

Privacybeleid gemeente Woensdrecht 2020

De raad van de gemeente Woensdrecht, in vergadering bijeen op 17 september 2020,

gelezen het voorstel van burgemeester en wethouders van 30 juni 2020,

gelet op artikel 24 van de Algemene verordening gegevensbescherming (AVG),

overwegende dat binnen de gemeente Woensdrecht veel met persoonsgegevens van burgers, ondernemers, medewerkers en (keten)partners wordt gewerkt, voornamelijk voor het goed uitvoeren van wettelijke taken en voorts, dat de gemeente Woensdrecht zich bewust is van het belang van privacybescherming en zorgt dat de privacy gewaarborgd blijft, dat betrokkenen er te allen tijde op moeten kunnen vertrouwen dat hun persoonsgegevens bij de gemeente Woensdrecht in veilige handen zijn,

besluit:

het Privacybeleid gemeente Woensdrecht 2020 vast te stellen.

1. Inleiding

Op 25 mei 2018 is de Algemene verordening gegevensbescherming (hierna: AVG) in werking getreden. Dat betekent dat vanaf die datum dezelfde privacywetgeving geldt in de gehele Europese Unie (EU). Lidstaten hebben slechts zeer beperkte vrijheid om aanvullende regelgeving vast te stellen. In Nederland is die aanvullende regelgeving neergelegd in de Uitvoeringswet AVG (UAVG).

Binnen de gemeente Woensdrecht werken we veel met persoonsgegevens van burgers, ondernemers, medewerkers en (keten)partners. Deze verzamelen we voornamelijk voor het goed uitvoeren van onze wettelijke taken. Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, 'internet of things', globalisering, 'common ground' en de (steeds meer) digitale overheid stellen andere eisen aan de bescherming van gegevens en privacy. De gemeente Woensdrecht is zich hier van bewust en zorgt dat de privacy gewaarborgd blijft, onder andere door maatregelen te treffen op het gebied van informatiebeveiliging, dataminimalisatie, transparantie en gebruikerscontrole, maar ook door te investeren in bewustwording en aandacht te schenken aan bijvoorbeeld integriteit. Betrokkenen moeten er te allen tijde op kunnen vertrouwen dat hun persoonsgegevens bij de gemeente Woensdrecht in veilige handen zijn.

Met privacybeleid geeft de gemeente Woensdrecht verdere invulling aan de uit de privacywetgeving voortvloeiende verplichtingen en bevoegdheden. Met dit beleid wordt duidelijk richting gegeven aan hoe de organisatie om moet gaan met privacy en laat zien dat zij de privacy waarborgt, beschermt en handhaaft.

Op 6 februari 2018 is het 'Algemeen privacybeleid van de gemeente Woensdrecht vanaf 2018'¹ vastgesteld. Inmiddels is de AVG al ruim anderhalf jaar van kracht en zijn er nadere inzichten over en ervaringen met de uitvoering daarvan opgedaan. Deze inzichten en ervaringen zijn door de Functionaris Gegevensbescherming (FG) in afzonderlijke rapportages verwoord en leiden tot actualisering/aanvulling van het gemeentelijk privacybeleid zoals nu voorligt.

2. Kernwaarden

De gemeente Woensdrecht gaat op een veilige manier met persoonsgegevens om en respecteert de privacy van betrokkenen. Hierbij wordt in lijn met de volgende kernwaarden gehandeld:

1. Eigen wijze
2. Betrokken
3. Daadkracht
4. Dienstbaar

1) Zaaknr. Z17.05297 / Docnr. 2017.42049

2.1 Eigen wijze

Wij nemen initiatief, zijn creatief in het maken en uitvoeren van plannen en het leveren van maatwerk, passend voor de Woensdrechtse gemeenschap. We hebben een trotse, open houding voor en naar inwoners en elkaar, waarbij verbinding centraal staat. Ons eigen wijze heeft een duidelijke rode draad: informeel ontmoeten en samenwerken.

Op het gebied van privacybescherming komt de 'eigen wijze' tot uiting in het verbinden, ontmoeten en samenwerken mét voldoende waarborging van de privacy van betrokkenen. Laagdrempelig, maatwerk en informeel, maar wél steeds bewust van en gepast handelend naar privacyrisico's.

2.2 Betrokken

We ontmoeten, verbinden en werken samen. We creëren het vermogen ons in te leven in anderen, of dit nu een inwoner of collega is. Op basis daarvan passen we ons handelen aan. We werken samen met aandacht voor elkaar, gedeelde verantwoordelijkheid en met zichtbare waardering voor zowel het resultaat als ieders aandeel in het bereiken daarvan. We spreken elkaar respectvol aan en waarderen elkaar als het goed gaat, maar ook als het niet goed gaat.

Betrokkenheid tonen bij de waarborging van de privacy van burgers en andere partijen die met de gemeente Woensdrecht te maken hebben, betekent dat je hen serieus neemt en dat ook laat zien. Dit kan door zorgvuldig om te gaan met de persoonsgegevens van de betrokkenen en zo nodig anderen erop aan te spreken als zij de vereiste zorgvuldigheid niet voldoende in acht nemen. Door als gemeente voor deze betrokkenen altijd goed bereikbaar en aanspreekbaar te zijn als deze een beroep doen op hun privacy rechten. Maar ook door het direct melden van datalekken, mocht er onverhoopt toch iets zijn misgegaan.

2.3 Daadkracht

Door onze betrokkenheid weten we samen met de inwoners wat we willen en werken daar resultaatgericht naar toe. We zijn daarin praktisch en nemen verantwoordelijkheid voor het eindresultaat ook als een ander dat even niet kan. We werken effectief en efficiënt en zoeken samen de rek in de regels als dat nodig is ten gunste van het resultaat.

Daadkracht als het gaat om privacybescherming, betekent vooral het creëren van meer bewustzijn bij de individuele medewerker: het bewustzijn dat het borgen van de privacy van de betrokkenen hand in hand gaat met het sturen op kwaliteit en resultaten. Bijvoorbeeld door tijdig te reageren op verzoeken van betrokkenen, maar ook door pro-actief te handelen als de situatie daarom vraagt. Daarnaast betekent het verantwoordelijkheid nemen als regelgeving tekort schiet en dan actie te ondernemen om – waar nodig – zaken alsnog geregeld te krijgen.

2.4 Dienstbaar

Door onze houding ervaren inwoners of bezoekers een passende, professionele en integrale dienstverlening. Ze ervaren ons als gastvrij door een warm welkom in een vertrouwde omgeving. We staan open voor initiatieven en helpen daarbij met onze kennis en professionaliteit. We hebben oog voor het geheel, ook als een ander dat even niet heeft, juist dan nemen we die mee in ons perspectief.

Dienstbaarheid staat in het kader van privacybescherming voor transparantie. We informeren de burgers op passende wijze, via alle relevante kanalen die daarvoor beschikbaar zijn, over de verwerking van hun gegevens en de mogelijkheid om hun rechten uit te oefenen op het gebied van privacyregulering.

Deze kernwaarden vormen het raamwerk waarbinnen het gemeentelijk privacybeleid verder is uitgewerkt.

3. Wettelijk kader

Het recht op eerbiediging van de persoonlijke levenssfeer bij het verwerken van persoonsgegevens is een grondrecht. Het recht op privacy is niet alleen nationaal als grondrecht erkend, maar ook internationaal in onder andere het Europees Verdrag voor de Rechten van de Mens en het Internationaal kinderrechtenverdrag.

3.1 Europese privacywetgeving

Vanaf 25 mei 2018 geldt de directe werking van de huidige privacywetgeving – de Algemene verordening gegevensbescherming (hierna: AVG) – in de Europese lidstaten. Per diezelfde datum is ook de Uitvoeringswet AVG (hierna: UAVG) in werking getreden.

De snelle technologische ontwikkelingen, de grote hoeveelheid beschikbare data en de aanzienlijke toename van de grensoverschrijdende stromen van persoonsgegevens heeft geleid tot harmonisatie van het Europees Unierecht met betrekking tot de bescherming van persoonsgegevens. Het begrip persoonsgegevens omvat alle gegevens die een natuurlijk identificeerbaar persoon betreffen. NAW-gegevens, burgerservicenummers, e-mail, maar ook kentekens en IP-adressen kunnen als persoonsgegevens worden aangemerkt.

De AVG zorgt voor een versterking en uitbreiding van privacyrechten en brengt meer verantwoordelijkheden voor organisaties. De gemeente dient aan te (kunnen) tonen dat er is voldaan aan de wettelijke eisen omtrent gegevensbescherming. Elke verwerking van persoonsgegevens geschiedt behoorlijk en rechtmatig. E voor betrokkenen dient transparant te zijn dat hun betreffende persoonsgegevens worden verzameld, gebruikt of geraadpleegd. Persoonsgegevens mogen alleen worden verwerkt, indien het doel van de verwerking niet redelijkerwijs op een andere wijze kan worden verwezenlijkt. Secundair gebruik van beschikbare persoonsgegevens is alleen toegestaan met instemming van betrokkene. Gebruik van persoonsgegevens is zonder voorafgaande toestemming aan één doel van verwerking gebonden. De opslagperiode dient niet langer te zijn dan noodzakelijk voor het doel.

Bij dit alles geldt dat materiële wetten waarop veel verwerkingen van de gemeentelijke overheid berusten, voorliggend zijn ten opzichte van de AVG. Indien voor de verwerking de geldende voorliggende materiële wetten niet voorzien in een bescherming van privacy- en/of informatiebeveiliging, geldt de AVG.

3.2 Sectorspecifieke wetgeving

De (U)AVG geldt als parapluwetgeving: bijna alle sectoren, instellingen en bedrijven in Nederland dienen eraan te voldoen². Naast dit algemeen wettelijk kader zijn er in sectorspecifieke wetten aanvullende regels opgenomen omtrent gegevensuitwisseling en het waarborgen van privacy. De Wet Basisregistratie Personen, de Jeugdwet en de Participatiewet zijn voorbeelden van dergelijke wetten met specifieke aanvullende eisen. De gemeente Woensdrecht handelt niet alleen conform de (U)AVG, maar uiteraard ook conform de sectorspecifieke wetgeving.

4. Uitgangspunten

Het privacybeleid is van toepassing op alle gemeentelijke taken en processen die vallen onder de toepassing van de (U)AVG en waar de gemeente Woensdrecht (verwerkings)verantwoordelijk voor is.

Bij het verwerken van persoonsgegevens worden de volgende uitgangspunten in acht genomen:

1. *Legitimiteit*: verwerking van persoonsgegevens vindt uitsluitend plaats voor zover hiervoor een geldige grondslag is;
2. *Doelbinding*: persoonsgegevens worden alleen verwerkt voor zover dat nodig is om het vastgestelde doel te bereiken, en worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen;
3. *Subsidiariteit*: het doel kan niet met minder dan de verzamelde persoonsgegevens worden bereikt;
4. *Proportionaliteit*: de verzamelde persoonsgegevens staan in verhouding tot het doel;
5. *Kwaliteit*: persoonsgegevens zijn juist, nauwkeurig en actueel;
6. *Design*: bij de inrichting, ontwikkeling of aanschaf van producten en/of diensten houdt de gemeente rekening met de eerbiediging van de persoonlijke levenssfeer van betrokkenen (privacy by design);
7. *Informatieveiligheid*: de gemeente hanteert geheimhoudingsafspraken; Informatievoorzieningen zijn beveiligd tegen aantastingen van de vertrouwelijkheid, integriteit en beschikbaarheid van persoonsgegevens;
8. *Integer*: de gemeente hanteert een integriteitsbeleid waarin tevens aandacht wordt geschonken aan integer handelen in relatie tot (persoons)informatie;
9. *Houdbaarheid*: persoonsgegevens die niet langer nodig zijn, worden onomkeerbaar vernietigd of geanonimiseerd;

2) Uitzonderingen worden genoemd in artikel 2, tweede lid, van de AVG en in de artikelen 2 en 3 van de UAVG.

10. *Borging rechten*: de gemeente Woensdrecht waarborgt de in de artikelen 15 – 22 van de AVG opgenomen rechten van betrokkenen;
11. *Transparantie*: betrokkenen worden proactief en op een transparante wijze geïnformeerd over de verwerking van persoonsgegevens door de gemeente c.q. over verstrekken van persoonsgegevens door de gemeente aan derde partijen. De informatie wordt in begrijpelijke taal gegeven;
12. *Derden*: in geval van samenwerking met derde partijen dan wel verstrekking van persoonsgegevens aan derde partijen worden afspraken gemaakt omtrent de voorwaarden waaraan de verwerkingen c.q. verstrekkingen dienen te voldoen. Hierbij geldt in principe minstens eenzelfde niveau van informatiebeveiliging. Er wordt gestreefd naar getekende overeenkomsten met derde partijen;
13. *Kinderen*: de gemeente Woensdrecht erkent de categorie ‘jongeren tot 16’ jaar als bijzondere doelgroep en waarborgt dat verwerking van persoonsgegevens van jongeren tot 16 jaar alleen na uitdrukkelijke toestemming van de ouders en/of wettelijke verzorgers plaatsvindt. De gemeente Woensdrecht controleert actief of die toestemming daadwerkelijk is gegeven;
14. *Verantwoording*: de gemeente Woensdrecht leeft niet alleen de in de AVG opgenomen regels na, maar kan dit ook aantonen³

5. Ambitie volwassenheidsniveau

Uiteraard moeten alle organisaties voldoen aan de wettelijke verplichtingen (bijv. het beschikken over een verwerkingsregister, het voldoen aan de meldplicht voor datalekken, het aanstellen van een FG, etc.), maar de mate waarin organisaties voor het overige ‘AVG-compliant’ zijn wordt mede bepaald door hun ambitie op dat vlak.

Het zogenaamde ‘Capability Maturity Model’ (CMM) – oftewel het Volwassenheidsniveau-model – is een algemeen gebruikt model dat aangeeft op welk niveau de software-ontwikkeling van een organisatie zit. Door ervaring in het gebruik is gebleken dat het niet alleen voor software-ontwikkeling toepasbaar is maar ook op andere processen, zoals bijvoorbeeld de AVG-compliance.

Capability Maturity Model

Volwassenheidsniveau (CMM)		
Geoptimaliseerd	5	Beleid wordt tot op het laagste niveau correct geïnterpreteerd en uitgevoerd. Systematische procesverbetering o.b.v. metingen is onderdeel geworden van de bedrijfsvoering.
Beheerst en meetbaar	4	Het beleid wordt gedragen door de organisatie en de bevoegdheden zijn belegd. Hoge awareness en bijsturing van beheersmaatregelen o.b.v. periodieke kwantitatieve analyse en evaluaties
Gedefinieerd proces	3	De belangrijkste processen zijn gestandaardiseerd, gedefinieerd en voorzien van bijpassende beheersmaatregelen. Procesverbetering vindt plaats o.b.v. een kwalitatieve analyse.
Herhaalbaar, maar intuïtief	2	Er is algemeen beleid of beleid voor belangrijke delen, maar niet noodzakelijk formeel vastgelegd. Er zijn beheersmaatregelen, maar risico's zijn niet overal afgedekt en gedocumenteerd.
Ad hoc / initieel	1	Processen en verantwoordelijkheden zijn niet gedefinieerd en slecht beheersbaar. Problemen worden pas opgelost als ze zich voordoen.

De gemeente Woensdrecht heeft de ambitie om binnen een periode van 2 jaren te voldoen aan volwassenheidsniveau 3; ‘Gedefinieerd proces’. Op dit niveau zijn processen gedocumenteerd en zijn betrokkenen bekend en vertrouwd met beleid, richtlijnen en procedures. Redelijkerwijs beschouwd, is dit het laagste niveau waarop er sprake is van een volledige AVG-compliance. Daarbij hoort een pro-actieve en lerende basishouding, met aandacht voor (de evaluatie van) behaalde resultaten. Op het standaardiseren en vastleggen van processen wordt gecontroleerd.

De gemeente Woensdrecht behaalt op dit moment een volwassenheidsniveau van ± 1.6 en gaat daarmee in de richting van het niveau ‘Herhaalbaar, maar intuïtief’. De concrete uitwerking van het geambieerde volwassenheidsniveau in activiteiten en planning vindt plaats in het privacy-werkprogramma.

6. Grondslagen

De gemeente Woensdrecht verwerkt in het kader van de rechtmatigheidstoets enkel persoonsgegevens indien en voor zover aan tenminste één van de onderstaande (in artikel 6 van de AVG opgenomen) voorwaarden – de zogenaamde ‘grondslagen’ – is voldaan:

- a. er is sprake van expliciete toestemming van de betrokkene;
- b. er is sprake van een overeenkomst met betrokkene;
- c. er is sprake van een wettelijke plicht;

3) In het kader van transparantie over de bedrijfsvoering is de gemeente verplicht medewerking te verlenen aan externe toezichhouders, zoals een accountant. Deze kunnen met wettelijke redenen omkleed inzage eisen in verzamelde persoonsgegevens. Bijzondere persoonsgegevens van betrokkenen zijn voor externe toezichhouders niet toegankelijk.

- d. er is sprake van een vitaal belang van de betrokkene;
- e. er is sprake van een publiekrechtelijke taak;
- f. er is sprake van een gerechtvaardigd belang dat boven het privacybelang van betrokkene staat⁴.

7. Soorten persoonsgegevens: algemene, bijzondere en gevoelige

De Algemene verordening gegevensbescherming (AVG) geeft aan dat een persoonsgegeven alle informatie is over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is. Gegevens van overleden personen of van organisaties zijn geen persoonsgegevens volgens de AVG.

Er zijn verschillende soorten persoonsgegevens. De soorten persoonsgegevens zijn onder te verdelen in categorieën: algemene, gevoelige en bijzondere.

Algemene persoonsgegevens zijn redelijk voor de hand liggende gegevens, zoals iemands naam, adres en woonplaats. Maar ook geboortedata, telefoonnummers en postcodes met huisnummers zijn persoonsgegevens.

Bijzondere persoonsgegevens zijn persoonsgegevens die betrekking hebben op iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele voorkeur en/of strafrechtelijk verleden. Op grond van artikel 9 van de AVG is verwerking van zodanige persoonsgegevens verboden, tenzij er sprake is van een uitzonderingsgrond zoals omschreven in het tweede lid van genoemd artikel.

Gevoelige persoonsgegevens zijn persoonsgegevens die door hun aard/context met extra zorg moeten worden behandeld, maar geen bijzondere persoonsgegevens zijn, bijvoorbeeld financiële of locatiegegevens. Bewindvoering, klantbeeld, betalingsachterstanden, BKR registratie, etc. behoren tot deze categorie. De gevoelige persoonsgegevens gelden exclusief voor Nederland en vragen dezelfde behandeling als de bijzondere persoonsgegevens, namelijk: niet verwerken, tenzij er sprake is van een uitzonderingsgrond als opgenomen in artikel 9, tweede lid, van de AVG.

De bijzondere en gevoelige persoonsgegevens worden door de gemeente Woensdrecht met extra zorgvuldigheid beveiligd en verwerkt.

8. Rechten van betrokkenen

In de artikelen 15 t/m 22 van de AVG zijn de zogenaamde rechten van betrokkenen opgenomen. In het gemeentelijke privacybeleid worden die rechten als volgt geborgd.

8.1 Rechten

8.1.1 Recht op informatie

De gemeente verzamelt gegevens om haar taken te kunnen uitvoeren. Indien dit persoonsgegevens betreffen, heeft de gemeente de plicht om betrokkenen, voor zover deze daar niet reeds van op de hoogte zijn, te informeren over verwerkingen van hun persoonsgegevens. De gemeente verstrekt dan aan betrokkenen informatie over de verwerking, zoals het doel daarvan, welke persoonsgegevens worden verwerkt en of de gegevens aan anderen worden verstrekt. Dit met inachtneming van de beperkingen zoals die neergelegd zijn in wet- en regelgeving. In dit kader publiceert de gemeente ook een privacyverklaring.

8.1.2 Recht op inzage

Betrokkenen hebben de mogelijkheid om te controleren of en op welke manier hun gegevens worden verzameld en verwerkt. Dit met inachtneming van de beperkingen zoals neergelegd in wet- en regelgeving. Voor de gebruikmaking van het 'recht op inzage' is een (digitaal) formulier ontwikkeld en ontsloten.

4) Deze grondslag geldt echter in principe niet voor overheden.

8.1.3 Recht op correctie

Als de gemeente persoonsgegevens van betrokkenen verwerkt die naar hun oordeel onjuist zijn, kunnen zij een verzoek indienen bij de gemeente om dit te verbeteren. Dit met inachtneming van de beperkingen zoals neergelegd in wet- en regelgeving.

8.1.4 Recht om vergeten te worden

Betrokkenen hebben het recht persoonsgegevens te laten verwijderen indien de gemeente niet langer een goede grond heeft voor het gebruik hiervan, bijvoorbeeld indien betrokkenen een gegeven toestemming intrekken, indien de gegevens onjuist zijn of de gegevens niet langer nodig zijn.

8.1.5 Recht op bezwaar tegen verwerking

Betrokkenen hebben het recht aan de gemeente te vragen hun persoonsgegevens niet meer te gebruiken en bezwaar te maken tegen de verwerking van hun persoonsgegevens. De gemeente moet aan het verzoek voldoen, tenzij er gerechtvaardigde gronden zijn voor de verwerking.

8.1.6 Recht op beperking van de verwerking

Het recht op beperking houdt in dat de gemeente de persoonsgegevens (tijdelijk en onder voorwaarden) niet mag verwerken en niet mag wijzigen, bijvoorbeeld wanneer betrokkenen de juistheid van de gegevens ter discussie stellen. De gemeente moet in principe aan het verzoek voldoen.

8.1.7 Recht op overdraagbaarheid van gegevens (dataportabiliteit)

De gemeente is op grond van de AVG op zich niet verplicht om invulling te geven aan de overdraagbaarheid van gegevens voor zover het werkzaamheden betreft in het kader van het algemeen belang, de uitoefening van een openbaar of publieke taak of ter voldoening aan een wettelijke verplichting. Desondanks zal de gemeente in voorkomende gevallen zo mogelijk voorzieningen treffen ten behoeve van dataportabiliteit

8.1.8 Recht niet te worden onderworpen aan geautomatiseerde individuele besluitvorming / profiling

Het in de AVG opgenomen recht niet onderworpen te worden aan geautomatiseerde individuele besluitvorming/profilering betreft feitelijk een verbod. Daarbij kan gedacht worden aan het zonder menselijke tussenkomst verwerken van sollicitaties via internet of het beslissen over het al dan niet toekennen van bijstand. Dit recht c.q. dit feitelijke verbod wordt gerespecteerd.

8.2 Uitoefening van rechten

Om gebruik te maken van de bovenstaande rechten kunnen betrokkenen een verzoek indienen. Zo'n verzoek moet schriftelijk ingediend worden. Verzoek om recht op inzage kan eventueel ook digitaal worden ingediend. Verzoeken worden binnen de in de AVG opgenomen kaders en termijnen afgedaan.

8.3 Klachten

Elke betrokkene heeft het recht bij de gemeente een klacht in te dienen tegen de wijze waarop zijn of haar persoonsgegevens worden verwerkt. Klachten worden direct doorgegeven aan de PrivacyOfficer (PO), die de klacht registreert en ter afdoening 'toewijst' aan de teammanager van het team waar de klacht betrekking op heeft. De desbetreffende teammanager is verantwoordelijk voor de (tijdige, d.w.z. binnen 4 weken) afwikkeling van de klacht en het zo nodig treffen van verbetermaatregelen. Daarnaast wordt de Functionaris Gegevensbescherming (FG) door de PrivacyOfficer geïnformeerd over de ontvangst van de klacht.

Is betrokkene niet eens met de reactie op de klacht? Of is niet tijdig (d.w.z. binnen 4 weken) gereageerd op de klacht? Dan kan een privacyklacht worden ingediend bij de Autoriteit Persoonsgegevens (AP).

Dat kan:

1. via het klachtenformulier op de website van de Autoriteit Persoonsgegevens⁵, of
2. door een brief te sturen naar Autoriteit Persoonsgegevens, Postbus 93374, 2509 AJ in Den Haag

5) Zie www.autoriteitpersoonsgegevens.nl

9. Derde partijen

Met het oog op de bescherming van persoonsgegevens maakt de gemeente Woensdrecht met externe partijen afspraken omtrent de omgang met persoonsgegevens. Dit kan in bijvoorbeeld verwerkersovereenkomsten of convenanten.

9.1 Verwerkersovereenkomst

Als 'verwerkingsverantwoordelijke' is de gemeente Woensdrecht verantwoordelijk voor de juiste verwerking van persoonsgegevens. Dat betekent dat de gemeente daar zelf zorgvuldig en correct mee moet omgaan, maar ook dat de gemeente ervoor moet zorgen dat leveranciers of partners die met die persoonsgegevens werken dat óók doen. De uitvoering van verwerkingen van persoonsgegevens door een derde wordt geregeld in een verwerkersovereenkomst.

Verwerkersovereenkomsten moeten inhoudelijk aan wettelijke eisen voldoen (opgenomen in artikel 28, derde lid, van de AVG). De VNG heeft een standaard-verwerkersovereenkomst opgesteld. Deze standaard is per 1 januari 2020 verplicht.

9.2 Convenanten

Verwerkersovereenkomsten hebben betrekking op de verhouding tussen een 'verwerkingsverantwoordelijke' en de 'verwerker'. Het kan zijn dat partijen gezamenlijk verantwoordelijk zijn voor de (verwerking van de) persoonsgegevens. In het geval van zo'n mede-verwerkingsverantwoordelijkheid bepaalt de AVG dat de verwerkingsverantwoordelijken in een 'onderlinge regeling' op 'transparante wijze' hun respectievelijke AVG-verantwoordelijkheden vaststellen; in de gemeente Woensdrecht gebruiken we hiervoor het instrument 'verwerkersconvenant'.

Niet alleen in het kader van gezamenlijke verwerkingsverantwoordelijkheid, maar ook indien de gemeente Woensdrecht anderszins structureel persoonsgegevens uitwisselt met externe partijen (denk bijvoorbeeld aan het Zorg- en Veiligheidshuis of Buurtbemiddeling), maakt de gemeente Woensdrecht duidelijke afspraken over de (wijze van) gegevensuitwisseling en de waarborging van privacy en informatieveiligheid.

9.3 Uitwisseling binnen internationale samenwerking tussen landen en met organisaties

Uitwisseling van persoonsgegevens met landen/organisaties buiten de Europese Economische Ruimte (EER) is in beginsel niet toegestaan, tenzij er sprake is van een wettelijke uitzondering of een passende overeenkomst (overdrachtsmechanisme). Er zijn verschillende soorten overdrachtsmechanismen in de AVG opgenomen. De gemeente Woensdrecht streeft ernaar om alleen in noodzakelijke gevallen en uiteraard binnen de voorwaardelijke kaders persoonsgegevens uit te wisselen met landen/organisaties buiten de EER.

10. Informatiebeveiliging en privacy

Informatiebeveiliging is de verzamelaar voor de processen die de gemeente inricht om de betrouwbaarheid van informatie te beschermen, ook als die zich in gemeentelijke processen of in informatiesystemen bevinden. Het begrip 'informatiebeveiliging' heeft betrekking op:

- beschikbaarheid: het zorg dragen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers;
- integriteit: het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking;
- vertrouwelijkheid: het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn.

De gemeente neemt passende technische en organisatorische maatregelen teneinde persoonsgegevens te beveiligen tegen verlies, onbevoegde toegang of onrechtmatige verwerking. Hoe gevoeliger de informatie is, des te hoger het beveiligingsniveau. Daarnaast besteedt de gemeente Woensdrecht reeds bij de ontwikkeling en aanschaf van producten/diensten alsook bij de ontwikkeling van (bedrijfsvoerings)beleid (bijv. het gemeentelijk mailbeleid) aandacht aan passende technische en organisatorische maatregelen in het kader van informatieveiligheid en privacy.

De gemeente Woensdrecht gebruikt een vastgesteld informatieveiligheidsbeleid, waarin kaders en maatregelen voor de beveiliging van (persoons)gegevens zijn opgenomen. Het thans vigerende 'Informatiebeveiligingsbeleid van de gemeente Woensdrecht 2018-2021'⁶ dat op 6 februari 2018 door het college is vastgesteld, heeft betrekking op alle gemeentelijke processen, waaronder de processen waarin (persoons)gegevens worden verwerkt. De Chief Information Security Officer (CISO) ziet toe op de naleving daarvan.

Wanneer de gemeente persoonsgegevens verwerkt of laat verwerken door een derde, zorgt de gemeente ervoor dat passende beveiligingsmaatregelen (conform het informatiebeveiligingsbeleid) worden getroffen om de betreffende persoonsgegevens te beschermen tegen de verschillende risico's. Denk hierbij aan anonimiseren en pseudonimiseren,

10.1 Logging

Niet alleen moeten organisaties moderne technieken gebruiken om persoonsgegevens te beveiligen, ook moet er gekeken worden hoe er met persoonsgegevens wordt omgegaan; wie heeft er bijvoorbeeld toegang tot welke gegevens? Het betreft hier de eis van (actieve) logging. De gemeente Woensdrecht zorgt ervoor dat de binnen de gemeente gebruikte applicaties logging technisch mogelijk is én dat er op basis van een 'loggingsprotocol' actieve logging en periodieke rapportage daarover c.q. opvolging naar aanleiding daarvan plaatsvindt.

11. Meldplicht datalekken

Op grond van artikel 33 van de AVG geldt er een meldplicht voor datalekken. Er is sprake van een datalek als er zich een inbreuk voordoet op de beveiligingsmaatregelen, wat leidt tot het per ongeluk, opzettelijk of onrechtmatig vernietigen, verliezen, aanpassen of tot ongeautoriseerde openbaarmaking van of toegang tot persoonsgegevens die overgedragen, bewaard of op een andere manier verwerkt zijn. Voorbeelden van een datalek zijn het verlies van een mobiel apparaat waarop (al dan niet gevoelige) persoonsgegevens staan of het verkeerd adresseren van een brief. Maar ook computerhacking, besmetting met ransomware of het technisch falen van apparatuur, stroomuitval, brand of wateroverlast kunnen leiden tot een datalek.

Een datalek moet op grond van artikel 33 van de AVG 'zonder onredelijke vertraging' en uiterlijk binnen 72 uur na ontdekking van het datalek door de verwerkingsverantwoordelijke worden gemeld aan de toezichthouder, de Autoriteit Persoonsgegevens. Indien de melding later gebeurt, dan moet de melding worden voorzien van uitleg omtrent de vertraging.

Niet ieder datalek-incident valt onder de meldplicht. Er geldt namelijk een meldingsplicht, 'tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen'. Als bijvoorbeeld verloren of gestolen persoonsgegevens goed versleuteld zijn opgeslagen, dan is er mogelijk geen aanzienlijk risico op schade aan de persoonlijke levenssfeer van betrokkenen.

Ingeval van een (vermoeden van een) datalek handelt de gemeente in overeenstemming met de 'Procedure melding datalekken'⁷ vastgestelde werkwijze. In aansluiting op het privacy- en informatieveiligheidsbeleid en onverminderd het bepaalde in andere procedures/protocollen (bijv. rond incidentmanagement) beschrijft deze procedure de wijze waarop binnen de gemeentelijke organisatie wordt omgegaan met de meldplicht voor datalekken. Het gaat hierbij zowel om interne als om externe meldingen.

12. Rollen en verantwoordelijkheden

12.1 Verwerkingsverantwoordelijke: college/burgemeester/gemeenteraad

Het college van burgemeester en wethouders respectievelijk de burgemeester en de gemeenteraad zijn de verantwoordelijke bestuursorganen die, ieder voor zover het hun taakuitoefening betreft, invulling geven aan de taken en verantwoordelijkheid die krachtens de AVG zijn toebedeeld aan de verwerkings-

6) Zaaknr. Z17.05540 / Docnr. 2017.43912. Er wordt momenteel aan een herziening van het informatieveiligheidsbeleid gewerkt waarbij de BIO (Baseline Informatiebeveiliging Overheid; treedt in werking per 1-1-2020) als uitgangspunt wordt genomen.

7) Zaaknr. Z19.02743 / Docnr. 2019.25245

verantwoordelijke. Formeel zijn het college van respectievelijk de burgemeester en de gemeenteraad dan ook verantwoordelijk voor de verwerkingen die onder de reikwijdte van de AVG vallen. De verwerkingen op grond van de richtlijn gegevensbescherming opsporing en vervolging vallen hier niet onder.

Het college van burgemeester respectievelijk de burgemeester en de gemeenteraad, ieder voor zover het hun taakuitoefening betreft:

- stellen privacybeleid vast;
- stellen op grond van artikel 37 van de AVG een Functionaris voor de Gegevensbescherming (FG) aan.

Het college van burgemeester en wethouders:

- bevordert de beschikbaarheid van voldoende middelen om privacybescherming passend te waarborgen;
- wijst uit zijn midden een portefeuillehouder Privacy & Informatieveiligheid aan die bestuurlijk verantwoordelijk is voor de uitvoering van het gemeentelijk privacybeleid;
- stelt een Privacy Officer (PO) aan.

12.2 Portefeuillehouder Privacy & Informatieveiligheid

De portefeuillehouder Privacy & Informatieveiligheid is bestuurlijk verantwoordelijk voor de uitvoering van het gemeentelijk privacybeleid. De portefeuillehouder informeert de Raad binnen de jaarlijkse P&C-cyclus over de uitvoering van het privacybeleid binnen de gemeente.

In het kader van de melding van datalekken fungeert de portefeuillehouder Privacy & Informatieveiligheid als 'gemandateerd verwerkingsverantwoordelijke' namens het college van burgemeester en wethouders. De portefeuillehouder Privacy & Informatieveiligheid neemt in dat kader in mandaat beslissingen omtrent het al dan niet melden van datalekken aan de AP c.q. het doen van mededeling aan betrokkene(n).

12.3 Management

Het nemen van maatregelen om te voldoen aan de AVG is een taak voor de organisatie. Het management draagt hiervoor de verantwoordelijkheid en heeft hiertoe ook een aantal bevoegdheden gemandateerd gekregen (bijv. de beslissing op verzoeken betreffende de uitoefening van rechten van betrokkenen en de ondertekening van de verwerkersovereenkomsten). De gemeentesecretaris/algemeen directeur geldt in dit kader als de ambtelijk eindverantwoordelijke.

In het verwerkingsregister zijn de processen opgenomen waarin persoonsgegevens worden verwerkt. Binnen de afzonderlijke teams zijn 'proceseigenaren' verantwoordelijk voor de naleving van de privacywetgeving en het Woensdrechtse privacybeleid. Het proceseigenaarschap is belegd bij de desbetreffende teammanagers. Bij de uitvoering van hun verantwoordelijkheden kunnen zij zich laten adviseren en zo mogelijk ondersteunen door de PO en (leden van) het Privacyteam.

12.4 Stuurgroep Privacy

De portefeuillehouder Privacy & Informatieveiligheid en de gemeentesecretaris/algemeen directeur vormen gezamenlijk de Stuurgroep Privacy. De Stuurgroep Privacy bestaat verder uit de FG als adviseerend lid. Deze Stuurgroep Privacy stelt het jaarlijkse Privacy-werkprogramma vast en stuurt op de uitvoering daarvan. De Stuurgroep Privacy komt minimaal eens per kwartaal bijeen en wordt ondersteund door de PO.

12.5 Functionaris voor de Gegevensbescherming (FG)

De AVG stelt het aanstellen van een FG verplicht voor overheidsinstanties en publieke organisaties. De FG ziet er op toe dat de gemeente Woensdrecht voldoet aan de wettelijke verplichtingen bij het verwerken van persoonsgegevens. Hij toetst onder andere de naleving van de wettelijke eisen, (de uitvoering van) het privacybeleid en de gemeentelijke richtlijnen op het gebied van privacy. Om deze taak uit te voeren heeft de FG controlebevoegdheden. Daarnaast geeft hij advies omtrent uit te voeren gegevensbeschermingseffectbeoordelingen en ziet hij toe op de uitvoering hiervan. De FG stelt periodiek rapportages op en rapporteert zo nodig rechtstreeks aan het college en/of andere verwerkingsverantwoordelijken.

12.6 Privacy Officer (PO)

Binnen de gemeente is een PO aangesteld. De PO adviseert over c.q. vormt de vraagbaak binnen de gemeente voor AVG-/privacyvraagstukken, geeft advies omtrent de uitvoering van het privacybeleid en draagt bij aan de vergroting van privacybewustzijn en -kennis. Daarnaast ondersteunt de PO bij het verrichten van zogenaamde gegevensbeschermingseffectbeoordelingen (GEB's), maar bijv. ook bij het onderhouden van diverse registers (met name het verwerkingsregister en het, datalekregister).

12.7 Privacyteam

Vanuit ieder team én vanuit de griffie is een medewerker vertegenwoordigd in het Privacyteam. Ook de CISO maakt hier deel van uit. Het Privacyteam fungeert als kennis- en leerplatform en ondersteunt het management bij de uitvoering van hun verantwoordelijkheden. De PO is voorzitter van het Privacyteam. De leden van het Privacyteam zijn privacy-ambassadeurs en vervullen de rol van kennis- en cultuur(uit)drager binnen hun team.

Het Privacyteam komt in principe één keer per maand bijeen. De stand van zaken van uitvoering van het Privacy-werkprogramma, actuele privacy-ontwikkelingen, interne knel-/ontwikkelpunten, recente datalekken etc. vormen onderwerp van gesprek. Op verzoek (van ofwel de PO ofwel de FG) sluit de FG aan voor kennisoverdracht of afstemming.

12.8 Chief Information Security Officer (CISO)

De CISO stelt kaders op voor informatiebeveiliging en adviseert het bestuur en management hierover. De CISO houdt toezicht op de informatiebeveiligingsmaatregelen die de organisatie neemt om gegevens, waaronder persoonsgegevens, te beveiligen. De CISO werkt hierbij nauw samen met de FG en PO.

13. Governance

Jaarlijks wordt er een 'Privacy-werkprogramma' opgesteld. Dit werkprogramma is 1-op-1 gebaseerd op het zgn. 'model AVG Borging' van de VNG/IBD⁸ en geeft aan welke activiteiten er dat jaar door wie worden uitgevoerd. Bij de opstelling van het werkprogramma wordt rekening gehouden met de in de FG-rapportage opgenomen bevindingen.

Het Privacy-werkprogramma wordt opgesteld door de PO en vastgesteld door de Stuurgroep Privacy. Het Privacy-werkprogramma geeft aan welke activiteit door wie c.q. onder wiens verantwoordelijkheid wordt uitgevoerd en is feitelijk op onderdelen een (gedelegeerde) taak-/werkopdracht voor de PO en het Privacyteam.

De uitvoering van het Privacy-werkprogramma wordt gemonitord, zo mogelijk via een Privacy Management Systeem (PMS). De PO ziet toe op een juist beheer van het PMS.

De FG rapporteert 'onafhankelijk' over de uitvoering van het privacybeleid. De Stuurgroep Privacy stuurt op de uitvoering van het privacybeleid en het Privacy-werkprogramma. De PO rapporteert periodiek de Stuurgroep Privacy over de uitvoering van het Privacy-werkprogramma.

14. Naleving van het beleid

14.1 Risicobeheersing en controlemechanismen

Vanuit de gedachte van risicobeheersing, neemt de gemeente Woensdrecht verschillende maatregelen om de risico's bij de verwerking van persoonsgegevens in kaart te brengen en te verminderen. Hiervoor gelden de volgende cycli van risicobeheersing:

1. het in kaart brengen verwerkingen met persoonsgegevens (verwerkingsregister);
2. het waar nodig uitvoeren van gegevensbeschermingseffectbeoordelingen (GEB's);

8) VNG/IBD: Vereniging Nederlandse Gemeenten/InformatieBeveiligingsDienst. VNG Realisatie heeft i.s.m. de IBD criteria ontwikkeld om de AVG te vertalen naar een kwaliteitscyclus voor gegevensbescherming en privacy voor gemeentelijke processen. Het model biedt gemeente concrete handvatten om een goede omgang met persoonsgegevens in de gehele organisatie te waarborgen.

3. het periodiek evalueren van privacy-incidenten.

Deze cycli van risicobeheersing worden in de praktijk aan de hand van de hieronder toegelichte controlemechanismen ten uitvoer gebracht.

14.1.1 Verwerkingsregister

De gemeente Woensdrecht houdt een register van verwerkingen (verwerkingsregister) bij met alle verwerkingsactiviteiten van persoonsgegevens per proces. Onder andere de doeleinden van de verwerkingen, de categorieën van persoonsgegevens, ontvangers, bewaartermijnen en de rechtmatige grondslag worden hierin opgenomen. Artikel 30 AVG geeft richtlijnen waar het register van verwerkingsactiviteiten initieel aan moet voldoen.

De gemeente stelt op haar website een publieke versie beschikbaar.

14.1.2 Gegevensbeschermingseffectbeoordelingen

Bij de invoering van nieuw beleid of regelgeving of bij het gebruik van nieuwe technologieën houdt de gemeente Woensdrecht al bij het 'ontwerp' rekening met de bescherming van de persoonlijke levenssfeer, de zgn. Privacy by Design. Bij nieuwe verwerkingen onderzoekt de gemeente vooraf het risico voor de bescherming van persoonsgegevens en de vrijheden van de betrokkene(n). De wijze waarop de gemeente Woensdrecht hieraan invulling geeft is o.a. door een gegevensbeschermingseffectbeoordeling uit te voeren.

In de gegevensbeschermingseffectbeoordeling komt op grond van artikel 35, zevende lid, van de AVG, ten minste naar voren:

- a. een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden;
- b. een beoordeling van de noodzaak en de evenredigheid van de verwerkingen;
- c. een beoordeling van de risico's voor de rechten en vrijheden van burgers;
- d. de beoogde passende technische en organisatorische maatregelen om de risico's aan te pakken.

Wanneer het effect van een verwerking beoordeeld is, wordt de FG geraadpleegd en om advies gevraagd. Bij een onverminderd getaxeerd hoog risico legt de gemeente de situatie voor aan de AP. Bij een positief besluit met voldoende waarborgen, kan de verwerking een aanvang nemen. Deze gang van zaken geldt ook voor voorgestelde verbeterprocessen.

14.1.3 Privacy-incidenten

Datalek-meldingen worden op initiatief van de PO 'evaluatief' besproken in het Privacyteam. Doel van deze bespreking is het trekken van 'lering' uit de datalek-meldingen, zowel inhoudelijk ter voorkoming van vergelijkbare datalekken in de toekomst als procesmatig v.w.b. het meldings-/afdoeningsproces van datalekken.

14.2 Privacy-bewustzijn

Privacy is voor een belangrijk deel een zaak van bewustwording, cultuur en communicatie. Bestuurders en medewerkers moeten zich bij de uitoefening van hun werkzaamheden voortdurend bewust zijn van het belang van het waarborgen van de privacy van betrokkenen, zoals burgers, eigen medewerkers en ZZP-ers. De gemeente ondersteunt dit bewustwordingsproces door het ontwikkelen van protocollen, het opstellen van afwegingskaders en het organiseren van trainingen en andere kennis- en bewustwordingsverhogende initiatieven.

Alle medewerkers van de gemeente Woensdrecht dienen bij te dragen aan de eerbiediging van de persoonlijke levenssfeer en bescherming bij de verwerking van persoonsgegevens. Privacy dient dan ook ingebed te zijn in de door hen te hanteren werkwijze(n). De gemeente werkt actief aan het optimaliseren van kennis omtrent privacy en een transparante procesuitvoering.

15. Samenwerking en privacy

De gemeente Woensdrecht werkt op verschillende terreinen in verschillende 'verbanden' met verschillende partners samen. Waar er in die samenwerkingen sprake is van privacygerelateerde thema's, werkt de gemeente Woensdrecht bij voorkeur ook samen in de uitvoering van die thema's/onderwerpen. Concreet kan bijvoorbeeld worden gedacht aan samenwerking in het kader van de risicobeheersing bij de gezamenlijke aankoop/ontwikkeling van applicaties in Equalit-verband of anderszins (het gezamenlijk

opstellen van een GEB of één gemandateerde partij die voor alle gezamenlijke deelnemers één GEB uitvoert). Ook kan bijv. worden gedacht aan het machtigen van één samenwerkingspartij om een verwerkersovereenkomst met een gezamenlijke verwerker ook namens de andere samenwerkingspartners op te stellen en te sluiten. De gemeente Woensdrecht blijft in dit kader zelf onverminderd (verwerkings)verantwoordelijk en zorgt ervoor deze verantwoordelijkheid indien nodig te (kunnen) nemen.

16. Aantoonbare verantwoording

De verantwoordingsplicht van de gemeente brengt met zich mee dat de gemeente niet alleen de regels moet naleven, maar dit ook moet kunnen aantonen. In dit kader:

1. publiceert de gemeente Woensdrecht het gemeentelijk privacybeleid op de gemeentelijke website;
2. publiceert de gemeente Woensdrecht de gemeentelijke privacyverklaring op de gemeentelijke website;
3. beschikt de gemeente Woensdrecht over een actueel en volledig verwerkingenregister en publiceert de gemeente een abstract van het register op de gemeentelijke website;
4. beschikt de gemeente over een actueel en volledig register van datalekken en van gegevensbeschermingseffectbeoordelingen (GEB-register);
5. zorgt de gemeente Woensdrecht voor aantoonbaarheid van genomen maatregelen en beslissingen.

17. Tot slot

Zoals reeds in de inleiding gesteld geeft het algemene privacybeleid van de gemeente Woensdrecht verdere invulling aan de uit de privacywetgeving voortvloeiende verplichtingen en bevoegdheden. Met dit beleid wordt duidelijk richting gegeven aan hoe de organisatie om moet gaan met privacy en laat zien dat zij de privacy waarborgt, beschermt en handhaaft.

Desgewenst wordt er ook 'domeinspecifiek' privacybeleid opgesteld/vastgesteld, al dan niet in samenwerking met andere gemeenten en/of (keten)partners, bijvoorbeeld op het gebied van het Sociaal Domein. Het algemene privacybeleid biedt in dat geval een algemeen (toetsings)kader voor het domeinspecifieke privacybeleid.

Aldus ondertekend door de gemeenteraad van Woensdrecht d.d. 17 september 2020

De griffier, De voorzitter,

Aldus vastgesteld door het college van burgemeester en wethouders van Woensdrecht d.d. 30 juni 2020

De secretaris, De burgemeester,

Aldus vastgesteld door de burgemeester van Woensdrecht d.d. 30 juni 2020

De burgemeester,

Drs. J.J.C. Adriaansen