



Privacybeleid gemeente Barneveld 2023

Vastgesteld bij besluit van 18 april 2023

Inhoud

1. Algemeen	4
1.1 Inleiding	4
1.2 Wetgeving	5
2. Uitgangspunten	5
3. Rollen en verantwoordelijkheden	6
3.1 College van burgemeester en wethouders	6
3.2 Directie	7
3.3 Functionaris voor de gegevensbescherming	7
3.4 Privacy officer	8
3.5 Chief information security officer	9
3.6 Teamleiders	9
3.7 Medewerkers	10
3.8 Ketenpartners en leveranciers	10
4. Borging en beheersing privacy	10
4.1 Data Protection Impact Assessment/ Privacy by design/ Privacy by default	10
4.2 Bewustwording en ondersteuning	11
4.3 Kwaliteitscyclus en evaluatie	11
5. Rechtmatige en zorgvuldige verwerking van persoonsgegevens	12
5.1 Grondslag, doelbinding en verwerking	12
5.2 Register van verwerkingen	13
5.3 Gegevensuitwisseling openbare orde en veiligheid	14
5.4 Gegevensuitwisseling sociaal domein	14
5.5 Bewaartermijnen	15
5.6 Data en ethiek	15
5.7 Informatiebeveiliging	15
5.8 Rechten van betrokkenen	16
5.9 Privacyverklaring	16
6. Foto- en beeldmateriaal	16
6.1 Cameratoezicht	16
6.1.1 Cameratoezicht gemeentehuis, -werf en milieustraat	17
6.1.2 Cameratoezicht stations	17
6.1.3 Cameratoezicht openbare ruimte	17
6.2 Bodycamera's buitengewoon opsporingsambtenaren	17

6.3 Gebruik van foto- en beeldmateriaal door de gemeente Barneveld.....	17
6.3.1 Foto- en beeldmateriaal van inwoners en medewerkers.....	17
6.3.2 Stockfotografie.....	18
6.4 Social Media	18
7. Incidenten met betrekking tot persoonsgegevens	18
7.1 Melding en afhandeling	18
7.2 Registratie en evaluatie	18

1. Algemeen

1.1 Inleiding

In de maatschappij is privacy een onderwerp dat veel in de belangstelling staat. Daarnaast stellen nieuwe technologische ontwikkelingen, innovatieve voorzieningen en een steeds meer digitale werkomgeving andere eisen aan de bescherming van persoonsgegevens en privacy. De gemeente Barneveld is zich hiervan bewust en zorgt ervoor dat de privacy gewaarborgd blijft, onder andere door maatregelen te treffen op het gebied van informatiebeveiliging, dataminimalisatie, transparantie en gebruikerscontrole.

Het beschermen van gegevens en het verwerken van persoonsgegevens is een zeer relevant onderwerp voor de gemeente Barneveld. De gemeente verwerkt persoonsgegevens voor de dienstverlening aan inwoners en bedrijven, voor de uitvoering van haar taken en als werkgever voor haar medewerkers. Bij gegevensbescherming gaat het om het zorgvuldig, veilig en doelmatig verwerken van persoonsgegevens.

Persoonsgegevens zijn de gegevens over een geïdentificeerde persoon of gegevens waarmee een persoon geïdentificeerd kan worden. Hierbij kan gedacht worden aan directe persoonsgegevens, zoals een naam, adresgegevens, foto of e-mailadres. Maar ook indirecte gegevens kunnen persoonsgegevens zijn, zoals een kentekenplaat op een voertuig of een IP-adres. Gevoelige en bijzondere persoonsgegevens zijn persoonsgegevens zoals het BSN en informatie over iemands gezondheid of godsdienst.

Privacy is samenvattend te omschrijven als respect voor de persoonlijke levenssfeer van een individu. Om te voorkomen dat een onnodige of te vergaande inbreuk wordt gemaakt op de persoonlijke levenssfeer, is onder meer bij wet voorzien in waarborgen.

Privacybeleid

De gemeente Barneveld hecht er veel waarde aan dat de verwerkingen van persoonsgegevens zorgvuldig, rechtmatig en veilig plaatsvinden. Binnen de gemeente is hiervoor veel aandacht. Om de positie van het privacyvraagstuk verder te versterken heeft het college van burgemeester en wethouders besloten dat privacybeleid wenselijk is. Dit privacybeleid is praktisch ingestoken en vormt een aanvulling op de verplichtingen die voortvloeien uit de Europese Algemene Verordening Gegevensbescherming (hierna: AVG) en de Wet politiegegevens (hierna: Wpg). Het college van burgemeester en wethouders stelt dit beleid dan ook vast.

In dit beleid staan kaders beschreven voor het verwerken van persoonsgegevens, de bescherming van deze gegevens en de omgang met deze gegevens. De kaders gelden voor de gemeente Barneveld. Verder kan het beschermen van persoonsgegevens niet geborgd worden zonder adequate informatiebeveiliging. Het privacybeleid hangt daarom ook samen met het Informatiebeveiligingsbeleid. Dit privacybeleid treedt in werking op 1 mei 2023 en is van toepassing op alle verwerkingen van persoonsgegevens door alle bestuursorganen van de gemeente Barneveld. Oftewel: voor alle verwerkingen die binnen de gemeente Barneveld plaatsvinden. Dit betekent dat het privacybeleid zowel betrekking heeft op de verwerking van persoonsgegevens onder de AVG als

de verwerking van politiegegevens onder de Wpg. Als in het vervolg van dit stuk gesproken wordt over persoonsgegevens, worden daarmee zowel persoons- als politiegegevens bedoeld.

Contact

Vragen met betrekking tot privacy, het privacybeleid of de overige wet- en regelgeving op het gebied van privacy kunnen gericht worden aan de Privacy Officer van de gemeente Barneveld:

privacy@barneveld.nl.

1.2 Wetgeving

Bij de verwerking van persoonsgegevens staat respect voor de persoonlijke levenssfeer van de betrokkenen voorop. Er moet voorkomen worden dat onnodige of te vergaande inbreuken op iemands persoonlijke levenssfeer worden gemaakt. De AVG en de Uitvoeringswet AVG bieden hiervoor het wettelijk kader. Voor de verwerking van politiegegevens biedt de Wpg het wettelijk kader. Politiegegevens zijn persoonsgegevens die voor de uitvoering van de politietaak worden verwerkt. Binnen de gemeente Barneveld betreft dit de verwerking van persoonsgegevens door buitengewoon opsporingsambtenaren in het kader van opsporingstaken.

De AVG zorgt onder andere voor versterking en uitbreiding van de privacyrechten van betrokkenen en meer verantwoordelijkheden voor de gemeente Barneveld. Met de naleving van het privacybeleid spant de gemeente Barneveld zich in om aan de AVG, Uitvoeringswet AVG en de Wpg te voldoen. In dit privacybeleid zijn de in de AVG en Wpg opgenomen definities integraal van toepassing.

2. 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:

Rechtmatigheid, behoorlijkheid, transparantie

Persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt. Alle communicatie over de verwerking van persoonsgegevens vindt duidelijk, begrijpelijk en in de Nederlandse taal plaats. Betrokkenen zijn er zelf verantwoordelijk voor om dit indien nodig te (laten) vertalen in een voor hen begrijpelijke taal.

Grondslag en verwerken

De gemeente zorgt ervoor dat het verwerken van persoonsgegevens gebaseerd is op één van de grondslagen zoals benoemd in de AVG en Wpg¹. Met verwerken wordt onder meer het verzamelen, vastleggen, opslaan, opvragen, raadplegen of vernietigen van persoonsgegevens bedoeld².

¹ Artikel 6 AVG

² Artikel 4 lid 2 AVG

Doelbinding

Voor de verwerking van persoonsgegevens plaatsvindt, wordt bepaald voor welk doel de persoonsgegevens worden verwerkt. Het doel moet duidelijk en zo specifiek mogelijk worden geformuleerd. Bij elke verwerking wordt getoetst in hoeverre het verwerken van persoonsgegevens noodzakelijk is. Hierbij worden de verschillende belangen afgewogen en wordt gekeken naar de doelmatigheid, proportionaliteit en subsidiariteit. Verder mogen persoonsgegevens niet verwerkt worden voor een ander doel dan waarvoor zij zijn verkregen.

Subsidiariteit

Voor het bereiken van het doel waarvoor de persoonsgegevens worden verwerkt, wordt inbreuk op de persoonlijke levenssfeer van de betrokken burger zoveel mogelijk beperkt.

Proportionaliteit

De inbreuk op de belangen van de betrokkene mag niet onevenredig zijn in verhouding tot het met de verwerking te dienen doel.

Dataminimalisatie

De gemeente streeft naar minimale gegevensverwerking. Waar mogelijk worden minder of geen persoonsgegevens verwerkt of worden de gegevens geanonimiseerd of gepseudonimiseerd³.

Bijzondere persoonsgegevens

Bijzondere persoonsgegevens mogen niet worden verwerkt, tenzij een wettelijke grondslag aanwezig is om op dit verbod een uitzondering te maken.

Strafrechtelijke gegevens

Strafrechtelijke gegevens mogen niet worden verwerkt, tenzij een wettelijke grondslag aanwezig is om op dit verbod een uitzondering te maken.

Integriteit, vertrouwelijkheid en informatiebeveiliging

De gemeente gaat zorgvuldig om met persoonsgegevens en behandelt deze vertrouwelijk. Zo worden persoonsgegevens alleen verwerkt door personen met een geheimhoudingsplicht en voor het doel waarvoor deze gegevens zijn verzameld. Daarbij zorgt de gemeente voor passende beveiliging van persoonsgegevens. Deze beveiliging is vastgelegd in het informatiebeveiligingsbeleid.

3. Rollen en verantwoordelijkheden

3.1 College van burgemeester en wethouders

De verantwoordelijke voor de verwerking van persoonsgegevens is het college van burgemeester en wethouders (hierna: het college), de burgemeester, de ambtenaar van de burgerlijke stand, de Heffingsambtenaar of de Invorderingsambtenaar. Welk bestuursorgaan verantwoordelijk is, is afhankelijk van hetgeen waarop de verwerking van persoonsgegevens betrekking heeft.

³ Geanonimiseerde gegevens zijn niet herleidbaar tot een persoon en gepseudonimiseerde gegevens zijn middels een koppeling te herleiden tot een persoon.

Aan de burgemeester als bestuursorgaan is een aantal wettelijke taken toegekend. Wanneer in het kader van deze taken verwerking van persoonsgegevens plaatsvindt, valt dit onder zijn verantwoordelijkheid. Aan het college als bestuursorgaan is ook een aantal wettelijke taken toegekend. Wanneer in het kader van deze taken verwerking van persoonsgegevens plaatsvindt, valt dit onder de verantwoordelijkheid van het college. Namens het college is de portefeuillehouder met de portefeuille 'Bedrijfsvoering' het eerste aanspreekpunt.

Verantwoording aan de gemeenteraad

Het college legt verantwoording af aan de gemeenteraad over de uitvoering en realisatie van beleid. Met ingang van 2018 neemt het college in de programmabegroting een passage op over de uitvoering en realisatie van het privacybeleid. Naast de jaarlijkse verantwoording in de programmabegroting heeft het college de algemene informatieplicht om de gemeenteraad te informeren over bijzonderheden.

3.2 Directie

De eindverantwoordelijkheid voor de ambtelijke uitvoering van het privacybeleid ligt bij de directie van de gemeente. Tussen de directie, functionaris gegevensbescherming en de chief information security officer vindt elk kwartaal overleg plaats over privacy en informatiebeveiliging.

De concerndirecteur in- en externe dienstverlening rapporteert door middel van een periodieke kennisgeving aan de portefeuillehouder.

Elke concerndirecteur is binnen zijn of haar aandachtsgebied verantwoordelijk voor de naleving van het privacybeleid en een zorgvuldige verwerking van persoonsgegevens.

Vastlegging privacybeleid

De burgemeester en het college van burgemeester en wethouders stellen het gemeentelijk privacybeleid vast, ieder voor zover het hun bevoegdheid betreft. Bij de vaststelling dan wel herziening van het privacybeleid zal de burgemeester of het college de adviezen van de privacy officer en functionaris gegevensbescherming in overweging nemen.

3.3 Functionaris voor de gegevensbescherming

De functie van functionaris gegevensbescherming is wettelijk verplicht. De functionaris gegevensbescherming ziet toe op naleving van de privacywetgeving en het privacybeleid binnen de gemeente. Hiervoor is het noodzakelijk dat de functionaris gegevensbescherming zijn taken en plichten onafhankelijk vervult en geen instructies ontvangt met betrekking tot de uitoefening van zijn functie. De werkzaamheden die de functionaris gegevensbescherming uitvoert hebben een wettelijke grondslag in de AVG (artikel 39) en Wpg (artikel 36).

Taken functionaris gegevensbescherming:

- Informeren en adviseren van de organisatie en verwerkers over de verplichtingen die zij hebben op grond van de AVG, Wpg en overige regelgeving op het gebied van privacy en persoonsgegevens;

- Advisering van de burgemeester, het college en de directie;
- Toezien op naleving van AVG, Wpg en overige regelgeving op het gebied van privacy en persoonsgegevens. Hieronder valt o.a. het toezicht op doelbinding, noodzaak en rechtmatigheid en de toepassing van privacy by design;
- Toezien op naleving van het privacybeleid;
- Rapporteren van bevindingen aan het college en directie;
- Toezien op toewijzing van verantwoordelijkheden, bewustmaking en opleiding van medewerkers;
- Advisering met betrekking tot Data Protection Impact Assessments (hierna: DPIA's), toezien op de uitvoering daarvan en adviseren over noodzakelijke vervolgacties;
- Advisering van de privacy officer en de chief information security officer;
- Advisering van de privacy officer bij de afhandeling van ingewikkelde klachten;
- Samenwerken met de Autoriteit Persoonsgegevens (hierna: AP): contactpersoon en intermediair tussen het college en de AP zoals benoemd in de AVG en Wpg.

De taken zoals hierboven uitgewerkt moeten bij de functionaris gegevensbescherming worden belegd. Een aantal taken kunnen echter ook in (nauwe) samenwerking met of door de privacy officer en de chief information security officer worden uitgevoerd. Hierover worden werkafspraken gemaakt. De functionaris gegevensbescherming blijft niettemin altijd eindverantwoordelijke.

Bevoegdheden functionaris gegevensbescherming

De functionaris gegevensbescherming heeft controlebevoegdheden tot zijn beschikking zoals beschreven in titel 5.2 van de Algemene wet bestuursrecht (hierna: Awb). Deze bevoegdheden zijn noodzakelijk voor de uitoefening van geloofwaardig en effectief toezicht. Tevens gelden ook de waarborgen en beperkingen zoals beschreven in titel 5.2 Awb. In de bijlage zijn de belangrijkste (wettelijke) bevoegdheden van de functionaris gegevensbescherming opgenomen.

De functionaris gegevensbescherming is te bereiken via fg@barneveld.nl.

3.4 Privacy officer

De privacy officer heeft een brede functie, waarbij de privacy officer hoofdzakelijk dient als interne (juridische) ondersteuning van de gehele organisatie voor alle privacy gerelateerde vraagstukken en dilemma's.

Taken privacy officer:

- Ondersteuning bieden aan de functionaris gegevensbescherming;
- Implementeren privacyregelgeving (AVG en Wpg) en privacybeleid in de organisatie;
- Zorgdragen voor kennisoverdracht en bewustwording in de gemeente;
- Advisering van de burgemeester, het college en de directie;
- Functioneren als (juridische) vraagbaak voor de organisatie;
- Advisering bij gegevensuitwisseling met derden;
- Bijhouden register van verwerkingsactiviteiten;
- Uitvoeren van DPIA's;

- Uitvoeren van een jaarlijkse interne audit voor de Wpg en het coördineren van de externe audit Wpg die eens in de vier jaar wordt uitgevoerd;
- Feitelijke afhandeling van datalekken en het beheren van het register waarin datalekken worden geregistreerd:
 - Een datalek beoordelen op ernst en consequenties en vertrouwelijk behandelen.
 - Afhankelijk onder wiens verantwoordelijkheid het datalek valt de personen informeren zoals genoemd in paragraaf 7.1.
- In mandaat afhandelen van klachten met betrekking tot de verwerking van persoonsgegevens;
- In mandaat afhandelen van verzoeken van betrokkenen, zoals recht op inzage, rectificatie en recht van bezwaar;

De privacy officer is te bereiken via privacy@barneveld.nl.

3.5 Chief information security officer

Persoonsgegevens kunnen niet geborgd worden zonder adequate informatiebeveiliging. De chief information security officer draagt zorg voor de informatiebeveiliging. De werkzaamheden die de chief information security officer uitvoert worden beschreven in het Informatiebeveiligingsbeleid. De chief information security officer stuurt op en evalueert de naleving van het Informatiebeveiligingsplan. Concreet adviseert de chief information security officer het management over informatiebeveiliging, mogelijke risico's en de daarbij behorende mitigerende maatregelen. Dit zijn alle maatregelen die negatieve effecten van het besluit of handelen voorkomen of beperken.

Tevens is de chief information security officer samen met de privacy officer en indien nodig de functionaris gegevensbescherming, betrokken bij de afhandeling van een datalek. De chief information security officer mag correctieve en/of preventieve maatregelen met betrekking tot informatiebeveiliging nemen en stemt dit af met de privacy officer en indien nodig de functionaris gegevensbescherming. De maatregelen worden pas genomen nadat de chief information security officer het verantwoordelijke bestuursorgaan, de burgemeester of het college in de persoon van de portefeuillehouder 'Bedrijfsvoering', hierover heeft geïnformeerd. Indien een datalek vereist dat direct maatregelen worden getroffen met betrekking tot informatiebeveiliging, wordt de burgemeester en/ of de portefeuillehouder 'Bedrijfsvoering' over de genomen maatregelen zo spoedig mogelijk geïnformeerd.

3.6 Teamleiders

Elke teamleider is binnen zijn team verantwoordelijk voor de naleving van het privacybeleid en een zorgvuldige verwerking van persoonsgegevens. Hieronder vallen onder andere de volgende verantwoordelijkheden en taken:

- Het tijdig betrekken van de privacy officer bij samenwerkingen met derde partijen, zodat de juiste afspraken gemaakt kunnen worden;
- Het tijdig betrekken van de privacy officer bij wijzigingen in de verwerking van persoonsgegevens, zodat de privacy officer kan adviseren over maatregelen die vanuit de AVG of Wpg genomen moeten worden (zoals aanpassing in het register van verwerkingen en de uitvoering van een DPIA);

- Het binnen het team op peil houden van het kennisniveau van medewerkers op het gebied van privacy en op de geldende werkprocessen (bijvoorbeeld voor het melden van datalekken en inzageverzoeken);
- Het tijdig melden van datalekken bij de privacy officer;
- Het informeren van de privacy officer over verzoeken die door burgers worden ingediend, zoals een verzoek om inzage.

3.7 Medewerkers

Alle medewerkers hebben een eigen verantwoordelijkheid in het goed omgaan met persoonsgegevens en zijn verantwoordelijk om kennis te nemen van het privacybeleid, de maatregelen en procedures op het gebied van gegevensverwerking en dienen deze na te leven. Van iedereen binnen de gemeente Barneveld wordt verwacht dat zij zorgvuldig en integer omgaan met persoonsgegevens.

3.8 Ketenpartners en leveranciers

Ketenpartners

De (keten)partners waarmee de gemeente Barneveld samenwerkt en waarmee tijdens het samenwerken persoonsgegevens worden gedeeld, zijn vaak zelf verantwoordelijk voor het voldoen aan alle geldende privacywetgeving. Het is aan de (keten)partner om te voldoen aan de AVG en Wpg. Per samenwerking en proces wordt beoordeeld of er een overeenkomst moet worden afgesloten en zo ja, wat voor een overeenkomst. Dit kan een verwerkersovereenkomst, overeenkomst gegevensuitwisseling, een convenant of een andere vorm van een overeenkomst zijn. Wat in elk geval hierin terugkomt zijn afspraken over de eisen waar de gegevensuitwisseling en de beveiliging aan moeten voldoen.

Leveranciers

Wanneer gemeente Barneveld als verwerkingsverantwoordelijke bij een externe partij een product of bepaalde diensten afneemt waarbij sprake is van het verwerken van persoonsgegevens, wordt een verwerkersovereenkomst afgesloten. Hierbij wordt de standaard verwerkersovereenkomst (van de IBD) gehanteerd die door de VNG is vastgesteld.

De teamleider die een dergelijke uitbesteding, samenwerking of uitwisseling van persoonsgegevens aangaat, ziet toe op en is verantwoordelijk voor het afsluiten van een overeenkomst. Voor dit proces is een handleiding opgesteld die beschikbaar is gesteld op intranet.

4. Borging en beheersing privacy

4.1 Data Protection Impact Assessment/ Privacy by design/ Privacy by default

Vanuit het oogpunt van een zorgvuldige omgang met persoonsgegevens wordt een Data Protection Impact Assessment (DPIA) uitgevoerd voor verwerkingen die waarschijnlijk een verhoogd risico opleveren voor betrokkenen en/ of processen waarvan de Autoriteit persoonsgegevens heeft gesteld dat er verplicht een DPIA moet worden uitgevoerd. Deze beoordeling zorgt ervoor dat alle risico's van een verwerking (vroegtijdig) in kaart worden gebracht en maatregelen kunnen worden getroffen.

Privacy by design en default worden bij nieuwe processen en/of applicaties als eis meegenomen. Dit wordt onder meer vormgegeven door deelname van de privacy officer aan het Planatelier en het pro-actief handelen van collega's door de privacy officer vroegtijdig te betrekken bij het ontwerpen en implementeren van nieuwe processen en/ of applicaties.

4.2 Bewustwording en ondersteuning

Het is belangrijk dat het college, leidinggevenden en medewerkers bewust met persoonsgegevens omgaan. Om bewustwording te realiseren is kennisoverdracht noodzakelijk. De functionaris gegevensbescherming, privacy officer en chief information security officer zorgen ervoor dat informatie over privacy en informatiebeveiliging blijvend onder de aandacht worden gebracht van de gehele organisatie. Dit vindt onder meer plaats door het geven van workshops, het aansluiten bij teamoverleggen, het plaatsen van berichten op intranet en het uitvoeren van ludieke acties.

Om de medewerkers te instrueren in het omgaan met en verwerken van persoonsgegevens, zijn er procedures en werkinstructies beschikbaar voor medewerkers. Tevens wordt voorzien in adequate (juridische) ondersteuning van medewerkers door de privacy officer.

4.3 Kwaliteitscyclus en evaluatie

VNG Realisatie heeft criteria ontwikkeld om de AVG te vertalen naar een kwaliteitscyclus voor privacy en informatiebeveiliging voor gemeentelijke processen in een borgingsproduct. De criteria zijn uitgewerkt in maatregelen die aangeven hoe aan een criterium kan worden voldaan. De criteria, en daarmee de maatregelen, zijn vervolgens ingedeeld in thema's om inzicht te krijgen waar de gemeente staat op het gebied van de AVG. Hiermee wordt inzicht verkregen in het beheer en de bescherming van persoonsgegevens en is overzichtelijk op welke punten eventueel nog niet (volledig) is voldaan aan de AVG. De zeven thema's die tezamen alle aspecten van gegevensbescherming afdekken zijn:

1. Beleid
2. Processen
3. Organisatorische inbedding
4. Rechten van betrokkenen
5. Samenwerking
6. Beveiliging
7. Verantwoording

Het borgingsproduct wordt jaarlijks in Q4 door de functionaris gegevensbescherming en privacy officer ingevuld. De uitkomsten hiervan zijn vervolgens input voor het jaarverslag van de functionaris gegevensbescherming, evaluatie van dit beleid en actiepunten voor het daarop volgende kalenderjaar.

5. Rechtmatige en zorgvuldige verwerking van persoonsgegevens

5.1 Grondslag, doelbinding en verwerking

Grondslag

De AVG zegt dat voor elke verwerking van persoonsgegevens een rechtmatige grondslag uit de wet van toepassing moet zijn. Dat betekent dat de verwerking alleen mag plaatsvinden op grond van één van de onderstaande grondslagen:

1. Wanneer de betrokkene toestemming heeft gegeven voor de specifieke verwerking;
2. Voor de uitvoering van een overeenkomst waarbij de betrokkene partij is;
3. Om een wettelijke verplichting na te komen;
4. Om de vitale belangen van de betrokkene te beschermen;
5. Voor de goede vervulling van een taak van algemeen belang of een aan de gemeente wettelijk opgedragen taak;
6. Wanneer de verwerking noodzakelijk is voor de behartiging van een gerechtvaardigd belang.



4

De Wpg kent andere grondslagen dan de AVG en deelt de grondslagen in naar opsporingswerkzaamheden. De verwerking van politiegegevens door buitengewoon opsporingsambtenaren kan plaatsvinden op grond van de volgende grondslagen:

1. Artikel 8 Wpg: dagelijkse politietaak;
2. Artikel 9 Wpg: handhaving van de rechtsorde in een bepaald geval;
3. Artikel 13 Wpg: ondersteunende taken.

Doelbinding

Volgens de AVG en Wpg mogen persoonsgegevens alleen verzameld worden als daarvoor een doel is vastgesteld. Het doel moet uitdrukkelijk omschreven en gerechtvaardigd zijn. Veelal is het doel omschreven in de wet. Per verwerking moet worden afgewogen of de gegevens verwerkt mogen worden. Wanneer het gebruik van gegevens noodzakelijk is voor andere doelen dan waarvoor de gegevens zijn verzameld, dan mogen alleen met ondubbelzinnige toestemming van de betrokkene de gegevens worden verwerkt. Het kan voorkomen dat bij casussen binnen de domeinen van openbare orde en veiligheid en het sociaal domein, geen toestemming wordt verkregen voor het verwerken van gegevens voor andere doeleinden. Dit wordt nader toegelicht in paragraaf 5.3 en 5.4.

⁴ www.autoriteitpersoonsgegevens.nl

Verwerking

Op de verwerking van persoonsgegevens is de AVG en/of Wpg van toepassing. De verwerking van persoonsgegevens is elke geheel of gedeeltelijke geautomatiseerde handeling met persoonsgegeven(s)⁵. In de AVG en Wpg wordt verwerking als volgt omschreven:

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

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

Wijze van verwerking

Bij de verwerking van persoonsgegevens gelden een aantal regels⁶:

- De verwerking moet in overeenstemming zijn met de wet;
- De verwerking moet zorgvuldig gebeuren;
- De persoonsgegevens worden zoveel mogelijk verzameld bij de betrokkene zelf en waar mogelijk eenmalig uitgevraagd in het kader van deregulering en vermindering van de lastendruk bij de betrokkene;
- Persoonsgegevens worden alleen verzameld als het doel niet op een andere manier kan worden bereikt;
- Het verzamelen van persoonsgegevens staat in verhouding tot het doel. Er wordt dus niet meer gevraagd dan nodig;
- Persoonsgegevens worden alleen verwerkt door personen met een geheimhoudingsplicht;
- Op de verwerking van persoonsgegevens is tevens het Informatiebeveiligingsbeleid van toepassing.

5.2 Register van verwerkingen

Als organisatie, zowel als verwerkingsverantwoordelijk als verwerker, is gemeente Barneveld verplicht tot het hebben van een register van verwerkingen⁷. In dit register moeten alle processen waarbij persoonsgegevens worden verwerkt zijn opgenomen. Het register bevat een beschrijving van wat er tijdens een verwerking plaatsvindt en welke gegevens daarvoor worden gebruikt. Wat in het register van verwerkingen moet staan is opgenomen in artikel 30 van de AVG en artikel 31d van de Wpg.

Het register van verwerkingen is een document dat altijd aan verandering onderhevig is. De meest recente versie wordt centraal en onder verantwoordelijkheid van de privacy officer bijgehouden. Jaarlijks wordt het register van verwerkingen beoordeeld door de functionaris gegevensbescherming

⁵ Artikel 2 lid 1 AVG, artikel 1 sub c Wpg

⁶ Artikel 5 AVG

⁷ Artikel 30 AVG

op volledigheid en juistheid. De teamleiders zijn verantwoordelijk voor het doorgeven van tussentijdse wijzigingen in de verwerkingen en processen aan de privacy officer. Voor dit proces is een handleiding opgesteld welke beschikbaar is gesteld op intranet.

5.3 Gegevensuitwisseling openbare orde en veiligheid

Binnen het domein van openbare orde en veiligheid zijn verschillende overheidsinstanties werkzaam zoals politie, Belastingdienst, het Parket en gemeenten. Elke instantie heeft zijn eigen bij wet vastgestelde taken en bevoegdheden.

Bij de bestrijding van ondermijnende criminaliteit kan sprake zijn van complexe problematiek, waarbij een integrale aanpak vanuit de verschillende overheidsinstanties noodzakelijk is. Overheidsinstanties moeten dan onderling informatie en expertise met elkaar kunnen uitwisselen. Hiertoe is een convenant⁸ opgesteld door het LIEC⁹, waarin afspraken zijn gemaakt over het uitwisselen van informatie, expertise en krachten tussen overheidsinstanties. Het RIEC¹⁰ vervult hierbij een verbindende rol tussen de verschillende overheidsinstanties.

5.4 Gegevensuitwisseling sociaal domein

Binnen het sociaal domein is per domein¹¹ strikt vastgelegd of gegevens uitgewisseld mogen worden met ander domeinen binnen het sociaal domein.

Bij bepaalde casussen kan sprake zijn van complexe en domein overstijgende problematiek, waarbij het wenselijk kan zijn dat gegevens tussen de sectoren worden uitgewisseld in het belang van de cliënt of zijn omgeving. In dergelijke casussen kan aan de cliënt toestemming worden gevraagd of hun gegevens tussen de sectoren mogen worden uitgewisseld. Wanneer de cliënt hiervoor geen toestemming geeft én de betrokken gespreksvoerder maakt zich ernstige zorgen over de cliënt of zijn omgeving, dan kan de casus bij het casuïstiekoverleg worden ingebracht en/ of bij Veilig Thuis worden gemeld. Indien de casus bij Veilig Thuis wordt gemeld, dan gebeurt dit volgens de meldcode¹². Binnen de gemeente Barneveld zijn hiervoor drie Meldcode – functionarissen aangesteld met wie de casus besproken kan worden. Op deze wijze is geborgd dat indien noodzakelijk en in het belang van de cliënt of zijn omgeving overleg kan plaatsvinden. Gesprekvoerders dienen zich wel altijd te houden aan de wetgeving die voor hun beroepsgroep toepasselijk is¹³.

⁸ Convenant ten behoeve van een Bestuurlijke en Geïntegreerde Aanpak van Georganiseerde Criminaliteit, Bestrijding van Handhavingsknelpunten en Bevordering Integriteitsbeoordelingen

⁹ Landelijk Informatie en Expertise Centrum

¹⁰ Regionaal Informatie en Expertise Centrum

¹¹ Onder andere Wmo 2015, Jeugdwet, Participatiewet en de Leerplichtwet

¹² Meldcode Huiselijk geweld en kindermishandeling: <https://www.rijksoverheid.nl/onderwerpen/huiselijk-geweld/meldcode>

¹³ Elke beroepsgroep heeft zijn eigen wetgeving waaraan zij zich dienen te houden. Wanneer dit niet gebeurt, dan kan dit consequenties hebben voor de uitvoering van hun beroep.

5.5 Bewaartermijnen

Voor de verwerking van politiegegevens zijn concrete bewaartermijnen opgenomen in de Wpg. Voor de verwerking van persoonsgegevens onder de AVG gelden geen concrete bewaartermijnen. In de AVG is slechts opgenomen dat persoonsgegevens niet langer bewaard worden dan noodzakelijk is voor de verwerking, dan wel bewaard volgens de van toepassing zijnde wettelijke bewaartermijnen zoals de Archiefwet, van toepassing zijnde sectorspecifieke wetgeving of de selectielijst van de VNG¹⁴. Wanneer persoonsgegevens niet langer bewaard (mogen) worden, worden deze gegevens vernietigd of aangepast zodat personen daarmee niet langer geïdentificeerd kunnen worden.

5.6 Data en ethiek

De wereld om ons heen verandert snel door alle technologische ontwikkelingen en innovaties. Datagedreven werken is voor veel organisaties niet langer slechts een ‘nice to have’ maar een ‘must have’. De gemeente Barneveld wil naast innoveren, ook datagedreven werken. Als gemeente beschikken we over een grote hoeveelheid data, naast de beschikbare (openbare) externe data. De stap van data naar inzicht is een hele grote. Laat staan van inzicht naar toepassing. Correlaties, koppeling en verbanden in gestructureerde en ongestructureerde data geven voorspellend vermogen en kunnen de kennis van de organisatie versterken.

Maar het gebruik van data brengt ook ethische vraagstukken met zich mee: wat kunnen gevolgen en consequenties zijn van innovatie en datagedreven werken voor zowel medewerkers als inwoners? Om organisaties te helpen bij technologische innovatie en het gebruik van data heeft de universiteit Utrecht in samenwerking met data- analisten van de gemeente Utrecht een toolkit ontwikkeld, De Ethische Data Assistent (DEDA)¹⁵. Deze toolkit helpt bij het in kaart brengen van ethische kwesties bij het gebruik van data, het documenteren van het besluitvormingsproces en de bevordering van de verantwoording aan betrokken stakeholders zoals medewerkers en inwoners. Deze toolkit gebruikt gemeente Barneveld om transparant te zijn bij innovaties en het gebruik van data en kennis op te doen over het gebruik van data.

Naast de toolkit heeft het Rathenau Instituut in opdracht van de VNG het rapport “Waardevol digitaliseren” uitgebracht¹⁶. Dit rapport legt een routekaart voor waaruit handelingsperspectieven volgen om digitalisering in de openbare ruimte vorm te geven. Zowel kansen als risico’s van deze ontwikkelingen worden gaandeweg het proces ontdekt en in kaart gebracht. Deze routekaart hanteert gemeente Barneveld naast de toolkit van DEDA.

5.7 Informatiebeveiliging

Samenhang privacy beleid met informatiebeveiligingsbeleid

Bescherming van persoonsgegevens kan niet zonder informatiebeveiliging. Informatiebeveiliging is specifiek gericht op de beschikbaarheid, integriteit en vertrouwelijkheid van de gemeentelijke informatievoorzieningen.

¹⁴ <https://vng.nl/artikelen/selectielijst>

¹⁵ <https://dataschool.nl/deda/>

¹⁶ [Waardevol digitaliseren | Rathenau Instituut](#)

De gemeente Barneveld hanteert een uniform beleid ten aanzien van informatiebeveiliging. Dat wil zeggen: er is één informatiebeveiligingsbeleid dat van toepassing is op alle informatie die binnen de gemeente wordt verwerkt.

Gemeente Barneveld hanteert bij de uitvoering van het beleid de Baseline Informatiebeveiliging Overheid (BIO). Verantwoording wordt jaarlijks afgelegd aan de gemeenteraad en toezichthouders van het Rijk door middel van ENSIA (Eenduidige Normatiek Single Information Audit).

Rol van de Chief Information Security Officer

Op het gebied van informatiebeveiliging heeft de chief information security officer een controlerende en toezichthoudende rol. Waar het gaat over privacy heeft de chief information security officer een rol in ondersteuning en advies. Hij adviseert dan voornamelijk bij projecten en het beheersen van risico's en trekt samen met de privacy officer op waar het gaat om bewustwording en gedrag van medewerkers.

5.8 Rechten van betrokkenen

De AVG en Wpg bevatten niet alleen de plichten van degenen die de persoonsgegevens verwerken, maar geven ook rechten aan de personen van wie gegevens worden verwerkt. Deze rechten zijn opgenomen in de artikelen 12 t/m 22 van de AVG en artikel 24a t/m 28 van de Wpg. Betrokkenen, bijvoorbeeld medewerkers en inwoners, hebben het recht om na te gaan wat er met hun persoonsgegevens gebeurt en hier invloed op uit te oefenen. Gemeente Barneveld respecteert de rechten van betrokkenen. Om betrokkenen in staat te stellen om hun rechten te kunnen uitoefenen, worden zij hierover geïnformeerd op de website van de gemeente Barneveld.

Wanneer een betrokkene gebruik wenst te maken van zijn rechten onder de AVG of Wpg kan de betrokkene een verzoek indienen. Dit verzoek kan schriftelijk of via de website van de gemeente worden ingediend. De verzoeker om informatie moet zich altijd identificeren. De informatie waarom wordt verzocht wordt kosteloos verstrekt, tenzij het verzoek buitensporig is.

Na ontvangst van een verzoek ontvangt betrokkene binnen één maand een besluit en de informatie waarom is verzocht. Deze termijn kan met twee maanden worden verlengd. Een verzoek kan worden geweigerd als het verzoek ofwel kennelijk ongegrond is ofwel buitensporig is. Tegen het besluit kan betrokkene bezwaar maken of een klacht indienen bij de Autoriteit Persoonsgegevens.

5.9 Privacyverklaring

Op de website van gemeente Barneveld wordt in begrijpelijk en duidelijk Nederlands uitgelegd waarom de gemeente Barneveld persoonsgegevens verzamelt en verwerkt, welke rechten een betrokkene heeft en waar betrokkenen terecht kunnen met vragen en klachten.

6. Foto- en beeldmateriaal

6.1 Cameratoezicht

In de gemeente Barneveld is er cameratoezicht bij zowel gemeentelijke locaties als in de openbare ruimte. In deze paragraaf wordt aangegeven op welke locaties (mobiel) cameratoezicht plaatsvindt, met welk doel en wie voor het cameratoezicht als verantwoordelijke kan worden aangemerkt.

6.1.1 Cameratoezicht gemeentehuis, -werf en milieustraat

Gemeente Barneveld gebruikt camera's om de veiligheid van medewerkers en bezoekers te waarborgen op de locaties van de gemeente, zoals het gemeentehuis, -werf en de milieustraat. Het cameratoezicht wordt duidelijk kenbaar gemaakt door middel van stickers en borden. Het gaat concreet om camera's die:

- Gebouwen en eigendommen bewaken;
- Medewerkers en bezoekers beschermen;
- Helpen bij de preventie van misdrijven waaronder diefstal en vandalisme.

6.1.2 Cameratoezicht stations

Op de stations vindt cameratoezicht plaats bij de fietsenstallingen en bij de toiletten. Bij de toiletten is cameratoezicht bij de toegang van de toiletten, op de toiletten zelf hangen geen camera's. Bij zowel de fietsenstallingen als de toiletten hangen borden dat er cameratoezicht plaatsvindt. Opnames worden continu gemaakt.

De beelden kunnen op vordering met de politie worden gedeeld. De politie kan dit pas doen bij verdenking van een misdrijf, zoals mishandeling of diefstal en beslist of de beelden worden gebruikt voor het opsporingsonderzoek. Burgers kunnen geen aanspraak maken op de beelden.

6.1.3 Cameratoezicht openbare ruimte

Door de burgemeester zijn een aantal openbare gebieden aangewezen waar cameratoezicht plaatsvindt op basis van artikel 151c van de Gemeentewet. Deze camera's zijn ingesteld voor de handhaving van de openbare orde. De verantwoordelijkheid voor de verwerking van deze beelden ligt bij de politie. Dit betekent dat de politie verantwoordelijk is voor de naleving van de AVG en Wpg.

6.2 Bodycamera's buitengewoon opsporingsambtenaren

Het doel van het gebruik van de bodycamera's is om de veiligheid van de buitengewoon opsporingsambtenaren te bevorderen door de preventieve werking van de camera's. Vooraf wordt aan betrokkenen medegedeeld dat er gefilmd wordt.

6.3 Gebruik van foto- en beeldmateriaal door de gemeente Barneveld

6.3.1 Foto- en beeldmateriaal van inwoners en medewerkers

Bij zowel interne als externe bijeenkomsten worden door de gemeente Barneveld of door derden die de gemeente heeft ingehuurd foto's genomen. Dat er foto's van een bijeenkomst worden gemaakt en gepubliceerd mag, mits met het volgende rekening wordt gehouden:

- Vooraf aankondigen dat er foto's worden gemaakt;
- Aangeven waarvoor de foto's worden gebruikt;
- Betrokkenen moeten de mogelijkheid hebben om niet gefotografeerd te worden als zij dit niet willen. Dit moeten betrokkenen bij de organisatie van de bijeenkomst kunnen aangeven;
- Voordat de foto's worden geplaatst worden deze beoordeeld. Wanneer dit mogelijk is worden alleen foto's gepubliceerd waarop betrokkenen niet herkenbaar op staan;
- Betrokkenen moeten de mogelijkheid hebben om achteraf foto's te laten verwijderen;
- Er wordt een bewaartermijn voor de foto's vastgelegd.

6.3.2 Stockfotografie

Bij gevoelige onderwerpen kiest de gemeente voor stockfotografie. De gemeente koopt dan een rechtenvrij beeld aan, specifiek voor het onderwerp. Denk hierbij bijvoorbeeld aan een foto op de gemeentelijke website voor schuldhulpverlening of een foto voor een folder over ziekteverzuim.

6.4 Social Media

Door het team Communicatie is een Social Media beleid opgesteld en deze staat op [intranet](#).

7. Incidenten met betrekking tot persoonsgegevens

7.1 Melding en afhandeling

Op grond van de AVG (artikel 33 en 34) en Wpg (artikel 33a) geldt een meldplicht voor datalekken. Deze meldplicht houdt in dat organisaties zodra zij een datalek hebben ontdekt binnen 72 uur een melding van het datalek moeten doen bij de AP, tenzij het niet waarschijnlijk is dat het datalek een risico vormt voor de betrokkene. Soms moet dit lek ook worden gemeld aan de betrokkene van wie de gegevens zijn gelekt.

Om in het geval van een datalek snel en daadkrachtig te kunnen handelen is een procedure ingericht die in werking treedt bij melding van een datalek. De beoordeling van een gemeld datalek vindt plaats door de privacy officer, chief information security officer en indien nodig de functionaris gegevensbescherming. Zij beoordelen de ernst en consequenties van een datalek en behandelen een lek vertrouwelijk.

Bij ernstige datalekken, wordt afhankelijk van het datalek, het verantwoordelijke bestuursorgaan, de burgemeester of het college in de persoon van de portefeuillehouder 'Bedrijfsvoering, de directie en de betrokken teamleider bij kennisgeving geïnformeerd. Deze kennisgeving gebeurt geanonimiseerd, tenzij dit omwille van de afhandeling van het datalek niet mogelijk is. Het gehele college van burgemeester en wethouders wordt geïnformeerd en geadviseerd als dat gelet op de ernst van een datalek noodzakelijk is.

Een datalek kan gemeld worden via datalek@barneveld.nl.

7.2 Registratie en evaluatie

Alle datalekken worden geregistreerd in de beveiligde omgeving van Topdesk. Alleen de functionaris gegevensbescherming, chief information security officer en privacy officer hebben toegang tot deze omgeving. Het is belangrijk om incidenten in de toekomst te voorkomen door verbetermaatregelen te nemen middels evaluatie(s). Registratie van incidenten en een periodieke rapportage daarover zijn onderdeel van een professionele manier van het verwerken van persoonsgegevens. De rapportage over incidenten met betrekking tot persoonsgegevens maakt een vast onderdeel uit van het jaarverslag van de functionaris gegevensbescherming.

Bijlage: Bevoegdheden functionaris gegevensbescherming

- Betreden van ruimten: Indien het noodzakelijk is voor de uitvoering van bovengenoemde taken is de functionaris gegevensbescherming bevoegd om ongevraagd alle ruimten te betreden, voor zover die ruimten vallen onder de reikwijdte van het aan de functionaris gegevensbescherming wettelijk opgedragen toezicht.
- Vragen van inlichtingen: De functionaris gegevensbescherming verkrijgt alle inlichtingen die noodzakelijk zijn voor de uitvoering van bovengenoemde taken. De verwerkingsverantwoordelijke verleent alle medewerking om deze inlichtingen binnen een redelijke termijn te verstrekken. Geen medewerking hoeft te worden verleend in het geval de verwerkingsverantwoordelijke of diens ondergeschikte uit hoofde van het ambt, beroep of wettelijk voorschrift is verplicht tot geheimhouding.
- Vragen om inzage: de functionaris gegevensbescherming is bevoegd om inzage te vragen van zakelijke gegevens en bescheiden. Hiervan mag de functionaris gegevensbescherming tevens kopieën maken. Het gaat hierbij niet alleen om fotokopieën, maar ook van kopieën van (gedeelten van) geautomatiseerde gegevensbestanden. De verwerkingsverantwoordelijke moet hieraan meewerken, tenzij de verwerkingsverantwoordelijke of diens ondergeschikte uit hoofde van het ambt, beroep of wettelijk voorschrift is verplicht tot geheimhouding.
- Onderzoeken van zaken: Voor de uitvoering van bovengenoemde taken kan het betreden van ruimten soms niet voldoende zijn om toezicht uit te oefenen. Indien noodzakelijk verkrijgt de functionaris gegevensbescherming daarom toegang tot (computer-)systemen waarin persoonsgegevens worden verwerkt. De functionaris gegevensbescherming zal desnoods de beschikking dienen te krijgen over de relevante inloggegevens. Tevens zal de functionaris gegevensbescherming op de hoogte dienen te zijn hoe, na het inloggen, de relevante bestanden kunnen worden bevraagd.