Nota voor burgemeester en wethouders
Onderwerp
Rapportage en jaarplan privacy gemeente Deventer

Team
DEV-CS

1- Notagegevens	
Notanummer	2021-001082
Datum	20-04-2021
Programma:	
11 Bedrijfsvoering	
Portefeuillehouder	Burgemeester

2- Bestuursorgaan	
[X]B & W	01-06-2021
[ ]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	01-06-2021	[ ]Besloten	--

Routing	d.d.
Programmamanager	09-05-2021
Burgemeester	27-05-2021

	par.
[ ]adj.secr.	--
[X]gem.secr.	28-05-2021
BIS Openbaar	
Status	Definitief2021-06-02

Bijlagen

B & W d.d.: 01-06-2021

Besloten wordt:
1 De stukken 'Zelfmeting privacy gemeente Deventer 2020' en 'Grip op privacy 2021: rapportage en jaarplan Deventer' vast te stellen;
2 De raadsmededeling vast te stellen en met de bijlage 'Grip op privacy 2021' aan te bieden aan de raad;
3 De nota en het besluit openbaar te maken, m.u.v. de zelfmeting.

Financiële aspecten:

Financiële gevolgen voor de gemeente?	Nee
Begrotingswijziging	Nee

Voorstel openbaarmaking conform Wet Openbaarheid Bestuur (Wob)

[ ] 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

[X] De nota en het besluit openbaar te maken, behalve…
- VERTROUWELIJK 07-2021-001082-Zelfmeting privacy gemeente Deventer 2020
[ ] 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

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. Daarnaast werkt de gemeente steeds meer samen met andere overheidsinstanties, met maatschappelijke partners en met zorgpartners, waarbij waar nodig gegevens van inwoners van Deventer worden gedeeld. De gemeente wil op een zorgvuldige manier omgaan met deze persoonsgegevens. De Algemene Verordening Gegevensbescherming (AVG) verplicht tot het aantoonbaar treffen van beheersmaatregelen binnen de gemeente om privacy en gegevensbescherming te borgen. Onvoldoende naleving kan leiden tot forse boetes van de Autoriteit Persoonsgegevens, tot reputatie- en imagoschade en tot schadeclaims van gedupeerde inwoners.

De bijlage 'Grip op privacy 2021' bevat een rapportage en jaarplan omtrent de naleving van de AVG en is een adviesstuk van de Functionaris Gegevensbescherming (FG). De rapportage vloeit voort uit een zelfmeting op een aantal privacythema's over 2020. Deze thema's zijn door VNG Realisatie ontwikkeld om de eisen uit de AVG te kunnen vertalen naar een kwaliteitscyclus voor gegevensbescherming en privacy voor gemeentelijke processen. Met deze nota wordt gevraagd om de stukken vast te stellen en de actiepunten uit het jaarplan over te nemen.

Beoogd resultaat

- Inzicht in de voortgang als het gaat om het naleven van de AVG.
- Structurele aandacht van het college van B&W en de gemeentelijke organisatie voor privacy- en gegevensbescherming.
- 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 de rapportage wordt inzichtelijk welke stappen en acties de gemeente Deventer in 2020 op de verschillende privacythema's heeft gemaakt en heeft uitgezet. Met het bijbehorende jaarplan wordt vervolgens inzichtelijk welke actiepunten er voor 2021 en verder zijn.

Het overnemen van de actiepunten uit het jaarplan leidt tot een realistisch en praktisch werkbaar plan voor de gemeente dat bijdraagt aan het verder verhogen van de zorgvuldige omgang met persoonsgegevens en het daarmee voldoen aan de AVG.

Extern draagvlak (partners)

Niet van toepassing.

Financiële consequenties

Niet van toepassing.

Aanpak/uitvoering

De stukken zijn besproken in het MT en vastgesteld door de directie.

Na vaststelling door het college van B&W zullen de stukken worden gedeeld met de rest van de gemeentelijke organisatie. Communicatie o.a. via intranet.

RAADSMEDEDELING

Onderwerp	Rapportage en jaarplan privacy gemeente Deventer		
Mededelingennr	2021-001082	**Portef.houder**	Burgemeester
Team	DEV-CS	**BenW-besluit d.d.:**	1 juni 2021

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

In 2020 zijn alle verwerkingen van persoonsgegevens in een register van verwerkingsactiviteiten opgenomen en heeft de gemeentelijke organisatie ervaring opgedaan met het uitvoeren van Data Protection Impact Assessments (DPIA's). Voor alle privacygevoelige werkprocessen is inzichtelijk gemaakt wie de verantwoordelijke teammanagers zijn en zij zijn gewezen op hun verantwoordelijkheden onder de privacywetgeving.

Er is een nieuwe interne Functionaris voor Gegevensbescherming aangesteld en een nieuwe Privacy Officer. De Privacy Officer adviseert over de naleving van de AVG en fungeert als eerste aanspreekpunt voor de gemeentelijke organisatie. De Functionaris voor Gegevensbescherming is verantwoordelijk voor het toezicht op de naleving van de AVG. Verder heeft de gemeentelijke organisatie ervaring opgedaan met het doorlopen van het proces bij AVG-verzoeken en er is een inhaalslag gemaakt bij het maken van afspraken met derden over het verwerken van persoonsgegevens.

4. Nadere toelichting

De gemeente Deventer verwerkt op grote schaal persoonsgegevens van inwoners. Daarnaast werkt de gemeente steeds meer samen met andere overheidsinstanties, met maatschappelijke partners en met zorgpartners, waarbij waar nodig gegevens van inwoners van Deventer worden gedeeld. De gemeente wil zorgvuldig omgaan met deze persoonsgegevens. De Algemene Verordening Gegevensbescherming (AVG) verplicht tot het aantoonbaar treffen van beheersmaatregelen binnen de gemeente om privacy en gegevensbescherming te borgen.

Het door het college vastgestelde stuk *Grip op privacy 2021* bevat zowel een rapportage over de uitvoering tot nog toe, als een concreet plan met actiepunten voor de rest van dit jaar. De rapportage vloeit voort uit een zelfmeting op een aantal privacythema's over 2020. Deze thema's zijn door VNG Realisatie ontwikkeld om de eisen uit de AVG te kunnen vertalen naar een kwaliteitscyclus voor gegevensbescherming en privacy voor gemeentelijke processen.

Het jaar 2020 gaat als een bijzonder jaar de geschiedenisboeken in door de pandemie COVID-19. Ten gevolge daarvan zijn we als gemeentelijke organisatie massaal gaan thuiswerken, waardoor onze ICT-omgeving en verbonden apparaten sindsdien zwaarder worden belast en de (cyber)-dreiging is toegenomen. In deze veranderende wereld wil de gemeente Deventer een betrouwbare digitale partner zijn. Dit is waar de uitvoering van het jaarplan in *Grip op privacy 2021* zich dan ook op richt.

Deventer, Olst-Wijhe en Raalte: samen staan we sterker.

Grip op privacy 2021

Rapportage en jaarplan gemeente Deventer

Uitgave : versie 1 (definitief)
Opsteller : L.M. Schieving, Functionaris voor Gegevensbescherming
Mail : lotte.schieving@dowr.nl

Deventer, Olst-Wijhe en Raalte: samen staan we sterker.

Inhoud

Deventer, Olst-Wijhe en Raalte: samen staan we sterker.

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

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), waarbij het college en de proceseigenaren tijdig worden voorzien van stuur- en verantwoordingsinformatie. Om dit te bereiken zijn er in 2020 op verschillende privacythema's beheersmaatregelen getroffen. *Grip op privacy 2021* bevat een rapportage van de Functionaris Gegevensbescherming over de uitvoering tot nog toe en een concreet jaarplan met actiepunten voor de komende jaren.

De rapportage geeft weer welke acties er in 2020 zijn ondernomen. Zo zijn alle verwerkingen van persoonsgegevens in een register van verwerkingsactiviteiten opgenomen en heeft de gemeentelijke organisatie ervaring opgedaan met het uitvoeren van Data Protection Impact Assessments (DPIA's). Voor alle privacygevoelige werkprocessen is inzichtelijk gemaakt wie de verantwoordelijke teammanagers zijn en zij zijn gewezen op hun verantwoordelijkheden onder de privacywetgeving. Er is een nieuwe interne Functionaris Gegevensbescherming aangesteld en een nieuwe Privacy Officer. Verder heeft de gemeentelijke organisatie ervaring opgedaan met het doorlopen van het proces bij AVG-verzoeken en er is een inhaalslag gemaakt bij het maken van afspraken met derden over het verwerken van persoonsgegevens.

Het jaar 2020 gaat als een bijzonder jaar de geschiedenisboeken in door de pandemie COVID-19. Ten gevolge daarvan zijn we als gemeentelijke organisatie massaal gaan thuiswerken, waardoor onze ICT-omgeving en verbonden apparaten sindsdien zwaarder worden belast en de (cyber-)dreiging is toegenomen. In deze veranderende wereld wil de gemeente Deventer een betrouwbare digitale partner zijn. Dit is waar de uitvoering van het jaarplan in *Grip op privacy 2021* zich dan ook op richt.

De Functionaris Gegevensbescherming adviseert de bij de AVG-implementatie ingezette lijn in 2021 door te zetten. Daarbij zal het privacybeleid moeten worden geëvalueerd en

daar waar nodig moeten worden geactualiseerd. Om dit privacybeleid actief uit te kunnen dragen wordt geadviseerd een plan op te zetten voor communicatie en bewustzijn rondom privacy en gegevensbescherming. Naast het uitvoeren van de (reeds) geplande DPIA's zal in DOWR-verband moeten worden onderzocht of er tot een eenduidige procedure voor het uitvoeren van deze assessments en het actualiseren van het verwerkingsregister kan worden gekomen. Om vervolgens de uitwisseling van opgedane privacykennis op werkprocesniveau tussen de DOWR-gemeentes soepel te laten verlopen, wordt geadviseerd per team een aanspreekpunt aan te wijzen in de vorm van een medewerker. Tot slot leert ervaring ons dat het handmatig monitoren van de resultaten en opvolging van een DPIA, het registreren van incidenten, het bijhouden van het register van verwerkingsactiviteiten en het periodiek rapporteren over de voortgang tot veel administratieve werkzaamheden lijdt. De Functionaris Gegevensbescherming adviseert daarom een tool aan te schaffen die het plannen, voorbereiden, uitvoeren, monitoren en afwikkelen van dit soort activiteiten kan borgen.

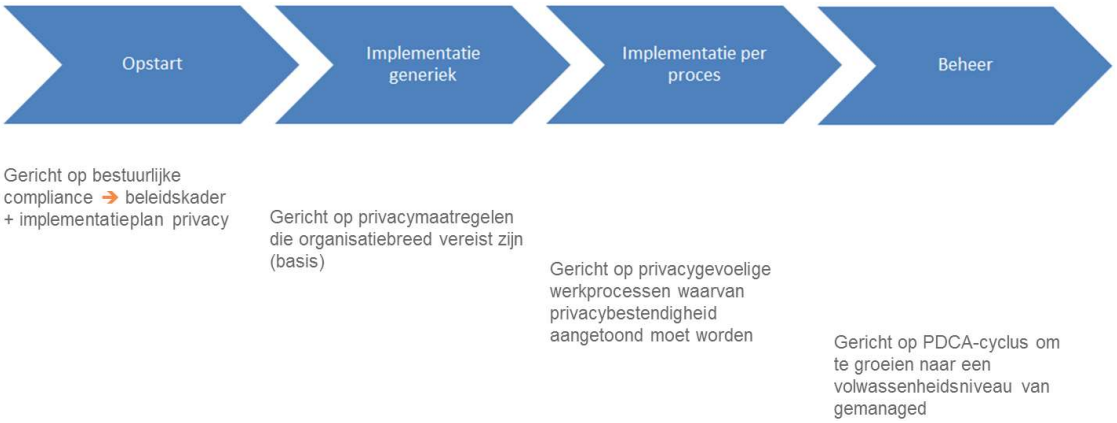
Aanpak

Risicogebaseerde benadering

De uitgangspunten voor de aanpak bij privacy liggen vast in artikel 24 AVG[1]. 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 geëvalueerd worden om te kijken of de (te nemen) beheersmaatregelen toereikend zijn. De aard van de gegevens en de context zijn hierin allesbepalende factoren. Concrete risico's zijn vervolgens beslissend bij de prioritering van werkzaamheden en vormen een indicatie voor zowel de urgentie als de keuze voor generieke of specifieke oplossingen en beheersmaatregelen.

[1] 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.

De uitvoering van de aanpak bij privacy vindt gefaseerd plaats. Schematisch vertaalt de aanpak zich als volgt:



De ambitie, zoals beschreven in het privacybeleid dat in 2018 door het college is vastgesteld, is om toe te werken naar het privacyniveau ‘gemanaged’. Dit niveau typeert zich door organisatiebreed privacybeleid gekenmerkt door awareness en bijsturing van beheersmaatregelen op basis van meetbaarheid, rekenschap en periodieke evaluaties. Het college moet daarbij als verwerkingsverantwoordelijke op ieder moment kunnen aantonen dat privacyrisico’s voldoende zijn afgedekt. Dit vereist monitoring. Monitoring op de uitvoering van het privacybeleid, maar ook op de werkprocessen, de organisatorische inbedding, de rechten van betrokkenen, de verstrekkingen van persoonsgegevens, de informatiesystemen en de handhaving van gegevensbeveiliging. Dit alles vraagt om een cyclisch plan-do-check-act-proces (PDCA-proces) waarbij het proces de inhoud borgt. Het privacyniveau ‘gemanaged’ wordt bereikt op het moment dat een dergelijk proces is ingericht, dat op basis van rapportages het college en de proceseigenaren in tijdige stuur- en verantwoordingsinformatie voorziet.

Resultaten meting privacy

Om dit privacyniveau te bereiken heeft de gemeente Deventer in 2020 stappen gemaakt in het verder implementeren van de AVG. In de bijlage bij deze rapportage is een meting opgenomen. Met deze meting wordt inzichtelijk welke score de gemeente Deventer zichzelf eind 2020 op de privacythema’s geeft ten opzichte van eind 2019. Deze zelfevaluatiethema’s zijn door VNG Realisatie ontwikkeld om de AVG te vertalen naar een kwaliteitscyclus voor gegevensbescherming en privacy voor gemeentelijke processen. Het betreft: *beleid, processen, organisatorische inbedding, rechten van betrokkenen, samenwerking, beveiliging en verantwoording*. Deze indicatoren zijn uitgekozen als referentiebeeld om de voortgang te garanderen van een maatstaf. Alle drie de DOWR-gemeentes hebben deze indicatoren in vorige jaren gebruikt om de voortgang te monitoren. 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 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 privacythema’s van de VNG bieden de organisatie daarbij een praktisch handvat om privacy in beleid en uitvoering controleerbaar te implementeren en

te borgen. Zoals de meting laat zien, zijn er in 2020 op veel thema's stappen gemaakt. Dit geeft een indicatie van de voortgang als het gaat om het implementeren van de AVG.

Actiepunten

De meting op de verschillende privacythema's kan vervolgens vertaald worden naar concrete actiepunten voor de gemeente Deventer voor 2021 en de komende jaren. Belangrijk is om op te merken dat de drie gemeentelijke organisaties in DOWR-verband bij het vaststellen van dit jaarplan elk een ander privacy vertrekpunt hebben. Zij hebben wel de uitdrukkelijke wens om bij de aanpak privacy zo veel mogelijk samen te doen. Daar wordt rekening mee gehouden door steeds eerst per thema toe te lichten welke concrete actiepunten de gemeente Deventer bij dit thema heeft. Vervolgens wordt per actiepunt toegelicht of het advies is om dit actiepunt in de gemeente Deventer zelf op te pakken of in DOWR-verband met de twee andere gemeentes. In de tekst hieronder, en de planning die aan de hand daarvan is opgesteld, is steeds terug te vinden of er sprake is van een actiepunt met een hoge, gemiddelde of lage prioriteit, zodat het college daarop kan anticiperen.

Beleid

Het college heeft in 2018 een overkoepelend privacybeleid vastgesteld waarin het haar visie op gegevensbescherming verwoordt en beschrijft hoe het waarborgt dat de gemeente Deventer persoonsgegevens behoorlijk, zorgvuldig en in overeenstemming met de wet verwerkt. Met het vaststellen van dit privacybeleid zijn de verantwoordelijkheden op strategisch en uitvoeringsniveau geborgd. In 2019 en 2020 is daar waar nodig als aanvulling daarop domeinspecifiek privacybeleid ontwikkeld. Daarin is beschreven hoe verschillende domeinen in de gemeente Deventer omgaan met (sectorspecifieke) wet- en regelgeving, persoonsgegevens en gegevensbescherming. Bijvoorbeeld daar waar het gaat om de handelingsperspectieven voor medewerkers in het Sociaal domein.

Sinds 2018 hebben zich verschillende ontwikkelingen voorgedaan op het gebied van privacy. Om de doelmatigheid en doeltreffendheid van het overkoepelend privacybeleid te blijven borgen, is het raadzaam om het beleid in 2021 door de Functionaris Gegevensbescherming te laten evalueren en daar waar nodig te actualiseren. *Dit actiepunt heeft het prioriteitstype: 'hoog'.* Om daarnaast te onderzoeken of de domeinspecifieke uitwerkingen daarvan ook in DOWR-verband gezamenlijk kunnen worden ingezet, wordt geadviseerd de Privacy Officer de opdracht te geven deze voor de drie gemeentes in kaart te brengen en een overzicht te maken van de gehanteerde afspraken over de wijze van omgang met persoonsgegevens. Dit overzicht kan vervolgens ter beschikking worden gesteld aan de gemeentelijke organisaties met een advies omtrent de harmoniseringslag die in het gebruik van deze afspraken gemaakt kan worden. *Dit actiepunt heeft het prioriteitstype: 'midden'.*

Twee domeinoverstijgende onderwerpen vragen specifieke aandacht, namelijk de omgang met persoonsgegevens van medewerkers en de omgang met kopieën van identiteitsbewijzen van inwoners. Datalekken met dit soort gegevens leveren over het

algemeen een hoog risico op (identiteits-)fraude op voor de betrokkene(n). Net als de twee andere gemeentes heeft het college van Deventer nog geen specifiek beleid vastgesteld over de borging van de gegevensbescherming bij de omgang met deze gegevens in de werkprocessen. Geadviseerd wordt hier in 2021 gezamenlijk in op te trekken door de Privacy Officer de opdracht te geven samen met de Information Security Officer hier beleid op te ontwikkelen. *Dit actiepunt heeft het prioriteitstype: 'midden'.* Waar het beleid ziet op de omgang met persoonsgegevens van medewerkers kan er dan gelijk ervaring worden opgedaan met het actief betrekken van de ondernemingsraad bij zaken die spelen op het gebied van privacy en gegevensbescherming.

De afgelopen jaren heeft het college door middel van de inzet van verschillende communicatiekanalen aandacht geschonken aan hoe medewerkers om moeten gaan met de persoonsgegevens waar zij dagelijks mee te maken krijgen. Bijvoorbeeld hoe men om moet gaan met het verstrekken van persoonsgegevens aan collega's of derden. Ook is er gecommuniceerd over de procedure datalekken en hoe medewerkers een beveiligingsincident kunnen herkennen. Zowel het management als de medewerkers zijn verder gewezen op de risico's bij het gebruik van eenvoudige en veel gebruikte gegevensverwerkingsmiddelen, zoals mailverkeer. Om het privacybeleid actief uit te kunnen dragen, en bij zowel het management als de medewerkers opnieuw bekend te maken, verdient het aanbeveling om de Functionaris voor Gegevensbescherming in 2021 een plan op te laten zetten voor communicatie en bewustzijn rondom privacy en gegevensbescherming. *Dit actiepunt heeft het prioriteitstype: 'hoog'.* Structurele aandacht voor communicatie en bewustzijn dient het reeds opgebouwde kennisniveau te verbreden, bijvoorbeeld daar waar het herkennen van AVG-verzoeken betreft, maar ook nieuwe kennis te introduceren. Denk daarbij bijvoorbeeld aan kennis over de toepassing van bepaalde algoritmen nu er steeds meer nieuwe technologieën beschikbaar komen.

Processen

Om als gemeentelijke organisatie te kunnen sturen op gegevensbescherming is inzicht nodig in de werkprocessen waar persoonsgegevens in worden verwerkt. Het college heeft inmiddels de werkprocessen in beeld gebracht voor zover zij daarbij als (mede)verantwoordelijke of verwerker optreedt. Alle verwerkingen van persoonsgegevens zijn in een register van verwerkingsactiviteiten opgenomen. Dit heeft tot een duidelijk overzicht van de verwerkingen van persoonsgegevens geleid, geclusterd naar werkprocessen, dat op de privacy SharePoint staat en indien nodig ter beschikking kan worden gesteld aan de Autoriteit Persoonsgegevens. In 2020 heeft de gemeentelijke organisatie daarnaast ervaring opgedaan met het uitvoeren van Data Protection Impact Assessments (DPIA's) bij verwerkingen die een hoog privacyrisico opleveren voor de betrokkene(n).

Aangezien de Privacy Officer en de Functionaris voor Gegevensbescherming inmiddels allebei voor alle drie de gemeentes werken, verdient het aanbeveling in 2021 duidelijkheid te krijgen over wanneer er DPIA's voor de gemeente Deventer uitgevoerd zullen gaan worden en op welke wijze dit zal gebeuren. De Privacy Officer dient daartoe een overzicht van de uitvoerdata van (reeds) geplande DPIA's te maken. Daarbij moet er ruimte worden gereserveerd voor nieuwe of gewijzigde verwerkingen met een hoog risico die zich gedurende het jaar kunnen aandienen. Of het uitvoeren van een DPIA op deze verwerkingen voorrang verdient boven de geplande DPIA's op reeds bestaande

verwerkingen is ter beoordeling van de Privacy Officer. *Dit actiepunt heeft het prioriteitstype: 'hoog'.*

Daarnaast wordt aangeraden gezamenlijk met de andere twee gemeentes de Privacy Officer de opdracht te geven te inventariseren op welke wijze de afgelopen tijd DPIA's zijn uitgevoerd en hem daarin de gemene delers te laten onderscheiden. Dit om te onderzoeken of er in DOWR-verband tot een eenduidige procedure voor het uitvoeren van DPIA's kan worden gekomen. *Dit actiepunt heeft het prioriteitstype: 'hoog'.* In de procedurebeschrijving moet in ieder geval komen te staan hoe het proces voor het uitvoeren en actualiseren van DPIA's verloopt, hoe intern verantwoordelijken er zorg voor dragen dat relevante verwerkingen in beeld komen bij de Privacy Officer, hoe de resultaten gedeeld worden met de organisatie en hoe de te nemen maatregelen opvolging krijgen. Daarbij zal ook gekeken moeten worden naar inhoudelijke harmonisering. De Privacy Officer zal daartoe bij de gemeentes ophalen welke ervaringen er met verschillende DPIA-formats zijn en daar uiteindelijk in samenspraak met de Functionaris Gegevensbescherming één DPIA-format uit kiezen wat bij het doorlopen van de procedure ingezet kan gaan worden. Voorts kan er door middel van een toelichting op de procedure in de managementoverleggen door de Privacy Officer en de Functionaris Gegevensbescherming opnieuw aandacht worden gevraagd voor het bestaan en de werking van de DPIA bij het management.

Harmonisering op dit thema heeft nog een andere component, namelijk het uitwisselen van DPIA's. Om er voor te zorgen dat de kennis die is opgedaan bij een DPIA in één van de gemeentes hergebruikt wordt bij een vergelijkbaar werkproces in de twee andere gemeentes, is het raadzaam de Privacy Officer hierin een verbindende rol te laten spelen. Dit betekent dat hij de opdracht krijgt van de drie gemeentes samen om de uitkomsten, aanbevelingen en het adviezen van de FG niet alleen te delen met de betrokken medewerkers, maar ook, daar waar relevant met de tegenhangers daarvan in de twee andere gemeentes. Om dit mogelijk te maken zal er naast de hierboven beschreven DPIA-planning tevens door de Privacy Officer moeten worden gekeken naar reeds bij de gemeente Deventer uitgevoerde DPIA's en door hem moeten worden beoordeeld of zo'n kennisuitwisseling op zijn plaats is. *Dit actiepunt heeft het prioriteitstype: 'midden'.*

Organisatorische inbedding

De afgelopen jaren is gebleken dat het omwille van het tijdig en laagdrempelig kunnen betrekken van de Functionaris Gegevensbescherming bij vraagstukken en incidenten het de voorkeur verdient om een interne Functionaris voor Gegevensbescherming te hebben. Op voorstel van de organisatie heeft het college in 2020 dan ook een nieuwe interne Functionaris Gegevensbescherming aangesteld. Zij staat inmiddels geregistreerd bij de Autoriteit Persoonsgegevens. Ook is er een nieuwe Privacy Officer aangesteld. Deze twee privacyfunctionarissen voeren samen zowel de privacywerkzaamheden voor de gemeente Deventer als voor de twee andere gemeentes uit. De Privacy Officer adviseert daarbij over de naleving van de AVG en fungeert als eerste aanspreekpunt voor de gemeentelijke organisatie. De Functionaris voor Gegevensbescherming is verantwoordelijk voor het toezicht op de naleving van de AVG. Door middel van een introductiebericht op intranet zijn de functionarissen aan de gemeentelijke organisatie van Deventer voorgesteld en is duidelijk gemaakt wat de specifieke taken van de Privacy

Officer en de Functionaris Gegevensbescherming zijn. Het verdient aanbeveling om in 2021 te blijven monitoren of de Privacy Officer ook daadwerkelijk door managers en medewerkers gevonden wordt als eerste aanspreekpunt bij vraagstukken die verband houden met privacy en het uitvoeren van DPIA's. *Dit actiepunt heeft het prioriteitstype: 'midden'.*

In 2018 is een privacyoverlegorgaan opgericht, het Privacy Implementatie Team (PIT). Dit team bestaat uit de directeur met in zijn portefeuille AVG/privacy, de Privacy Officer, de Information Security Officer, de Chief Information Security Officer en de Functionaris Gegevensbescherming. Vier keer per jaar behandelt dit team een verscheidenheid aan strategische vraagstukken op het gebied van privacy en informatieveiligheid. In 2020 hebben er geen formele PIT-overleggen plaatsgevonden. De specifieke reden daarvoor is onduidelijk. Het overleg heeft dit jaar bestaan uit incidentele werkoverleggen met de bevoegde directeur of de portefeuillehouder en een wekelijks (digitaal) samenkomen van de Privacy Officer, de Information Security Officer, de Chief Information Security Officer en de Functionaris Gegevensbescherming. Om te borgen dat er structureel aandacht blijft voor de implementatie van de AVG is het raadzaam om in 2021 naast het wekelijks samenkomen van de privacy- en informatieveiligheidsfunctionarissen weer formele gemeentelijke PIT-overleggen plaats te laten vinden. *Dit actiepunt heeft het prioriteitstype: 'hoog'.* Op deze manier blijven de directieleden, managers en medewerkers van de individuele gemeentes aangesloten bij de uitvoering van de privacy aanpak door de in DOWR-verband opererende functionarissen. Een bijkomend voordeel is dat men bij het opstellen van een formele agenda voor een bepaalde gemeente er toe gedwongen wordt specifieke gemeentelijke agendapunten op te halen in de gemeente die het betreft. Deze gemeentelijke input zorgt er voor dat er oog blijft voor de verschillen tussen de DOWR-gemeentes en er voldoende maatwerk geleverd kan worden waar dat nodig is bij de behandeling van strategische vraagstukken op het gebied van privacy en informatieveiligheid.

De proceseigenaar is verantwoordelijk voor het privacybestendig maken van zijn of haar werkprocessen. In het beleidskader privacy en gegevensbescherming zijn de teammanagers aangewezen als proceseigenaren. Dit komt overeen met de verantwoordelijkheid voor het nemen van beheersmaatregelen bij de implementatie van de Baseline Informatiebeveiliging Overheid. Ondertussen is van alle privacygevoelige werkprocessen bekend wie de verantwoordelijke teammanager is en zijn deze gewezen op hun verantwoordelijkheden onder de privacywetgeving. Er wordt geadviseerd bij het opzetten van een plan voor communicatie en bewustzijn rondom privacy en gegevensbescherming in 2021 het management niet te vergeten. Voor de effectiviteit van het privacybeleid is het van groot belang dat zij zich bewust zijn van hun verantwoordelijkheid voor het privacybestedig maken van de werkprocessen. Bijvoorbeeld van het feit dat het eventueel reserveren van budget voor de nodige privacymaatregelen een vorm van integraal privacymanagement is. *Dit actiepunt heeft het prioriteitstype: 'midden'.*

Om de uitwisseling van opgedane privacykennis op werkprocesniveau tussen de DOWR-gemeentes soepel te laten verlopen, verdient het aanbeveling dat de Privacy Officer per team een aanspreekpunt krijgt aangewezen in de vorm van een medewerker. Deze medewerker weet wat er op zijn of haar team in de werkprocessen speelt en krijgt als taak de ontwikkelingen op het gebied van privacy, adviesmateriaal en resultaten van DPIA's te verspreiden onder zijn of haar collega's. Hij of zij wordt in voorbereiding op het

PIT-overleg voor Deventer ook gevraagd om agendapunten aan te leveren. Op die manier wordt geprobeerd een brug te slaan tussen het PIT, de privacyfunctionarissen en de medewerkers van de gemeente Deventer. *Dit actiepunt heeft het prioriteitstype: 'hoog'.*

Rechten van betrokkenen

In 2018 is door middel van het vaststellen van het privacybeleid ruimte gecreëerd voor betrokkenen om effectief gebruik te kunnen maken van hun privacyrechten. Deze ruimte is praktisch ingevuld door een aantal ontwikkelingen. Op de website van de gemeente Deventer is bijvoorbeeld een beveiligd selfserviceportaal ter beschikking gesteld waarmee betrokkenen eenvoudig digitaal hun rechten, zoals de inzage en wijziging van persoonsgegevens, kunnen uitoefenen. Deze mogelijkheid bestaat nu naast de mogelijkheid om een schriftelijk verzoek te doen en een afspraak te maken op het stadhuis. In 2020 heeft de gemeentelijke organisatie daarnaast ervaring opgedaan met het doorlopen van het proces wat is ingericht om AVG-verzoeken van betrokkenen adequaat af te kunnen handelen. De teammanager waar de betreffende gegevensverwerking onder valt, is daarbij verantwoordelijk 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 die aan de behandeling van een dergelijk verzoek hebben meegewerkt weten inmiddels hoe zij een verzoek kunnen herkennen en wat zij moeten doen op het moment waarop zij een dergelijk verzoek ontvangen. Het is raadzaam om in 2021 structureel aandacht te vragen voor dit soort verzoeken door dit onderwerp door de Functionaris Gegevensbescherming mee te laten nemen in het plan voor communicatie en bewustzijn rondom privacy en gegevensbescherming. Zo wordt geborgd dat ook nieuwe medewerkers, managers en medewerkers die nog geen ervaring hebben met dit soort verzoeken kennis opdoen over de rechten die het daarbij betreft, de termijnen die moeten worden bewaakt en de manier van afhandeling. *Dit actiepunt heeft het prioriteitstype: 'midden'.*

Ook verdient het aanbeveling om als college in 2021 de focus te leggen op hoe we als gemeentelijke organisatie tijdens de ontwikkeling van nieuwe producten en diensten zo goed mogelijk rekening houden met de rechten van betrokkenen. Een eerste stap daarin zou zijn dat de Functionaris Gegevensbescherming gevraagd wordt inzichtelijk te maken hoe privacy geïntegreerd kan worden bij de inkoop van een product of dienst, het toepassen van de inkoopstrategie in DOWR-verband en eventueel doorlopen van een aanbestedingsprocedure. De daartoe gehanteerde criteria moeten op zo'n manier worden geformuleerd dat wordt gewaarborgd dat ingekochte producten en diensten ook daadwerkelijk voorzien in de uitoefening van de rechten van betrokkene(n). Aangeraden wordt om dan ook meteen andere AVG-uitgangspunten hierin naar voren te laten komen, zoals het aangaan van verwerkersovereenkomsten en het beginsel van dataminimalisatie. *Dit actiepunt heeft het prioriteitstype: 'hoog'.* Dit privacykader bij inkoop zal worden afgestemd met de stakeholders bij de geldende aansluitvoorwaarden, het SLA-format en andere reeds geldende afwegingscriteria. Daarbij moet tevens stil worden gestaan bij de fase waarin bepaalde criteria een rol gaan spelen en het privacykader gehanteerd dient te worden.

Het is aan te raden door middel van het uitvoeren van DPIA's in 2021 meer inzicht te vergaren over of betrokkenen voor- en tijdens concrete gegevensverwerkingen op beknopte en begrijpelijke wijze over verwerkingen wordt geïnformeerd en of, daar waar de grondslag toestemming wordt gebruikt, aan de randvoorwaarden voor toestemming wordt voldaan. Waar nodig kan dan een verbeteringsslag worden uitgevoerd in de communicatie of het vragen van toestemming. *Dit actiepunt heeft het prioriteitstype: 'laag'.*

Samenwerking

Aan het laten verwerken van persoonsgegevens door andere organisaties zijn wettelijke voorwaarden verbonden. De afgelopen jaren wisten managers en medewerkers de Privacy Officer te vinden bij vragen over de inschakeling van derde partijen, gegevensverwerking bij samenwerkingsverbanden of gemeenschappelijke verwerkers in DOWR-verband. De Baseline Informatiebeveiliging Overheid dwingt een vergelijkbare voorafgaande toets af. Op dat gebied is in 2020 dan ook intensief samengewerkt met informatiebeveiliging. Bij het ontwerpen en inkopen van applicaties en producten is bijvoorbeeld vroegtijdig samen gescreend welk beveiligingsniveau, conform het privacybeleid en het informatieveiligheidsbeleid, passend en toereikend zou moeten zijn.

De gemeentelijke organisatie heeft vanaf 2018 een inhaalslag gemaakt daar waar er nog geen afspraken waren met betrekking tot het verwerken van persoonsgegevens of daar waar deze afspraken niet AVG-proof bleken. Bij het sluiten van nieuwe contracten zijn deze schriftelijke afspraken inmiddels een standaard onderdeel geworden. Het is raadzaam in 2021 extra aandacht te schenken aan de afspraken met zelfstandig verantwoordelijken. Vaak wordt er in dit soort situaties door de andere partij een verwerkersovereenkomst voorgesteld, terwijl er aan de hand van de feitelijke omstandigheden kan worden vastgesteld dat de verwerking van persoonsgegevens onder de verantwoordelijkheid valt van één van de twee zelfstandig verantwoordelijken. Afspraken over de wijze van verstrekking, bijvoorbeeld in de vorm van beveiligd mailverkeer, zijn dan op zijn plaats in plaats van het sluiten van een verwerkersovereenkomst. Het college heeft een overzicht gemaakt van de gesloten en geactualiseerde verwerkersovereenkomsten en in het register van verwerkingen aangegeven voor welke processen deze afspraken wel en niet zijn gemaakt. Of er in bepaalde gevallen nog andere afspraken moeten worden gemaakt, bijvoorbeeld bij de gegevensuitwisseling met zelfstandig verantwoordelijken, en waar deze precies ontbreken is nog niet duidelijk. Om dit overzicht te krijgen is meer informatie nodig over concrete gegevensverwerkingen. Dit kan door middel van DPIA's en op initiatief van medewerkers uit de organisatie worden opgehaald. Waar nodig kunnen dan alsnog afspraken worden gemaakt over de gegevensverwerking. *Dit actiepunt heeft het prioriteitstype: 'midden'.*

Op 16 juli 2020 verklaarde het Hof van Justitie van de Europese Unie in het zogenoemde 'Schrems II' arrest het Privacy Shield ongeldig (HvJ EU 16 juli 2020, C-311/18). Op verzoek van de Functionaris Gegevensbescherming is er door de Information Security Officer en de Privacy Officer een onderzoek gestart naar de impact van deze uitspraak op de doorgiften van persoonsgegevens naar derde landen van de gemeente Deventer en de twee andere gemeentes. Na de uitspraak heeft zowel de Autoriteit Persoonsgegevens als het Europees Comité voor

gegevensbescherming (EDPB) aanbevelingen gepubliceerd over de doorgiften van persoonsgegevens. Daarin werd bijvoorbeeld aangegeven hoe organisaties de praktische gevolgen van de uitspraak moesten onderzoeken en dat doorgiften na de uitspraak alleen plaats mocht vinden wanneer het door de AVG beschermde beveiligingsniveau daarbij niet werd ondermijnd. Aan de hand van de verwerkingsregisters van de drie gemeentes zijn vervolgens de doorgiften in kaart gebracht die verband houden met onder het Privacy Shield gecertificeerde bedrijven. Daarbij is gekeken naar de hosting, de hostinglocatie en de onderliggende contracten (incl. de verwerkersovereenkomsten). Er werd vastgesteld dat er op dit moment geen aanvullende maatregelen genomen hoeven te worden nu deze doorgiften ook zonder het Privacy Shield onder een gelijkwaardig AVG-beschermingsniveau plaats kunnen vinden en dus nog steeds geoorloofd zijn. Het verdient desalniettemin aanbeveling de resultaten uit dit onderzoek periodiek te evalueren. *Dit actiepunt heeft het prioriteitstype: 'midden'.*

Informatiebeveiliging

Sinds 1 januari 2016 geldt de meldplicht datalekken. Een datalek is een incident waar persoonsgegevens bij verloren zijn gegaan, waar onrechtmatige verwerking van persoonsgegevens bij heeft plaatsgevonden, of wanneer dit niet met zekerheid uitgesloten kan worden. Het voorkomen van incidenten met betrekking tot persoonsgegevens is voor een groot deel ingebed in de set van preventieve beveiligingsmaatregelen die zijn opgenomen in de Baseline Informatiebeveiliging Overheid. Wanneer een dergelijk incident zich toch voordoet, dient de gemeente Deventer voorbereid te zijn op het nemen van de nodige vervolgstappen en beheersmaatregelen.

In 2018 is de procedure meldplicht datalekken, die gevolgd dient te worden in het geval van een datalek, geactualiseerd en in alle drie de DOWR-gemeentes vastgesteld. De gewijzigde procedure beschrijft de stappen die voor en na het melden van een datalek door de verschillende actoren moeten worden doorlopen. Sinds 2018 hebben zich verschillende ontwikkelingen voorgedaan op het gebied van privacy en informatieveiligheid. Om de doelmatigheid en doeltreffendheid van de procedure te blijven borgen, verdient het aanbeveling deze procedure in 2021 door de Functionaris Gegevensbescherming en de Chief Information Security Officer te laten evalueren en daar waar nodig te actualiseren. *Dit actiepunt heeft het prioriteitstype: 'hoog'.*

Beveiligingsmaatregelen dienen een passend niveau van beveiliging (BBN) te waarborgen rekening houdend met de privacyrisico's, de stand van de techniek en de uitvoeringskosten. Opmerking verdient dat in 2020 nog niet bij alle voor verwerking gebruikte geautomatiseerde systemen de inrichting van de standaardinstelling zo is ingesteld dat er rekening wordt gehouden met de privacy van betrokkenen en de AVG-beginselen. Er wordt bijvoorbeeld niet bij alle systemen gezorgd voor periodieke controles op de autorisaties. Ook worden nog niet alle verwerkingsactiviteiten binnen geautomatiseerde systemen voldoende gelogd. Er wordt geadviseerd om in 2021 de nodige maatregelen te nemen om 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 blijven en worden verder uitgewerkt in het jaarplan voor informatiebeveiliging. *Dit actiepunt heeft het prioriteitstype: 'midden'.*

Verantwoording

Om grip te houden op het beheer en onderhoud van het register van verwerkingen is centrale coördinatie en registratie van verwerkingen nodig. De Privacy Officer is met deze coördinatie en registratie belast. Alle verwerkingen van persoonsgegevens zijn inmiddels in het register opgenomen. Vanwege het belang van een actueel verwerkingsregister verdient het aanbeveling om in 2021 een actualisatieslag uit te voeren. Dat betekent dat managers gevraagd zullen worden om de verwerkingen in het register die onder hun verantwoordelijkheid vallen na te gaan en daarbij aan te geven of zij nog up-to-date zijn. *Dit actiepunt heeft het prioriteitstype: 'hoog'.*

Er wordt geadviseerd de mate van AVG-compliance op procesniveau, die per geregistreerde verwerking uit het register blijkt, vervolgens bij te houden. Daartoe dient de hierboven genoemde actualisatieslag periodiek plaats te vinden. Aangezien er veel overeenkomsten zijn tussen het register van verwerkingen van de gemeente Deventer en de andere twee gemeentes wordt aangeraden de Privacy Officer de opdracht te geven te onderzoeken of er in DOWR-verband één proces kan worden ontwikkeld voor het tijdig nalopen van wijzigingen in de structurele verwerkingen van persoonsgegevens. *Dit actiepunt heeft het prioriteitstype: 'hoog'.* Om achterstanden of vervuiling in de geregistreerde structurele verwerkingen zoveel mogelijk te voorkomen, dient er in dit proces in ieder geval aandacht te zijn voor de opzet van het register van verwerkingen, de manier van registreren en de rol van de medewerkers die als aanspreekpunt per team worden aangewezen.

In 2020 zijn nieuwe verwerkingen of wijzigingen van bestaande verwerkingen actief aangemeld bij de Privacy Officer en is de belangenafweging om al dan niet over te gaan tot een DPIA vastgelegd. Bij het uitvoeren van DPIA's is duidelijk geworden dat de activiteiten die verbonden zijn aan het voorbereiden, uitvoeren, afwikkelen, opvolgen en beheren van DPIA's in veel documentatie resulteren. Niet alleen de ingevulde vragenlijst, maar ook de rapportage, de consultatie en advisering van de Functionaris Gegevensbescherming, eventueel de gemotiveerde afwijking van het FG-advies door een teammanager en de opvolging van beheersmaatregelen moet worden gedocumenteerd. Het is dan ook raadzaam om als gemeente Deventer samen met de twee andere gemeentes hiervoor één efficiënte werkwijze uit te laten kiezen. *Dit actiepunt heeft het prioriteitstype: 'hoog'.* Aandacht voor het aantoonbaar vastleggen van bevindingen en bijbehorende documentatie maakt dat de resultaten van een DPIA verifieerbaar en vindbaar blijven. Teveel focus op de vastlegging kan echter ten koste gaan van het uiteindelijke doorvoeren van de resultaten van een DPIA in het werkproces en het nemen van beheersmaatregelen. Het is dan ook belangrijk om hier een middenweg in te vinden.

Het handmatig monitoren van de voortgang bemoeilijkt nu nog het periodiek kunnen rapporteren over de AVG-compliance in de werkprocessen. Aangezien het ambitieniveau 'gemanaged' daar wel om vraagt, wordt geadviseerd in 2021 een tool aan te schaffen die het plannen, voorbereiden, uitvoeren, monitoren en afwikkelen van DPIA's kan borgen. *Dit actiepunt heeft het prioriteitstype: 'hoog'.* In deze tool moet tevens het incidenteel advies en de uitwerking daarvan in de structurele verwerkingen

kunnen worden vastgelegd bij die processen waar nog geen DPIA voor is uitgevoerd. Dit om te voorkomen dat veranderingen in de AVG-compliance die ten gevolge van deze wijzigingen zich voordoen onopgemerkt blijven in de rapportages op verwerkingsniveau. Het vastleggen van de bewijsstukken, zoals de resultaten van een DPIA of de ontwikkelingen bij het doorvoeren van een bepaalde beheersmaatregel, moet daarmee worden vergemakkelijkt. Wie de verantwoordelijkheid krijgt om deze stukken in de tool te zetten en welke rol de medewerkers die als aanspreekpunt per team worden aangewezen daarbij kunnen spelen zal daartoe moeten worden uitgewerkt.

Planning

De meting op de verschillende privacythema's en de actiepunten die daaruit voortvloeien worden hieronder in een planning voor 2021 en verder weergegeven. Daarbij wordt onderscheid gemaakt tussen actiepunten waarbij het advies is om die in de gemeente Deventer zelf op te pakken en actiepunten waarbij het raadzaam is om die in DOWR-verband met de twee andere gemeentes op te pakken. Per actiepunt wordt steeds aangegeven of er sprake is van hoge, gemiddelde of een lage prioriteit. Dit is aangeduid in de planning door middel van de voorgestelde periode van implementatie:

- Bij de actiepunten met een hoge prioriteit is dit Q2 en Q3;
- Bij de actiepunten met een gemiddelde prioriteit is dit Q4 en 2022 en verder; en
- Bij de actiepunten met een lage prioriteit is dit 2022 en verder.

	Periode				
	2021				2022 e.v.
Actiepunt	Q1	Q2	Q3	Q4	>
Beleid					
Evaluatie en actualisatie beleidskader privacy (hoog, decentraal)		X			
Overzicht en advies domeinspecifieke beleidsuitwerkingen (midden, DOWR)				X	
Ontwikkelen privacybeleid medewerkersdossier en gebruik identiteitsbewijzen (midden, DOWR)				X	
Ontwikkelen communicatie- en bewustzijnsplan (hoog, DOWR)		X			
Implementatie communicatie- en bewustzijnstraject (hoog, DOWR)			X		
Processen					
Overzicht uitvoerdata DPIA's (hoog, decentraal)			X		
Ontwikkelen DPIA-procedure (hoog, DOWR)		X			

Start proces kennisuitwisseling resultaten DPIA's (midden, DOWR)			X	
Organisatorische inbedding				
Monitoren vindbaarheid advisering Privacy Officer (midden, decentraal)			X	
Plannen gemeentelijke PIT-overleggen (hoog, decentraal)	X			
Aandacht voor het communicatie- en bewustzijnsthema 'governance' (midden, DOWR)			X	
Aanwijzen aanspreekpunten privacy (hoog, decentraal)	X	X		
Rechten van betrokkenen				
Aandacht voor het communicatie- en bewustzijnsthema 'AVG-verzoeken' (midden, DOWR)				X
Privacy by design bij inkoop (hoog, DOWR)		X		
Borging transparantie en rechtsgeldige toestemming bij concrete verwerkingen (laag, decentraal)				X
Samenwerking				
Borging afspraken bij concrete verwerkingen (midden, decentraal)			X	
Evaluatie onderzoek doorgiften derde landen (midden, DOWR)				X
Beveiliging				
Evaluatie en actualisatie procedure datalekken (hoog, decentraal)	X			
Start kwaliteitsslag beveiligingsniveau bij informatiesystemen (midden, DOWR)			X	
Verantwoording				
Actualisatie register van verwerkingen (hoog, decentraal)	X			
Ontwikkelen proces voor actualisatie verwerkingsregister (hoog, DOWR)		X		
Ontwikkelen werkwijze documentatie DPIA (hoog, DOWR)	X			
Aanschaffen beheerstool (hoog, DOWR)	X			