten

1.1 Inleiding

In deze beleidsnota geeft de gemeente Veenendaal de kaders aan voor de verwerking van persoonsgegevens die binnen de verantwoordelijkheid van de gemeente valt. Dit beleidskader biedt een overkoepelend raamwerk waarin de visie van de gemeente Veenendaal ten aanzien van privacy naar voren komt.

De nota beschrijft het privacybeleid vanaf 2020 en vervangt de in 2016 vastgestelde ‘Bestuurlijke nota privacy 2015’. Deze nota is kaderstellend en richtinggevend en wordt waar nodig aangevuld met onderwerpspecifieke beleidsdocumenten en vastgelegde instructies op operationeel niveau. Het privacybeleid geeft op bestuurlijk en strategisch niveau duidelijkheid en daarmee sturing aan de inrichting van privacy en de keuzes die daarbij gemaakt moeten worden. Dit is van belang om te waarborgen dat de verwerking van persoonsgegevens op een rechtmatige wijze plaatsvindt conform de geldende wet- en regelgeving.

1.2 Leeswijzer

Hoofdstuk 1 benoemt de kernpunten van het privacybeleid, waaronder visie, doel en uitgangspunten van het beleid. Hoofdstuk 2 beschrijft aan welke voorwaarden processen en systemen moeten voldoen en hoe dit beleid wordt toegepast. In hoofdstuk 3 is beschreven wat de verantwoordelijkheid voor privacy inhoudt. Dit biedt kaders voor het handelen van de gemeente. Hoofdstuk 4 besteedt aandacht aan het toezicht op de naleving van privacyregels en hoe controle op de uitvoering plaatsvindt. In hoofdstuk 5 gaat in op de positie van de betrokkenen van wie persoonsgegevens worden verwerkt. Hoofdstuk 6 benoemt de beleidsevaluatie.

1.3 Visie

Het raadsprogramma 2018-2022, ‘Iedereen doet mee’, verwoordt de visie en ambitie op het gebied van privacy als volgt:

> *“Wij zijn ons goed bewust van de geldende wet- en regelgeving rondom privacy. Uitgangspunt is dat wij voldoen aan die vereisten en wel op een zodanige manier dat een en ander werkbaar blijft en niet onnodig belemmert. We gaan op zoek naar een goede balans tussen efficiënte uitvoering en het respecteren van de privacy.”*

Het privacybeleid wordt elke twee jaar geëvalueerd. Een eventuele wijziging van de visie in het raadsprogramma vanaf 2022 wordt in de evaluatie meegenomen.

1.4 Doel

Het doel van het privacybeleid is om te waarborgen dat de gemeente Veenendaal persoonsgegevens verwerkt op een rechtmatige en behoorlijke wijze en dit kan aantonen. De gemeente biedt goede privacybescherming aan onze burgers en medewerkers over wie persoonsgegevens worden verwerkt. De organisatie en processen worden gebruiksvriendelijk ingericht. Hiermee wordt de privacywetgeving nageleefd en invulling gegeven aan actuele privacyprincipes voortvloeiend uit geldende wetgeving en jurisprudentie.

1.5 Wettelijk kader

Vanaf 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. Dit is de privacywet die binnen Europa geldt en die het algemene kader vormt voor de verwerking van persoonsgegevens. Voor Nederland zijn enkele onderwerpen uitgewerkt in de Uitvoeringswet AVG (UAVG). Privacyvoorschriften zijn verder te vinden in (sector)specifieke wetgeving.

1.6 Uitgangspunten

Op grond van artikel 24 AVG moet privacybeleid passend zijn voor de verwerkingen die onder verantwoordelijkheid van de gemeente worden uitgevoerd en rekening houden met risico's voor de rechten en vrijheden van betrokkenen. Hiervoor zijn de beginselen uit artikel 5 AVG richtinggevend. Tevens sluit dit beleid aan bij het normenkader voor de overheid op het gebied van informatiebeveiliging: de Baseline Informatiebeveiliging Overheid (BIO). In het bijzonder wordt aangesloten bij de uitgangspunten voor de operationele borging van privacy binnen de organisatie. Dit is een doorlopend proces. Risicomanagement is een belangrijk onderdeel hierin.

Hieruit vloeien de volgende uitgangspunten voort, die in de volgende hoofdstukken uitgebreider aan bod komen:

1) Zorg voor privacy is een verantwoordelijkheid van bestuur en management. Zij sturen op privacy:
   a) De formele eindverantwoordelijkheid berust bij de afzonderlijke bestuursorganen van de gemeente. Het college van B&W, de burgemeester en de gemeenteraad stellen de uitgangspunten van het privacybeleid vast, ieder voor zover het de eigen bevoegdheid betreft.
   b) De verantwoordelijkheden in de organisatie volgen de lijnen van het mandaatbesluit van de gemeente Veenendaal.
2) Het borgen van privacy in de uitvoering van gemeentelijke processen vindt risicogestuurd plaats. De verantwoordelijken in de organisatie maken afwegingen ter naleving van privacyregels en op basis van een risico-inschatting.
3) Het college legt verantwoording af aan de gemeenteraad over het privacybeleid.
4) Er is voorzien in een team van professionals dat ondersteuning biedt in de toepassing van het privacybeleidskader.

5) De gemeente Veenendaal heeft een Adviseur privacy in dienst voor de borging van privacy in de organisatie en het toezien hierop. Er is een functionaris voor gegevensbescherming (FG) aangesteld als interne toezichthouder.
6) Er wordt voorzien in communicatie over het beleid en faciliteiten voor bewustwording en training, zodat iedere medewerker conform het privacybeleid kan handelen.
7) De gemeente Veenendaal beschikt over procedures voor privacy-incidentmanagement, zodat adequaat gehandeld kan worden in geval van datalekken.
8) De gemeente Veenendaal evalueert tweejaarlijks de doeltreffendheid en de doelmatigheid van dit beleidskader.

1.7 Risico's

Het niet naleven van de AVG, de Uitvoeringswet AVG en privacyvoorschriften in (sector)specifieke wetten kan verregaande (negatieve) consequenties voor de gemeente hebben. De Autoriteit Persoonsgegevens (AP) heeft als landelijke toezichthouder enkele bevoegdheden:

- Onderzoek naar mogelijke overtredingen;
- Handhavend optreden: bestuurlijke sanctie (inclusief betaling geldsom), last onder bestuursdwang);
- Boete opleggen: hoogte van de boete is afhankelijk van de overtreding en de ernst daarvan, de AP heeft boetebandbreedtes vastgesteld in beleidsregels[1]. De hoogte van de boete kan variëren van minimaal € 120.000,- tot maximaal € 1.000.000,- (de maximale boete voor niet naleving van de wet bij een datalek is bijvoorbeeld € 525.000,-).

Betrokkenen van wie de gemeente persoonsgegevens verwerkt hebben de mogelijkheid de gemeente aansprakelijk te stellen en schadevergoeding te vragen als er sprake is van handelen in strijd met de AVG en Uitvoeringswet AVG.

De gemeente kan reputatieschade oplopen en het vertrouwen van de burger in de gemeente kan verminderen, bijvoorbeeld als een datalek het nieuws haalt. Dit kan ertoe leiden dat de gemeente haar taken niet meer naar behoren kan uitvoeren en niet benodigde hulp, ondersteuning of diensten kan bieden, omdat burgers de gemeente onvoldoende als betrouwbare partner zien.

1.8 Scope

Het strategisch beleidskader is van toepassing op de gehele bedrijfsvoering van de gemeente Veenendaal, voor zover in bedrijfsprocessen gewerkt wordt met persoonsgegevens en de gemeente daar zeggenschap over heeft.

[1] Boetebeleidsregels Autoriteit Persoonsgegevens 2019 (Stcrt. 2019, nr. 14586)

Het beleidskader is de kapstok voor het privacybeleid van de gemeente Veenendaal waaraan aanvullende regelingen zijn opgehangen zoals protocollen, richtlijnen en reglementen.

Het privacybeleid van de gemeente Veenendaal omvat zowel bedrijfsprocessen als de onderliggende voorzieningen voor gegevensverwerking en gegevensopslag. Dit betreft zowel papieren als digitale gegevensverwerking.

Het privacybeleid is ook van toepassing op processen die de gemeente uitbesteedt of op een andere manier organiseert. Voorbeelden hiervan zijn respectievelijk de uitbesteding van gemeentelijke taken aan een externe organisatie en deelname in een rechtspersoon die voor de gemeente Veenendaal diensten verricht. Het privacybeleid is tevens van toepassing op de inkoop van producten of diensten, zoals de aanschaf van informatiesystemen.

Het privacybeleid is van toepassing op gegevensuitwisseling met derden, zoals met de Belastingdienst, de Raad voor de Kinderbescherming, de politie en zorgaanbieders en bij gegevensuitwisseling in het kader van deelname aan samenwerkingsverbanden.

Het privacybeleid omvat de gehele ‘data life cycle’: van het genereren of verzamelen van gegevens, het dagelijkse gebruik ervan en de gegevensopslag tot en met de archivering en vernietiging ervan.

Het privacybeleid is van toepassing op de verwerking van statistische en/of geanonimiseerde, dan wel gepseudonimiseerde gegevens, voor zover niet kan worden uitgesloten dat personen kunnen worden geïdentificeerd of geprofileerd.

Het privacybeleid is van toepassing op informatiebeveiligingsvraagstukken, voor zover het de beveiliging van persoonsgegevens betreft.

2 Privacybeleid

De gemeente Veenendaal is zich bewust van de maatschappelijke verantwoordelijkheid die gepaard gaat met de verwerking van persoonsgegevens. Om deze reden voert de gemeente Veenendaal proactief privacybeleid op basis van dit beleidskader en wordt de goede naleving van wet- en regelgeving op het gebied van privacybescherming bewaakt. De gemeente Veenendaal faciliteert de uitoefening van rechten van personen.

2.1 Begrippen

Allereerst volgt een korte beschrijving van de AVG-begrippen ‘persoonsgegevens’ en ‘verwerken’.

Persoonsgegevens en bijzondere categorieën gegevens
Persoonsgegevens zijn alle gegevens waarmee een natuurlijk persoon te identificeren is of geïdentificeerd kan worden. Voorbeelden zijn: naam en geboortedatum, adres, e-mailadres en bankrekeningnummer.

Bepaalde persoonsgegevens zijn privacygevoeliger, bijvoorbeeld gegevens over gezondheid, strafrecht (waaronder gegevens uit registers van politie en justitie), religie of etniciteit. Deze zogenaamde bijzondere gegevens mag de gemeente daarom alleen verwerken in de gevallen dat dit wettelijk is toegestaan. Het burgerservicenummer (BSN) is eveneens een extra gevoelig persoonsgegeven waaraan extra bescherming toekomt en dat een wettelijke basis moet hebben.

Verwerken van persoonsgegevens
‘Verwerken’ omvat alle handelingen met persoonsgegevens, waaronder verzamelen, opslaan, verstrekken en vernietigen van de gegevens. Verzamelen vindt vaak plaats bij een aanvraag of melding en soms ook doordat de gemeente navraag doet. De verzamelde gegevens worden opgeslagen in de gemeentelijke systemen en indien nodig voor de taakuitvoering ook verstrekt. Als de gegevens niet meer nodig zijn voor het doel waarvoor ze zijn verzameld, worden ze vernietigd.

2.2 Eisen aan gegevensverwerking

Verwerkingen van persoonsgegevens vinden plaats in overeenstemming met AVG-beginselen. Het gaat dan om eisen benoemd in artikel 5 AVG:

a) Rechtmatigheid en behoorlijkheid
b) Transparantie
c) Doelbinding
d) Minimaal noodzakelijke gegevensverwerking (incl. toepassing proportionaliteit/subsidiariteit)
e) Juistheid

f) Opslagbeperking en bewaartermijnen
g) Integriteit en vertrouwelijkheid (inclusief organisatorische en technische beveiligingsmaatregelen)

a. Rechtmatige en behoorlijke verwerking
Persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt. De verwerking van persoonsgegevens dient gebaseerd te zijn op een van de zes grondslagen als benoemd in artikel 6 AVG:

1. Toestemming van betrokkene
2. Overeenkomst met betrokkene
3. Nakomen wettelijke verplichting
4. Bescherming vitale belangen betrokkene
5. Uitoefening taken algemeen belang of uitoefening openbaar gezag
6. Gerechtvaardigd belang organisatie

Voor de gemeente Veenendaal is de grondslag in de meeste gevallen gelegen in de uitoefening van taken van algemeen belang of de uitoefening van openbaar gezag, alsmede het nakomen van een wettelijke plicht. In levensbedreigende situaties of situaties waarin de veiligheid van kinderen in gevaar is, kan de grondslag vitaal belang van toepassing zijn. In het geval er een overeenkomst met een betrokken persoon is, kan dat als grondslag dienen. De grondslag gerechtvaardigd belang van de organisatie kan niet van toepassing zijn als het gaat om uitoefening van taken van algemeen belang of openbaar gezag. Soms kan deze grondslag wel van toepassing zijn als bijvoorbeeld voldaan moet worden aan een gerechtelijke opdracht waarvoor verwerking van persoonsgegevens nodig is. De grondslag toestemming kan vrijwel nooit van toepassing zijn, omdat toestemming vereist dat een betrokkene in vrijheid deze toestemming kan geven. Echter, vanwege de afhankelijkheidsrelatie tussen burger en gemeente kan hier geen sprake van zijn, zoals aangegeven in de considerans van de AVG.

Toestemming als grondslag voor gegevensverwerkingen moet onderscheiden worden van toestemming voor het doorbreken van een geheimhoudingsplicht. In dit laatste geval kan toestemming wél een geldige grondslag zijn. Dit speelt bijvoorbeeld in het sociaal domein waar het in bepaalde situaties noodzakelijk kan zijn gegevens uit te wisselen met anderen. Vanwege de geheimhoudingsplichten in het sociaal domein kan deze gegevensuitwisseling enkel plaatsvinden als aan de betrokkene hiervoor toestemming gevraagd wordt.

b. Transparantie
Voor de betrokken burger moet duidelijk zijn wat er met de persoonsgegevens gebeurt. Het is van belang dat de burger geïnformeerd wordt over het doel van de verwerking van diens gegevens, welke gegevens nodig zijn en met wie gegevens noodzakelijkerwijze gedeeld gaan worden.

De informatieplicht richting de burger is in de procesinrichting van de gemeente Veenendaal en haar partners voorzien. Daarnaast worden betrokkenen geïnformeerd via gemeentelijke informatiekanalen, zoals de website van de gemeente. Burgers kunnen tevens een verzoek indienen ter uitoefening van hun privacyrechten, zoals een verzoek om inzage of een verzoek om correctie van gegevens.

In bepaalde wettelijke uitzonderingsgevallen kan deinformatieplicht achterwege blijven. Dit zal in individuele gevallen beoordeeld worden.

c. Doelbinding
De gemeente Veenendaal verzamelt persoonsgegevens alleen voor een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel en verstrekt deze gegevens alleen voor zover dat binnen het doel is toegestaan. Afwijkend gebruik voor ándere doelen is slechts mogelijk na afweging van de wettelijke criteria. Deze afweging gebeurt in de vorm van een ‘verenigbaarheidstoets’ conform artikel 6 lid 4 AVG.

d. Minimaal noodzakelijke gegevensverwerking
De gemeente Veenendaal verwerkt alleen die gegevens die strikt noodzakelijk om het doel waarvoor ze nodig zijn te bereiken. De gegevensverwerking moet toereikend, ter zake dienend en niet bovenmatig zijn. Gemeente Veenendaal hanteert daarbij de regel ‘need to know’ in plaats van ‘nice to know’.

Bij de beoordeling van de noodzaak van de gegevensverwerking spelen de beginselen van proportionaliteit en subsidiariteit een belangrijke rol. Het beginsel van proportionaliteit verlangt een redelijke verhouding tussen het te dienen belang van het gegevensgebruik en de inbreuk op de privacy van betrokkenen. De inbreuk mag niet onevenredig zijn in verhouding tot het te bereiken doel. Het beginsel van subsidiariteit houdt in dat gekozen moet worden voor een manier die voor de betrokkenen het minst inbreuk maakt op de privacy. Als het doel ook te bereiken is op een minder privacyschendende manier moet daarvoor gekozen worden.

e. Juistheid
Persoonsgegevens moeten altijd juist, volledig en actueel zijn. In alle processen vinden controles plaats om te verifiëren dat de juiste persoonsgegevens gebruikt worden. Dit kan mede voorkomen dat datalekken ontstaan.

f. Opslagbeperking en bewaartermijnen
De gemeente Veenendaal bewaart gegevens volgens de wettelijk geldende termijnen of anders altijd zo kort mogelijk en ‘vernietigt’ deze daarna. In diverse wetten zijn bewaartermijnen opgenomen. Voor persoonsgegevens in archiefwaardige bescheiden geldt een bewaartermijn die is vastgesteld in de ‘Selectielijst voor gemeenten en intergemeentelijke organen’, vastgesteld op grond van de Archiefwet. Als er geen regeling is die voorziet in een verplichte bewaartermijn, kan het college een besluit over de bewaartermijn nemen. Deze termijn zal zo kort mogelijk zijn.

g. Integriteit en vertrouwelijkheid
De gemeente Veenendaal neemt passende technische of organisatorische maatregelen zodat persoonsgegevens integer en vertrouwelijk worden verwerkt. Daarbij horen ook maatregelen ter beveiliging van de persoonsgegevens. Bij het nemen van maatregelen ter beveiliging van gegevens zijn de BIO en het informatiebeveiligingsbeleid van de gemeente Veenendaal richtinggevend.

2.3 Gegevensuitwisseling bij samenwerking

Het beleid van de gemeente Veenendaal richt zich in belangrijke mate op het samen met andere overheidsorganisaties en sociale partners aanpakken van sociale, maatschappelijke en veiligheidsvraagstukken. In de samenwerkingsverbanden die daardoor ontstaan komen ook casussen van individuele burgers aan de orde en zullen indien noodzakelijk hun persoonsgegevens worden gedeeld. Dit kan ook aan de orde zijn wanneer er binnen de organisatie samengewerkt wordt bij specifieke thema's, opgaven en programma's.

Bij de uitvoering moet rekening gehouden worden met de wettelijke privacyvoorschriften die van toepassing zijn op de gemeente zelf en op haar partners waarmee samengewerkt wordt. Deze privacyregels kan en wil de gemeente Veenendaal niet negeren, maar stelt haar wel voor dilemma's in de uitvoering van bepaalde werkzaamheden, zoals:

- bij de gegevensuitwisseling die nodig is in het kader van integrale dienstverlening die de gemeente nastreeft, bijvoorbeeld in het sociaal domein;
- bij de handhaving van vergunningen, ruimtelijke voorschriften en de openbare orde en veiligheid.

Als uitgangspunt van haar handelen bij dit soort dilemma's hanteert de gemeente de volgende werkwijze:

1. Allereerst zorgt de gemeente ervoor dat het verwerken van gegevens, waaronder de uitwisseling van gegevens bij externe of interne samenwerking, binnen de kaders van de verschillende wetten kan plaatsvinden.
2. Mochten de wetten niet in de uitwisseling van gegevens voorzien, dan valt de gemeente Veenendaal terug op de mogelijkheid van artikel 6 lid 4 AVG: het uitvoeren van een verenigbaarheidstoets. Bekeken wordt dan of gebruik van de gegevens mogelijk is voor ándere doelen dan de oorspronkelijke doelen waarvoor de gegevens verzameld zijn in de uitvoering van de taak. Gegevensuitwisseling met derden kan dan mogelijk worden.
3. Wanneer het gaat om verwerkingen die een hoog risico voor betrokkenen inhouden, wordt een data protection impact assessement (DPIA) uitgevoerd. Een DPIA maakt inzichtelijk welke maatregelen er nodig zijn om op een rechtmatige en zorgvuldige manier met persoonsgegevens om te gaan, inclusief de uitwisseling met derden.

Deze uitgangspunten legt de gemeente Veenendaal vast in zowel privacyconvenanten als het gaat om het delen van gegevens met externen als in privacyreglementen voor het delen van gegevens binnen de eigen organisatie. De afspraken in deze documenten integreert de gemeente in haar werkprocessen.

2.4 Risicogestuurde aanpak

Het privacybeleid van de gemeente Veenendaal is erop gericht aantoonbaar te voorzien in passende maatregelen voor doeltreffende bescherming van persoonsgegevens en de bescherming van rechten van personen. Wat ‘passend’ is, hangt af van de concrete risico’s die de verwerking van persoonsgegevens voor burgers met zich meebrengt wanneer er geen doeltreffende beschermingsmaatregelen genomen zouden zijn. Inzichtelijk moet zijn of een gegevensverwerking te classificeren is als laag, midden of hoog risico, en of het mitigeren van deze risico’s een inspanning vergt die laag, midden of hoog is. Door het uitvoeren van risico-analyses wordt de risicoclassificatie bepaald. Afhankelijk van de risicoclassificatie geldt een ander toetsingsregime.

Bij nieuw in te stellen processen wordt privacy vanaf het begin van het ontwerpproces meegenomen, door na te denken over de benodigde technische en organisatorische maatregelen en die in te bouwen in processen en systemen (‘privacy by design’). Aan nieuwe verwerkingen en risicovolle processen liggen data protection impact assessments (DPIA’s) ten grondslag. DPIA’s zijn instrumenteel voor het inzichtelijk krijgen van het proces, de omgang met persoonsgegevens daarin met bijbehorende risico’s en om passende beheersmaatregelen te bepalen. De mate waarin en de manier waarop bedrijfsprocessen en gegevensverwerking aandacht nodig hebben, hangen samen met de uitkomsten van de DPIA. DPIA-rapporten worden opgesteld conform artikel 35 lid 7 AVG. Met behulp van de aanbevelingen in het DPIA-rapport wordt voorzien in passende organisatorische en technische privacybeschermende maatregelen. Voor processen met een laag privacyrisico volstaan algemene oplossingen. Zolang een proces als laag risico gekwalificeerd is, is daarvoor in mindere mate aandacht nodig.

De risicogestuurde aanpak voorkomt dat in strijd met privacynormen en privacyprincipes wordt gehandeld, bijvoorbeeld bij:

1. Onrechtmatige gegevensverwerking, zoals wanneer er een verbod of beperking geldt voor gebruik, opslag of uitwisseling van persoonsgegevens;
2. Disproportionele gegevensverwerking, zoals (a) ontoereikende of bovenmatige gegevensverwerking of (b) gegevensverwerking waarbij het organisatiebelang onevenredig klein is in verhouding tot de impact van de verwerking op personen;
3. Irrelevante gegevensverwerking, zoals gegevensverwerking voor niet ter zake dienende of verouderde doeleinden;

4. Onnauwkeurige gegevensverwerking, zoals wanneer de gebruikte, opgeslagen of uitgewisselde gegevens geen juiste weergave van de werkelijkheid bieden;
5. Onveilige gegevensverwerking, zoals wanneer gegevens toegankelijk zijn of dreigen te worden voor onbevoegden waardoor misbruik mogelijk is;
6. Niet-inachtneming van bijzondere wettelijke voorschriften, zoals niet-nakoming van meldplichten, wettelijke termijnen, toestemmingsverplichtingen;
7. Onbewaakte gegevensverwerking, zoals wanneer niet gecontroleerd wordt of privacywaarborgende maatregelen geëffectueerd zijn of bijstelling behoeven.

3 Verantwoordelijkheid voor privacy

Het beleid is van toepassing op het college van B&W, de burgemeester en de gemeenteraad en op de ambtelijke organisatie van de gemeente Veenendaal en zal uitgangspunt van handelen zijn. De uitvoering van het privacybeleid is onderdeel van de bedrijfsvoering van de ambtelijke organisatie en het handelen van de griffie en volgt de verantwoordelijkheidslijnen van de mandaatbesluiten.

3.1 Verantwoordelijkheid voor verwerking

De AVG kent het begrip ‘verwerkingsverantwoordelijke’. De verwerkingsverantwoordelijke is verantwoordelijk voor de verwerking van persoonsgegevens in overeenstemming met wetgeving, regelingen en beleid op het gebied van privacy. De verwerkingsverantwoordelijke stelt doel en middelen vast voor de verwerkingen van persoonsgegevens.

De bestuurlijke verantwoordelijkheid voor de verwerking van persoonsgegevens volgt de lijnen van de wetgever bij het toedelen van taken. Het gemeentelijk bestuursorgaan dat in de wet een taak krijgt opgedragen is niet alleen verantwoordelijk voor die taak, maar ook voor de bijbehorende verwerking van persoonsgegevens. De meeste taken, waaronder bijvoorbeeld die in het sociaal domein en het fysieke domein, zijn toebedeeld aan het college van B&W. Het college is dan de verwerkingsverantwoordelijke. Bij sommige andere taken, bijvoorbeeld op het gebied van openbare orde en veiligheid en onderdelen binnen het vakgebied burgerzaken, is de burgemeester verwerkingsverantwoordelijke. Daarnaast is de gemeenteraad verwerkingsverantwoordelijke voor zover het verwerking van persoonsgegevens betreft bij inwonersbrieven aan de raad en andere raadsstukken.

3.2 Bestuurlijke verantwoordelijkheid

De bestuurlijke en strategische verantwoordelijkheid voor privacy berust bij het college van B&W, de burgemeester en de gemeenteraad. Zij dragen zorg voor passend gemeentelijk privacybeleid. Binnen het college is een portefeuillehouder Privacy aangewezen. Het college legt over de uitvoering van het privacybeleid verantwoording af aan de gemeenteraad. Privacy heeft zelfstandige aandacht in de planning- en controlcyclus.

3.3 Verantwoordelijkheid gemeentelijke organisatie

De verantwoordelijkheid van het college en de burgemeester wordt praktisch vertaald naar de ambtelijke organisatie volgens de lijnen van het mandaatbesluit. Daarnaast is er voor de operationele ondersteuning en aansturing op het gebied van privacy een Adviseur privacy benoemd. Privacy raakt vaak aan informatiebeveiliging, waarmee afstemming wordt gezocht. Voor informatiebeveiliging is een CISO (Chief

Information Security Officer) aangesteld. Ook is de wettelijk verplichte interne toezichthouder aangesteld: de functionaris voor gegevensbescherming (FG).

Alle verwerkingen van persoonsgegevens door de gemeente Veenendaal worden bijgehouden in een register van verwerkingen, conform artikel 30 AVG. Het register is een digitaal overzicht van alle processen die de gemeente uitvoert. Aan de hand van dit register is vast te stellen welke gegevens de gemeente in welke processen verwerkt en wat ermee gebeurt. Per proces worden verschillende componenten geregistreerd, zoals de grondslag, doelen, categorieën van persoonsgegevens, categorieën betrokkenen en ontvangers van de persoonsgegevens.

In geval van een datalek voldoet de gemeente aan de meldplicht, conform artikelen 33 en 34 AVG. Alle datalekken worden bijgehouden in een register. Er is een procedure ingesteld voor het melden van datalekken. De procedure maakt deel uit van het proces ter afhandeling van incidenten informatiebeveiliging.

4 Toezicht

Landelijk toezicht wordt uitgevoerd door de Autoriteit Persoonsgegevens (AP). Gemeentelijk toezicht wordt uitgevoerd door de functionaris voor gegevensbescherming (FG), de wettelijk verplichte interne toezichthouder. Daarnaast zijn er interne controles op toepassing van de privacynormen.

4.1 Controle op werking en naleving

Beleid, procedures en maatregelen worden steekproefsgewijs en periodiek getoetst op opzet, bestaan en werking in de praktijk. Een periodieke toets op het onderdeel privacy vindt plaats aan de hand van het kwaliteitssysteem. Verantwoordelijken in de organisatie dienen ook zelf periodiek te (laten) controleren in hoeverre de feitelijke situatie in overeenstemming is met toepassing van het privacybeleid. De toetsing aan de hand van het kwaliteitssysteem helpt hen hierbij. Daarnaast zijn vragen, klachten, incidentmanagement, verenigbaarheidstoetsen en DPIA's steekproefsgewijze toetsing van naleving van het privacybeleid.

4.2 Functionaris voor gegevensbescherming

De functionaris voor gegevensbescherming (FG) is de interne toezichthouder van de gemeente Veenendaal op de naleving van privacywetgeving. De FG is aangesteld door de verschillende gemeenteorganen. Het toezicht ziet op deze organen: burgemeester, college van B&W en gemeenteraad. Het college informeert interne en externe doelgroepen over de FG en communiceert zijn contactgegevens aan de landelijke toezichthouder, de Autoriteit Persoonsgegevens (AP).

De FG voert zijn rol en taken uit conform artikelen 37 tot en met 39 AVG. Conform artikel 37 lid 5 AVG is de FG aangewezen op grond van: (a) zijn professionele kwaliteiten en, in het bijzonder, zijn deskundigheid op het gebied van de wetgeving en de privacymanagement-praktijk; (b) zijn vermogen om de onderstaande taken te vervullen en (c) zijn onafhankelijkheid, met name de afwezigheid van een belangenconflict.

Vanwege zijn expertise van wetgeving en de praktijk, geldt een advies van de FG als zwaarwegend en de geëigende wijze voor naleving van privacywetgeving door de gemeente Veenendaal. De FG doet jaarlijks verslag van zijn werkzaamheden aan het college van B&W. Het college besluit over bijstelling van het gemeentelijk privacybeleid met inachtneming van de aanbevelingen van de FG.

5 Privacy voor betrokkenen

Een fundamenteel uitgangspunt, dat opgenomen is in de considerans van de AVG, is dat de verwerking van persoonsgegevens ‘ten dienste van de mens’ staat. Mede hierom moeten personen controle over hun eigen persoonsgegevens hebben. Dit hoofdstuk beschrijft de manieren waarop betrokkenen dit kunnen doen.

5.1 Rechten

Personen van wie de gemeente gegevens verwerkt mogen ervan uitgaan dat dit in overeenstemming met privacyregels gebeurt. Tevens zijn in de AVG specifieke privacyrechten voor personen opgenomen. Personen hebben recht op het volgende:

- Dat de gemeente Veenendaal handelt conform privacywetgeving en het privacybeleidskader;
- Dat de gemeente Veenendaal transparant is over doelen van gegevensverwerking en toepassing van het privacybeleid;
- Dat zij inzage in hun *eigen* gegevens hebben (recht van inzage);
- Dat zij – in geval van fouten – hun gegevens kunnen (laten) verbeteren of verwijderen (recht op rectificatie en recht op gegevenswissing);
- Dat de verwerking van hun persoonsgegevens beperkt wordt of tijdelijk niet toegestaan is (recht van beperking van de verwerking en recht van bezwaar); dit verplicht de gemeente Veenendaal tot het maken van een afweging;
- Dat zij de gemeente Veenendaal bij niet-naleving van de wet of het gemeentelijk privacybeleid hierop mogen aanspreken.

5.2 Vragen en klachten

Personen hebben altijd de mogelijkheid om vragen te stellen over de verwerkingen van persoonsgegevens. Dit verloopt via de dienstverleningskanalen van de gemeente. Bij beantwoording van de vragen kan het advies gevraagd worden aan de FG. Met klachten over de verwerking van persoonsgegevens door de gemeente moeten personen altijd terecht kunnen bij de gemeente, of direct bij de FG:

Een niet tot tevredenheid afgehandelde vraag of klacht over gegevensverwerking door gemeente Veenendaal wordt voorgelegd aan de FG. Personen hebben altijd het recht een klacht in te dienen bij de landelijke toezichthouder, de AP.

Bij klachten over de bejegening door medewerkers van de gemeente is de Klachtenregeling Veenendaal van toepassing.

6 Beleidsevaluatie

Elke twee jaar wordt het privacybeleid geëvalueerd. Daarbij wordt de FG om advies gevraagd.

De FG doet jaarlijks verslag aan het college en geeft aanbevelingen die strekken tot verdere optimalisering van het beleid en de uitvoering daarvan. Het college besluit over bijsturing van het gemeentelijk privacybeleid met inachtneming van de aanbevelingen van de FG.