gemeente Deventer

Beleidskader privacy en gegevensbescherming

Januari 2018

Vastgesteld door het college van burgemeester & wethouders van Deventer op 16 januari 2018

Inhoud

1 Privacy algemeen

1.1 Algemeen

Iedereen heeft recht op privacy. Het recht op privacy omvat meerdere aspecten. Lichamelijke integriteit, het huisrecht en het briefgeheim valt bijvoorbeeld onder dat begrip. Dit beleidskader gaat over de wijze waarop de gemeente Deventer omgaat met (persoons)gegevens en hoe de gemeente in dat verband de privacy van burgers borgt.

De gemeente Deventer verwerkt op grote schaal persoonsgegevens van burgers. Dat gebeurt lang niet alleen in het sociale domein maar ook op veel andere beleidsterreinen. Daarnaast werkt de gemeente steeds meer samen met andere overheidsorganisaties en met maatschappelijke en zorgpartners waarbij het delen van gegevens van burgers inherent is aan de samenwerking. De gemeente hecht aan een adequate wijze van dienstverlening en samenwerking met een daarop ingerichte efficiënte verwerking van persoonsgegevens. Maar de burger moet er ook op kunnen vertrouwen dat de gemeente en haar partners de privacywetgeving in acht nemen en zodanig zorgvuldig omgaan met persoonsgegevens dat de privacybescherming geborgd is.

In dat verband is van belang dat de Europese Algemene Verordening Gegevensbescherming (AVG) op 25 mei a.s. in volle omvang in werking treedt. Deze verordening vervangt onze Wet bescherming persoonsgegevens (Wbp) en stelt niet alleen eisen aan de gegevensverwerking van organisaties maar verplicht ook tot het aantoonbaar treffen van beheersmaatregelen binnen organisaties zoals de gemeente om privacy en gegevensbescherming te borgen.

1.2 Reikwijdte en afbakening privacy

Het gemeentelijk privacybeleid is van toepassing op alle taken en processen waar de gemeente voor verantwoordelijk is. Het privacybeleid heeft betrekking op de persoonsgegevens van personen van wie de gemeente Deventer gegevens verwerkt of laat verwerken.

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

Er is al snel sprake van ‘*verwerken*’ van persoonsgegevens. 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 valt allemaal onder het verwerken van persoonsgegevens.

2 Privacybeleid

2.1 Ambitie en doelstelling

Doel van dit beleidskader privacy is het beschrijven van kaders voor het verantwoord omgaan met persoonsgegevens en het waarborgen van de privacyrechten van personen waarvan de gemeente Deventer persoonsgegevens verwerkt.

De gemeente Deventer ziet de bescherming van persoonsgegevens als een zaak van behoorlijk bestuur. In onze huidige datamaatschappij moeten inwoners en medewerkers erop kunnen vertrouwen dat persoonsgegevens rechtmatig, zorgvuldig en veilig worden verwerkt. Wie voor de gemeente werkt, begrijpt dit en laat zich hierdoor leiden in zijn of haar dagelijks werk. Het college van B&W schept de voorwaarden voor een privacybewuste organisatiecultuur. We zijn transparant over onze gegevensverwerking en de manier waarop wij persoonsgegevens beschermen. Bij dilemma's gaan wij de dialoog met betrokkenen aan en zoeken naar oplossingen.

Deze ambitie en dit doel kan niet in één keer bereikt worden. De eerste mijlpaal is het toewerken naar het voldoen aan de Europese Algemene Verordening Gegevensbescherming (AVG) welke op 28 mei 2018 volledig in werking treedt. Deze verordening heeft rechtstreekse werking en vervangt de Wet bescherming persoonsgegevens (Wbp). Een belangrijk verschil met de Wbp is dat de AVG sterker de nadruk legt op de organisatorische waarborgen ter bescherming van persoonsgegevens. Ook worden zwaardere eisen gesteld aan organisaties waarvan de bedrijfsvoering verhoogde privacy risico's met zich meebrengt zoals gemeenten.

Het hebben van een beleidskader privacy geeft invulling aan één van de basiseisen die in de AVG wordt gesteld. In een separaat uitvoeringsplan 'Grip op privacy' worden aanvullende maatregelen benoemd om concreet invulling te geven aan de organisatorische waarborgen waar de AVG op doelt.

2.2 Uitgangspunten

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

a. *Rechtmatigheid, behoorlijkheid, transparantie*

Persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt.

b. *Grondslag en doelbinding*

De gemeente zorgt ervoor dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen worden verzameld en verwerkt. Persoonsgegevens worden alleen met een rechtvaardige grondslag verwerkt.

c. *Dataminimalisatie*

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

d. Bewaartermijn

Persoonsgegevens worden niet langer bewaard dan nodig is. Het bewaren van persoonsgegevens kan nodig zijn om de gemeentelijke taken goed uit te kunnen oefenen of om wettelijke verplichtingen te kunnen naleven.

e. Integriteit en vertrouwelijkheid

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

f. Delen met derden

In het geval van samenwerking met externe partijen, waarbij sprake is van gegevensverwerking van persoonsgegevens, maakt de gemeente afspraken over de eisen waar gegevensuitwisseling aan moet voldoen. Deze afspraken voldoen aan de wet. De gemeente controleert deze afspraken [termijn].

g. Subsidiariteit

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

h. Proportionaliteit

De gegevensverwerking gaat niet verder dan strikt genomen nodig is voor het doel.

i. Rechten van betrokkenen

De gemeente honoreert de rechten van betrokkenen.

2.3 Beleidskader en uitvoeringsplan

Dit beleidskader privacy en gegevensbescherming bevat de bestuurlijke dimensie van het privacybeleid en fungeert als raamwerk waarin het overkoepelende beleid van de gemeente Deventer wordt beschreven. Dit kader bevat ook de aanzet voor het regelen van aspecten van privacy-beleidsvoering. Dit beleidskader zoomt niet in op de spelregels die gelden voor specifieke activiteiten en werkzaamheden.

In het uitvoeringsplan ‘Grip op privacy’ wordt de organisatorische en operationele dimensie van privacy geadresseerd. Het beleidskader moet nader worden uitgewerkt in procesplannen waarin de werkprocessen beschreven worden. In deze procesplannen worden de gegevensverwerking en de privacywaarborgen nader uitgewerkt zodat een privacybestendige aanpak ontstaat. Voor zover van toepassing, houden proceseigenaren daarbij ook rekening met bijzondere wettelijke voorschriften en dan met name privacy-relevante bepalingen in de Wet basisregistratie personen, de Participatiewet, de Jeugdwet, de Wet maatschappelijke ondersteuning e.d.

Het beleidskader privacy en gegevensbescherming, het uitvoeringsplan ‘grip op privacy’, de procesplannen en de daadwerkelijke uitvoering hiervan via organisatorische, technische en juridische oplossingen vormen samen het privacybeleid van de gemeente Deventer.

2.4 Verantwoording en risico's

Door bestuurlijk privacybeleid, eventueel nader uitgewerkt voor bepaalde thema's, komen de beleidsmatige ijkpunten 'op groen' te staan. Door procesplannen en bewijs van uitvoering komen ook de uitvoeringsijkpunten 'op groen' te staan. Op deze manier is er een sluitend en aantoonbaar stelsel van privacywaarborgen en dus bewijs van adequaat privacymanagement.

Gemeenten hebben daarbij een documentatieplicht. Er moet op elk moment met documenten kunnen worden aangetoond dat de juiste organisatorische en technische maatregelen zijn getroffen om aan de AVG te voldoen. Dit vergt een privacy-boekhouding, bv. in de vorm van 'GRC-tooling', voor management, monitoring en documentatie waarmee het overzicht behouden wordt en sturing mogelijk is.

Bij schending van de privacy is het college van B&W wettelijk aansprakelijk. Het verwijtbaar onvoldoende beschermen van persoonsgegevens en het niet naleven van privacywet- en regelgeving kan leiden tot:

- het betalen van schadevergoeding;
- reputatieschade en herstelkosten;
- onderzoeken, dwangmaatregelen en hoge bestuurlijke boetes. Bij overtreding van de AVG kan de Autoriteit Persoonsgegevens (AP), de landelijke toezichthouder, zeer forse boetes opleggen tot zelfs € 20 miljoen.

Binnen bepaalde domeinen wordt er gewerkt met bijzondere persoonsgegevens zoals medische gegevens, gegevens over iemands financiële situatie of strafrechtelijke gegevens. Voorbeelden zijn het sociale domein, leerlingzaken, burgerzaken. De verwerking van deze persoonsgegevens is alleen onder specifieke voorwaarden toegestaan. De risico's bij de verwerking van bijzondere persoonsgegevens zijn hoger.

De risico's van schending van de privacy voor personen variëren van ongemak, substantiële benadeling, ernstige sociale beschadiging of gevaren voor de gezondheid en de persoonlijke veiligheid.

3 Privacymanagement

Privacymanagement omvat alle maatregelen die ervoor zorgen dat de gemeente zich houdt aan de AVG en daarover verantwoording (accountability) aflegt. Daarbij wordt zoveel mogelijk aangesloten op bestaande structuren en procedures waarbij privacy een structureel aandachtspunt binnen de reguliere planning & control cyclus moet worden. Privacymanagement is dus gericht op het uitvoeren van het privacybeleidskader.

3.1 Taken en verantwoordelijkheden

Het college van B&W is eindverantwoordelijk voor de naleving van privacywetgeving met de burgemeester als portefeuillehouder. Directie en lijnmanagement hebben 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 evenwichtig plaatsvindt. Dat wil zeggen; behoorlijk, zorgvuldig en in overeenstemming met de wet.

Het college legt over de privacybeleidsvoering verantwoording af aan de gemeenteraad. Het college zorgt ook 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.

Onderstaande tabel brengt de verantwoordelijkheden in beeld aan de hand van het RASCI-model:

Verantwoordelijk		Rol
R	Responsible / feitelijk verantwoordelijk	1e lijn - Gemeentesecretaris - Directie - Teammanagers - Alle medewerkers (incl. inhuur en externen)
A	Accountable / eindverantwoordelijk	1e lijn - College van burgemeester en wethouders
S	Supporting / ondersteunend	2e lijn - Privacyadviseur - Informatieadviseurs - Juristen
C	Consulted / controlerend	3e lijn - FG - CISO - Controller - Accountant
I	Informed / geïnformeerd	Belanghebbenden - Inwoners - Medewerkers - Gemeenteraad - AP

3.2 Managementstructuur

De gemeenteraad:
- controleert de uitvoering van de privacykaders door het college

Het college van B&W:
- is eindverantwoordelijk om te waarborgen dat persoonsgegevens worden beschermd op een manier welke in overeenstemming is met de geldende wet- en regelgeving en de zorgvuldigheidsvereisten. Er is een directe relatie met de beginselen van behoorlijk bestuur.
- stelt kaders voor de bescherming van de privacy op wet- en regelgeving;
- rapporteert aan de gemeenteraad over de uitvoering van het privacybeleid.

De directie:
- is verantwoordelijk voor kaderstelling en sturing;
- stuurt op concernrisico's;
- controleert of de getroffen maatregelen voldoende bescherming bieden om de privacy van betrokkene(n) te beschermen;
- beoordeelt periodiek het privacybeleid op basis van de evaluatie en aanpassingen van het privacybeleid.

De teammanager:
- is operationeel eindverantwoordelijk voor de uitvoering van gemeentelijke taken; is verantwoordelijk voor kaderstelling en sturing;
- zorgt daarbij voor naleving van wet- en regelgeving en het privacybeleid zoals rechtmatige, behoorlijke en transparante verwerking, bewustwording, gebruikt en evalueert Privacy Impact Assessments (PIA's), past 'Privacy by design/default' toe en zorgt voor registratie van verwerkingsactiviteiten;
- meldt aan de privacyadviseur een nieuwe, een wijziging of een beëindiging van een verwerking van persoonsgegevens ten behoeve van het register van verwerkingsactiviteiten;
- stelt het privacy- en informatiebeveiligingsbeleid regulier aan de orde in het werkoverleg.

De medewerker:
Alle medewerkers, inclusief inhuur en externen, zijn verantwoordelijk voor de bescherming van de privacy van betrokkene(n). Dat betekent dat iedereen zorgt voor een rechtmatige, behoorlijke en transparante verwerking van persoonsgegevens.

3.3 Proceseigenaarschap

De teammanager is er verantwoordelijk voor dat de gemeentelijke taakuitoefening binnen de grenzen van dit privacybeleidskader plaatsvindt en rapporteert hierover aan de directie die op haar beurt rapporteert aan het college. Het college legt verantwoording af aan de gemeenteraad.

Een teammanager is proceseigenaar. Proceseigenaren voeren regie over hun proces(sen) op basis van procesplannen die voldoende overzicht bieden van de procesvoering voor effectieve sturing. Een procesplan dient te passen binnen dit privacybeleidskader en is steeds in overeenstemming met de feitelijke situatie.

Bij teamoverstijgende processen kan een coördinerend teammanager of een andere functionaris, bv. een directeur, worden aangewezen.

De proceseigenaar kan verantwoordelijkheden mandateren aan medewerkers ('subproceseigenaren')

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

3.4 Toezicht op naleving : de FG

De Functionaris voor Gegevensbescherming (FG) is de toezichthouder van de gemeente Deventer op de naleving van privacywetgeving conform de AVG. Een FG is voor gemeenten zelfs verplicht.

De FG is wettelijk toezichthouder náást de Autoriteit Persoonsgegevens. Tevens fungeert de FG als ombudsman voor personen die klagen over gebrekkige gegevensverwerking.

Grofweg moet een FG over de volgende kwaliteiten beschikken:

- expert op het gebied van privacywetgeving
- praktijkdeskundig (kennis van organisaties, processen, ICT en informatiebeveiliging)
- onafhankelijk en betrouwbaar
- beroepservaring die past bij zijn verantwoordelijkheden
- vaardigheden op het gebied van communicatie en PR

Een FG moet dus multidisciplinair zijn en kunnen fungeren als sparring partner voor zowel het college als voor onderdelen van de gemeentelijke organisatie en stevig in zijn schoenen staan. Tegelijkertijd moet de FG ook in staat zijn om pragmatisch, eerlijk en met tact te signaleren waar de gemeente buiten de kaders van de privacywetgeving opereert (eerder grensrechter/coach dan politieagent).

Vanwege die wettelijke status is het oordeel van de FG juridisch zwaarwegend. De FG is de aangewezen persoon om de knopen door te hakken in juridische discussies. Voor zover de FG en de AP afwijkende standpunten innemen, is het uitsluitend aan de rechter om een beslissende uitspraak doen.

4 Privacyrechten

4.1 Rechten

De AVG bepaalt niet alleen de plichten van degenen die persoonsgegevens verwerken maar ook de rechten van personen van wie de gegevens worden verwerkt. Deze betrokkenen hebben de volgende rechten:

- Recht op informatie: betrokkenen hebben het recht om aan de gemeente te vragen of zijn/haar persoonsgegevens worden verwerkt;
- Inzagerecht: betrokkenen hebben de mogelijkheid de eigen gegevens in te zien en daarmee te controleren op welke manier die gegevens verwerkt worden;
- Correctierecht: het recht om gegevens te laten corrigeren als duidelijk is dat die niet kloppen;
- Recht van verzet: het recht om te vragen om de persoonsgegevens niet meer te gebruiken;
- Recht om vergeten te worden: in gevallen dat toestemming is gegeven om gegevens te verwerken, kan verzocht worden om die gegevens te laten verwijderen;
- Recht op bezwaar: het recht om bezwaar te maken tegen de verwerking van zijn/haar gegevens. De gemeente zal hieraan voldoen tenzij er gerechtvaardigde gronden zijn voor de verwerking.

Om gebruik te maken van zijn/haar rechten kan schriftelijk of via een e-mail een verzoek worden ingediend. De gemeente heeft vier weken de tijd om te beoordelen of het verzoek gerechtvaardigd is.

4.2 Vragen en klachten

Bij vragen en klachten kan men terecht bij de gemeente. Klachten worden behandeld via de klachtenregeling van de gemeente.

5 Uitvoeringsplan ‘Grip op privacy’

Het college stelt een uitvoeringsplan vast waarin dit beleidskader wordt uitgewerkt. In dit plan komen diverse thema’s aan de orde:

- **Bewustwording en communicatie**

Het college bevordert samen met proceseigenaren een privacybewuste organisatiecultuur via voorbeeldgedrag en door te voorzien in de middelen voor bewustwording en, zo nodig, training van medewerkers en leidinggevenden.

- **Register van verwerkingen**

Zodra de AVG van toepassing is, gaat er een documentatieplicht gelden. Dit betekent dat de gemeente moet kunnen aantonen dat de juiste organisatorische en technische maatregelen zijn genomen om aan de bepalingen uit de AVG te kunnen voldoen. In het kader van die documentatieplicht is het vereist om een register van de verwerkingsactiviteiten bij te houden. Dit zogeheten ‘*verwerkingsregister*’ moet op schrift gesteld worden, in elektronische vorm beschikbaar zijn en de noodzakelijke informatie bevatten over de verwerkingen.

Het verwerkingsregister is een dynamisch document, dat up-to-date gehouden moet worden. De Autoriteit Persoonsgegevens kan het verwerkingsregister ter controle opvragen en de verantwoordelijke een boete opleggen als deze verplichting niet of onvoldoende wordt nageleefd.

- **Functionaris Gegevensbescherming (FG)**

Er moet een FG worden benoemd (zie onder 3.4).

- ***Privacy by design* of *privacy by default***

Privacy by design houdt in dat vanaf het ontwerpen van een nieuw of aangepast proces, product, dienst of informatiesysteem wordt nagedacht over:

- het rechtmatig, behoorlijk en transparant verwerken van persoonsgegevens;
- de maatregelen die hiervoor nodig zijn.

Privacy by default betekent dat technische en organisatorische maatregelen nodig zijn om ervoor te zorgen dat alleen persoonsgegevens worden verwerkt die nodig zijn voor het specifieke doel.

- **Privacy Impact Assessment (PIA’s)**

Voor nieuwe processen en diensten, waar persoonsgegevens worden verwerkt, moeten soms PIA’s worden uitgevoerd. De AVG noemt dit een Gegevenbeschermingseffectbeoordeling. Het doel daarvan is om de impact van de verwerking op de bescherming van persoonsgegevens in kaart te brengen.

- **Informatiebeveiliging**

Het college ziet erop toe dat informatieveiligheid van de gemeente Deventer in lijn met de geldende norm wordt georganiseerd. De gemeente Deventer beschikt over een gekwalificeerde coördinerende informatiebeveiliger (CISO) die nauw samenwerkt met de privacyfunctionaris en de FG.

- **Datalekken en privacy-incidenten**

Het college voorziet in een procedure voor datalekken en privacy-incidenten. Deze procedure bevat in ieder geval een meldplicht voor gebeurtenissen die de beschikbaarheid, integriteit en vertrouwelijkheid van informatievoorzieningen en gegevensopslag aantasten. Ook bevordert het college het oefenen op privacy-incidenten, incidentmanagement en crisiscommunicatie.

- **Verwerkersovereenkomsten**

Bij het uitbesteden van de verwerking van persoonsgegevens is een schriftelijke overeenkomst vereist indien de “verantwoordelijke” (lees: de gemeente) persoonsgegevens laat bewerken door een “verwerker”: externe ICT-leveranciers en andere partijen waaraan gemeentelijke werkzaamheden zijn

uitbesteed waarbij persoonsgegevens worden verwerkt. Dit is de zgn. verwerkersovereenkomst. Het opstellen van een verwerkersovereenkomst heeft tot doel te waarborgen dat de verplichtingen die vanuit de privacyregelgeving op de gemeente rusten, ook door de bewerker worden nageleefd. Daartoe dienen in de verwerkersovereenkomst afspraken en maatregelen te staan die de verwerker moet naleven. Wettelijk is het college van burgemeester en wethouders namelijk verantwoordelijk en aanspreekbaar voor de gegevens die door de verwerker worden verwerkt. Zo komen datalekken e.d. voor rekening en risico van het college óók als deze zich buiten zicht en invloed van de gemeente voordoen bij de verwerker.

- x - x -