

Privacybeleid

Het college van burgemeester en wethouders (verder te noemen: het college);

gelet op de AVG en de UAVG,

overwegende dat het wenselijk is om beleid vast te stellen voor de wijze waarop de raad bij de uitoefening van zijn bevoegdheden omgaat met de verwerking van persoonsgegevens,

hebben besloten het volgende vast te stellen:

Privacybeleid

Privacy is een grondrecht en een voorwaarde om vrij te zijn in wie je bent en wat je doet.

Privacy gaat erover dat mensen regie houden over hun gegevens en dat bijvoorbeeld één foto waar een persoon als dronken tiener op staat, niet de toekomst van deze persoon bepaalt .

Het gaat erom dat we niet continu gevolgd worden, dat onze medische gegevens veilig zijn, dat we iets kunnen doen tegen een automatisch genomen besluit over ons.

Het gaat over zeggenschap over onze eigen persoonsgegevens.

Met deze uitspraken geeft de Autoriteit Persoonsgegevens (AP) goed aan waarom privacy in onze samenleving van belang is. Dit grondrecht, dat is vastgelegd in diverse internationale verdragen en ook in onze grondwet, is binnen EU-verband vertaald naar de Algemene Verordening Gegevensbescherming, die vanaf 28 mei 2018 rechtstreeks als wet geldt. In dit document geven wij richting aan de vertaling van de uitgangspunten van bescherming van persoonsgegevens in onze organisatie.

1. Inleiding

Binnen gemeente Culemborg (hierna genoemd: gemeente) wordt veel gewerkt met persoonsgegevens van burgers, medewerkers en (keten)partners. Persoonsgegevens worden van burgers voornamelijk verzameld voor het goed uitvoeren van de gemeentelijke (meestal wettelijke) taken, van medewerkers waar het gaat om werkgeverstaken en van (keten)partners van burgers waar het nodig is om met andere partijen samen te werken. Betrokkenen moeten erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met haar persoonsgegevens omgaat.

Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds meer digitale overheid stellen hogere eisen aan de bescherming van persoonsgegevens en privacy. Het dataverkeer neemt toe en er worden meer gegevens verzameld en gedeeld. De hoeveelheid gevoelige informatie van personen is vrij groot en neemt toe, evenals de risico's van bijvoorbeeld cybercrime. De samenleving wordt steeds kritischer en burgers hebben steeds meer behoefte aan rechten om inzicht te krijgen in de verwerking van hun persoonsgegevens.

Het doel van de Algemene Verordening Gegevensbescherming (AVG) is met name om een goede bescherming van persoonsgegevens te bieden en het vrije verkeer van persoonsgegevens binnen de Europese Unie te waarborgen.

In dit beleid wordt uitgewerkt hoe de gemeente met de bescherming van persoonsgegevens omgaat. Na de paragrafen in dit hoofdstuk waarin wij onder andere kort in algemene zin ingaan op het verwerken van persoonsgegevens en het juridisch kader komen achtereenvolgens aan de orde: de algemene uitgangspunten van het privacybeleid, het privacymanagement, informatiebeveiliging, samenwerking met andere partijen, bewustwording/communicatie/evaluatie en tot slot toezicht/rapportage.

1.1 Wat houdt het verwerken van persoonsgegevens in?

Onder persoonsgegevens verstaan we alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de 'betrokkene'). Dit betekent dat deze informatie direct over iemand gaat of naar deze persoon te herleiden is.

Er is al snel sprake van het verwerken van persoonsgegevens. Onder andere verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, combineren, afschermen, wissen of vernietigen van gegevens: het valt allemaal onder het verwerken van persoonsgegevens.

Dus alleen al het 'bekijken' van informatie is een verwerking die valt onder de AVG. Dit geldt ook voor het samenstellen van een nieuwe verwerking uit meerdere bronssystemen (het combineren van gegevens). Het is van belang om hiervoor de juiste rechtmatige grondslag te hebben.

1.2 Wie verwerken persoonsgegevens?

In de gehele gemeentelijke organisatie worden persoonsgegevens verwerkt. Dit varieert van het gebruik van een beperkte gegevensverzameling, door bijvoorbeeld het team Projecten en Regie Ruimte, tot het gebruik van grote gegevensverzamelingen, zoals bij het team Burgerzaken (Basisregistratie Personen (BRP)).

De gegevens worden in de basis in de eigen (vak)administratiesystemen verwerkt, maar kunnen ook voor een deel direct of indirect via het centrale gegevensmagazijn worden verwerkt. In dit centrale gegevensmagazijn zitten (binnengemeentelijke) persoonsgegevens (BRP) en BAG-gegevens. Daarnaast kunnen persoonsgegevens in een datawarehouse worden opgenomen. Persoonsgegevens worden dan vanuit verschillende vakapplicaties samengevoegd om op die manier managementrapportages en beleidsinformatie op te stellen.

1.3 Opstellen privacybeleid

De gemeente hecht veel waarde aan het zorgvuldig, rechtmatig en veilig verwerken van persoonsgegevens. Bestuur en management hebben een primaire verantwoordelijkheid in het waarborgen van de privacy.

Dit beleid is van toepassing op de gehele organisatie, in alle processen, onderdelen, objecten en gegevensverzamelingen van de gemeente. Het is in lijn met het algemene beleid van de gemeente en de relevante lokale, nationale en Europese wet- en regelgeving. In dit algemene privacybeleid staan kaders beschreven voor het verwerken van persoonsgegevens, de bescherming van deze gegevens en de omgang ermee.

Dit beleid is richtinggevend en kaderstellend en wordt aangevuld met onderwerpspecifieke beleidsdocumenten voor privacy op tactisch niveau en werkinstructies op operationeel niveau (bv. privacybeleid in het sociaal domein). Verder worden naar aanleiding van dit beleid werkprocessen opgesteld en vastgesteld die als handvat fungeren om het beleid in de dagelijkse praktijk toe te passen.

Het verwerken van persoonsgegevens moet gebeuren in overeenstemming met de wet en op behoorlijke wijze. Dit privacybeleid geeft daar de richtlijnen voor. Het privacybeleid heeft betrekking op de persoonsgegevens van personen van wie de gemeente gegevens verwerkt of laat verwerken en is van toepassing op alle taken en processen waarvoor de gemeente verantwoordelijk is. Hieronder valt ook de uitwisseling van persoonsgegevens door de gemeente. Daarnaast maakt de gemeente op een aantal terreinen aparte samenwerkingsafspraken met haar partners.

In de uitvoering van dit privacybeleid handelt het college als volgt:

1. Het beschermt de inwoners tegen risico's van de informatiemaatschappij;
2. Het draagt bij aan maatschappelijk vertrouwen en draagvlak;
3. Het kan met vertrouwen verantwoording afleggen aan de raad, waar nodig de Autoriteit Persoonsgegevens of de rechter;
4. Het beheerst gemeentelijke afbreuk- en aansprakelijkheidsrisico's;
5. Het speelt adequaat in op de technologische en wettelijke ontwikkelingen.

1.4 Juridisch kader

Bij de verwerking van persoonsgegevens staat respect voor de persoonlijke levenssfeer van de betrokkene(n) voorop. De AVG biedt hiervoor het wettelijk kader, samen met de Uitvoeringswet Algemene Verordening Gegevensbescherming.

Als algemene regel geldt dat persoonsgegevens op een behoorlijke en zorgvuldige manier moeten worden verwerkt. Degene die verantwoordelijk is voor de gegevensverwerking moet daarbij transparant zijn. De AVG bepaalt verder dat persoonsgegevens alleen voor een specifiek omschreven doel mogen worden verwerkt en niet voor andere doelen dan waarvoor zij verzameld zijn. Daarbij bepaalt de AVG

dat deze gegevens alleen mogen worden verwerkt als dat noodzakelijk is om het specifiek beschreven doel te bereiken en dat er zo min mogelijk gegevens worden verwerkt. Dat houdt ook in dat persoonsgegevens niet langer mogen worden bewaard dan noodzakelijk is voor het doel waarvoor ze zijn verzameld.¹

De AVG is een algemene wet, met algemene bepalingen en uitgangspunten. In specifiekere wetten (bijvoorbeeld de Jeugdwet, de Wmo, de Participatiewet) zijn ook bepalingen rond verwerkingen van persoonsgegevens opgenomen.

De bepalingen in specifieke (sectorale) wetgeving over de verwerking van persoonsgegevens geven een specifieke invulling van de bepalingen van de AVG. Zo mogen bijvoorbeeld medische gegevens alleen worden verwerkt indien hier een wettelijke grondslag voor is; deze wetten geven dan die grondslag. Maar dat neemt niet weg dat de algemene uitgangspunten vanuit de AVG, zoals 'niet meer dan nodig', 'alleen indien nodig' en 'niet langer dan nodig', nog steeds gelden en dienen te worden vertaald naar werkprocessen.

1.5 Raakvlakken en overlap met andere beleidsthema's

Het privacybeleid van de gemeente heeft raakvlakken met andere beleidsthema's of vertoont hiermee overlap.

Integriteitsbeleid

Privacybeleidsvoering is wettelijk gekoppeld aan de beginselen van behoorlijk bestuur en is daarmee ondersteunend aan de Gedragscode Gemeente Culemborg.

Kwaliteitsbeleid

Privacybeleid richt zich in belangrijke mate op het waarborgen van een kwalitatief goede administratieve organisatie. Een kwalitatief goede administratie is randvoorwaardelijk voor een klantgerichte en klantvriendelijke gemeentelijke taakuitoefening en goed werkgeverschap ('de mens centraal').

Continuïteits- en risicomanagement

Continuïteits- en risicomanagement is gericht op het tegengaan van afbreuk- en aansprakelijkheidsrisico's en het voorkomen dat werkprocessen spaak lopen.

Dit zou bij de desbetreffende gegevensverwerkingen kunnen leiden tot inbreuken op de bescherming van persoonsgegevens.

Informatiebeveiliging

Het beschermen van persoonsgegevens kan niet geborgd worden zonder adequate informatiebeveiliging. Het privacybeleid hangt daarom samen met het informatiebeveiligingsbeleid.

2. Privacybeleid

2.1 Visie op gegevensbescherming

De gemeente wil dicht bij de burger staan. Zij wil de burger begrijpen en waar mogelijk zorgen voor maatwerk. Ze creëert ruimte voor initiatieven vanuit de burgers en is omgevingsbewust.

Om de burger te kunnen helpen is het verwerken van gegevens nodig. Bij het verwerken van persoonsgegevens gaat de gemeente op een veilige manier met deze gegevens om en respecteert zij de privacy van de betrokkenen. Daarbij zorgt ze ervoor dat de burgers hun privacyrechten kunnen uitoefenen.

2.2 Uitgangspunten privacy

De gemeente houdt zich bij het verwerken van persoonsgegevens conform de AVG aan de volgende uitgangspunten²:

Rechtmatige grondslag

De gemeente mag alleen persoonsgegevens verwerken indien hiervoor een rechtmatige grondslag bestaat. Deze rechtmatige grondslag is in de regel gelegen in de uitoefening van haar taken van algemeen belang/uitoefening van openbaar gezag.

In sommige gevallen verwerkt ze gegevens om een overeenkomst uit te voeren of op basis van toestemming.

1) Deze algemene uitgangspunten zijn terug te vinden in de artikelen 5 en 6 van de AVG en de uitgangspunten inzake transparantie in de artikelen 13 en 14 van de AVG. Beide onderdelen worden in paragraaf 2.2 nader uitgewerkt.

2) Zie in dezen de artikelen 5 en 6 van de AVG.

Ten aanzien van het gebruik van de website verwerkt de gemeente persoonsgegevens voor de uitvoering van wettelijke verplichtingen (informatievoorziening aan het publiek) of op basis van een gerechtvaardigd belang (van administratieve aard³). In sommige gevallen gebeurt dit op basis van toestemming (bijvoorbeeld voor het plaatsen van toestemmingsplichtige cookies).

De gemeente verwerkt vanuit haar wettelijke taken ook bijzondere persoonsgegevens, zoals gegevens over de gezondheid voor de aanvraag van een hulpmiddel in het kader van de Wmo.

In de specifieke wetten is hiervoor dan de rechtmatige grondslag gegeven. Is deze grondslag er niet, dan vindt een dergelijke verwerking niet plaats. De gemeente is ook wettelijk bevoegd, op grond van de Wet algemene bepalingen burgerservicenummer (Wabb), om het burgerservicenummer (BSN) te verwerken voor overheidstaken.⁴

Doelbinding

Met doelbinding wordt bedoeld dat gegevens alleen worden verwerkt voor het doel waarvoor ze zijn verzameld. Als gegevens toch voor andere doelen worden gebruikt, wordt beoordeeld of dit nieuwe doel verenigbaar is met het oorspronkelijke doel van verzamelen van de gegevens.⁵

De gemeente verwerkt alleen gegevens voor de doelen waarvoor ze van de burgers verkregen zijn en zorgt ervoor dat de persoonsgegevens alleen voor deze doelen worden verwerkt.

Persoonsgegevens worden veelal verwerkt in vakapplicaties. Applicaties zijn veelal verbonden met andere applicaties. Zo is de applicatie van het Sociaal Domein verbonden met de applicatie van de afdeling Financiën in verband met het doen van betalingen. Hierbij worden persoonsgegevens uitgewisseld. Ook hiervoor gelden de regels van de AVG (bijvoorbeeld 'alleen indien nodig' en 'niet meer dan nodig'). Om dit goed in beeld te krijgen en te houden beschikt de gemeente over een geactualiseerd applicatielandschap.

Transparantie

De gemeente is transparant over hoe ze persoonsgegevens verwerkt.⁶ Hierdoor weten burgers en personen die benaderd worden dat de persoonsgegevens door de gemeente worden verwerkt, waarom dit gebeurt en welke maatregelen genomen worden om zorgvuldig met de gegevens om te gaan.

De belangrijkste manieren om betrokkenen te informeren over de verwerking van persoonsgegevens zijn:

- het geven van algemene informatie bij inschrijving en op de website;
- het geven van aanvullende informatie bij het aanvragen van specifieke diensten;
- het geven van een cookiemelding op alle gemeentelijke websites en het hebben van een privacyverklaring, inclusief cookieverklaring;
- het bieden van laagdrempelige mogelijkheden om inzage te krijgen in de verwerking van persoonsgegevens.

Betrokkenen worden in ieder geval geïnformeerd over:

- wie verantwoordelijk is voor de gegevensverwerking met contactgegevens;
- de contactgegevens van de Functionaris Gegevensbescherming;
- de doeleinden en rechtsgrond(en) van de gegevensverwerking;
- (indien van toepassing:) de ontvangers;
- (indien van toepassing:) nadere informatie met betrekking tot eventuele doorgifte van persoonsgegevens naar een derde land of internationale organisatie;
- hoelang gegevens bewaard worden;
- hoe wordt omgegaan met de rechten van betrokkenen.

Dataminimalisatie en proportionaliteit (niet meer dan nodig, alleen indien nodig, niet langer dan nodig)

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

3) *Let op: het gebruik van 'gerechtvaardigd belang' als grondslag is zeer beperkt en mag niet leiden tot vergaande verwerking van persoonsgegevens binnen de organisatie.*

4) *Dit is in overeenstemming met het bepaalde in artikel 87 AVG en artikel 46 van de Uitvoeringswet AVG.*

5) *Zie artikel 6 lid 4 AVG.*

6) *Verplichting op grond van de artikelen 13 en 14 van de AVG.*

Als de gemeente de gegevens niet meer nodig heeft, vernietigt zij deze, tenzij er een wettelijke verplichting is om de gegevens langer te bewaren (niet langer dan nodig).

Soms worden bewaartermijnen genoemd in specifieke wetten waarvoor gegevensverwerking nodig is; in andere gevallen bepaalt de Archiefwet de bewaartermijnen. De gemeente vernietigt in die gevallen de gegevens zodra de wettelijke bewaartermijn en/of de termijn uit de selectielijst van de VNG is afgelopen.

Vóór het verwerken van de gegevens bepaalt de gemeente of het doel van de verwerking niet op een andere, minder ingrijpende manier bereikt kan worden dan door het verwerken van de persoonsgegevens (subsidiariteit). Soms kunnen doelen ook worden bereikt door bijvoorbeeld geanonimiseerd een casus uit te wisselen. Dan worden er geen persoonsgegevens uitgewisseld.

Integriteit en vertrouwelijkheid

De gemeente gaat zorgvuldig om met persoonsgegevens en behandelt deze vertrouwelijk met de juiste beveiliging. Dit gebeurt conform de bepalingen vanuit de Baseline Informatiebeveiliging Overheid (BIO) die voor gemeenten verplicht zijn.

De gemeente treft maatregelen om de kwaliteit van de gegevens te borgen; onder 'kwaliteit' wordt verstaan dat ze juist, nauwkeurig en actueel zijn. Voordat gegevens worden verwerkt vinden er (geautomatiseerde) controles plaats om te voorkomen dat personen niet goed benaderd worden (denk aan het versturen van brieven naar een oud adres, het versturen van brieven met een verkeerde tenaamstelling of het versturen van een brief naar een overledene).

In ieder geval zijn de volgende maatregelen getroffen:

- Bij de invoer van gegevens vindt er een kwaliteitscontrole plaats door gegevens te verifiëren.
- ICT-systemen valideren gegevens door middel van invoercontroles.
- ICT-systemen zijn daar waar persoonsgegevens worden gebruikt veelal direct of indirect gekoppeld aan de BRP, zodat men altijd beschikt over actuele gegevens. Als deze koppeling niet mogelijk is, worden de gegevens in de BRP geverifieerd voordat zij worden gebruikt.
- Betrokkenen hebben de mogelijkheid om gegevens in te zien en te laten corrigeren indien nodig.

Delen met derden

In het geval van samenwerking met externe partijen waarbij sprake is van verwerking van persoonsgegevens maakt de gemeente afspraken over de eisen waaraan gegevensuitwisseling moet voldoen. Deze afspraken voldoen aan de wet. De gemeente controleert jaarlijks steekproefsgewijs het nakomen van de gemaakte afspraken.

Integrale dienstverlening

De gemeente verwerkt persoonsgegevens in beginsel alleen voor het doel waarvoor ze verzameld worden en dit wordt alleen gedaan door medewerkers die hierbij betrokken zijn. In verband met integrale dienstverlening kan het nodig zijn persoonsgegevens ook te delen met andere medewerkers, die andere wetten/taken uitvoeren. Wanneer dit gebeurt wordt de betrokkene hiervan vooraf op de hoogte gebracht. Een voorbeeld vinden we terug in het Sociaal Domein. Indien het vanuit bijvoorbeeld een Wmo-aanvraag voor ambulante begeleiding nodig is om meteen ook te schakelen met medewerkers die de Wet gemeentelijke schuldhulpverlening uitvoeren, is dit vanuit integrale dienstverlening mogelijk. De betrokkene wordt hiervan op de hoogte gesteld.

Rechten van betrokkenen

De AVG bepaalt niet alleen de plichten van degenen die persoonsgegevens verwerken, maar ook de rechten van personen van wie de gegevens worden verwerkt. Hieronder een korte opsomming van deze rechten⁷:

- Recht op inzage
- Recht op rectificatie
- Recht op gegevenswissing (vergetelheid)
- Recht op beperking van de verwerking
- Kennisgevingsplicht inzake rectificatie of wissing van persoonsgegevens of verwerkingsbeperking
- Recht op overdraagbaarheid van gegevens
- Recht op bezwaar
- Recht om niet onderworpen te worden aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit

⁷) Zie in dezen de artikelen 15 t/m 22 van de AVG.

De gemeente verstrekt onverwijld maar in ieder geval binnen een maand na ontvangst van een verzoek informatie over of er, en zo ja op welke wijze, gevolg aan dat verzoek is gegeven.

In complexe situaties kan deze termijn worden verlengd met 2 maanden extra.⁸

Het voert bij de beschrijving van dit privacybeleid te ver om deze onderdelen te behandelen. Op basis van nieuwe richtlijnen en jurisprudentie zal de inhoud continu aan verandering onderhevig zijn. Voor de diverse rechten gelden voorwaarden en deze kennen wettelijke beperkingen (zo is bijvoorbeeld het recht op wissing niet van toepassing op registraties in de BRP).

De gemeente richt werkprocessen in om zorg te dragen voor een juiste en tijdige afhandeling van verzoeken van betrokkenen. Via de website worden betrokkenen geïnformeerd over deze rechten en wordt hun de mogelijkheid geboden om op eenvoudige wijze gebruik te maken van deze rechten.

Klachten van burgers

Voor burgers is het mogelijk om klachten over de toepassing van de AVG in te dienen bij de gemeente, en ook bij de Autoriteit Persoonsgegevens. Deze klachten worden binnen de gemeente conform de reguliere klachtenprocedure afgehandeld. Daarbij wordt de FG om advies gevraagd.

Register van Verwerkingen

De gemeente heeft een Register van Verwerkingen overeenkomstig artikel 30 AVG opgesteld en op de website gepubliceerd en houdt dit actueel.

Privacy by Design en Privacy by Default

Voorafgaand aan de start van een (nieuwe) gegevensverwerking zorgt de gemeente ervoor dat er zowel technisch als organisatorisch een zorgvuldige omgang met persoonsgegevens wordt afgedwongen. Dit heet 'Privacy by Design'. Hierbij wordt onder andere gekeken naar de noodzaak van deze gegevens voor het te behalen doel en de benodigde beveiliging van de persoonsgegevens.

Een onderdeel van 'Privacy by Design' is 'Privacy by Default', waarmee de gemeente ervoor zorgt dat de standaardinstellingen (denk aan de mogelijkheid om tweefactorauthenticatie in te schakelen) zo privacyvriendelijk mogelijk zijn.

Gegevensbeschermingseffectbeoordeling/Data Protection Impact Assessment (DPIA)

Op grond van de AVG is de gemeente verplicht om in een aantal gevallen vóór de verwerking van de gegevens een gegevensbeschermingseffectbeoordeling (DPIA) uit te voeren. Het uitvoeren van een DPIA is verplicht als een gegevensverwerking waarschijnlijk een hoog privacyrisico oplevert voor de personen van wie de gemeente gegevens verwerkt.⁹

Bij de beoordeling hiervan maakt de gemeente gebruik van de beoordelingscriteria die hiervoor zijn opgesteld door het Europees Comité voor gegevensbescherming (European Data Protection Board - EDPB) en door de AP. De AP heeft een lijst opgesteld van verwerkingen waarvoor een DPIA verplicht is. Deze lijst is terug te vinden op de website van de AP.

Een DPIA dient te worden gehouden voorafgaand aan de verwerking. Daarnaast heeft de AP aangegeven dat een DPIA eens per drie jaar herhaald moet worden - of eerder/vaker, indien er wijzigingen zijn die dit noodzakelijk maken.

De gemeente zorgt ervoor tijdig in beeld te brengen voor welke verwerkingen een DPIA verplicht is. Met gebruikmaking van het Register van Verwerkingen bepaalt de procesverantwoordelijke of een DPIA verplicht is en wanneer deze dient te worden uitgevoerd. Dit wordt in beeld gebracht en meegenomen in de rapportages richting het college. Het is van belang om hierbij ook aan te sluiten bij ontwikkelingen rond een verwerking, zoals:

- nieuwe wettelijke bepalingen, taken of grote wijzigingen;
- organisatiewijzigingen of samenwerkingen met derden dan wel overdracht van taken;
- de aanschaf van nieuwe software of ICT-apparatuur.

Samenwerkingsverbanden

De gemeente werkt samen in regionaal verband, bijvoorbeeld in samenwerkingen op het gebied van zorg en van veiligheid, zoals het Veiligheidshuis. De gemeente zorgt ervoor dat zij met deze samenwerkingspartners afdoende afspraken maakt om de privacy te waarborgen.

Vóór de deelname in een (nieuw) samenwerkingsverband voert zij een DPIA uit om de risico's van deelname aan het samenwerkingsverband te analyseren en hierop maatregelen te nemen.

8) Artikel 12 lid 3 AVG.

9) Artikel 35 AVG.

3. Privacymanagement

Voor een behoorlijke en zorgvuldige verwerking van persoonsgegevens in overeenstemming met de wet is goed privacymanagement van de gemeente noodzakelijk. Het gaat hierbij om vragen als 'Hoe is privacy ingebed in de organisatiestructuur?' en 'Bij wie ligt het proceseigenaarschap en wie houdt toezicht op de naleving?' Bij privacymanagement gaat het er uiteindelijk om dat er een vorm van bedrijfsvoering ontstaat waarin privacy op een natuurlijke manier bij de organisatie is gaan behoren ('Privacy by Design'). Daarbij is het uitgangspunt dat de standaard zo privacybestendig mogelijk is ('Privacy by Default').

3.1 Taken en verantwoordelijkheden

Het college is eindverantwoordelijk voor de naleving van privacywetgeving met de burgemeester als portefeuillehouder.

Het management heeft de ambtelijke verantwoordelijkheid om een proactief privacybeleid te voeren op basis van afweging van belangen en risico's bij de verwerking van persoonsgegevens, zodat dit behoorlijk, zorgvuldig en in overeenstemming met de wet plaatsvindt.

Het college legt over de uitvoering van het privacybeleid verantwoording af aan de gemeenteraad en zorgt voor een zodanige documentatie van beleid en maatregelen dat het op ieder moment maatschappelijk en juridisch uitleg kan geven over de deugdelijkheid van de aanpak.

3.2 Proceseigenaarschap

De teamleider is ervoor verantwoordelijk dat de gemeentelijke taakuitoefening binnen de grenzen van dit privacybeleid plaatsvindt en rapporteert hierover aan de directie, die op haar beurt rapporteert aan het college.

De teamleider is proceseigenaar. Proceseigenaren voeren regie over hun proces(sen). Bij teamoverstijgende processen kan de programmaregisseur worden aangewezen.

De proceseigenaar kan verantwoordelijkheden beleggen bij medewerkers. Een voorbeeld: De proceseigenaar geeft aan dat er voor een proces een DPIA nodig is. De proceseigenaar geeft dan de opdracht voor het uitvoeren van een DPIA en kan hiervoor medewerkers (bijv. juridisch, applicatiebeheer, systeembeheer, contactpersoon privacy) inzetten of eventueel externe ondersteuning inhuren. De proceseigenaar is en blijft verantwoordelijk opdrachtgever voor een dergelijke taak.

Het college is voor het merendeel van de verwerkingen verwerkingsverantwoordelijke in de zin van de AVG en blijft dus eindverantwoordelijk voor de privacybestendigheid van de gemeentelijke processen.

3.3 Uitwerking privacy governance

In bijlage 1 is de privacy governance van de gemeente toegevoegd. De hiervoor genoemde verantwoordelijkheden zijn hierin geïmplementeerd. De proceseigenaar is verantwoordelijk voor het voldoen aan de vereisten vanuit de AVG en wordt daarbij ondersteund door de contactpersoon privacy en/of privacy officer en in sommige gevallen door de CISO. De Functionaris Gegevensbescherming controleert of er conform de AVG wordt gewerkt.

4. Informatiebeveiliging

Om zorgvuldig met persoonsgegevens te kunnen omgaan moeten er passende beschermende maatregelen worden getroffen.¹⁰ Deze maatregelen moeten de geheimhouding en beveiliging van de gegevens borgen. Ze gelden voor iedereen die onder verantwoordelijkheid van het college van de gemeente werkt: interne medewerkers, verwerkers en subverwerkers. De maatregelen gelden ook voor diensten en goederen die onderdeel zijn van de beveiliging, zoals de beveiliging van het pand, de schoonmaak of de leveranciers van hardware.

Op grond van de Meldplicht datalekken¹¹ meldt het college van de gemeente een beveiligingsincident bij de AP, tenzij het niet aannemelijk is dat de inbreuk op de beveiliging een privacyrisico inhoudt. De gemeente houdt een Datalekregister bij.¹² De procedure rond de meldplicht van datalekken is uitgewerkt in een handleiding voor de medewerkers van de gemeente.

¹⁰ *Zie artikel 24 AVG.*

¹¹ *Zie artikel 33 AVG*

¹² *Zie artikel 33 lid 5 AVG.*

4.1 Geheimhouding

Alle personen die onder het gezag van het college werken zijn tot geheimhouding verplicht. Elke werknemer in vaste dienst legt bij indiensttreding een eed of belofte af als onderdeel van de arbeidsovereenkomst. Daarnaast wordt bij de ondertekening van de arbeidsovereenkomst een geheimhoudingsverklaring getekend. Inhuurkrachten tekenen in ieder geval bij de ondertekening van de inhuurovereenkomst een geheimhoudingsverklaring.

Daarnaast worden medewerkers in een apart document gewezen op de geheimhoudingsplicht en op het belang van een zorgvuldige omgang met de gegevens. Voor een aantal aparte functies worden medewerkers specifiek op hun geheimhoudingsplicht gewezen, zoals bij het gebruik van Suwinet en van de BRP.

Verwerkers en externen in algemene zin worden door middel van verwerkersovereenkomsten en contracten verplicht tot geheimhouding. Dit is opgenomen in de standaard- verwerkersovereenkomst. In alle contracten met leveranciers, verwerkers en overige externen die toegang krijgen tot het pand of tot de systemen is een bepaling met betrekking tot de geheimhouding opgenomen.

4.2 Informatiebeveiliging

Voor de informatiebeveiliging geldt de norm van de Baseline Informatiebeveiliging Overheid (BIO). De gemeente volgt hiermee de richtlijnen vanuit de BIO die door de Ministerraad in december 2018 zijn vastgesteld als de verplichte norm voor overheidsorganisaties, waaronder gemeenten.

Er is hiervoor een strategisch en tactisch informatiebeveiligingsbeleid opgesteld, dat iedere drie jaar wordt herzien en opnieuw wordt vastgesteld.

5. Samenwerken met andere partijen

De gemeente werkt in meerdere situaties samen met andere partijen. Afhankelijk van de samenwerkingsrelatie wordt dit vastgelegd in convenanten, in verwerkersovereenkomsten of in een overeenkomst gezamenlijke verwerkingsverantwoordelijkheid.

5.1 Convenanten

Daar waar partijen samenwerken maar zelf verantwoordelijk zijn en blijven voor hun eigen verwerkingen is een convenant van belang om afspraken te maken over bijvoorbeeld de wijze waarop persoonsgegevens worden uitgewisseld.

In een dergelijk convenant gaat het om de onderlinge verantwoordelijkheden en ook om hoe er moet worden omgegaan met onder andere de rechten van betrokkenen en met datalekken. Het zijn vooral werkafspraken tussen partijen om het samenwerken vast te leggen waarbij het nodig is om persoonsgegevens uit te wisselen. Een convenant biedt geen rechtsgeldige grondslag voor een uitwisseling van persoonsgegevens. Die vloeit voort uit de rechtmatige verwerking door de partijen zelf en zal eenieder voor zichzelf dienen in te vullen.

5.2 Verwerkersovereenkomsten

Verwerkers zijn derden die in opdracht van de gemeente persoonsgegevens verwerken zonder dat zij verwerkingsverantwoordelijke worden; denk aan het bedrijf dat gegevens van personeelsleden verwerkt om de salarissen te kunnen uitbetalen. Alleen verwerkers die afdoende garanties bieden ten aanzien van de bescherming van persoonsgegevens worden ingehuurd. Met alle verwerkers wordt een verwerkersovereenkomst gesloten conform het VNG- standaardmodel.

5.3 Gezamenlijke verwerkingsverantwoordelijken

Het kan voorkomen dat de gemeente samen met een andere organisatie persoonsgegevens verwerkt. In dat geval wordt er een overeenkomst opgesteld waarin op transparante wijze de verantwoordelijkheden voor de nakoming van de verplichtingen uit de AVG worden vastgesteld, met name ten aanzien van de uitoefening van de rechten van betrokkenen en de informatieplicht.¹³

6. Bewustwording, communicatie en evaluatie

Privacybeleid moet niet beperkt blijven tot het formuleren van uitgangspunten en door het college na te streven doelen. Alle medewerkers van de gemeente dragen in de praktijk zorg voor de eerbiediging van de persoonlijke levenssfeer bij de verwerking van persoonsgegevens. Privacy is daarmee voor een

¹³ Zie artikel 26 AVG.

belangrijk deel een zaak van bewustwording, cultuur en communicatie. Bestuur, management en medewerkers moeten zich bij de uitoefening van hun werk voortdurend bewust zijn van het belang van het waarborgen van de rechten van de burgers.

Naast het inrichten van het privacybeleid en werkprocessen is het belangrijk dat personen die daadwerkelijk werken met deze gegevens weten wat hun verantwoordelijkheid is en hoe ze zorgvuldig moeten omgaan met persoonsgegevens. Daarom is het belangrijk dat de medewerkers van de gemeente zich bewust zijn van de regels en gedragsnormen rondom privacy. De gemeente ondersteunt dit proces door het ontwikkelen van bijvoorbeeld privacyprotocollen en afwegingskaders.

Om ervoor te zorgen dat medewerkers zich bewust zijn van het belang van privacy en weten hoe zij persoonsgegevens op een zorgvuldige manier moeten verwerken wordt er jaarlijks een bewustwordingsplan opgesteld. Hierin staan verschillende aandachtspunten met het oog op bewustwording (en het bewust blijven) bij de personen die met deze gegevens werken. Omdat het veilig omgaan met persoonsgegevens direct verband houdt met informatiebeveiliging, wordt het oppakken van bewustwording op het gebied van privacy gecombineerd met bewustwording op het gebied van informatiebeveiliging. In het bewustwordingsprogramma wordt ook aandacht besteed aan bijvoorbeeld trainingen en opschoondagen.

De gemeente streeft naar een cultuur waarin medewerkers elkaar in alle openheid aanspreken op het gedrag rondom privacy en daarmee van elkaar leren. Communicatie, openheid en toetsing zijn belangrijke randvoorwaarden voor het realiseren van een optimaal privacybeleid.

Aan het eind van elk jaar wordt geëvalueerd wat de opbrengst was van het bewustwordingsprogramma, zodat hier rekening mee gehouden kan worden bij het opstellen van een dergelijk programma voor het volgende jaar.

7. Toezicht en rapportage

Jaarlijks evalueert het management met het college de uitvoering van dit beleidsplan. Hierbij wordt aangegeven in hoeverre de gemeente (conform artikel 5 lid 2 van de AVG) voldoet aan de uitgangspunten van de AVG.

De Functionaris Gegevensbescherming stelt voor de verantwoording van zijn werkzaamheden en bevindingen een eigen jaarverslag op, voegt hierbij een eigen visie op de evaluatie van het management en geeft een eigen oordeel over de vraag in hoeverre de gemeente voldoet aan de uitgangspunten van de AVG.¹⁴

Het college biedt dit verslag, met zijn reactie, ter vaststelling aan de gemeenteraad aan.

8. Tot slot

Dit privacybeleid treedt in werking na vaststelling door het college. Het beleid geldt voor de jaren 2021 tot en met 2024 en wordt iedere drie jaar geëvalueerd en indien nodig herzien.

Ondertekening

Aldus vastgesteld door het college van burgemeester en wethouders

gemeente Culemborg

11 januari 2022

¹⁴ Zie artikel 5 lid 2 AVG.