gemeente Tiel

GEMEENTEBLAD

Officiële uitgave van de gemeente Tiel

Nr. 96376

9 maart

2023

Privacybeleid Gemeente Tiel 2023-2025

1. Inleiding

De gemeente werkt met (persoons)gegevens van burgers, ondernemers, medewerkers en (keten)partners. Deze gegevens verzamelt de gemeente om de gemeentelijke (meestal wettelijke) taken goed uit te kunnen voeren. Denk hierbij aan taken in het sociaal domein, op het gebied van openbare orde en veiligheid of voor burgerzaken. Om deze taken goed uit te kunnen voeren is het noodzakelijk dat de gemeente persoonsgegevens verwerkt. De burger moet erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met deze persoonsgegevens omgaat.

Technologische ontwikkelingen, innovatie, 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. Ook de hoeveelheid gevoelige informatie die van personen wordt vastgelegd neemt toe, evenals de risico's van bijvoorbeeld cybercrime. Tegelijkertijd wordt de samenleving kritischer en hebben burgers steeds meer behoefte aan rechten om inzicht te krijgen in de verwerking van hun persoonsgegevens.

1.1 Visie op privacy

Privacy speelt een belangrijke rol in de relatie tussen burger en overheid. Het is een grondrecht en vormt een vereiste voor het kunnen uitoefenen van andere vrijheden, zoals de vrijheid van meningsuiting.

De gemeente Tiel wil het belang van privacy uitdragen en een betrouwbare overheid zijn. Hieraan geeft ze invulling door in haar handelen de persoonlijke levenssfeer van betrokkenen te eerbiedigen, transparant te zijn over de manier waarop ze persoonsgegevens verwerkt en door te zorgen dat burgers hun privacyrechten kunnen uitoefenen. De komende jaren zet de gemeente in op het vergroten van de privacy bewustwording en het verder integreren van privacy in gemeentelijke processen.

1.2 Doel

Met dit privacybeleid wil de gemeente aangeven hoe zij in algemene zin invulling geeft aan nationale en Europese wet- en regelgeving op het gebied van privacy, waaronder de Algemene Verordening Gegevensbescherming (hierna te noemen: AVG). Daarnaast worden in dit beleid de verschillende rollen, taken en verantwoordelijkheden op het gebied van privacy beschreven.

1.3 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 bronsystemen (het combineren van gegevens). Het is van belang om hiervoor de juiste rechtmatige grondslag te hebben.

Voor alle in dit beleid gebruikte begrippen geldt dat hun betekenis overeenkomt met de definities uit de AVG.

1.4 Waar worden persoonsgegevens verwerkt?

In de gehele gemeentelijke organisatie worden persoonsgegevens verwerkt. Dit varieert van het gebruik van een beperkte gegevensverzameling, zoals een lijst met email-adressen door communicatie, tot het gebruik van grote gegevensverzamelingen, zoals de Basisregistratie Personen (BRP) door burgerzaken.

De gegevens worden in de basis in de eigen (vak)applicaties vastgelegd, maar kunnen ook via het centrale gegevensmagazijn worden verwerkt. Via dit centrale gegevensmagazijn is het mogelijk om gegevens afkomstig uit basisregistraties (BRP, BAG) te verstrekken aan aangesloten applicaties. Daarnaast kunnen persoonsgegevens in een datawarehouse worden opgenomen. Persoonsgegevens worden

dan vanuit verschillende vakapplicaties samengevoegd om op basis daarvan managementrapportages en beleidsinformatie op te stellen.

1.5 Reikwijdte privacybeleid

Dit privacybeleid is van toepassing op alle verwerkingen van persoonsgegevens door of namens de gemeente. Het algemene privacybeleid is richtinggevend en kaderstellend en wordt aangevuld met onderwerpspecifieke beleidsdocumenten en werkinstructies. Denk bijvoorbeeld aan privacybeleid voor het sociaal domein of een procedure voor het opvolgen van datalekken.

1.6 Juridisch kader

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

De AVG is een algemene wet, met algemene bepalingen en uitgangspunten. In specifieke wetten (bijvoorbeeld de Jeugdwet, Wet maatschappelijke ondersteuning en Participatiewet) zijn ook bepalingen over het verwerken 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 op grond van de AVG medische gegevens alleen worden verwerkt als hiervoor een wettelijke grondslag aanwezig is; deze grondslag is dan opgenomen in de specifieke wet. Dat neemt echter niet weg dat de algemene uitgangspunten van de AVG, zoals ‘niet meer gegevens verwerken dan nodig’, ‘alleen indien nodig’ en ‘niet langer dan nodig’, nog steeds gelden en moeten worden vertaald naar werkprocessen.

1.7 Raakvlakken met andere beleidsthema’s

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

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

Integriteitsbeleid
Privacybeleidsvoering is gekoppeld aan de beginselen van behoorlijk bestuur en heeft daardoor raakvlakken met het gemeentelijke integriteitsbeleid (de Tielse Gedragscode).

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

2. Uitgangspunten voor het verwerken van persoonsgegevens

De AVG is gebaseerd op een aantal principes voor de verwerking van persoonsgegevens. De gemeente onderschrijft deze principes en stelt zich ten doel persoonsgegevens slechts te verwerken in overeenstemming met deze principes.

Rechtmatige grondslag
Persoonsgegevens worden door de gemeente slechts verwerkt in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze. Dit betekent onder meer dat verwerkingen alleen plaatsvinden indien hiervoor een rechtmatige verwerkingsgrondslag bestaat. Veelal vloeit de grondslag voor een verwerking voort uit een wettelijke verplichting of is dit gebaseerd op een publiekrechtelijke taak of openbaar gezag. In sommige gevallen verwerkt de gemeente gegevens om een overeenkomst uit te voeren of op basis van toestemming.

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

Dit is alleen toegestaan als hiervoor in een specifieke wet een grondslag is gegeven. Is deze grondslag er niet, dan worden geen bijzondere persoonsgegevens verwerkt.

Op grond van de Wet algemene bepalingen burgerservicenummer (Wabb) is de gemeente bevoegd om het burgerservicenummer (BSN) te verwerken wanneer dit noodzakelijk is voor het uitvoeren van een overheidstaak.[1]

Doelbinding
Met doelbinding wordt bedoeld dat gegevens alleen worden verwerkt voor een vooraf bepaald en voldoende concreet omschreven doel. Alleen persoonsgegevens die noodzakelijk zijn om dat doel te bereiken worden verwerkt.

Persoonsgegevens worden in veel gevallen verwerkt in applicaties. Soms zijn deze weer 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 overzicht van het applicatielandschap.

Verdere verwerking
Persoonsgegevens kunnen in bepaalde gevallen worden verwerkt voor andere doelen dan waarvoor ze in eerste instantie zijn verzameld. Daarbij geldt onder andere dat de twee doelen aan elkaar verwant moeten zijn, er zich geen nadelige effecten voor de betrokkenen voordoen, dan wel dat hiervoor extra waarborgen zijn getroffen.[2] De gemeente voert, voordat de verwerking start, een toets uit om te bepalen of de gegevens voor andere doelen mogen worden gebruikt op grond van de wet- en regelgeving.

Minimale gegevensverwerking
De gemeente verwerkt alleen de persoonsgegevens die noodzakelijk zijn voor het vooraf bepaalde doel en streeft naar minimale gegevensverwerking. Het uitgangspunt is: niet meer dan nodig, alleen indien nodig, niet langer dan nodig.

Gegevens mogen alleen worden verwerkt als dit in verhouding staat tot het doel. Als het doel waarvoor persoonsgegevens worden verwerkt, zonder of met minder persoonsgegevens kan worden bereikt, dan kiest de gemeente bij voorkeur voor die mogelijkheid.

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 persoonsgegevens. Soms kunnen doelen bijvoorbeeld ook worden bereikt door met geanonimiseerde gegevens te werken, zoals bij het bespreken van een bepaalde casus. In dat geval worden er geen persoonsgegevens uitgewisseld.

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

Juiste en actuele gegevens
De gemeente zorgt ervoor dat alleen persoonsgegevens worden verwerkt die juist en actueel zijn gelet op het doel waarvoor zij verzameld zijn of verder worden verwerkt. De gemeente neemt redelijke maatregelen om persoonsgegevens juist en actueel te houden, onjuiste persoonsgegevens te actualiseren, te rectificeren en/of te wissen.

Om te waarborgen dat gegevens juist en actueel zijn, worden in ieder geval de volgende maatregelen genomen:
- 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 automatisch beschikt over actuele gegevens. Als deze koppeling niet mogelijk is, worden de gegevens in de BRP handmatig geverifieerd voordat zij worden gebruikt.

1) Dit is in overeenstemming met het bepaalde in artikel 87 AVG en artikel 46 van de Uitvoeringswet AVG.
2) Zie artikel 6 lid 4 AVG.

- Betrokkenen hebben de mogelijkheid om gegevens in te zien en te laten corrigeren indien nodig.

Integriteit en vertrouwelijkheid
De gemeente neemt passende technische en organisatorische maatregelen om persoonsgegevens, en zeker bijzondere persoonsgegevens, te beschermen tegen misbruik en onrechtmatige of ongeautoriseerde verwerking. De gemeente handelt hierbij in overeenstemming met de bepalingen van de Baseline Informatiebeveiliging Overheid (BIO) en het op de BIO gebaseerde informatiebeveiligingsbeleid (zie ook 4.2 Informatiebeveiligingsbeleid).

Toegang tot gegevens
Uitsluitend geautoriseerde gebruikers zijn bevoegd tot onder meer het invoeren, rechtstreeks raadplegen, wijzigen en verwijderen van persoonsgegevens. Deze bevoegdheden worden toegekend op grond van het binnen de gemeente geldende beleid voor toegang tot gegevens, waaronder het informatiebeveiligingsbeleid. Het beheer van bevoegdheden wordt periodiek gecontroleerd. De gemeente hanteert daarnaast specifieke oplossingen en toepassingen, waaronder het bijhouden van loggegevens, om ongeautoriseerde toegang tot en niet toegestane verwerkingen van persoonsgegevens zo veel mogelijk te voorkomen en aan te pakken.

Inbreuk in verband met persoonsgegevens (datalek)
Bij toegang tot, verlies of wijziging van persoonsgegevens bij de gemeente, zonder dat dit de bedoeling is, is er sprake van een datalek. Dit moet, afhankelijk van het risico, worden gemeld bij de toezichthouder (de Autoriteit Persoonsgegevens) en soms bij de getroffen betrokkenen. De gemeente registreert datalekken, zet de bevindingen om in verbeterpunten en ziet toe op de opvolging hiervan. Nadere regels ten aanzien van het vaststellen, melden en afhandelen van datalekken zijn opgenomen in de procedure datalekken.

Privacy by design en privacy by default
De gemeente houdt bij de ontwikkeling van nieuwe diensten, systemen of processen rekening met aspecten van privacy en gegevensbescherming om zo te komen tot een zo optimaal mogelijke bescherming van persoonsgegevens. Dit uitgangspunt wordt ‘privacy by design’ genoemd. Hierbij wordt onder andere gekeken naar de noodzaak van deze gegevens voor het te behalen doel en de benodigde beveiliging van de persoonsgegevens. De gemeente draagt er zorg voor dat concrete maatregelen zoveel mogelijk doorgevoerd worden in het ontwerp.

Daarbij neemt de gemeente ‘privacy by default’ als uitgangspunt. Hiermee wordt bedoeld dat de standaardinstellingen van een systeem zo privacyvriendelijk mogelijk moeten zijn.

Transparantie
De gemeente informeert de betrokkenen tijdig, op een zo eenvoudig mogelijke, begrijpelijke en toegankelijke wijze over het feit dat zij persoonsgegevens verwerkt, op welke wijze dit gebeurt en voor welke doeleinden. De betrokkene wordt op heldere en laagdrempelige wijze geïnformeerd over zijn rechten en de wijze waarop hij deze kan uitoefenen. Alleen indien de wet anders bepaalt, wijkt de gemeente van deze informatieplicht af.[3]

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 hebben van een privacyverklaring, inclusief cookieverklaring op de gemeentelijke websites;
- 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;
- hoelang gegevens bewaard worden;
- hoe wordt omgegaan met de rechten van betrokkenen;
- (indien van toepassing) de ontvangers van de gegevens;
- (indien van toepassing) nadere informatie met betrekking tot eventuele doorgifte van persoonsgegevens naar een derde land of internationale organisatie.

Rechten van betrokkenen

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

De AVG bepaalt niet alleen de plichten van degenen die persoonsgegevens verwerken, maar ook de rechten van personen van wie de gegevens worden verwerkt. De AVG kent aan betrokkenen de volgende rechten toe[4]:

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

De gemeente verstrekt zo snel mogelijk maar in ieder geval binnen een maand na ontvangst van een verzoek informatie over of, en zo ja op welke wijze, gevolg aan dat verzoek wordt gegeven.
In complexe situaties kan deze termijn worden verlengd met twee maanden.[5]

Voor de diverse rechten gelden voorwaarden en deze kennen soms wettelijke beperkingen (zo is bijvoorbeeld het recht op gegevenswissing niet van toepassing op registraties in de BRP).
Op de website van de gemeente wordt informatie gegeven over de verschillende rechten en de wijze waarop betrokkenen daar gebruik van kunnen maken. De gemeente heeft een werkproces ingericht om te zorgen dat verzoeken van betrokkenen juist en tijdig worden afgehandeld.

Register van Verwerkingen
De gemeente heeft de verwerkingen van persoonsgegevens vastgelegd in een verwerkingsregister. In het verwerkingsregister staat welke persoonsgegevens worden verwerkt en met welk doel. Ook wordt vastgelegd hoe de gegevens zijn beveiligd, of deze gedeeld worden met andere partijen en hoe lang de gegevens bewaard worden. Het verwerkingsregister wordt regelmatig bijgewerkt. Dit gebeurt bijvoorbeeld wanneer een verwerking verandert, wanneer een nieuwe verwerking wordt gestart of een verwerking wordt beëindigd.

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 Data Protection Impact Assessment (DPIA) uit te voeren (de AVG spreekt van een gegevensbeschermingseffectbeoordeling). Het uitvoeren van een DPIA is verplicht als een gegevensverwerking waarschijnlijk een hoog privacyrisico oplevert voor de personen van wie de gemeente gegevens verwerkt.[6] 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 of EDPB) en door de Autoriteit Persoonsgegevens (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 moet voorafgaand aan de verwerking worden uitgevoerd. Daarnaast heeft de AP aangegeven dat een DPIA eens per drie jaar herhaald moet worden of eerder/vaker, als 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 moet worden uitgevoerd. 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.

Klachten van burgers
Wanneer burgers vinden dat de gemeente onzorgvuldig is omgegaan met hun privacy of dat de gemeente ten onrechte hun persoonsgegevens heeft verwerkt, kunnen zij een klacht indienen bij de gemeente en bij de Autoriteit Persoonsgegevens. Binnen de gemeente worden deze klachten conform de

4) Zie de artikelen 15 t/m 22 van de AVG.
5) Artikel 12 lid 3 AVG.
6) Artikel 35 AVG.

reguliere klachtenprocedure afgehandeld. Bij privacyklachten wordt de Functionaris Gegevensbescherming om advies gevraagd.

3. Privacy management

Om aantoonbaar te kunnen voldoen aan de AVG is goed privacy management noodzakelijk. Het gaat hierbij om vragen als:

- Hoe is privacy ingebed in de organisatiestructuur?
- Bij wie ligt het proceseigenaarschap?
- Wie houdt toezicht op de naleving?
- Kan er adequaat verantwoording worden afgelegd over de verwerking van persoonsgegevens?

3.1 Privacy governance

Hoe de gemeente de bescherming van persoonsgegevens binnen de organisatie heeft belegd, is vastgelegd in een privacy governance model. Hierin zijn de verschillende rollen, taken en verantwoordelijkheden op het gebied van privacy beschreven.

College van B&W
Het college van B&W is als bestuursorgaan voor het merendeel van de gemeentelijke processen verwerkingsverantwoordelijke in de zin van de AVG en daarmee eindverantwoordelijk voor de naleving van de privacywetgeving. Binnen het college ligt deze verantwoordelijkheid bij de portefeuillehouder bedrijfsvoering. Het college stelt het privacybeleid vast.

Directie en management
Directie en management zijn operationeel verantwoordelijk voor de naleving van de privacywetgeving en de implementatie en uitvoering van het privacybeleid. Afdelingsmanagers zijn proceseigenaar. Proceseigenaren zijn ervoor verantwoordelijk dat persoongegevens worden verwerkt conform de privacywetgeving en het privacybeleid. Ze worden daarbij ondersteund door de privacy contactpersonen en/of privacy officer.

Functionaris Gegevensbescherming
De Functionaris Gegevensbescherming (FG) is verantwoordelijk voor het toezicht op de naleving van de AVG. De FG heeft een onafhankelijke adviserende en toezichthoudende positie in de organisatie. De FG beschikt hiertoe over de noodzakelijke faciliteiten, middelen en bevoegdheden.

Privacy Officer
De Privacy Officer (PO) is het eerste aanspreekpunt voor de gemeente rondom privacygerelateerde vraagstukken. De PO heeft een monitorende en ondersteunende functie rondom het naleven en uitvoeren van het privacybeleid. De PO ontwikkelt privacybeleid en procedures en bevordert de privacybewustwording binnen de organisatie.

Privacy contactpersonen
De privacy contactpersonen vormen binnen het team waar ze werkzaam zijn een belangrijke schakel in het uitdragen van het privacybeleid en bij het signaleren van privacygerelateerde ontwikkelingen. Ze hebben hiertoe regelmatig overleg met de Privacy Officer.

Chief Information Security Officer
De Chief Information Security Officer (CISO) is verantwoordelijk voor het implementeren van het informatiebeveiligingsbeleid en het toezicht daarop. De CISO adviseert met betrekking tot de technische en organisatorische maatregelen die moeten worden genomen in het kader van de bescherming van (persoons)gegevens. De CISO adviseert en ondersteunt bij de afhandeling van datalekken.

3.2 PDCA Cyclus

De gemeente streeft ernaar om rondom de verwerking van persoonsgegevens in control te zijn en daarover op professionele wijze verantwoording af te leggen. In control betekent in dit verband dat de gemeente weet welke maatregelen genomen zijn ten aanzien van de verwerking van persoonsgegevens, dat er een planning is van de maatregelen die nog niet genomen zijn en dat dit geheel verankerd is in een Plan-Do-Check-Act-cyclus.

Daarnaast gebruikt de gemeente het borgingsproduct van de VNG als het beoordelingskader voor het waarborgen van privacy compliance binnen de gemeente. Het borgingsproduct is een normenkader dat door de gemeente gebruikt wordt voor het duiden van privacyrisico's en de daarbij behorende beheersmaatregelen.

4. Beveiligingsmaatregelen

Om zorgvuldig met persoonsgegevens te kunnen omgaan moeten er passende beschermende maatregelen worden getroffen.[7] Deze maatregelen moeten de geheimhouding en beveiliging van de gegevens waarborgen. Ze gelden voor iedereen die onder verantwoordelijkheid van het college werkt: interne medewerkers, verwerkers en subverwerkers. De maatregelen gelden ook voor ingehuurde dienstverleners, zoals beveiligers, schoonmakers of de leveranciers van hardware.

4.1 Geheimhouding

Alle personen die onder het gezag van het college werken zijn tot geheimhouding verplicht. Elke medewerker 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 bij de ondertekening van de inhuurovereenkomst een geheimhoudingsverklaring.

Het college heeft een gedragscode integriteit voor medewerkers vastgesteld. Hierin zijn (onder meer) richtlijnen opgenomen voor het vertrouwelijk omgaan met privacygevoelige informatie.

Wanneer het voor hun functie nodig is dat medewerkers toegang krijgen tot de Basisregistratie Personen of tot Suwinet, dan tekenen zij een specifieke verklaring omtrent geheimhouding en het juiste gebruik van deze systemen.

Verwerkers en externe partijen worden door middel van verwerkersovereenkomsten en contracten verplicht tot geheimhouding. 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 geheimhouding opgenomen.

4.2 Informatiebeveiligingsbeleid

Informatiebeveiliging en de bescherming van persoonsgegevens zijn onlosmakelijk met elkaar verbonden. Informatiebeveiliging is een randvoorwaarde voor de borging van privacy bij het verwerken van persoonsgegevens. In het informatiebeveiligingsbeleid van de gemeente zijn maatregelen genoemd om (persoons)gegevens te beschermen. Deze maatregelen dienen om misbruik, verlies, onbevoegde toegang en andere ongewenste handelingen met (persoons)gegevens tegen te gaan. Het informatiebeveiligingsbeleid is gebaseerd op de normen van de Baseline Informatiebeveiliging Overheid (BIO). De gemeente volgt hiermee de richtlijnen die door de Ministerraad in december 2018 zijn vastgesteld voor overheidsorganisaties, waaronder gemeenten. Naleving van het privacybeleid en het informatiebeveiligingsbeleid zorgen er samen voor dat persoonsgegevens op een adequaat niveau worden beschermd.

5. Samenwerking met andere partijen

De gemeente werkt in meerdere situaties samen met andere partijen. Wanneer daarbij persoonsgegevens worden verwerkt, zorgt de gemeente ervoor dat zij met haar samenwerkingspartners afdoende afspraken maakt om de privacy van betrokkenen te waarborgen. Afhankelijk van de samenwerkingsrelatie worden afspraken vastgelegd in een convenant, een verwerkersovereenkomst of in een overeenkomst gezamenlijke verwerkingsverantwoordelijkheid.

Voordat de gemeente deelneemt aan een samenwerkingsverband waarin met andere publieke of private partijen bijzondere persoonsgegevens of persoonsgegevens van gevoelige aard worden uitgewisseld, wordt een Data Protection Impact Assessment uitgevoerd. Hiermee worden de privacyrisico's van de beoogde verwerking in kaart gebracht om daarna maatregelen te kunnen nemen om deze risico's te verkleinen.

De gemeente controleert jaarlijks steekproefsgewijs het nakomen van de met derden gemaakte afspraken.

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.

Het convenant beschrijft de onderlinge verantwoordelijkheden en ook hoe er moet worden omgegaan met onder andere de rechten van betrokkenen en met datalekken. Het zijn vooral werkafspraken over de samenwerking en uitwisseling van persoonsgegevens. Een convenant vormt geen rechtsgeldige

7) Zie artikel 24 AVG.

grondslag voor de uitwisseling van persoonsgegevens. De grondslag hiervoor vloeit voort uit de rechtmatige verwerking door de partijen en moet door partijen zelf worden ingevuld.

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 standaardmodel van de VNG.

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.[8]

6. Doorgifte buiten de EER

De gemeente streeft ernaar om persoonsgegevens uitsluitend binnen het werkingsgebied van de AVG te (laten) verwerken. Wanneer doorgifte van persoonsgegevens aan landen buiten de Europese Economische Ruimte (EER) toch noodzakelijk is, vindt deze alleen plaats in overeenstemming met de bepalingen in toepasselijke wet- en regelgeving en dit privacybeleid.

7. Bewustwording

De medewerkers van de gemeente zijn de belangrijkste schakel in een zorgvuldige omgang met persoonsgegevens. Ze moeten zich in hun werk voortdurend bewust zijn van hun verantwoordelijkheid voor het waarborgen van de rechten van burgers. Privacybescherming is daarmee voor een belangrijk deel een zaak van bewustwording, cultuur en communicatie.

Naast het opstellen van privacybeleid en het inrichten van werkprocessen is het belangrijk dat personen die daadwerkelijk werken met de gegevens weten wat hun verantwoordelijkheid is en hoe ze zorgvuldig moeten omgaan met persoonsgegevens. Medewerkers moeten op de hoogte zijn van de regels en gedragsnormen rondom privacy. De gemeente ondersteunt dit onder meer door het ontwikkelen van privacyprotocollen, procedures en afwegingskaders.

Daarnaast wordt jaarlijks een bewustwordingsplan opgesteld. Hierin staan verschillende actiepunten gericht op het creëren (en onderhouden) van bewustwording bij medewerkers. Omdat het veilig omgaan met persoonsgegevens direct verband houdt met informatiebeveiliging, wordt het bevorderen van bewustwording op het gebied van privacy gecombineerd met bewustwording op het gebied van informatiebeveiliging. Door middel van voorlichting, presentaties en trainingen, wordt het belang van informatiebeveiliging en gegevensbescherming herhaaldelijk onder de aandacht gebracht van medewerkers en management.

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 het programma voor het volgende jaar.

8. Toezicht en rapportage

Jaarlijks evalueert het management de uitvoering van het privacybeleid en rapporteert hierover aan het college. Hierbij wordt aangegeven in hoeverre de gemeente voldoet aan de uitgangspunten van de AVG.[9]

De Functionaris Gegevensbescherming stelt voor de verantwoording van zijn werkzaamheden en bevindingen een jaarverslag op en biedt dit aan het college aan. Hij voegt hierbij een eigen visie op de door het management uitgevoerde evaluatie.

8) Zie artikel 26 AVG.
9) Zie artikel 5 lid 2 AVG.

9. Inwerkingtreding en evaluatie

Dit privacybeleid treedt in werking na vaststelling door het college. Het beleid geldt voor de periode 2023-2025 en wordt iedere drie jaar geëvalueerd en indien nodig herzien. Wanneer daar aanleiding toe is (bijvoorbeeld bij grote organisatorische veranderingen, wetswijzigingen of uitkomsten van DPIA's) kan het college besluiten tot een tussentijdse herziening.