Nota voor burgemeester en wethouders
Onderwerp
Rapportage-privacy-2019

Team
DEV-CS

1- Notagegevens	
Notanummer	2020-000262
Datum	24-02-2020
Programma:	
12 Bedrijfsvoering	
Portefeuillehouder	Burgemeester

2- Bestuursorgaan	
[X]B & W	07-04-2020
[ ]Raad	--
[ ]Burgemeester	--

College van B & W	
- Burgemeester	- Weth. Grijsen
- Weth. De Geest	- Weth. Verhaar
- Weth. Walder	- Weth. Rorink

Besluitenlijst	d.d.		d.d.		d.d.
[ ]Akkoordstukken	--	[X]Openbaar	07-04-2020	[ ]Besloten	--

Routing	d.d.
Burgemeester	31-03-2020
Directeur	02-04-2020
Programmamanager	31-03-2020

	par.
[ ]adj.secr.	--
[X]gem.secr.	02-04-2020
BIS Openbaar	
Status	Definitief2020-04-08

Bijlagen
Rapportage Grip op privacy 2020

B & W d.d.: 07-04-2020

Besloten wordt:
1 Grip op privacy 2020, inhoudende een jaarrapportage over 2019 en het meerjarenplan inzake privacy en gegevensbescherming, op grond van artikel 5 lid 2 van de Algemene verordening gegevensbescherming (AVG) vast te stellen;
2 de raadsmededeling vast te stellen en aan te bieden aan de raad;
3 de nota en het besluit openbaar te maken.

Financiële aspecten:

Financiële gevolgen voor de gemeente?	Nee
Begrotingswijziging	Nee

Voorstel openbaarmaking conform Wet Openbaarheid Bestuur (Wob)

[X] De nota en het besluit openbaar te maken
[ ] De nota en het besluit openbaar te maken vergezeld van bijgaand persbericht
[ ] De nota en het besluit openbaar te maken nadat

[ ] De nota en het besluit openbaar te maken, behalve…

[ ] Het besluit openbaar te maken, maar niet de nota, gelet op artikel:

[ ] De nota en het besluit niet openbaar te maken, gelet op artikel:

Kennisgeving/ Bekendmaking Awb

Kennisgeving (publicatie) conform Awb	Nee
Bekendmaking conform Awb	Nee

gemeente Deventer

ADVIESRADEN:

Moet een van de adviesraden gehoord worden of op de hoogte gesteld? Nee

Toelichting

Inleiding

De gemeente Deventer verwerkt op grote schaal persoonsgegevens van inwoners. Dat gebeurt niet alleen in het sociale domein, maar ook op veel andere beleidsterreinen. Daarnaast werkt de gemeente steeds meer samen met andere overheidsorganisaties, met maatschappelijke partners en met zorgpartners, waarbij waar nodig gegevens van inwoners van Deventer worden gedeeld.

Inwoners van Deventer moeten er op kunnen vertrouwen dat de gemeente en haar partners de privacywetgeving in acht nemen en zorgvuldig omgaan met deze persoonsgegevens. Met dat doel is op 25 mei 2018 de Europese Algemene Verordening Gegevensbescherming (AVG) in volle werking getreden. Deze AVG verplicht tot het aantoonbaar treffen van beheersmaatregelen binnen de gemeente Deventer om privacy en gegevensbescherming te borgen. Onvoldoende naleving kan leiden tot forse boetes van de Autoriteit Persoonsgegevens (AP), tot reputatie- en imagoschade van de gemeente en tot schadeclaims van gedupeerde inwoners.

Daarom is in 2019 *Grip op privacy 2.0* vastgesteld en uitgevoerd. Op basis van een aantal bouwstenen werd daarin de verdere implementatie van de regelgeving en het beleid uitgewerkt.

Grip op privacy 2020 bevat zowel een jaarrapportage over 2019 als een concreet plan met actiepunten voor de komende jaren.

Beoogd resultaat

Inzicht in de voortgang als het gaat om het implementeren van de AVG.

Structurele aandacht van het bestuur en de gemeentelijke organisatie voor privacy- en gegevensbescherming.

De basis leggen voor een proces, gebaseerd op de plan-do-check-act-cyclus (PDCA), waarbij het college en de proceseigenaren tijdig voorzien worden van stuur- en verantwoordingsinformatie.

Einddoel is het in control zijn als het gaat om het op aantoonbare wijze naleven van de privacywetgeving in de organisatie

Kader

Algemene verordening gegevensbescherming (AVG)

Argumenten voor en tegen

Voor

Door middel van het vaststellen van Grip op privacy 2020, een jaarrapportage over 2019, wordt inzichtelijk welke stappen en acties in 2019 zijn ondernomen op de verschillende privacythema’s.

Daarnaast wordt met het bijbehorende meerjarenplan inzichtelijk welke actiepunten er op de verschillen privacythema's zijn voor de komende jaren.

Extern draagvlak (partners)

Niet van toepassing

Financiële consequenties

Niet van toepassing

Aanpak/uitvoering

Communicatie door middel van bezoek aan MT's en via intranet.

RAADSMEDEDELING

Onderwerp	Rapportage-privacy-2019		
Mededelingennr	2020-000262	**Portef.houder**	Burgemeester
Team	DEV-CS	**BenW-besluit d.d.:**	7 april 2020

1. Inleiding: waarom deze mededeling

Uw raad informeren over de mate waarin de gemeente Deventer op aantoonbare wijze de privacywetgeving naleeft.

2. Kader

Algemene verordening gegevensbescherming (AVG)

3. Kern van de boodschap

Inwoners van Deventer moeten er op kunnen vertrouwen dat de gemeente en haar partners de privacywetgeving in acht nemen en zorgvuldig omgaan met deze persoonsgegevens. Met dat doel is op 25 mei 2018 de Europese Algemene Verordening Gegevensbescherming (AVG) in volle werking getreden. Deze AVG verplicht tot het aantoonbaar treffen van beheersmaatregelen binnen de gemeente Deventer om privacy en gegevensbescherming te borgen.

Daarom is in 2019 *Grip op privacy 2.0* vastgesteld en uitgevoerd. Op basis van een aantal bouwstenen werd daarin de verdere implementatie van de regelgeving en het beleid uitgewerkt.

Grip op privacy 2020 bevat zowel een jaarrapportage over 2019 als een concreet plan met actiepunten voor de komende jaren.

4. Nadere toelichting

In 2019 is er een aantal maatregelen getroffen. Alle werkprocessen en gegevensverwerkingen zijn in beeld gebracht en er is domeinspecifiek privacybeleid ontwikkeld. Ook zijn er organisatorische maatregelen getroffen. Een voorbeeld daarvan is het besluit om een Functionaris voor Gegevensbescherming in dienst te nemen voor de drie gemeenten. Er is veel aandacht geweest voor het creëren van bewustzijn, draagvlak en kennis bij de proceseigenaren en de medewerkers. Ook zijn medewerkers meer actief getraind op de kennis van het privacyrecht, bijvoorbeeld door middel van e-learning. Het uitvoeren van Data Protection Impact Assessments (DPIA's) bij gemeentelijke gegevensverwerkingen met een hoog privacyrisico is in 2019 een belangrijk onderwerp geweest. Er is veel tijd gestoken in het ontwerp van de procedure waarbinnen deze risicoanalyse plaatsvindt en het doorlopen van deze procedure. Dit geldt ook voor de procedure rondom het behandelen van AVG-verzoeken. Verder zijn er in 2019 nieuwe standaarden ontwikkeld op het gebied van samenwerkende partijen en gegevensbescherming.

De Autoriteit Persoonsgegevens legt de komende jaren als toezichthouder extra de nadruk op de focusgebieden digitale overheid, artificiële intelligentie en algoritmes. Dat heeft zij bekend gemaakt in het visiedocument 'Dataprotectie in een digitale samenleving'. Extra aandacht voor deze thema's de komende jaren is nodig om de bescherming van persoonsgegevens te borgen. Misbruik of onverantwoordelijk gebruik van persoonsgegevens kan bijvoorbeeld leiden tot foutieve beslissingen, uitsluiting van mensen en discriminatie. De focusgebieden van de Autoriteit Persoonsgegevens zijn ook de gemeentelijke gebieden waar de uitvoering van het meerjarenplan *Grip op privacy 2020* op is gericht.

In 2020 zal de ingezette lijn bij het uitvoeren van DPIA's worden voortgezet. Ervaring leert ons dat het monitoren van de uitkomsten van een DPIA, het registreren van incidenten, het bijhouden van het register van verwerkingsactiviteiten en het periodiek rapporteren over de voortgang niet gemakkelijk handmatig kan worden bijgehouden. Er zal in 2020 dan ook een tool worden aangeschaft om dit op geautomatiseerde wijze te kunnen doen.

Er zal verder gewerkt worden aan het functioneel inbedden van de rechten van betrokkenen en de AVG-beginselen in systemen en voorzieningen. Daarbij zal aansluiting worden gezocht bij de maatregelen die nodig zijn om compliant te worden met de Baseline Informatiebeveiliging Overheid. Tenslotte zullen zal er opnieuw aandacht zijn voor het bevorderen van bewustzijn en kennis bij de medewerkers vanuit het gegeven dat de menselijke factor wezenlijk is voor het privacybestendig werken.

gemeente Deventer

Grip op privacy 2020

Rapportage 2019 en meerjarenplan

www.deventer.nl

Uitgave : versie 3 (definitief)
Naam : L.M. Schieving
Mail : l.schieving@deventer.nl

Inhoud

Managementsamenvatting

De gemeente Deventer verwerkt op grote schaal persoonsgegevens van inwoners. 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, met maatschappelijke partners en met zorgpartners, waarbij waar nodig gegevens van inwoners van Deventer worden gedeeld. Inwoners moeten er op kunnen vertrouwen dat de gemeente en haar partners de privacywetgeving in acht nemen en zorgvuldig omgaan met deze persoonsgegevens. Met dat doel is op 25 mei 2018 de Europese Algemene Verordening Gegevensbescherming (AVG) in volle werking getreden. Deze AVG verplicht tot het aantoonbaar treffen van beheersmaatregelen binnen de gemeente Deventer om privacy en gegevensbescherming te borgen. Onvoldoende naleving kan leiden tot forse boetes van de Autoriteit Persoonsgegevens (AP), tot reputatie- en imagoschade van de gemeente en tot schadeclaims van gedupeerde inwoners.

Daarom is in 2019 het meerjarenplan *Grip op privacy 2.0* vastgesteld en uitgevoerd. Op basis van een aantal bouwstenen werd daarin de verdere implementatie van de regelgeving en het beleid uitgewerkt. Dit nieuwe plan *Grip op privacy 2020* bevat zowel een rapportage over de uitvoering tot nog toe, als een concreet plan met actiepunten voor de komende jaren. Privacy- en gegevensbescherming vergt structurele aandacht van het bestuur en de gemeentelijke organisatie. Einddoel is het inrichten van een proces, gebaseerd op de plan-do-check-act-cyclus (PDCA), waardoor het college en de proceseigenaren tijdig voorzien worden van stuur- en verantwoordingsinformatie.

In 2019 zijn er een aantal maatregelen getroffen. Alle werkprocessen en gegevensverwerkingen zijn in beeld gebracht en er is domeinspecifiek privacybeleid ontwikkeld. Ook zijn er organisatorische maatregelen getroffen. Een voorbeeld daarvan is het besluit om een FG in dienst te nemen voor de drie gemeenten. Er is veel aandacht geweest voor het creëren van bewustzijn, draagvlak en kennis bij de proceseigenaren en de medewerkers. Ook zijn medewerkers meer actief getraind op de kennis van het privacyrecht, bijvoorbeeld door middel van e-learning. Het uitvoeren van Data Protection Impact Assessments (DPIA's) bij gemeentelijke gegevensverwerkingen met een hoog privacyrisico is in 2019 een belangrijk onderwerp geweest. Er is veel tijd gestoken in het ontwerp van de procedure waarbinnen deze risicoanalyse plaatsvindt en het doorlopen van deze procedure. Dit geldt ook voor de procedure rondom het behandelen van AVG-verzoeken. Verder zijn er in 2019 nieuwe standaarden ontwikkeld op het gebied van samenwerkende partijen en gegevensbescherming.

De AP legt de komende jaren als toezichthouder extra de nadruk op de focusgebieden digitale overheid, artificiële intelligentie en algoritmes. Dat heeft zij bekend gemaakt in het visiedocument 'Dataprotectie in een digitale samenleving'. Extra aandacht voor deze thema's de komende jaren is nodig om de bescherming van persoonsgegevens te borgen. Misbruik of onverantwoordelijk gebruik van persoonsgegevens kan bijvoorbeeld leiden tot foutieve beslissingen, uitsluiting van mensen en discriminatie. De focusgebieden van de AP zijn ook de gemeentelijke gebieden waar de uitvoering van het meerjarenplan *Grip op privacy 2020* op is gericht.

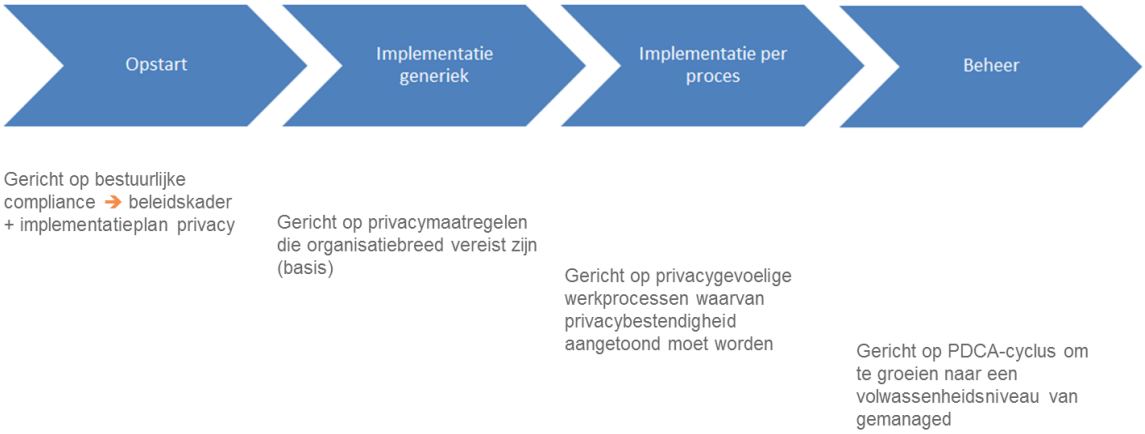
In 2020 zal de ingezette lijn bij het uitvoeren van DPIA's worden voortgezet. Ervaring leert ons dat het monitoren van de uitkomsten van een DPIA, het registreren van incidenten, het bijhouden van het register van verwerkingsactiviteiten en het periodiek rapporteren over de voortgang niet gemakkelijk handmatig kan worden bijgehouden. Er zal in 2020 dan ook een tool worden aangeschaft om dit op geautomatiseerde wijze te kunnen doen. Er zal verder gewerkt worden aan het functioneel inbedden van de rechten van betrokkenen en de AVG-beginselen in systemen en voorzieningen. Daarbij zal aansluiting worden gezocht bij de maatregelen die nodig zijn om BIO compliant te worden. Tenslotte zullen zal er opnieuw aandacht zijn voor het bevorderen van bewustzijn en kennis bij de medewerkers vanuit het gegeven dat de menselijke factor wezenlijk is voor het privacybestendig werken.

Aanpak

Risicogebaseerde benadering

De uitgangspunten voor de aanpak bij privacy liggen vast in artikel 24 AVG[1]. In het implementatieplan *Grip op privacy* en het meerjarenplan *Grip op privacy 2.0* werd al ingegaan op wat het betekent om grip te krijgen en te behouden op het implementeren van de AVG. De AVG gaat uit van een risicogebaseerde benadering. Per verwerking van persoonsgegevens moet de ernst van de privacyrisico's die zich daarbij aandienen worden vastgesteld en worden geëvalueerd om te kijken of de (te nemen) maatregelen toereikend zijn. De aard van de gegevens en de context zijn hierin allesbepalende factoren. Dit alles vraagt om een cyclisch PDCA-proces waarbij het proces de inhoud borgt.

Schematisch vertaalt de aanpak bij privacy zich als volgt:



Het college moet als verwerkingsverantwoordelijke op ieder moment kunnen aantonen dat privacyrisico's voldoende zijn afgedekt. Dit vereist monitoring. Monitoring op het privacybeleid, maar ook op de werkprocessen, de organisatorische inbedding, de rechten van betrokkenen, de verstrekkingen van persoonsgegevens aan derde partijen of verwerkers, de technische systemen en de handhaving van gegevensbeveiliging. Deze rapportage, genaamd *Grip op privacy 2020,* maakt inzichtelijk welke stappen en acties in 2019 zijn ondernomen op deze privacythema's. Ook geeft deze rapportage inzicht in de mate waarin we inmiddels 'in control' zijn als het gaat om het op aantoonbare wijze naleven van de privacywetgeving in de organisatie. Per thema worden actiepunten geformuleerd voor het komende jaar en een toekomstvisie geschetst.

Resultaten meting privacy

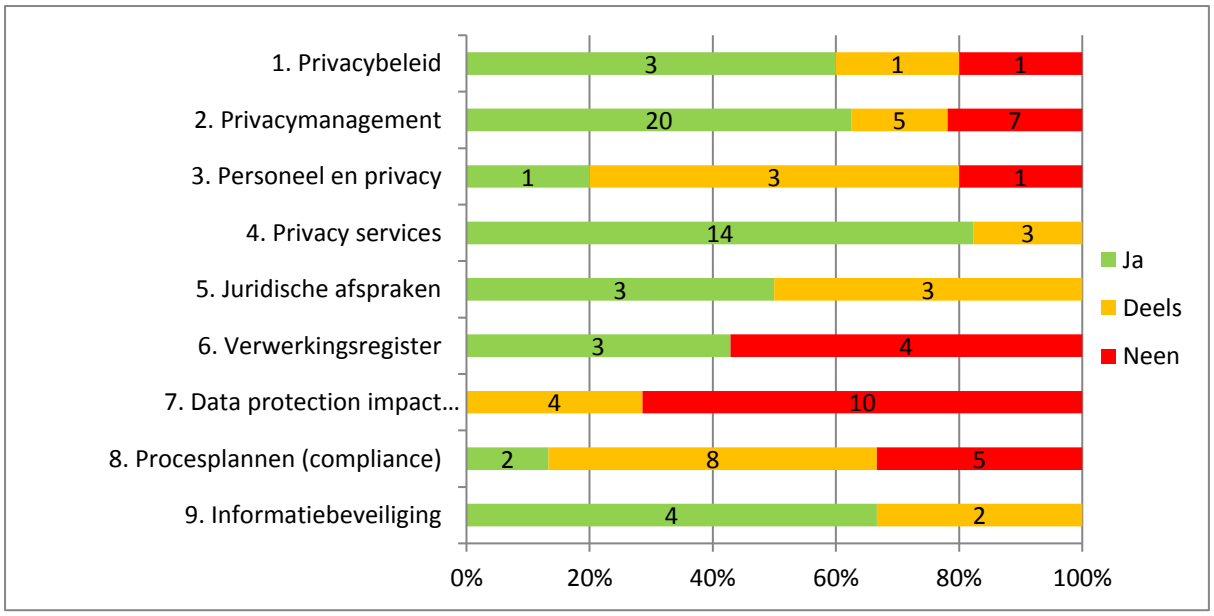
De ambitie, zoals beschreven in het implementatieplan *Grip op privacy,* was om in 2018 toe te werken naar het privacyniveau 'gemanaged'. Dit niveau typeert zich door organisatiebreed privacy-beleid gekenmerkt door hoge awareness en bijsturing van beheersmaatregelen op basis van meetbaarheid, rekenschap en periodieke evaluaties. In 2019 zijn er weer een grote stappen gedaan om dit privacyniveau te bereiken. Het privacyniveau 'gemanaged' wordt bereikt op het moment dat er een

[1] Zie artikel 24 AVG: Rekening houdend met de aard, de omvang, de context en het doel van de verwerking, alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, treft de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd. Die maatregelen worden geëvalueerd en indien nodig geactualiseerd.

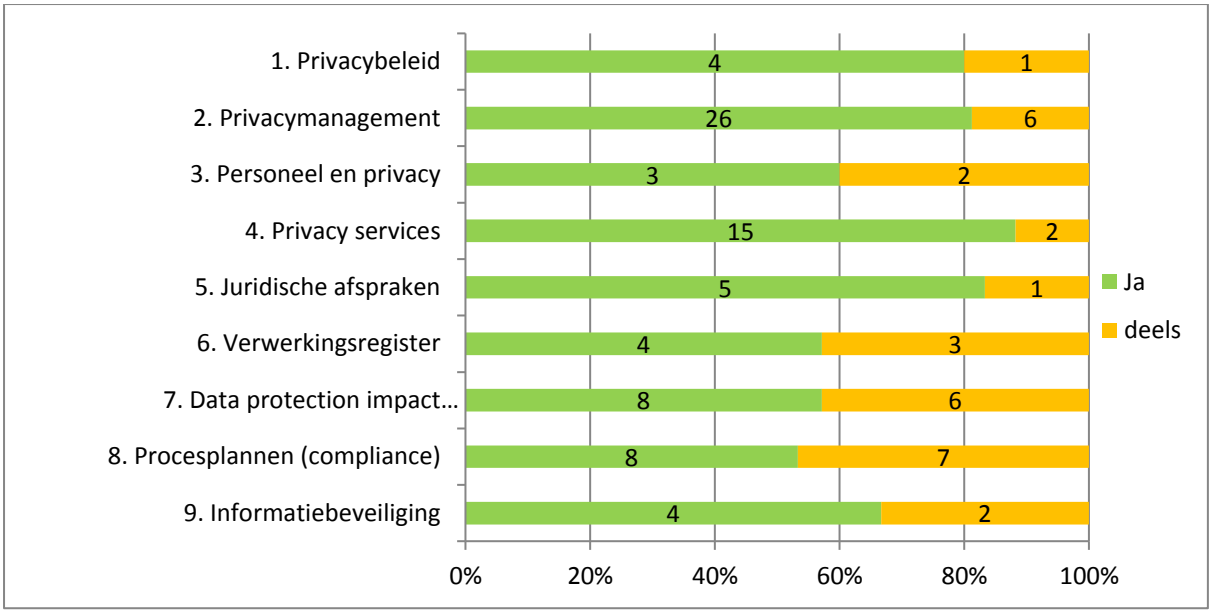
proces is ingericht, gebaseerd op de plan-do-check-act-cyclus (PDCA), dat op basis van rapportages het college en de proceseigenaren in tijdige stuur- en verantwoordingsinformatie voorziet. De privacyaanpak wordt hiermee procesmatig en draagt zorg voor de planning, implementatie, onderhoud, beoordeling en het verder verbeteren van gegevensbescherming. Om dit te bereiken, zal in 2020 onder andere GRC-tooling worden aangeschaft.

In 2018 werd op basis van een negental privacyindicatoren in samenwerking met de directeur met in zijn portefeuille AVG/privacy, teammanagers, alsmede de CISO, de Privacy officer en de kwartiermaker privacy een nulmeting uitgevoerd. Deze indicatoren zijn uitgekozen als referentiebeeld om de voortgang te garanderen van een maatstaf. Het relatieve belang van de indicatoren voor de implementatie van de AVG is onbekend. In control zijn als het gaat om het implementeren van de AVG verwijst überhaupt niet naar een toestand op enig moment, bijvoorbeeld een gemiddelde score van 100%. Dit is een continu doorlopend proces, gericht op het ontdekken- en beheersen van privacyrisico's.

De gemiddelde score in 2018 was **32%**. Op basis van dezelfde indicatoren werd in 2019 een tweede meting uitgevoerd. Dit gaf het volgende resultaat:



De gemiddelde score was op dat moment **60%**. Het streven voor 2019 was om in dit jaar in ieder geval te komen tot een gemiddelde score van **80%**. Dit doel is bereikt. De gemiddelde score is op dit moment **86%**. Dit levert het volgende overzicht op:



Zoals hierboven is te zien, zijn er in 2019 op alle gebieden weer flinke stappen gezet (groen en oranje). Dit geeft een goede indicatie van de voortgang als het gaat om het implementeren van de AVG.

Hieronder wordt gerapporteerd aan de hand van de thema's die VNG Realisatie heeft ontwikkeld om de AVG te vertalen naar een kwaliteitscyclus voor gegevensbescherming en privacy voor gemeentelijke processen. Dit betreft de volgende thema's: beleid, processen, organisatorische inbedding, rechten van betrokkenen, samenwerking, beveiliging en verantwoording. De actiepunten bij de negen indicatoren hierboven (oranje) zijn daarbij vertaald in concrete actiepunten voor 2020.

Actiepunten

Beleid

Het college heeft op 16 januari 2018 een overkoepelend privacybeleid vastgesteld waarin het haar visie op gegevensbescherming verwoordt en beschrijft hoe het concreet waarborgt dat de gemeente persoonsgegevens behoorlijk, zorgvuldig en in overeenstemming met de wet verwerkt. Door het vaststellen van dit privacybeleid worden de verantwoordelijkheden op strategisch en uitvoeringsniveau geborgd. In 2019 is als aanvulling daarop domeinspecifiek privacybeleid ontwikkeld waarin wordt beschreven hoe de verschillende domeinen omgaan met (sectorspecifieke) wet- en regelgeving, persoonsgegevens en gegevensbescherming. Daar waar dat nodig bleek, is het oude privacybeleid tevens herijkt. Om de doelmatigheid en doeltreffendheid van het gemeentelijk privacybeleid te blijven borgen zal dit in het vierde kwartaal van 2020 opnieuw worden geëvalueerd. Gaandeweg is duidelijk geworden dat het bij veranderende bedrijfsprocessen en omstandigheden het aanbeveling verdient nodige verbeteringen of actualisatie van het privacybeleid direct door te voeren. Dit is dus tevens een doorlopende actiepunt voor 2020.

Processen

Verwerkingsregister
Om als gemeentelijk organisatie te kunnen sturen op gegevensbescherming is inzicht nodig in de werkprocessen waar persoonsgegevens in worden verwerkt. Het college heeft de werkprocessen in 2019 in beeld gebracht voor zover zij daarbij als (mede)verantwoordelijke of verwerker optreedt. Alle

verwerkingen van persoonsgegevens zijn in een register van verwerkingsactiviteiten opgenomen, zoals verplicht gesteld in artikel 30 AVG. Dit heeft tot een duidelijk overzicht van de verwerkingen van persoonsgegevens geleid, geclusterd naar werkprocessen, dat ter beschikking kan worden gesteld aan de AP. Verder is in 2019 naar aanleiding van een vraag van een onderzoeksorganisatie door het college besloten dat dit een document is voor interne doeleinden en niet verstrekt zal worden aan derden anders dan de AP. Dit borgt de vertrouwelijkheid van de informatie die in dit overzicht is opgenomen.

AVG-dossiers
Wanneer er bij een werkproces sprake is van een verhoogd risico voor de privacyrechten van betrokkenen moet een AVG-dossier worden opgesteld waaruit de privacybestendigheid van het werkproces blijkt. Vanwege de risicogebaseerde benadering is er geen uitgebreid dossier nodig voor elk werkproces waarbij sprake is van verwerking van persoonsgegevens. In 2019 is aan de hand van Europese AVG-criteria voor alle gemeentelijke werkprocessen de privacygevoeligheid (hoog, gemiddeld, laag) in beeld gebracht en vastgesteld voor welke werkprocessen er een Data protection impact assessment (DPIA) moet worden uitgevoerd. Het uitvoeren van deze risicoanalyse bij werkprocessen die een hoog privacyrisico opleveren, vormt een belangrijk onderdeel van het AVG-dossier en van de compliance. Ook bij nieuwe verwerkingen of bij de aanschaf van nieuwe systemen is in 2019 in kaart gebracht of dit een hoog risico voor de eerbiediging van de persoonlijke levenssfeer van betrokkene(n) oplevert. Waar dat het geval was, is er een DPIA uitgevoerd.

In de bijlage bij deze jaarrapportage is een overzicht opgenomen van de 25 bestaande werkprocessen en nieuwe verwerkingen waar in 2019 een DPIA op is uitgevoerd en een AVG-dossier is opgesteld. De rapportages van de DPIA's staan in procesmappen op de SharePoint site van privacy. De betreffende proceseigenaar kan zijn of haar werkproces met de daarbij horende rapportages daar raadplegen. In 2020 zullen we doorgaan met het uitvoeren van DPIA's op de bestaande werkprocessen en nieuwe verwerkingen van persoonsgegevens. Er is een planning opgesteld waarin staat wanneer deze risicoanalyse voor welke privacygevoelige processen zal plaatsvinden.

Organisatorische inbedding

Voor een adequaat privacybeschermingsniveau binnen de gemeentelijke organisatie is er naast de inbreng van de portefeuillehouder privacy binnen het college coördinatie door de Privacy officer en toezicht door de Functionaris Gegevensbescherming vereist. In 2019 is gebleken dat het voor het tijdig en naar behoren betrekken van de FG bij actuele en prangende privacy aangelegenheden het voorkeur verdient om een interne FG te hebben. Het directieberaad DOWR heeft daarom in oktober besloten een FG in dienst te nemen voor de drie gemeenten en de gemeente Deventer als gastheergemeente de opdracht te geven zorg te dragen voor de invulling van de vacature. De strategisch juridisch adviseur is vervolgens aangesteld als tijdelijk FG voor de gemeente Deventer en aangemeld bij de Autoriteit Persoonsgegevens, zodat de functie van interne toezichthouder vervult blijft.

De Privacy officer heeft in 2019 zowel op casusniveau als gemeentebreed en in DOWR-verband geadviseerd omtrent de bescherming- en de verwerking van persoonsgegevens. De advisering en informatieverstrekking rondom privacy richting de leden van het college heeft daardoor een meer structurele plek gekregen in de werkzaamheden van de Privacy officer. Inmiddels is voor de gehele organisatie duidelijk wat een FG is en wat zijn of haar taken zijn. Ondanks dat de Privacy officer als eerste aanspreekpunt voor teammanagers en medewerkers dient als het gaat om zaken die verband houden met privacy wordt in 2020 gekeken of en hoe de FG een meer zichtbare positie kan krijgen

als interne toezichthouder en als het gaat om het gevraagd en ongevraagd adviseren van de gemeentelijke organisatie, het college en de directie.

De leden van het Privacy Implementatie Team (PIT), de directeur met in zijn portefeuille AVG/privacy, de CISO, de Privacy officer, de FG en de kwartiermaker privacy, hebben in 2019 als adviesorgaan voor de directie nauw samengewerkt bij de behandeling van strategische vraagstukken op het gebied van privacy en informatieveiligheid.

De teammanager is als proceseigenaar in het privacybeleid aanwezen als de verantwoordelijke voor het privacybestendig maken van zijn of haar werkprocessen. Dit komt overeen met het proceseigenaarschap in het informatieveiligheidsbeleid en de verantwoordelijkheid voor het nemen van beheersmaatregelen bij de implementatie BIO. In 2019 is dan ook in gezamenlijkheid voor alle werkprocessen in kaart gebracht wie de verantwoordelijke teammanager is. Op afdelingsniveau zijn inmiddels, wanneer noodzakelijk, procedures en werkafspraken opgesteld over de wijze van omgang met persoonsgegevens. Bijvoorbeeld daar waar het de omgang met persoonsgegevens van binnen de gemeentelijke organisatie betreft, zoals de gegevens van medewerkers zelf. Er is ervaring opgedaan met het actief informeren van de OR over de zaken die spelen op het gebied van privacy en gegevensbescherming. In 2020 zal deze lijn worden doorgezet.

De teamoverleggen zijn gebruikt om privacyafspraken te communiceren, zodat de medewerkers op de hoogte zijn van de inhoud hiervan. Middels diverse andere communicatiekanalen, zoals nieuwsbrieven, trainingen en presentaties, is het privacybeleid van de gemeente in 2019 teamspecifiek toegelicht. Ook zijn medewerkers meer actief getraind op de kennis van het privacyrecht, bijvoorbeeld door middel van e-learning. Er is onder andere aandacht geweest voor de uitspraak van 28 mei 2019 waarin de gemeente Deventer door de rechtbank Overijssel veroordeeld werd tot een schadevergoeding van € 500,- wegens het schenden van de privacy bij het verzenden van een mail in het kader van het voorkomen van Wob-misbruik. Zowel het management als de medewerkers zijn gewezen op de risico’s bij het gebruik van eenvoudige en veel gebruikte gegevensverwerkingsmiddelen, zoals bij mailverkeer. Het college heeft inmiddels hoger beroep aangetekend tegen deze uitspraak. In 2020 zullen actualiteiten en ontwikkelingen die betrekking hebben op de werkwijze van de gemeente in zijn geheel in het kader van privacy breder worden gedeeld en toegelicht. Dit verbreed het inmiddels opgebouwde kennisniveau van medewerkers en bevordert de effectiviteit van het privacybeleid. De FG zal om advies en ondersteuning gevraagd worden bij het verdere verloop van het bewustwordingstraject.

Rechten van betrokkenen

In 2018 is door middel van het vaststellen van het privacybeleid ruimte gecreëerd voor betrokkenen om gebruik te kunnen maken van hun privacyrechten. Als aanvulling daarop is in 2019 de afhandeling en het proces rondom AVG-verzoeken van betrokkenen in een uniforme procedure vastgelegd. De teammanager waar de betreffende gegevensverwerking onder valt, is daarbij verantwoordelijk gemaakt voor het aanleveren van de informatie die noodzakelijk is voor het beoordelen van deze verzoeken. De Privacy officer is verantwoordelijk voor de verdere afhandeling van het verzoek en het opstellen van het besluit. Medewerkers zijn geïnstrueerd over hoe zij een verzoek kunnen herkennen en wat zij moeten doen op het moment waarop zij een dergelijk verzoek ontvangen. Verder hebben zij algemene informatie gekregen over de rechten die het daarbij betreft, de termijnen die moeten worden bewaakt en de manier van afhandeling.

Bij de aanschaf van nieuwe systemen in 2019 is de mogelijkheid voor betrokkenen om hun rechten op grond van de AVG uit te oefenen als criterium meegenomen. Voor 2020 is het de uitdaging om

systemen en voorzieningen ook daadwerkelijk zelf functioneel te laten voorzien in de uitoefening van deze rechten.

Voorafgaand aan de verwerking van persoonsgegevens zijn betrokkenen in 2019 zoveel mogelijk geïnformeerd over de soort gegevens die worden verwerkt, de bron van gegevens, het doel van de verwerking, de grondslag van de verwerking, aan wie de gegevens worden verstrekt. Bij aanvraagformulieren voor producten of diensten bijvoorbeeld staat nu duidelijker welke gegevens worden verwerkt.

Voor de verwerkingen waarbij de gemeente toestemming als grondslag voor de verwerking gebruikt, is gebleken dat niet altijd aan de randvoorwaarden voor toestemming wordt voldaan. Bijvoorbeeld wanneer de toestemming niet vrijelijk kan worden gegeven. Ook worden er bij de aanvraag van producten en diensten nog weleens meer persoonsgegevens uitgevraagd dan noodzakelijk. In 2020 zal hier in de organisatie aandacht aan worden besteed.

Samenwerking

Aan het verwerken van persoonsgegevens door een derde partij zijn wettelijke voorwaarden verbonden. De teammanagers wisten in 2019 de Privacy officer te vinden wanneer zij vragen hadden over de inschakeling van derde partijen, gegevensverwerking bij samenwerkingsverbanden of gemeenschappelijke verwerkers. De standaarden die daartoe zijn opgesteld voor wat betreft juridische afspraken zijn beschikbaar gesteld op de SharePoint site van privacy. Ook is er een toetsingskader ontwikkeld op grond waarvan teammanagers of medewerkers ook gemakkelijk zelf kunnen vaststellen of een derde partij verwerker, gezamenlijk verwerkingsverantwoordelijke of zelfstandig verwerkingsverantwoordelijke is en welke afspraken over de verwerking moeten worden gemaakt. Dit kader zal in 2020 worden vastgesteld en gepubliceerd.

Beveiliging

In 2019 is ervaring opgedaan met de nieuwe procedure meldplicht datalekken, waarbij de Privacy officer's van de verschillende DOWR-gemeentes afzonderlijk incidenten dienden te beoordelen en te melden bij de AP. Dit heeft geen veranderingen gebracht in de in Deventer al bestaande afwikkelingspraktijk bij (vermoedens van) incidenten in verband met persoonsgegevens. Door in trainingen stil te staan bij waarom de gemeente in voorkomende gevallen inbreuken en incidenten wel of niet heeft bestempeld als een datalek is er in 2019 gemeentebreed wel meer discussie gevoerd over het afwegingskader bij dit soort gevallen. Een voorbeeld van een veel besproken geval is het incident waarbij een medewerker per ongeluk een groot aantal collega's en een aantal externen een mail verzendt over de afwezigheid van collega's wegens ziekte. Omdat het voorkomen van incidenten met betrekking tot persoonsgegevens voor een groot deel is ingebed in de set van preventieve beveiligingsmaatregelen die zijn opgenomen in het informatieveiligheidsbeleid is de Privacy officer in 2019 ook betrokken bij het nieuw op te stellen beleid in het kader van de BIO. Voor wat betreft het registreren van incidenten is het documenteren in de e-suite geen passend alternatief bevonden. In 2020 zal daarom gekeken worden naar een tool, die zowel in het documenteren van incidenten ondersteund als in het documenteren van andere AVG-documentatie.

Beveiligingmaatregelen dienen een passend niveau van beveiliging met inbegrip van vertrouwelijkheid, te waarborgen, rekening houdend met de stand van de techniek en de uitvoeringskosten afgezet tegen de risico's en de aard van de te beschermen persoonsgegevens. Opmerking verdient dat in 2019 nog niet bij alle voor verwerking gebruikte geautomatiseerde systemen de inrichting van de standaardinstelling zo is ingesteld dat er rekening gehouden wordt met

de privacy van betrokkenen en de AVG-beginselen. Er wordt bijvoorbeeld niet altijd gezorgd voor een minimale gegevensverwerking doordat medewerkers binnen systemen niet altijd alleen toegang hebben tot die gegevens die zij nodig hebben voor ter uitvoering van hun werkzaamheden. Ook worden niet alle verwerkingen binnen geautomatiseerde systemen gelogd. In 2020 zullen er acties en maatregelen genomen worden om het beveiligingsniveau van persoonsgegevens en de zorgvuldige omgang van persoonsgegevens op dat gebied naar een hoger niveau te tillen. Dit sluit aan bij de maatregelen die zijn beoogd om BIO compliant te zijn.

Verantwoording

Verwerkingsregister
Vanwege het belang van een actueel verwerkingsregister is er in 2019 een procedure voor het beheer van het verwerkingsregister in het leven geroepen en is de Privacy officer belast met het beheer van het verwerkingsregister. Met het doorlopen van de procedure is echter duidelijk geworden dat het overzicht met betrekking tot het verwerkingsdoel, de grondslag, de getoetste beginselen, de inschakelde verwerkers, (gezamenlijk) verantwoordelijken en de te nemen beheersmaatregelen, vanwege het aantal gemeentelijke verwerkingen, niet handmatig in een Excellijst actueel kan worden gehouden. Bij de halfjaarlijkse controles op de kwaliteit van het verwerkingsregister is geconstateerd dat achterstanden in de mutaties in het verwerkingsregister zich gemakkelijk voordoen wanneer medewerkers nieuwe verwerkingen of wijzigingen in de werkprocessen niet op geautomatiseerde wijze namens de proceseigenaar kunnen doorgeven. In 2020 zal dan ook een oplossing worden gezocht voor de onnodige vervuiling in de verwerkingen die daardoor kan optreden en een volgende stap worden gemaakt in het efficiënt beheren van het verwerkingsregister.

Data protection impact assessments (DPIA's)
Gelet op diversiteit aan activiteiten die verbonden zijn aan het voorbereiden, uitvoeren, afwikkelen, opvolgen en beheren van DPIA's is er in 2019 een DPIA-procedure ontworpen en ervaring opgedaan met het doorlopen van deze procedure. Er is veel tijd gestoken in het ontwerp van de kaders waarbinnen een dergelijke risicoanalyse verplicht is. Daarbij zijn verschillende DPIA-formats ontwikkeld in de vorm van formulieren, die door middel van de SharePoint site van privacy beschikbaar zijn gesteld voor de gehele organisatie.

Er is aansluiting gezocht bij de implementatie van de BIO. Deze implementatie dwingt namelijk een vergelijkbare inventarisatie van de werkprocessen af. Op het gebied van het definiëren van de werkprocessen en het samenvoegen- en hergebruiken van analyses is in 2019 dan ook intensief samengewerkt met informatiebeveiliging. Bij het ontwerpen en inkopen van gegevensverwerkende processen en systemen bijvoorbeeld is er vroegtijdig samen gescreend welk beveiligingsniveau, conform het privacybeleid en het informatieveiligheidsbeleid, passend en toereikend zou moeten zijn. Ook bij bestaande werkprocessen zijn risico's samen met informatiebeveiliging geadresseerd en gecontroleerd. Dit leidt uiteindelijk tot privacy by design en default.

De Privacy officer heeft bij de eerste DPIA's het invullen van de DPIA-vragen begeleid. Het doen van een DPIA is verder een vast onderdeel geworden in het trainingsaanbod voor privacy, zodat de gehele organisatie in 2019 bekend is geworden met de toepassing van een dergelijke risiconalanyse en met wie daartoe wanneer de opdracht doet. Het management en de medewerkers zullen ook in 2020 blijvend worden geïnformeerd over de werking en het bestaan van de DPIA.

Het efficiënt en duidelijk aantoonbaar vastleggen van bevindingen en bijbehorende documentatie stond centraal in 2019. Nieuwe verwerkingen of wijzigingen van bestaande verwerkingen zijn actief aangemeld bij de Privacy officer en de belangenafweging om al dan niet over te gaan tot een DPIA is daarbij vastgelegd. Er is een planning gemaakt voor de uit te voeren DPIA's en voor nieuwe

verwerkingen met een hoog risico is voorafgaand aan de invoering daarvan een DPIA uitgevoerd en advies ingewonnen bij de FG.

Uit de ervaringen die daarbij zijn opgedaan blijkt wel dat het doorlopen van dit proces in veel documentatie resulteert. Niet alleen de ingevulde vragenlijsten en het DPIA-advies, maar ook bijvoorbeeld de gemotiveerde afwijking van het FG-advies door een teammanager of de opvolging van beheersmaatregelen moet worden gedocumenteerd. De verifieerbaarheid en vindbaarheid van de resultaten van een DPIA is van groot belang gebleken, maar maakt de procedure tevens een administratief zware exercitie. Om grip te houden op de uitvoer van DPIA's, de verslaglegging en de navolging op de adviezen uit de DPIA's zal in 2020 een tool worden aangeschaft voor het plannen, voorbereiden, uitvoeren, monitoren en afwikkelen van DPIA's. Op die manier kan ook transparanter periodiek over het beheer van het DPIA-proces en de uitvoer van DPIA's worden gerapporteerd. Daarbij zal het volgende worden betrokken. De al uitgevoerd DPIA's moeten op een gegeven moment worden geactualiseerd. Ten minste om de 3 jaar, of vaker, indien nodig. De tool moet dit proces, bijvoorbeeld bij wijzigingen in bestaande verwerkingen, vergemakkelijken. Ook is gebleken dat het proces van het ondertekenen van het DPIA-verslag, de rapportage van de uitgevoerde DPIA met het advies van de FG, soms een lange doorlooptijd heeft, omdat er geen gemakkelijke geautomatiseerde wijze is om dit te doen. Dit zal bij het aanschaffen van de tool een belangrijk afwegingspunt zijn.

Verder zal er in 2020 ook worden gekeken naar het actiever delen van de uitkomsten van de verschillende DPIA's met de betrokken medewerkers en de gehele organisatie. Met het organisatiebreed beschikbaar stellen van dit soort uitkomsten kan het lerend vermogen op het gebied van privacy worden versterkt.

Conclusie

De Gemeente Deventer beschikt over een grote hoeveelheid – vaak gevoelige en bijzondere – persoonsgegevens. De bescherming van persoonsgegevens is een belangrijk grondrecht voor burgers, zodat zij grip kunnen houden op hun gegevens en daarmee op hun persoonlijke levenssfeer. Dat betekent niet dat de implementatie van privacywetgeving, zoals de AVG, digitale ontwikkeling en gemeentelijke innovatie in 2020 in de weg moeten staan. Bij de acties die in 2020 zullen worden ondernomen zal het zorgvuldig omgaan met persoonsgegevens dan ook voorop moeten staan, als onderdeel van ontwikkeling en innovatie. Dit biedt voordelen en leidt tot nuttige toepassingen van het gebruik van deze gegevens.

Meerjarenplanning

	2020				2021
Norm/taak	Q1	Q2	Q3	Q4	>
Beleid					
Zelfevaluatie doelmatigheid en doeltreffendheid privacybeleid	X	X	X	X	X
Processen					
AVG-dossiers					
AVG-dossiers inrichten voor nieuwe verwerkingen van persoonsgegevens met een hoog privacyrisico	X	X	X	X	X
DPIA's					
Uitvoeren verplichte DPIA's bij privacygevoelige werkprocessen	X	X	X	X	X
Organisatorische inbedding					
FG meer zichtbaar positioneren als interne toezichthouder en adviseur college/directie		X	X		
Periodieke informatie-uitwisseling met OR	X	X	X	X	X
Het geven van doelgerichte trainingen en opleidingen	X	X	X	X	X
Communicatietraject uitzetten over actualiteiten en ontwikkelingen privacy		X	X		
Opzetten domeinspecifieke programma's voor privacybewustzijn			X	X	X
Rechten van betrokkenen					
Onderzoek mogelijkheden functioneel inrichten privacyrechten			X	X	
Randvoorwaarden voor toestemming en dataminimalisatie implementeren			X	X	
Borging transparantie tijdens concrete gegevensverwerkingen	X	X	X	X	X
Samenwerking					
Toetsingskader juridische afspraken laten vaststellen en publiceren	X				
Beveiliging					
Passend beveiligingsniveau garanderen bij persoonsgegevens in geautomatiseerde systemen	X	X			
Verantwoording					

Verwerkingsregister					
Efficiënt beheer verwerkingsregister borgen	X	X			
DPIA's					
Instrueren proceseigenaren en medewerkers over toepassing DPIA's	X	X	X	X	X
Privacy by design en default			X	X	X
DPIA-planning uitvoeren	X	X	X	X	X
Beheerstool aanschaffen DPIA's en verwerkingsregister		X			
Periodieke rapportage over het beheer en de voortgang van de DPIA's	X	X	X	X	X
Actief en gemeentebreed delen van resultaten DPIA's				X	X

Bijlage 1: Overzicht DPIA's

2019 Q1

1. Wifisensoren
2. Maximaal Jezelf
3. 1Gezin1plan
4. Beoordeling Wob-verzoeken
5. Digipanel KV

2019 Q2

6. Parkeervergunningssysteem
7. Microsoft Office 365
8. Meldingen openbare ruimte (MOOR)
9. Leerlingenvervoer (Jeugdwet en dagbesteding)
10. Hosting Deventer websites
11. Pilot Data Analyse Fraudeonderzoek (SR)
12. Bijplaatsen van afval

2019 Q3

13. Ketenvoorziening voetbal
14. Vrijwillige en gedwongen mobiliteit
15. Intelligente verkeersregelingsinstallaties (iVRIs)
16. Aanmelden leerlingen basisscholen
17. Portaal medische adviezen

2019 Q4

18. Gezinscoaches
19. Bemoeizorg Wmo en uitvoering WBOPZ (Wvggz)
20. Steekproef controle Wmo-leveranciers
21. Agressieincidenten registreren (GIR)
22. Inzet verkeerscamera's
23. Belastingen
24. Cameratoezicht bedrijventerreinen
25. Kwetsbare overstap RMC
26. Leerplicht