Gemeente Midden-Delfland

# GEMEENTEBLAD

Officiële uitgave van de gemeente Midden-Delfland

Nr. 261731

6 december 2018

## Besluit van het college van burgemeester en wethouders van de gemeente Midden-Delfland houdende regels omtrent privacybeleid

### 1. Inleiding

De gemeente Midden-Delfland vindt het belangrijk om goede afspraken te maken met haar medewerkers over hoe zij omgaan met persoonsgegevens die zij gebruiken in de uitvoering van hun taken. Daarom stelt zij het 'Privacybeleid gemeente Midden-Delfland' op.

Persoonsgegevens zijn alle gegevens die herleidbaar zijn naar een (natuurlijk) persoon. Een persoonsgegeven kan bijvoorbeeld iemands naam zijn, een huisadraes of een e-mailadres. Ook meer indirecte gegevens kunnen persoonsgegevens zijn, zoals een bankrekeningnummer. Doorslaggevend is dat je met deze gegevens zonder al te veel inspanning een identiteit kunt vaststellen.

De gemeente verwerkt persoonsgegevens van burgers, maar ook van ondernemers, (keten)partners en medewerkers. De verwerking van deze gegevens is aan wet- en regelgeving gebonden. Alle betrokkenen moeten erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met de persoonsgegevens omgaat.

De geldende privacywetgeving, de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG) stellen kaders waarbinnen verwerking van persoonsgegevens mag plaatsvinden. Om hier handen en voeten aan te geven wordt in dit beleid uitgelegd hoe de gemeente Midden-Delfland omgaat met persoonsgegevens. Dit beleid is van toepassing op de gemeente Midden-Delfland en organisaties die uitvoering geven aan de gemeentelijke taken.

De Functionaris voor Gegevensbescherming is belast met het toezicht op de uitvoering van dit beleid.

In dit privacybeleid maakt de gemeente afspraken hoe haar medewerkers omgaan met de taken en verplichtingen die de AVG meebrengt. Gebruikte begrippen in dit beleid hebben dezelfde betekenis als in de AVG.

### 2. Kernwaarden

De gemeente heeft kernwaarden opgesteld als uitgangspunten voor het handelen van haar medewerkers. Deze kernwaarden vormen ook de basis voor de omgang met persoonsgegevens:

> **Betrouwbaar**: Inwoners zijn vaak verplicht om hun persoonsgegevens aan de gemeente te verstrekken. Bijvoorbeeld omdat zij voor een dienst (subsidie, uitkering, verstrekking) alleen bij de gemeente terecht kunnen. Zij moeten er daarom op kunnen vertrouwen dat de gemeente zorgvuldig met de persoonsgegevens omgaat. De gemeente zorgt ervoor dat de gegevens goed beveiligd zijn en dat zij alleen rechtmatig gebruikt worden.

> **Respect**: Persoonsgegevens kunnen gevoelige informatie bevatten. Daarom gaat de gemeente altijd respectvol om met deze persoonsgegevens. Persoonsgegevens worden alleen gedeeld binnen en buiten de organisatie als dat noodzakelijk is voor het uitvoeren van de taken.

> **Afspraken nakomen**: Met dit privacybeleid maakt de gemeente afspraken over hoe zij omgaat met persoonsgegevens. Medewerkers zorgen er gezamenlijk voor dat deze afspraken worden nagekomen. Dit doen zij door een cultuur te creëren waarbinnen medewerkers elkaar durven aan te spreken op overschrijdend gedrag. Maar ook door het onderwerp privacy regelmatig terug te laten komen in werkoverleggen en zo bewustwording te creëren.

> **Betrokken**: Betrokkenheid bij de inwoner houdt in dat de gemeente transparant is in de omgang met persoonsgegevens. De gemeente informeert inwoners zo veel mogelijk over waarom zij gegevens vragen en wat zij ermee doet. Dit geldt ook bij het delen van de gegevens met derden.

> **Kwaliteit**: Kwaliteit van dienstverlening houdt in dat de gemeente zorgvuldig omgaat met persoonsgegevens, maar ook dat deze correct en up-to-date zijn. De gemeente gebruikt daarom – als dat mogelijk is – brongegevens en controleert regelmatig of de persoonsgegevens die zij gebruikt nog correct zijn. Persoonsgegevens die de gemeente niet meer nodig heeft voor haar taken en waarvan de bewaartermijn is verstreken, worden (veilig) verwijderd.

### 3. Uitgangspunten

De gemeente respecteert de privacy van betrokkenen en gaat op een veilige manier met persoonsgegevens om. De gemeente hanteert daarbij de volgende uitgangspunten:

> Persoonsgegevens mogen alleen verwerkt worden als daarvoor een rechtmatige grondslag bestaat. Deze grondslagen staan in de AVG en zijn uitgewerkt in bijlage 1;
> Persoonsgegevens worden gebruikt voor het doel waarvoor ze verkregen zijn. Verdere verwerking mag alleen als het nieuwe doel in lijn is met het oorspronkelijke doel;
> Er worden niet meer persoonsgegevens verwerkt dan noodzakelijk voor het vooraf bepaalde doel. De gemeente streeft naar minimale gegevensverwerking;
> Er wordt zorgvuldig en vertrouwelijk omgegaan met persoonsgegevens. Persoonsgegevens worden voldoende beveiligd, waarbij rekening wordt gehouden met de aard van de gegevens. Deze beveiliging is vastgelegd in het informatiebeveiligingsbeleid.
> Persoonsgegevens worden niet langer bewaard dan nodig of wettelijk verplicht is. Het bewaren van persoonsgegevens kan nodig zijn om de gemeentelijke taken goed uit te kunnen oefenen of om wettelijke verplichtingen te kunnen naleven.
> In geval van uitwisseling van persoonsgegevens met externe partijen legt de gemeente afspraken vast over de eisen waar gegevensuitwisseling aan moet voldoen.

**4. Verwerkingsverantwoordelijke**
Het college van burgemeester en wethouders is verantwoordelijk voor de verwerking van persoonsgegevens door of namens de gemeente. Naast het college kent de gemeente voor enkele specifieke processen andere verantwoordelijken. Namelijk:
- De burgemeester;
- De ambtenaar van de burgerlijke stand;
- De leerplichtambtenaar;
- De heffingsambtenaar en de invorderingsambtenaar.

De gemeenteraad is zelfstandig verantwoordelijk om te voldoen aan de AVG en daarmee om haar eigen processen conform de AVG uit te voeren.

**5. Functionaris voor gegevensbescherming (FG)**
Het college van burgemeester en wethouders benoemt een functionaris voor gegevensbescherming (FG), zoals bedoeld in de AVG. De FG houdt toezicht op het privacy- en beveiligingsbeleid van de gemeente. De contactgegevens van de FG publiceert de gemeente op de gemeentelijke website.

Voor de uitoefening van zijn toezichthoudende functie beschikt de FG over alle bevoegdheden die daarvoor redelijkerwijs noodzakelijk zijn. Iedereen die namens de gemeente bij een verwerking van persoonsgegevens is betrokken, verstrekt hierover desgevraagd alle informatie aan de FG. Ook verleent die persoon medewerking die nodig is voor de uitoefening van de taak van de FG. De FG heeft toegang tot alle ruimten waar een verwerking van persoonsgegevens plaatsvindt. Tot slot is de FG bevoegd om apparatuur, programmatuur, gegevensbestanden, boeken en bescheiden te onderzoeken en zich de werking van apparatuur en programmatuur te doen tonen.

De FG rapporteert ten minste jaarlijks zijn bevindingen aan het college van burgemeester en wethouders. Hij geeft zo nodig aanbevelingen over te nemen maatregelen voor een goede bescherming van persoonsgegevens.

Bij afwezigheid van de FG treedt de Chief Information Security Officer (CISO) van de gemeente op als vervanger. Het gaat dan om werkzaamheden rondom datalekken en informatiebeveiliging. Overige werkzaamheden, zoals advisering op het gebied van privacy en contact met de Autoriteit Persoonsgegevens, neemt team Juridische Zaken over.

**6. Privacy-ambassadeurs**
Iedere afdeling benoemt een contactpersoon die aanspreekpunt is voor de FG en die het privacybeleid van de betreffende afdeling coördineert. Deze persoon wordt privacy-ambassadeur genoemd.

De taken van de privacy-ambassadeur zijn in ieder geval:
- Organiseren van voldoende bewustwordingsactiviteiten op het terrein van privacybescherming en (het melden van) datalekken;
- Adviseren over privacyaangelegenheden en het doorverwijzen van vragen hierover naar de juiste persoon binnen de organisatie;
- Bij datalekken coördineren van het onderzoek op de afdeling;
- Adviseren en informeren van de FG in de uitvoering van zijn taken. De privacy-ambassadeurs zijn de ogen en oren van de FG op de afdeling.

De privacy-ambassadeur informeert zijn afdelingsdirecteur direct wanneer sprake is van enige schending van de privacyregels.

De afdelingsdirecteur van de privacy-ambassadeur zorgt ervoor dat de privacy-ambassadeur zijn werkzaamheden naar behoren kan uitvoeren. Dit houdt in dat de privacy-ambassadeur:
- Ruimte binnen zijn werkzaamheden krijgt om de bovengenoemde taken uit te voeren en om voldoende kennis te vergaren en te behouden;
- Voldoende ondersteuning krijgt om zijn rol als privacy-ambassadeur uit te dragen binnen de afdeling.

De FG en team Juridische Zaken houden de privacy-ambassadeurs op de hoogte van relevante ontwikkelingen binnen het privacyrecht. De CISO neemt deze rol op zich voor AVG-gerelateerde zaken met betrekking tot informatieveiligheid.

### 7. Register van verwerkingen
De FG houdt namens de verwerkingsverantwoordelijke een register bij van de verwerkingen van persoonsgegevens die plaatsvinden door of namens de gemeente. Iedere procesverantwoordelijke levert informatie aan over het proces waarvoor hij verantwoordelijk is, die nodig is voor een accurate bijhouding van het register van verwerkingen.

De FG houdt toezicht op de volledigheid en rechtmatigheid van de in het register van verwerkingen opgenomen processen. Bij wijzigingen van een proces levert de procesverantwoordelijke informatie aan bij de FG die nodig is voor aanpassing van het register.

De privacy-ambassadeur toetst jaarlijks of het register van verwerkingen voor zijn afdeling nog correct en compleet is. Hij brengt hiervan verslag uit aan de FG.

### 8. Beveiliging
Een betrouwbare informatievoorziening is essentieel voor het goed functioneren van de processen binnen de gemeente. De afdelingsdirecteur draagt daarom op zijn afdeling zorg voor een adequaat beveiligingsniveau. Ze voert passende technische en organisatorische beveiligingsmaatregelen uit om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking op grond van de AVG. Hij wordt hierin ondersteund door de Chief Information Security Officer (CISO). De gemeente neemt voor beveiliging van de processen waarin persoonsgegevens worden verwerkt de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) als uitgangspunt, of enig opvolger van de BIG.

### 9. Bewaartermijnen
De gemeente bewaart persoonsgegevens niet langer dan noodzakelijk is voor de doeleinden waarvoor zij zijn verzameld of worden gebruikt. Als een bewaartermijn in een wet of op de VNG Selectielijst is geregeld, wordt die termijn gevolgd. Als er geen wettelijke regeling is die voorziet in een verplichte bewaartermijn, dan beslist de procesverantwoordelijke over een onderbouwde bewaartermijn. In het register van verwerkingen staat per verwerking de bewaartermijn van de persoonsgegevens.

### 10. Nieuwe verwerkingen
De gemeente past bij nieuwe en gewijzigde verwerkingen altijd de volgende beginselen toe:
> **Privacy by design**: Voordat een nieuwe verwerking wordt gestart stelt de procesverantwoordelijk vast of de verwerking een risico inhoudt voor de privacy van betrokkenen en hoe dit risico ondervangen wordt. Daarnaast levert de procesverantwoordelijke informatie aan die nodig is voor het register van verwerkingen bij de FG. Ook bevestigt de procesverantwoordelijke dat de medewerkers die zijn betrokken bij de nieuwe verwerking op de hoogte zijn van de relevante privacyafspraken, waaronder dit privacybeleid en het Protocol Datalekken. Wanneer sprake is van een verwerking met een hoog risico, bijvoorbeeld wanneer bijzondere persoonsgegevens worden verwerkt, wordt een gegevensbeschermingseffectbeoordeling (DPIA) uitgevoerd. De Privacy-ambassadeur coördineert de uitvoering van de DPIA;
> **Privacy by default**: De gemeente treft technische en organisatorische maatregelen om ervoor te zorgen dat alleen persoonsgegevens verwerkt worden die noodzakelijk zijn voor het specifieke doel dat zij wil bereiken. Dit betekent ook dat in applicaties standaard de meest privacyvriendelijke opties worden gekozen (vinkjes om toestemming te verlenen staan bijvoorbeeld niet automatisch aangevinkt).

## 11. Datalekken

Wanneer een medewerker een (beveiligings)incident met persoonsgegevens ontdekt, meldt hij direct bij de Servicedesk en zijn privacy-ambassadeur. De privacy-ambassadeur informeert direct zijn afdelingsdirecteur en de FG.

De afdelingsdirecteur van de betreffende afdeling is verantwoordelijk voor het dichten van het datalek in samenwerking met de CISO en de betreffende applicatiebeheerder(s). Bij het vermoeden van een datalek worden de volgende stappen genomen:

> Stap 1: De FG en de CISO beoordelen of het datalek meldenswaardig is, zoals bedoeld in de AVG;
> Stap 2: Indien het datalek meldenswaardig is, meldt de FG het datalek direct aan de nationale toezichthouder, de Autoriteit Persoonsgegevens;
> Stap 3: De Afdelingsdirecteur van de betreffende afdeling is verantwoordelijk voor de onverwijlde melding aan betrokkenen;
> Stap 4: De CISO ziet er samen met de Chief Information Officer (CIO) op toe dat het datalek op adequate wijze wordt gedicht.

De CISO houdt namens de verwerkingsverantwoordelijke een logboek bij waarin datalekken zijn opgenomen. In dit logboek worden – naast gemelde datalekken – ook datalekken opgenomen die niet bij de Autoriteit Persoonsgegevens en/of de betrokkene zijn gemeld.

*Een uitgebreide beschrijving van het proces datalekken, de bijbehorende modeldocumenten en de handleiding over datalekken staan op intranet.*

## 12. Privacyrechten

Betrokkenen hebben het recht om geïnformeerd te worden over de verwerking van hun persoonsgegevens en om te beschikken over die gegevens. De gemeente stelt hiervoor processen op en informeert inwoners en medewerkers over deze rechten.

**a) Klachten**

Een betrokkene kan een klacht indienen, als hij in de veronderstelling is dat de gemeente onzorgvuldig is omgegaan met zijn privacy of zijn persoonsgegevens ten onrechte heeft verwerkt. De klacht wordt na binnenkomst direct aan de FG gestuurd voor verdere behandeling. De gemeente handelt een klacht volgens de klachtenregeling af.

Wanneer een betrokkene het niet eens is met de afhandeling van de klacht door de gemeente, kan hij een klacht indienen bij de Autoriteit Persoonsgegevens. De gemeente wijst de betrokkene op deze mogelijkheid bij de afhandeling van de klacht. De mogelijkheid wordt ook benoemd in het privacystatement dat te raadplegen is op de website van de gemeente.

**b) Recht op informatie**

De gemeente informeert betrokkenen adequaat over de verwerkingen die de gemeente uitvoert en de rechten die de betrokkenen hebben. De gemeente plaatst alle relevante informatie op haar website. Ook deelt de gemeente dit privacybeleid actief met alle medewerkers.

**c) Recht op inzage**

Iedere betrokkene kan de gemeente vragen om inzage in de persoonsgegevens die de gemeente van hem of haar heeft verzameld. Een verzoeker moet zich identificeren, voordat het verzoek om inzage in behandeling wordt genomen. Het moet namelijk vastgesteld worden of de informatie aan de juiste persoon wordt verstrekt.
Identificatie vindt plaats door gebruik van het digitale aanvraagformulier met DigiD op de website van de gemeente of door het tonen van een geldig identiteitsbewijs aan de balie op het gemeentehuis.

Nadat aan de identificatieplicht is voldaan, krijgt de betrokkene binnen de gestelde termijn informatie van de gemeente over het al dan niet verwerken van zijn persoonsgegevens. Als de gemeente persoonsgegevens van de betrokkene verwerkt, ontvangt hij informatie over:

- Het doel van de verwerking;
- De categorieën van persoonsgegevens;
- De (categorieën) van eventuele ontvangers;
- De bewaartermijnen;
- De rechten die de verzoeker heeft om gegevens te rectificeren en te wissen. De rechten om de verwerking van de persoonsgegevens te beperken of bezwaar tegen de verwerking van de verzoeker te maken;

- Of er gegevens van de betrokkene uit andere bronnen dan van de betrokkene zelf worden gehaald, en zo ja, welke;
- Welke passende waarborgen zijn genomen indien de persoonsgegevens buiten de grenzen van Europese Unie (EU) of Europese Economische Ruimte (EER) zijn verwerkt.

Op verzoek van de betrokkene kan de gemeente een kopie van de persoonsgegevens verstrekken. Uitgezonderd van inzage zijn persoonlijke afwegingen of interne adviezen van medewerkers.

De gemeente wijst de betrokkene op de mogelijkheid een klacht in te dienen over de verwerking van zijn persoonsgegevens, zowel bij de gemeente als bij de Autoriteit Persoonsgegevens.

De gemeente reageert binnen één maand op het verzoek van de betrokkene. Wanneer het verzoek complex is, kan de gemeente de termijn met twee maanden verlengen. De betrokkene wordt daarvan zo snel mogelijk, maar uiterlijk binnen één maand na binnenkomst van het verzoek op de hoogte gesteld.

*Een uitgebreide beschrijving van het proces inzage, de bijbehorende modeldocumenten en de handleidingen voor de coördinatoren en contactpersonen staan op intranet.*

**d) Recht op verbetering, aanvulling, verwijdering of afscherming**
De betrokkene kan vragen om zijn persoonsgegevens te wijzigen, te verbeteren, aan te vullen, te verwijderen of af te schermen. Ook na binnenkomst van een van deze verzoeken wordt aan de betrokkene gevraagd zich eerst te identificeren. Dit hoeft niet als de betrokkene al eerder een verzoek heeft ingediend en het vaststaat dat het om dezelfde persoon gaat en van dezelfde communicatiemiddelen gebruik wordt gemaakt als in het eerste verzoek.

De gemeente reageert binnen één maand op het verzoek van de betrokkene. Wanneer het verzoek complex is, kan de gemeente de termijn met maximaal twee maanden verlengen. De betrokkene wordt daarvan zo snel mogelijk, maar uiterlijk binnen één maand na binnenkomst van het verzoek op de hoogte gesteld.

**e) Recht op  dataportabiliteit**
De betrokkene kan de gemeente verzoeken om zijn persoonsgegevens te verstrekken in een vorm die het eenvoudig maakt zijn gegevens te hergebruiken. Bijvoorbeeld om door te geven aan een andere organisatie. Het gaat uitsluitend om persoonsgegevens die de betrokkene zelf aan de gemeente heeft verstrekt, die de gemeente verwerkt met toestemming van de betrokkene of voor de uitvoering van een overeenkomst met de betrokkene. De gemeente verstrekt deze gegevens in een gestructureerd, veelgebruikt en machine leesbaar formaat. De betrokkene moet zich altijd legitimeren voordat de gemeente het verzoek om gegevens over te dragen uitvoert. Het verzenden van persoonsgegevens naar verzoeker of een andere organisatie doet de gemeente op een veilige manier, bijvoorbeeld door gebruik van CryptShare.

De gemeente reageert binnen één maand op het verzoek van de betrokkene. Wanneer het verzoek complex is, kan de gemeente de termijn met maximaal twee maanden verlengen. De betrokkene wordt daarvan zo snel mogelijk, maar uiterlijk binnen één maand na binnenkomst van het verzoek op de hoogte gesteld.

**f) Recht van bezwaar**
Een betrokkene kan bezwaar maken tegen de verwerking van zijn persoonsgegevens. Betrokkene kan bijzondere persoonlijke omstandigheden aanvoeren op grond waarvan de verwerking van een gegeven onredelijk bezwarend is. Dit recht kan alleen ingeroepen worden bij persoonsgegevens die verzameld zijn op de grondslag ‘taak van algemeen belang’ of ‘gerechtvaardigd belang’.

De gemeente reageert binnen één maand op het verzoek van de betrokkene. Wanneer het verzoek complex is, kan de gemeente de termijn met maximaal twee maanden verlengen. De betrokkene wordt daarvan zo snel mogelijk, maar uiterlijk binnen één maand na binnenkomst van het verzoek op de hoogte gesteld.

‘Bezwaar’ in deze context is niet gelijk aan het bezwaar in het kader van de Algemene wet bestuursrecht (Awb). De regels rondom bezwaar in de Awb zijn hier dan ook niet van toepassing.

## 13. Uitwisseling van persoonsgegevens
Het delen van persoonsgegevens met andere organisaties, maar ook met andere afdelingen binnen de gemeente is een verwerking van persoonsgegevens. Hierop zijn dus alle voorwaarden van toepassing die de AVG stelt aan een verwerking. Voorafgaand aan de uitwisseling van persoonsgegevens wordt in ieder geval vastgesteld of er sprake is van een grondslag voor de uitwisseling en of er voldoende

waarborgen zijn voor de bescherming van de privacy van betrokkenen. Hiervoor worden de volgende procedures gevolgd:

> Als de gemeente persoonsgegevens verstrekt aan een *nieuwe verantwoordelijke* (de ontvangende partij is zelf verantwoordelijk voor de verwerking van de persoonsgegevens) buiten de gemeente sluit zij een **dataleveringsovereenkomst** af met de ontvangende partij. Hiervoor wordt gebruik gemaakt van het 'model dataleveringsovereenkomst', beschikbaar gesteld door team Juridische Zaken. De betrokken afdelingsdirecteur ondertekent namens het college de overeenkomst. Voorafgaand aan de ondertekening biedt de afdelingsdirecteur de overeenkomst ter kennisneming aan, aan de FG;
> Als de gemeente persoonsgegevens verstrekt aan een *verwerker* (een partij die in opdracht van de gemeente persoonsgegevens verwerkt) sluit zij een **verwerkersovereenkomst** met de ontvangende partij. Hiervoor wordt gebruik gemaakt van het 'model verwerkersovereenkomst', beschikbaar gesteld door team Juridische Zaken. De betrokken afdelingsdirecteur ondertekent namens het college de overeenkomst. Voorafgaand aan de ondertekening biedt de afdelingsdirecteur de overeenkomst ter kennisneming aan, aan de FG;
> Als een afdeling binnen de gemeente persoonsgegevens verstrekt aan een *andere afdeling* (collega's die een andere taak uitvoeren) binnen de gemeente en deze verstrekking niet al op een andere manier is vastgelegd, vult de ontvangende afdeling een **dataleveringsformulier** in. De afdelingsdirecteur van de verstrekkende afdeling ondertekent het formulier. Het ondertekende dataleveringsformulier wordt ter kennisneming aangeboden aan de FG. Wanneer het gaat om een repeterende verstrekking van persoonsgegevens wordt het dataleveringsformulier eenmalig ingevuld en ondertekend.

De gemeentesecretaris is verantwoordelijk voor de opslag van de documenten.

### 14. Gebruik van beeldmateriaal voor promotionele doeleinden

De gemeente gebruikt beeldmateriaal (foto's en filmpjes) ter onderbouwing van haar dienstverlening en communicatie naar de inwoners. Op de gebruikte beelden staan soms personen herkenbaar in beeld. Er is in dat geval sprake van verwerking van persoonsgegevens. Om deze verwerking zorgvuldig te laten plaatsvinden, neemt de gemeente de volgende regels in acht:

> Voor het gebruik van portretfoto's voor extern gebruik vraagt de gemeente (de fotograaf) toestemming aan de betrokkenen. Dit zijn foto's waarop 1 of een klein aantal personen groot in beeld wordt gebracht en zij het onderwerp van de foto zijn;
> Voor foto's waarop personen staan, maar waar niet een of een klein aantal personen als het onderwerp van de foto aangeduid kunnen worden (zoals een straatbeeld, een groep sportende mensen etc.) vraagt de gemeente of de fotograaf geen individuele toestemming, maar maakt zij een afweging van de schending van de privacy en het nagestreefde doel. Dit houdt in dat de gemeente rekening houdt met de herleidbaarheid van de personen naar datum en plaats, met eventuele kwetsbare groepen en met de (on)omkeerbaarheid van de plaatsing van het beeldmateriaal. Bij twijfel vraagt de gemeente de FG om advies;
> De gemeente gebruikt het beeldmateriaal niet als een geportretteerde of gefilmde aangeeft bezwaar te hebben tegen het gebruik. Reeds geplaatst beeldmateriaal verwijdert de gemeente direct.
> Wanneer beeldmateriaal wordt gebruikt ter illustratie van een onderwerp dat gevoelig ligt in de maatschappij gebruikt de gemeente nooit beeldmateriaal van personen die herkenbaar in beeld zijn gebracht. De gemeente vraag de FG om advies.
> De gemeente houdt altijd rekening met de privacy van de geportretteerde, bij gebruik van beeldmateriaal waarop personen herkenbaar in beeld zijn gebracht. Hierbij is het uitgangspunt dat het beeldmateriaal niet voor dat doel wordt gebruikt als de kans reëel is dat de geportretteerde negatief verrast is door het gebruik ervan.

### 15. Inzet van camera's in de openbare ruimte

Binnen de gemeente wordt gebruik gemaakt van camera's in de openbare ruimte (kort gezegd: in de openbare ruimte van het gemeentehuis, op straten, pleinen, fietspaden, wegen etc.). Dit gebeurt door de gemeente, maar ook door derden. Het doel van de camera-inzet is doorgaans de bescherming van personeel, burgers en eigendommen.

Camera's registreren bijna altijd persoonsgegevens in de vorm van beelden die geplaatst kunnen worden in een bepaalde tijd en plaats. Dit kan een (grote) inbreuk zijn op de privacy van betrokkenen en daarom is de AVG hierop van toepassing.
De Autoriteit Persoonsgegevens houdt toezicht op de naleving van de AVG.

De gemeente is zich ervan bewust – gelet op de inbreuk op de privacy van betrokkenen - dat de inzet van camera's een laatste middel moet zijn om een doel te bereiken. De waarborgen voor de inzet staan

in het 'Protocol camera's gemeente Midden-Delfland'. Inzet van camera's door de gemeente vindt alleen plaats conform dit gemeentelijke protocol en een door de FG goedgekeurde gegevensbeschermingseffectbeoordeling (DPIA).

Als een derde partij gebruik wil maken van cameratoezicht in de openbare ruimte, informeert de gemeente deze partij over de geldende privacybepalingen via de website en in directe communicatie.

### 16. Digitale verzending van persoonsgegevens

De gemeente is zich ervan bewust dat het (onbeveiligd) digitaal verzenden van persoonsgegevens een ernstig risico meebrengt voor de bescherming van die gegevens. Daarom treft de gemeente maatregelen om dit risico te beperken.
Uitgangspunt is om persoonsgegevens zo mogelijk uit de bron te verkrijgen. Dit betekent dat de gemeente persoonsgegevens die nodig zijn voor een gemeentelijke taak direct bij de bron opvraagt, zoals de Basisregistratie Personen (BRP). Op die manier borgt de gemeente de kwaliteit van de gegevens en voorkomt zij onveilige verzending.

Indien de verzending van persoonsgegevens binnen de gemeente noodzakelijk is, maakt de gemeente hiervoor altijd voor verzending én ontvangst gebruik gemaakt van een @middendelfland.nl e-mailadres. De verzendende medewerker is er alert op dat e-mailadressen automatisch afgemaakt kunnen worden en controleert voor verzending of de juiste geadresseerde staat vermeld.

Er vindt geen verzending van persoonsgegevens plaats naar een mailbox waarvan onbekend is welke ontvangers de mailbox inzien (zoals groepsmailboxen).

Voor verzending van persoonsgegevens naar partijen buiten de gemeente, maakt de gemeente gebruik van beveiligde e-mail (CryptShare of Zorgmail). Deze mailsystemen zijn beveiligd met een wachtwoord dat via een andere weg aan de ontvanger van de e-mail wordt verzonden.

### 17. Privacybewuste organisatie

Een privacybewuste organisatie komt alleen tot stand als alle medewerkers op hun eigen niveau kennis hebben van de regels over het omgaan met persoonsgegevens. De gemeente zorgt daarom voor een doorlopend aanbod van bewustwording op dit onderwerp, maar verwacht ook van haar medewerkers dat zij zich inspannen om deze kennis in de praktijk te brengen. Vragen, opmerkingen en klachten over de omgang met persoonsgegevens leggen medewerkers neer bij de FG.

Iedere afdelingsdirecteur is in samenwerking met de privacy ambassadeur verantwoordelijk voor het opstellen van een plan waarin activiteiten zijn opgenomen voor doorlopende bewustwording over privacy binnen de afdeling. Dit plan kan onderdeel uitmaken van de reguliere afdelingsjaarplannen. Hierin is in ieder geval opgenomen:

> Een jaarlijkse medewerkersbijeenkomst over privacy;
> De manier van communiceren over belangrijke ontwikkelingen binnen het privacyrecht;
> De manier waarop nieuwe medewerkers op de hoogte worden gebracht van de privacyregels, waaronder dit privacybeleid en het Protocol Datalekken;
> Een jaarlijkse controle van het register van verwerkingen bij de proceseigenaren.

### 18. Doorgifte persoonsgegevens buiten de EU/EER

De gemeente verstrekt geen persoonsgegevens naar landen buiten de EU/EER en ziet er op toe dat partijen die door de gemeente worden ingeschakeld dit ook niet doen. Wanneer hiertoe toch een noodzaak bestaat vraagt de gemeente voorafgaand aan de verstrekking advies aan de FG en treft zij passende maatregelen om de privacy van de betrokkenen te borgen.

### 19. Tot slot

Vragen over dit privacybeleid of over privacy in het algemeen worden voorgelegd aan de FG via het e- mailadres FG@middendelfland.nl.
De FG controleert jaarlijks of aanpassingen nodig zijn.

*Aldus vastgesteld door het college van burgemeester en wethouders van de gemeente Midden-Delfland op 20 november 2018,*
*Martien Born*
*gemeentesecretaris*
*Arnoud Rodenburg*
*burgemeester*

## Bijlage 1 Toelichting op grondslagen voor rechtmatige gegevensverwerking

De AVG schrijft voor dat verwerking van persoonsgegevens alleen mag plaatsvinden als hiervoor een rechtmatige grondslag bestaat. De AVG schrijft deze grondslagen uitputtend voor:

> **Toestemming van de betrokkene**: wanneer een betrokkene uitdrukkelijk toestemming heeft gegeven voor het gebruik van zijn gegevens, dan mogen die gegevens voor dat doel worden gebruikt. Er moet dus voorafgaand aan de toestemming wel duidelijk omschreven zijn welk doel de gemeente voor ogen heeft. En er moet geïnformeerde en nadrukkelijke toestemming zijn ('wanneer u niet reageert, geeft u toestemming' is dus niet toegestaan). Toestemming kan zelfstandig worden gegeven vanaf 16 jaar. Tussen de 14 en 16 jaar worden zowel de ouders als het kind om toestemming gevraagd. Let er bij toestemming altijd op dat er in beginsel een ongelijke verhouding is tussen de overheid en de burger, waardoor sprake kan zijn van niet vrij gegeven toestemming. Toestemming kan dus alleen als grondslag worden gebruikt wanneer de burger niet benadeeld wordt als hij 'nee' zegt. Ook kan toestemming altijd worden ingetrokken. Vanaf dat moment komt de grondslag van gegevensverwerking te vervallen en moet de verwerking stop gezet worden.

> **Uitvoeren van een overeenkomst met de betrokkene**: wanneer een overeenkomst wordt gesloten met een persoon dan kunnen van die persoon de persoonsgegevens worden gebruikt die nodig zijn voor de uitvoering van die overeenkomst. Deze grondslag houdt dus niet in dat er een overeenkomst wordt gesloten om over derden persoonsgegevens te verwerken;

> **Uitvoeren van een wettelijke plicht**: de wet kan voorschrijven dat bepaalde persoonsgegevens moeten worden verwerkt;

> **Uitvoeren van een overheidstaak** (een taak van algemeen belang): de gemeente voert taken uit die voorbehouden zijn aan de overheid (bijvoorbeeld de uitgifte van een rijbewijs). Als het nodig is om voor die taak persoonsgegevens te gebruiken, dan is dat toegestaan;

> **Vitaal belang**: in geval van een levensbedreigende situatie is het toegestaan om de persoonsgegevens van een derde te delen met bijvoorbeeld de hulpdiensten. Deze grondslag kan dus maar heel sporadisch worden gebruikt;

> **Een gerechtvaardigd belang**: wanneer geen van de andere grondslagen van toepassing is op de verwerking kan het gerechtvaardigd belang als grondslag worden ingeroepen. Deze grondslag houdt in dat de organisatie een afweging maakt tussen de schending van de privacy van betrokkenen en het belang van het doel dat de organisatie nastreeft met de verwerking. Deze grondslag mag een organisatie bijvoorbeeld gebruiken bij taken die vallen onder de 'reguliere bedrijfsvoering' van die organisatie. Een brede en enigszins vage grondslag dus.
Voor de gemeente is van belang dat deze grondslag niet toegepast mag worden door overheidsorganen. Overheidsorganen hebben immers hun vastgestelde taken en moeten deze niet uitbreiden met eigen organisatiedoeleinden. Een uitzondering hierop is opgenomen in de Uitvoeringswet AVG: wanneer een overheidsorgaan een taak uitvoert in het kader van zijn bedrijfsvoering (zoals de uitgifte van een gebruikersnaam en wachtwoord) kan hiervoor wel de grondslag gerechtvaardigd belang worden gebruikt. Dit betreft dus alleen die werkzaamheden die nodig zijn voor de bedrijfsvoering en die niet zijn voorbehouden aan overheden.