Privacy en informatieveiligheid in het sociaal domein

Werkbaarheid van wet- en regelgeving

Prof. Dr. J. (Hans) Bossert
E.I.A. (Emilie) Stumphius MSc LLM
G.S. (Gideon) van der Hulst MSc

Rekenkamer Dronten

Dhr. J. Vullings
Ambtelijk secretaris

T. 0321 – 388 288
j.vullings@dronten.nl

Postbus 100
8250 AC Dronten

Voorwoord

Namens de Rekenkamer van de gemeente Dronten bieden we u het rapport aan met betrekking tot een onderzoek naar “Werkbaarheid van wet- en regelgeving”. Het onderzoek richtte zich op “Privacy en informatieveiligheid in het sociale domein”. Het onderzoek is uitgevoerd door Necker van Naam in opdracht van de Rekenkamer Dronten. Samen met de bestuurlijke reactie, na ambtelijk wederhoor, bieden we de gemeenteraad van Dronten dit rapport aan.

Het onderzoek bevestigt ons beeld dat zorgvuldig omgaan met privacy en privacy gevoelige informatie veel aandacht verdient en krijgt. Sinds de invoering van de AVG, mei 2018, is hieraan ook in de media veel aandacht gegeven. Voor ons is de wetgeving een gegeven, waarmee op een goede wijze dient te worden omgegaan. In het onderzoek heeft daarom werkbaarheid centraal gestaan. De resultaten van het onderzoek , alsmede de conclusies en aanbevelingen, kunt u in het rapport lezen.

Graag willen we iedereen bedanken die aan het onderzoek hun medewerking hebben gegeven.

Rekenkamer Dronten,
Dick van Hemmen, voorzitter.
Jamilja van der Meulen
Mark Duijtshoff
Jules Vullings, ambtelijk secretaris
Dennie Kattenberg, ambtelijk secretaris.

Inhoudsopgave

Bestuurlijke nota

Onderzoeksverantwoording

Aanleiding

Het thema privacy staat in de maatschappelijke schijnwerpers. Ontwikkelingen zoals de introductie van de Algemene Verordening Gegevensbescherming (AVG) en de discussies rondom Facebook en CambridgeAnalytica wakkeren deze aandacht aan. Van organisaties, en zeker ook van gemeenten, wordt verwacht dat zij de privacy van personen beschermen. Tegelijkertijd krijgen gemeenten steeds meer verantwoordelijkheden en daarmee grotere hoeveelheden gegevens tot hun beschikking. Het sociaal domein is daar bij uitstek een voorbeeld van.

Nieuwe wetgeving zoals de AVG kan van invloed zijn op de uitvoeringspraktijk. Medewerkers in het sociaal domein kunnen spanning ervaren tussen de maatregelen die nodig zijn om de privacy van inwoners te waarborgen enerzijds, en het bieden van goede ondersteuning en dienstverlening anderzijds. Dit roept de vraag op of maatregelen die naar aanleiding van wet- en regelgeving worden genomen, werkbaar zijn in de praktijk. Werkbaarheid van privacywet- en regelgeving in het sociaal domein staat daarom in dit onderzoek centraal.

Doelstelling en vraagstelling

Doelstelling onderzoek

De doelstelling van dit onderzoek is om inzicht te krijgen in de werkbaarheid van de genomen maatregelen met betrekking tot informatieveiligheid en privacy in het sociaal domein (Zorg, Jeugd en Werk) en, daar waar nodig, aanbevelingen mee te geven om de werkbaarheid te vergroten door belemmeringen weg te nemen.

Hoofd- en deelvragen

Op basis van deze doelstelling is de volgende centrale vraag geformuleerd:

Welke gevolgen hebben de maatregelen, die door de gemeente Dronten naar aanleiding van en in voorbereiding op de AVG zijn getroffen op het gebied van privacy en informatieveiligheid, op de uitvoering van het sociaal domein?

Deze hoofdvraag is vertaald in de volgende deelvragen:

1. Hoe heeft de gemeenteraad kaders gesteld ten aanzien van informatiebeveiliging en privacybeleid in het sociaal domein; en welke rol neemt hij ten aanzien van dit onderwerp in?
2. Hoe is de organisatie van informatieveiligheid en privacy vormgegeven?
3. Hoe is wet- en regelgeving ten aanzien van informatieveiligheid en privacy geïmplementeerd en hoe functioneert deze opzet in de praktijk?
4. Hoe wordt de werkbaarheid ervan ervaren bij medewerkers van de gemeente Dronten en ketenpartners?

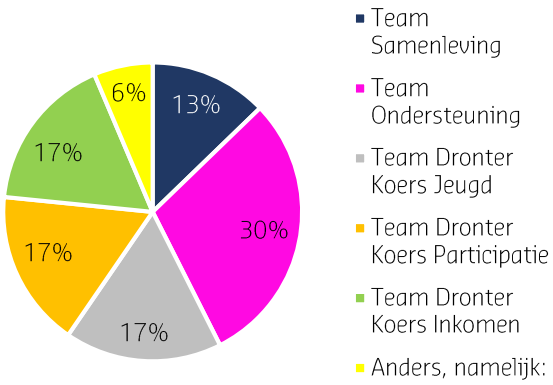
5. In hoeverre komt de werkwijze van medewerkers overeen met vastgestelde processen/werkwijzen rondom informatiebeveiliging en privacy (in het sociaal domein)?
6. Heeft de aangescherpte wet- en regelgeving op het gebied van informatiebeveiliging en privacy binnen het sociaal domein geleid tot langere doorlooptijden/afhandeltermijnen?
7. Wat is het effect van de AVG geweest op uitvoeringskosten en hoe verhoudt dit zich tot andere gemeenten?

Onderzoeksuitvoering

Op 12 december 2018 vond het startgesprek plaats tussen de onderzoekers en de rekenkamer. De onderzoekers voerden hun werkzaamheden uit in de periode december 2018-maart 2019. De werkzaamheden bestonden allereerst uit een documentstudie en interviews (zie bijlage I voor een overzicht van personen die de onderzoekers in het kader van dit onderzoek spraken). Van de interviews zijn verslagen gemaakt. De verslagen zijn ter verificatie aan de respondenten voorgelegd en geaccordeerd.

Zowel medewerkers uit het sociaal domein van de gemeente als externe samenwerkingspartners werden vervolgens uitgenodigd om digitaal een enquête in te vullen. De vragenlijst is op 8 april als eerste uitgestuurd naar medewerkers van de gemeente, zij konden deze vragenlijst invullen tot 30 april. Externe partners konden de vragenlijst invullen van 23 april tot en met 6 mei. Van de 149 uitgenodigde medewerkers van d e gemeente vulden 47 medewerkers de vragenlijst in (respons; 31,5%). De respons onder de groep medewerkers van de gemeente was verdeeld over de verschillende teams, met de grootste bijdrage van Team Ondersteuning, zie figuur 1.

Figuur 1 Binnen welk team van de gemeente Dronten bent u werkzaam? (N=47)



Van de 48 uitgenodigde externe partners vulden 30 personen de vragenlijst in (respons: 62,5%). Dit betreft 26 invullers namens een zorgleverancier en 4 invullers namens sociale veiligheidspartners. De vragenlijst voor de externe partners was minder uitgebreid dan de vragenlijst voor medewerkers van de gemeente zelf. In de vragenlijst is invullers enkele malen gevraagd om op 5- of 7-puntsschalen hun mening te geven over bepaalde stellingen. Om een zo helder mogelijk beeld te schetsen, zijn deze antwoorden in de analyse teruggebracht tot 3 categorieën (bv: eens, neutraal, oneens).

Op basis van de resultaten van de vragenlijst zijn vervolgens duidingsgesprekken gevoerd met medewerkers van de gemeente Dronten en externe partners.

Op 23 mei 2019 is de definitieve Nota van bevindingen aangeboden aan de rekenkamer. Op 24 mei 2019 is de rapportage aan de ambtelijke organisatie voorgelegd voor een verificatie van de feiten. Vervolgens heeft het bestuur vanaf 14 juni de kans gehad om een reactie te formuleren op de conclusies en aanbevelingen. Deze bestuurlijke reactie is een separate bijlage bij dit rapport. Op 4 juli is het definitieve rapport aangeboden aan de griffie.

Technisch onderzoek

De onderzoekers realiseren zich dat een onderzoek naar privacy in het sociaal domein leidt tot een rapportage met relatief veel jargon en technische termen. In de tekst zijn daarom voorbeelden uit gehouden interviews opgenomen om duiding aan te brengen, en in bijlage III is een lijst met verklaringen en begrippen opgenomen.

Leeswijzer

Dit rapport bestaat uit twee delen: de Bestuurlijke nota en de Nota van bevindingen. De Bestuurlijke nota bevat deze onderzoeksverantwoording en wordt gevolgd door de conclusies & aanbevelingen. De Nota van bevindingen bevat 3 hoofdstukken:

- Hoofdstuk 1 gaat in op de (beleids)kaders en organisatie van privacy en informatieveiligheid van de gemeente Dronten.
- Hoofdstuk 2 beschrijft de implementatie van de AVG en de effecten hiervan op het sociaal domein.
- Hoofdstuk 3 bevat informatie over de werkprocessen en het bewustzijn van medewerkers.

Achterin dit rapport vindt u de bijlagen. U vindt de vermelding van bronnen en respondenten in bijlage I, de resultaten van de schouw van de afdeling in bijlage II en een verklaringen- en begrippenlijst in bijlage III. In bijlage IV en V vindt u een visuele weergave van het onderzoek in de vorm van een infographic en de reactie van het college van de gemeente Dronten op de conclusies en aanbevelingen.

Conclusies & aanbevelingen

Conclusies

1. Werkbaarheid staat centraal in keuzes rondom privacy en informatieveiligheid

Binnen de wettelijke kaders hebben gemeenten keuzeruimte voor het waarborgen van privacy en informatiebeveiliging. In de keuzes die de gemeente Dronten maakt, staat 'werkbaarheid' centraal. Hoewel zowel de gemeente Dronten als zorgpartners merken dat de AVG soms maakt dat men geen informatie meer durft te delen die wel gedeeld mag worden, is het uitgangspunt dat de gemeente en externe partners samen zoeken naar een werkbare methode. Deze pragmatische, doelgerichte aanpak is bijvoorbeeld terug te zien in de keuze voor de Leertuinmethode, die wordt gebruikt voor het delen van gegevens met externen en collega-ambtenaren binnen de gemeente. In deze methode wordt niet met toestemmingsverklaringen gewerkt, maar met een afwegingskader om gegevens te delen. Met deze insteek voorkomt de gemeente dat er onnodig tijd gaat zitten in het 'organiseren' van privacy. Dit is bijvoorbeeld ook terug te zien in de afspraken over gegevensuitwisseling met externen. Toen bleek dat het niet mogelijk was om één convenant op te stellen voor alle partners, heeft Dronten er voor gekozen om alle externe partners aan te laten tonen dat ze AVG-proof werken. De verantwoordelijkheid ligt daarmee bij de organisaties, zodat extra werk voor de gemeente werd voorkomen. Deze pragmatische insteek zorgt ervoor dat uitvoerend medewerkers zich kunnen richten op het bieden van ondersteuning en in mindere mate op administratieve handelingen. Daarmee staat de werkbaarheid hoog in het vaandel.

2. Urgentie en noodzaak privacy en informatieveiligheid wordt niet breed gevoeld

De gemeente Dronten heeft op strategisch- en uitvoerend niveau aandacht voor privacy en informatieveiligheid. Toch is dit vaak reactief, en lijkt de gemeente (te) weinig urgentie voor het thema te voelen. Dit is onder andere terug te zien in de manier waarop relevante stukken worden opgesteld. In 2015 werd gestart met het opstellen van het eerder genoemde privacyconvenant, maar het is nooit afgerond door 'capaciteitstekort en ingewikkeldheid van het vraagstuk'. Pas nadat de raad hier in juni 2016 naar vroeg, is geconcludeerd dat één convenant niet werkbaar is en is er voor gekozen om externe partners te laten bewijzen dat ze AVG-proof werken. Deze dynamiek lijkt zich nu te herhalen: de oplevering van een gemeentebreed privacybeleid was voorzien voor het eerste kwartaal van 2019, maar dat beleid is er nog niet. Het informatiebeveiligingsbeleid is wel up-to-date.

Andere signalen dat urgentie maar beperkt wordt gevoeld, ziet de rekenkamer in het feit dat de voorbereidingen op de AVG pas laat van start gingen: een kleine drie maanden van tevoren werd een externe adviseur aangetrokken om te ondersteunen in de voorbereidingen. Dit leidde ertoe dat ook na de inwerkingtreding van de AVG nog veel geregeld moest worden. Er is voor 0,2 fte een Functionaris Gegevensbescherming aangetrokken, maar de werkzaamheden van deze FG kosten meer tijd dan van tevoren bedacht. Daarnaast geven medewerkers aan dat zij zich bewust zijn van privacy en informatieveiligheid, en dat dit bewustzijn toenam door de invoering van de AVG, maar rondde slechts 28,5% van de genodigden een e-learning module over privacy af. In dat kader

valt ook op dat 31,5% van de gemeentelijke genodigden in het kader van dit rekenkameronderzoek de enquête invulde, tegenover 62,5% van de externe partners. Privacy en informatieveiligheid heeft een logische plek in de dagelijkse praktijk, maar voor het thema an sich is er weinig belangstelling.

3.Verantwoordelijkheid en eigenaarschap ontbreekt soms

De gemeenteraad stelt geen kaders vast ten aanzien van privacy en informatieveiligheid: in die zin ligt de verantwoordelijkheid voor dit thema voornamelijk bij het college en de ambtelijke organisatie. Tegelijkertijd geven betrokkenen aan dat in de organisatie het gevoel van eigenaarschap voor bepaalde processen of handelingswijzen (zoals het opstellen van een verwerkersovereenkomst bij een nieuwe contractant) soms mist. Op uitvoeringsniveau voelen de medewerkers zich verantwoordelijk voor hun dossiers, en voor het bieden van goede ondersteuning. Medewerkers hebben onderling regelmatig contact over het al dan niet delen van gegevens.

Op het gebied van informatieveiligheid kunnen een aantal faciliteiten nog beter benut worden. In het kader van dit onderzoek hebben de onderzoekers een dagdeel op de afdeling van het sociaal domein gewerkt. Hier werd duidelijk dat men bewust omgaat met informatiebeveiliging, maar dat er ook enkele verbeterpunten zijn. Zo waren er met sleutels afsluitbare kasten beschikbaar op de afdeling, die niet allemaal op slot zaten of waar de sleutel zelfs in zat, terwijl de desbetreffende kamer niet werd gebruikt. Het betreft hier een afdeling waar niet iedereen zomaar binnen kan lopen, maar het toont wel aan dat optimaal gebruik maken van de faciliteiten een aandachtspunt is. In het nieuwe/verbouwde gemeentehuis gaat de gemeente over op digitaal werken en komen er lockers voor de medewerkers. Hiermee wordt naar verwachting ook een verbeterslag gemaakt.

4. Impact van de implementatie van de AVG niet eenduidig in beeld

Op uitvoeringsniveau zijn de AVG en de gevolgen van deze wetgeving voor de werkwijzen bekend. Op sturingsniveau kan dit echter nog beter verankerd worden, bijvoorbeeld door het opstellen van beleid. Hoewel het nu goed gaat, zijn dergelijke kaders nodig voor het geval er toch een incident plaatsvindt of aanpassingen nodig zijn.

In dit onderzoek is gekeken naar de mogelijkheid om objectief vast te stellen of de kosten en doorlooptijden in het sociaal domein (onnodig) oplopen ten gevolge van de AVG of andere regelgeving. De wijze waarop het administratief systeem is ingericht, maakte dit niet mogelijk en dus kunnen hierover geen uitspraken gedaan worden. Wel geven medewerkers aan dat hun werkzaamheden meer tijd vragen dan vóór de implementatie van de AVG. Bovendien is landelijk de verwachting dat de kosten zullen oplopen, waarbij de wijze waarop de AVG geïmplementeerd is, bepalend is.

Uit de ervaringen van ambtenaren en externe partners blijkt niet dat de wijze waarop de AVG is geïmplementeerd een voor de inwoners merkbare invloed op de kwaliteit van dienstverlening heeft. Zowel positieve als negatieve effecten worden benoemd. Een aandachtspunt hierbij is de samenwerking tussen verschillende afdelingen: vanuit privacy-oogpunt is dit niet altijd mogelijk, maar gewaakt moet worden voor tegenstrijdige adviezen van de verschillende bij een inwoner betrokken afdelingen.

Aanbevelingen

Raad

1. Geef actief uitvoering aan de controlerende taak op het gebied van privacy en informatieveiligheid

De gemeenteraad van Dronten stelt geen kaders vast ten aanzien van privacy en informatieveiligheid. Dat neemt niet weg dat de raad ook op dit terrein een controlerende rol te vervullen heeft, waarmee urgentie en eigenaarschap meegegeven kan worden aan de organisatie. Neem de kosten voor het waarborgen van privacy én informatieveiligheid mee in de P&C-cyclus, zodat een eventuele toename in kosten inzichtelijk wordt. Laat privacy en informatieveiligheid ook een onderwerp van evaluatie/monitoring zijn en zorg dat het met enige regelmaat een discussiepunt op de agenda is. Evalueer over enige tijd (2-3 jaar) opnieuw de stand van zaken rondom privacy en informatieveiligheid en de ontwikkeling in de gemaakte kosten.

College

1. Werk aan het eigenaarschap en de gevoelde urgentie voor het thema op verschillende niveaus.

Het borgen van privacy en informatieveiligheid is afhankelijk van de aandacht voor het thema in de dagelijkse praktijk én van de aandacht die hier vanuit de gebruikelijke sturingsstructuren voor is. Geef privacy en informatieveiligheid tijdelijk prioriteit, zodat iedereen zich verantwoordelijk gaat voelen voor de thema's. Concreet kan daarbij aan het volgende worden gedacht:

- Medewerkers: Betrek medewerkers bij het opstellen van bijvoorbeeld werkafspraken rondom privacy en zorg dat voor iedereen duidelijk is waar zij met hun vragen over privacy en informatieveiligheid terecht kunnen, zodat signalen uit de praktijk niet verloren gaan. Hetzelfde geldt voor externe partners: ook zij hebben relevante informatie over privacy in de praktijk.
- MT: inventariseer per afdeling of team welke knelpunten er worden ervaren ten aanzien van privacy en informatieveiligheid, en vergelijk dit met elkaar. Mogelijk zijn er aandachtspunten die in gezamenlijkheid opgepakt kunnen worden. Beoordeel tevens of de organisatie van personen met een verantwoordelijkheid op het gebied van privacy naar tevredenheid is. Er is voor 0,2 fte een FG aangesteld, maar de taken van de FG vragen om meer tijd. Breng deze twee aspecten met elkaar in lijn.
- College: geef prioriteit aan het afronden van het privacybeleid. Vanuit deze kaders kan de organisatie vervolgens aan het werk.

2. Zorg voor periodieke aandacht voor privacy en informatieveiligheid

Door privacy en informatieveiligheid regelmatig te behandelen ontstaat grip op deze thema's. Vanuit deze positie kan een leercyclus ingericht worden. Informatie over bijvoorbeeld deelnemersaantallen en slagingspercentages van e-learning modules kunnen gebruikt worden om aandachtspunten te inventariseren, en om een keuze te maken over de benodigde acties. De deelnemersaantallen van dergelijke e-learning modules zijn nu (te) laag: maak deze modules verplicht, zodat medewerkers zich ontwikkelen op dit thema en signalen van alle afdelingen gehoord worden. Vanuit deze positie kunt u keuzes maken over de inrichting van een privacybewuste gemeente Dronten.

Nota van bevindingen

1 (Beleids)kaders en organisatie

In dit hoofdstuk komen de kaders ten aanzien van privacy en informatieveiligheid aan bod. Het betreft zowel de kaders die gelden op beleidsniveau als kaders voor de uitvoeringspraktijk. Wat zijn bijvoorbeeld de visie en uitgangspunten van de gemeente, welke rol heeft de raad daarin en wat is de organisatiestructuur? De volgende deelvragen worden behandeld:

1. Hoe heeft de gemeenteraad kaders gesteld ten aanzien van informatiebeveiliging en privacybeleid in het sociaal domein; en welke rol neemt hij ten aanzien van dit onderwerp in?
2. Hoe is de organisatie van privacy en informatieveiligheid vormgegeven?

1.1 / Kaderstelling privacy en informatieveiligheid

Gemeenteraad stelt geen kaders vast voor privacy en informatieveiligheid

De gemeente Dronten kent verschillende beleidsstukken en handelingskaders ten aanzien van privacy en informatieveiligheid, maar de raad vervult op dit gebied geen kaderstellende rol. Het college stelt het informatieveiligheidsbeleid vast, en afdelingen kunnen zelf aanvullende werkafspraken maken. In de paragrafen 1.2 en 1.3 worden de bestaande kaders op het gebied van privacy en informatieveiligheid toegelicht.

Hoewel de raad volgens geïnterviewden betrokken en actief is ten aanzien van het sociaal domein, is deze betrokkenheid niet zichtbaar waar het privacy en informatieveiligheid betreft. Deze technische aspecten van het sociaal domein worden door de raad gezien als een aspect van de bedrijfsvoering waar vooral het college toezicht op dient te houden.

Visie ambtelijke organisatie: “werkbaarheid als uitgangspunt, beleid is functioneel”

De gemeente Dronten heeft een praktische instelling met betrekking tot privacyregelgeving en werkbaarheid. De gemeente heeft als taak om inwoners te ondersteunen en de kaders waarbinnen dat gebeurt moeten werkbaar blijven voor medewerkers. In de interviews bleek dat de gemeente dan ook niet nastreeft om een ‘koploper’ te zijn op het gebied van privacy; met de inwoner en de medewerker centraal, kiest de gemeente binnen de kaders van de wetgeving een eigen pad. Voorkomen moet worden, dat wetgeving het ondersteunen van inwoners bemoeilijkt. Medewerkers geven aan dat hier twee kanten aan zitten: enerzijds delen zij informatie als dat in het belang van bijvoorbeeld de inwoner is, anderzijds is dat – juist door te volgen procedures – niet altijd mogelijk.

De respondenten van de enquête hechten ongeveer evenveel waarde aan het pragmatisme als aan de procedures en regels. Op de stelling dat medewerkers cliëntgegevens eerder pragmatisch dan gebaseerd op procedures en regels behandelen, reageerde 31% dat zij het hier mee oneens was. 27% gaf aan het wel eens te zijn met de stelling. De meeste personen, 42%, reageerden neutraal op deze stelling.

1.2 / Privacybeleid

Beleidsstukken privacy niet aanwezig of ontwikkeling verloopt moeizaam

De Functionaris voor de Gegevensbescherming (FG) en een medewerker van Juridische zaken werken momenteel aan een organisatiebreed privacybeleid. Dit beleid zou in het eerste kwartaal van 2019 worden vastgesteld, maar is op het moment van schrijven (mei 2019) nog niet gereed voor besluitvorming. Dit beleid sluit aan bij de uitgangspunten uit het informatieveiligheidsbeleid en wordt volgens geïnterviewden ingericht naar de basisnormen van de AVG. Op dit moment is er geen organisatiebreed privacybeleid. Medewerkers geven aan dat er desondanks volgens de AVG wordt gewerkt.

Ook voor het sociaal domein heeft de gemeente geen privacybeleid. In 2015 is door medewerkers van de gemeente Dronten een eerste poging gedaan om een privacyconvenant voor het sociaal domein op te stellen. De doorontwikkeling van dit convenant is toen op de achtergrond geraakt door capaciteitstekort en ingewikkeldheid van het vraagstuk.[1] De gemeenteraad heeft dit thema in 2016 opnieuw onder de aandacht gebracht. Op 23 juni 2016 heeft de raad een motie aangenomen over een privacyconvenant voor het sociaal domein. In deze motie wordt de AVG niet benoemd. In de motie wordt het college verzocht:[2]

/ een privacyconvenant op te stellen conform de aanbeveling van de Vereniging van Nederlandse Gemeenten (VNG) en deze als beslisnota voor te leggen aan de raad;
/ te zorgen dat medewerkers van de gemeente en hulpverleners training krijgen in het gebruik van het privacyconvenant;
/ regelmatig te evalueren of het convenant nog aansluit bij de praktijk.

Protocollen en handvatten beschikbaar

Op basis van de eerste ervaring met het opstellen van een privacyconvenant trokken de betrokken medewerkers de conclusie dat één privacyconvenant niet werkbaar is binnen het sociaal domein.[3] De verschillende partijen hanteren (te) verschillende werkwijzen. Afspraken in één convenant kunnen voor de ene partij te streng zijn, terwijl deze voor de andere partij niet (volledig) voldoen aan de voor hem geldende eisen.[4] Als oplossing is besloten om ten eerste als gemeente zelf een privacyprotocol op te stellen. Van externe partijen vraagt/eist de gemeente Dronten, dat zij een privacyprotocol kunnen overhandigen dat goedgekeurd is door de Autoriteit Persoonsgegevens (AP).[5] Hiermee legt de gemeente de verantwoordelijkheid om de kaders voor gegevensuitwisseling te organiseren grotendeels bij externe partijen, om toch tot een werkbare oplossing te komen.

In de praktijk ontstaan toch afspraken tussen gemeente en externe partijen voor het delen van gegevens, op basis van contracten of in de dagelijkse werkzaamheden. De gemeente Dronten heeft bijvoorbeeld een standaard overeenkomst ontwikkeld ten aanzien van het uitwisselen van persoonsgegevens in samenwerkingsrelaties.[6] 63% van de medewerkers uit het sociaal domein geeft aan dat er afspraken zijn met externe partners over de manier waarop gegevens gedeeld mogen worden. 28% weet niet of er afspraken zijn gemaakt, 9% zegt dat er geen afspraken zijn. Niet iedereen vindt het wenselijk om afspraken te maken: 15% geeft aan het niet wenselijk te vinden, tegenover 85% die dat wel vindt. De antwoorden op deze verschillende vragen geven enerzijds aan dat er behoefte is aan afspraken, maar ook dat die op andere wijzen dan in een convenant al tot stand komen.

Privacyprotocol van de gemeente Dronten aan de hand van tien gouden regels

Het privacyprotocol van de gemeente Dronten is gebaseerd op de “Handreiking voor de professional: het verwerken van persoonsgegevens in het sociaal domein” van de VNG.[7] Het privacyprotocol van de gemeente

[1] Bijlage 1. Uitvoeringsplan implementatie privacyprotocol

[2] Motie “privacyconvenant” voor het sociaal domein (23 juni 2016)

[3] Bijlage 1. Uitvoeringsplan implementatie privacyprotocol, p. 9

[4] Bijlage 1. Uitvoeringsplan implementatie privacyprotocol, p. 9

[5] Bijlage 1. Uitvoeringsplan implementatie privacyprotocol, p. 10

[6] Overeenkomst omtrent persoonsgegevens Gemeente Dronten

[7] Bijlage 2. Handreiking privacy in Dronten, p. 2 (15 november 2016)

Dronten is specifiek gericht op de uitvoeringspraktijk van het sociaal domein en geldt als aanvulling op het wettelijke kader en het informatieveiligheidsbeleid.[8]
Het privacyprotocol benoemt tien gouden regels voor het verwerken van persoonsgegevens:[9]

Tabel 1 De 10 gouden privacyregels van de gemeente Dronten

De 10 gouden privacyregels[10]
1. *Minder is meer*
2. *Scheid feiten en meningen*
3. *Wees transparant*
4. *Motiveer en leg vast*
5. *Deel persoonsgegevens niet zomaar met anderen*
6. *Ga zorgvuldig om met persoonsgegevens (beveiliging)*
7. *Voldoe aan de rechten van de cliënt*
8. *Stel vragen als je niet zeker weet hoe en of je persoonsgegevens mag verwerken*
9. *Bespreek het onderwerp privacy regelmatig met andere professionals*
10. *Heb respect voor juridische kaders van andere beroepsgroepen*

Daarnaast beschrijft het protocol enkele aandachtspunten en basisprincipes, zoals transparantie naar de inwoner, toestemming voor gegevensverwerking, geheimhoudingsplicht, en persoonsgegevens delen met en opvragen bij externe partijen.

Op basis van het privacyprotocol is in een handreiking een praktische vertaalslag gemaakt naar de werkvloer, zodat medewerkers van de gemeente Dronten het verwerken van persoonsgegevens in de dagelijkse praktijk correct toe kunnen passen.[11] In deze handreiking worden specifieke werkprocessen toegelicht.[12] De visie uit de handreiking komt overeen met de uitgangspunten van de Leertuinmethode. De Leertuinmethode is de methode waarmee medewerkers van de gemeente Dronten werken ten aanzien van het verwerken en uitwisselen van persoonsgegevens in het sociaal domein. In *paragraaf 3.1: werkwijze* lichten wij deze methode verder toe.

1.3 / Informatieveiligheidsbeleid

Algemeen geldend informatieveiligheidsbeleid vastgesteld in 2019

Het huidige informatieveiligheidsbeleid van de gemeente Dronten is bij collegebesluit vastgesteld op 26 maart 2019. Dit beleid is bedoeld voor alle in- en externe medewerkers van de gemeente en omvat alle gemeentelijke processen, onderliggende informatiesystemen, informatie en gegevens van de gemeente en externe partijen. In het beleid worden op hoofdlijnen de organisatorische en technische kaders voor informatiebeveiliging uitgelegd.

Ten aanzien van het informatieveiligheidsbeleid zijn een aantal specifieke uitgangspunten van belang:

/ Het informatieveiligheidsbeleid van Dronten is in lijn met het algemeen beleid van de gemeente en de relevante wet- en regelgeving. Het beleid is gebaseerd op de Code voor Informatiebeveiliging (NEN/ISO 27002) en de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).[13] Ook de bepalingen uit de AVG zijn er in opgenomen.
/ De directie herijkt periodiek het informatieveiligheidsbeleid en stelt zo nodig aanpassingen voor.[14]
/ Dronten hanteert een risk-based informatiebeveiligingsbeleid. Beveiligingsmaatregelen worden getroffen op basis van een toets tegen de BIG. Indien een systeem meer maatregelen nodig heeft, wordt een

[8] Bijlage 2. Handreiking privacy in Dronten, p. 2 (15 november 2016)

[9] Bijlage 2. Handreiking privacy in Dronten, p. 13 (15 november 2016)

[10] Voor het volledige overzicht van deze gouden regels en toelichtingen verwijzen wij u naar het brondocument van de VNG: "Handreiking voor de professional: het verwerken van persoonsgegevens in het sociaal domein (2015)"

[11] Bijlage 2. Handreiking privacy in Dronten, p. 2 (15 november 2016)

[12] Handreiking privacy sociaal domein

[13] Informatieveiligheidsbeleid gemeente Dronten, p.9

[14] Informatieveiligheidsbeleid gemeente Dronten, p.9

risicoanalyse uitgevoerd. Daartoe inventariseert de proceseigenaar de kwetsbaarheid van zijn werkproces en mogelijke dreigingen.[15]

/ Het gehele gemeentelijk management geeft een duidelijk(e) commitment en richting aan informatieveiligheid en demonstreert dat zij informatieveiligheid ondersteunt en zich hierbij betrokken voelt. Door het uitbrengen en handhaven van een informatieveiligheidsbeleid van en voor de hele gemeente.[16]

Het relatief nieuwe beleid is nog niet toegeschreven naar de Baseline Informatiebeveiliging Overheid (BIO) die op 1 januari 2020 van kracht wordt. Op het moment dat de BIO van kracht wordt, zal het informatieveiligheidsbeleid van de gemeente geactualiseerd worden.[17] De gemeente Dronten verwacht dat de BIO uiteindelijk later van kracht zal gaan en dat er dus meer tijd is om het beleid aan te passen.

1.4 / Organisatie van de informatiebeveiligingsfunctie

Centrale rol CISO en FG; juridisch kwaliteitsmedewerker van belang voor het sociaal domein

De CISO en FG zijn de belangrijkste functionarissen op het gebied van privacy en informatieveiligheid in de gemeente Dronten. Zij werken regelmatig samen in projecten, bijvoorbeeld bij het opstellen van verwerkersovereenkomsten en beleidsstukken. De CISO en FG vallen onder de verantwoordelijkheid van het team Informatiemanagement en Facilitaire zaken.

Binnen het sociaal domein richt een juridisch kwaliteitsmedewerker zich ook op privacy en informatieveiligheid. Deze medewerker is zowel voor collega's binnen het sociaal domein als voor de CISO en FG een aanspreekpunt en vervult de rollen van security officer SUWInet en privacy coördinator van het sociaal domein.

Medewerkers uit het sociaal domein zijn goed bekend met bovenstaande functionarissen. Geïnterviewden gaven aan dat hierover voldoende is gecommuniceerd via de mail, in afdelingsoverleggen en via Intranet. Medewerkers stellen daarom hun vragen over informatieveiligheid en privacy meestal direct aan de juiste persoon.

FG-capaciteit in opstartfase onvoldoende

De CISO is 28 uur per week aanwezig. De medewerker die de functie van FG vervult is in april 2018 voor 0,2 fte aangesteld als FG. Daarnaast vervult deze medewerker voor 0,8 fte de functie van specialist data- en privacybescherming, gericht op dataclassificatie. De werkzaamheden die voortvloeien uit de implementatie van de AVG, vragen uit de organisatie en klachten van inwoners, maken dat deze medewerker op dit moment meer dan 0,2 fte besteedt aan FG-werkzaamheden. Hoewel er thans nog geen benchmark FG-fte beschikbaar is, is in ieder geval algemeen bekend dat deze 'opstartfase' veel vraagt van FG's. Hoe dit zich de komende periode ontwikkelt, is niet duidelijk.

Reorganisatie heeft invloed gehad op de privacy- en informatieveiligheidsfunctie; nog niet alle functies ingevuld

Binnen de gemeente Dronten is in de afgelopen jaren sprake geweest van meerdere personele wisselingen in het management, de bestuurlijke- en politieke toplaag. Bovendien is de gemeente Dronten gaan werken in teams in plaats van afdelingen. Dit werkt op verschillende punten door in de informatie- en veiligheidsorganisatie:

/ Hoewel de CISO al vier jaar de CISO-taken uitvoert, is het functieprofiel voor de CISO nog niet formeel vastgesteld. Op dit moment ligt een voorstel met formele vaststelling voor de functie voor ter audit.

/ Momenteel is de functie Chief Information Officer (CIO) niet ingevuld. Geïnterviewden schrijven dit toe aan een aantal personele wisselingen ten tijde van de reorganisatie. Zo zijn achtereenvolgens de gemeentesecretaris en een directeur die de functie van CIO vervulden, vertrokken. Recent is een nieuwe directeur bedrijfsvoering aangesteld die mogelijk de functie van CIO gaat vervullen. Een aantal CIO-taken worden nu door de CISO opgepakt.

/ De gemeente heeft geen privacyofficer in dienst. Deze functie is voorzien binnen het team Juridische zaken. De medewerker die deze taken zou oppakken, werkt niet meer bij de gemeente. De FG heeft hierdoor geen

[15] Informatieveiligheidsbeleid gemeente Dronten, p.9

[16] Informatieveiligheidsbeleid gemeente Dronten, p. 3

[17] Informatieveiligheidsbeleid gemeente Dronten, p.14

duidelijk aanspreekpunt voor privacy binnen het team Juridische zaken op het gebied van zaken rondom privacy en neemt zelf een aantal uitvoerende taken op zich. Dat heeft impact op de beschikbare tijd van de FG en strookt niet met het toezichthoudende en adviserende karakter van de functie.

"Gebrek aan verantwoordelijkheidsgevoel voor processen"

Tijdens de interviews werd benadrukt dat er binnen de gemeente Dronten weinig verantwoordelijkheidsgevoel is voor proceseigenaarschap. Dit speelt door de gehele gemeente, maar als gevolg van de AVG is het proceseigenaarschap op scherp komen te staan ten aanzien van informatieveiligheid en privacyvraagstukken. Dit geldt ook voor de daarop te nemen maatregelen. De FG merkt dit bijvoorbeeld in het beheer van de verwerkersovereenkomst. Momenteel wordt van de FG verwacht dat zij dit proces doorloopt, terwijl het eigenaarschap daarvan per team bij de teammanager ligt. Gezien de beperkte capaciteit die beschikbaar is gesteld voor FG-taken (0,2 fte), vraagt dit meer inzet dan voor FG-taken is voorzien.

1.5 / Informatievoorziening aan de raad

Raad stelt weinig vragen over privacy en informatieveiligheid

De gemeenteraad wordt op meerdere momenten geïnformeerd over privacy en informatieveiligheid. Zo wordt in de jaarstukken aandacht besteed aan de stand van informatiebeveiliging middels de ENSIA-systematiek, is in 2017 een informatiebeleidsplan voorgelegd aan de raad en heeft de verantwoordelijk wethouder de raad meermaals geïnformeerd over hack-pogingen en datalekken. In 2018 werd de gemeenteraad na het tweede en het derde kwartaal geïnformeerd over de ontwikkelingen in voorbereiding op de AVG.

Geïnterviewden geven aan dat de raad in deze gevallen weinig vragen stelt of concrete acties onderneemt. Als verklaring hiervoor wordt gegeven dat het technische onderwerp lastig te doorgronden is voor de gemeenteraad.

2 Implementatie van de AVG

Om in kaart te brengen wat de effecten van de AVG zijn geweest, is het van belang om te beoordelen welke voorbereidende stappen de gemeente nodig achtte. Dit hoofdstuk behandelt daarom de volgende deelvragen:

3. Hoe is wet- en regelgeving ten aanzien van informatieveiligheid en privacy geïmplementeerd en hoe functioneert deze opzet in de praktijk?
4. Hoe wordt de werkbaarheid ervaren bij medewerkers van de gemeente Dronten en ketenpartners?
6. Heeft de aangescherpte wet- en regelgeving op het gebied van informatiebeveiliging en privacy binnen het sociaal domein geleid tot langere doorlooptijden/afhandeltermijnen?
7. Wat is het effect van de AVG geweest op uitvoeringskosten en hoe verhoudt dit zich tot andere gemeenten?

2.1 / Voorbereiding en uitvoering AVG

Extern adviseur laat ingehuurd in voorbereiding op AVG

In de periode 5 maart 2018 tot 1 juli 2018 heeft de gemeente Dronten een externe adviseur ingehuurd om te ondersteunen in de voorbereiding op en implementatie van de AVG, die op 25 mei 2018 van kracht werd. De FG werd aangesteld in april 2018, te laat om alle werkzaamheden vóór de inwerkingtreding van de AVG af te ronden. De externe adviseur kreeg daarom de concrete opdracht om de verwerkersovereenkomsten vorm te geven en het register van verwerking op te stellen. Eén van de werkzaamheden van de adviseur was het opstellen van een stappenplan om als gemeente te voldoen aan de AVG.[18]

Plan van aanpak opgesteld nadat de AVG van kracht werd

Na de inwerkingtreding van de AVG, te weten in juni 2018, hebben de FG en de externe adviseur een plan van aanpak voor de AVG opgesteld.[19] Het moment waarop dit gebeurde is opvallend: er moesten na de inwerkingtreding van de AVG nog stappen worden gezet op het gebied van privacy binnen de gemeente Dronten.[20] Het plan van aanpak is een zeer beknopt document waarin op zes onderdelen de stand van zaken wordt gegeven:

/ **Bewustwording**: in 2017 is in presentaties aandacht geschonken aan de AVG, en het was een onderwerp in het E-learning programma van 2018. Er komt een organisatiebreed privacybeleid/privacyreglement.

[18] Zo bleek uit interviews en het Plan van aanpak AVG gemeente Dronten, p.1

[19] Plan van aanpak AVG gemeente Dronten, p.1

[20] Plan van aanpak AVG gemeente Dronten, p.1

- **Rechten van betrokkenen:** gaat om rechten als inzage, correctie, dataportabiliteit en dergelijke in kaart te brengen. Voor geregistreerde verwerkingen is dit makkelijk te achterhalen, in ongestructureerde data is het lastiger. In juni 2018 is met de applicatie Varonis daarom een assessment hiervan uitgevoerd. Er wordt een online aanvraagformulier voor rechten van betrokkenen ontwikkeld, maar dat is nog niet beschikbaar.[21]
- **Overzicht verwerkingen**: er is een register van gegevensverwerkingen opgesteld. Dit is een dynamisch document.
- **Gegevensbeschermingseffect beoordelingen (GEB):** de planning was om dit vanaf september 2018 op te pakken. Op basis van het verwerkingenregister zouden verwerkingen gekozen worden met een hoog privacyrisico. Er hebben nog geen GEB's plaatsgevonden.
- **Aanstellen Functionaris voor de Gegevensbescherming (FG)**: de FG werd in april 2018 aangenomen, dus dit actiepunt was al direct voldaan.
- **Verwerkersovereenkomsten:** in juni 2018 heeft de externe consultant dit opgepakt; ook ten tijde van het onderzoek vraagt dit nog steeds aandacht van de FG.

Overkoepelend wordt in het plan van aanpak opgemerkt dat de gemeente op hoofdlijnen klaar is voor de invoering van de AVG, maar dat er nog werk te verzetten is op het gebied van gegevensbeschermingseffect beoordelingen, persoonsgegevens in ongestructureerde data, opstellen verwerkersovereenkomsten en het blijvende aandachtspunt bewustwording van medewerkers.

Stand van zaken AVG gerapporteerd na het derde kwartaal van 2018

Op 2 oktober 2018 rapporteerde de FG aan het college en directieteam over het derde kwartaal van 2018. Deze rapportage is ook gedeeld met de gemeenteraad.[22] Ondanks het verstrijken van een aantal maanden, is er veel overlap tussen het plan van aanpak en de rapportage. De FG rapporteert in dit memo in negen thema's, die deels overeenkomen met de thema's uit het plan van aanpak:[23]

- **Bewustwording:** Volgens de FG zijn er op het gebied van bewustwording nog stappen te zetten. Er komt een tweede ronde voor de E-learning, ditmaal met een onderdeel privacy. Daarnaast is medewerking van de medewerkers nodig. Hierin ziet de FG een taak voor managers weggelegd.
- **Rechten van betrokkenen:** Tussen 25 mei en 2 oktober 2018 zijn drie verzoeken ingediend omtrent de rechten van betrokkenen. Bij één verzoek is overgegaan tot het verwijderen van persoonsgegevens, de andere twee verzoeken zijn ingetrokken door de betreffende burger na uitleg van de gemeente.
- **Register van verwerkingen:** Het register helpt om gestructureerde data inzichtelijk te maken, de ongestructureerde data is echter problematischer. In juni is er een test uitgevoerd door Varonis. De resultaten hiervan worden naar verwachting in het vierde kwartaal van 2018 bekend.[24]
- **DPIA (Data Protection Impact Assessments):**[25] Een DPIA moet uitgevoerd worden indien een gegevensverwerking een hoog risico voor de rechten en vrijheden van een natuurlijke persoon bevat. De verwachting was dat de eerste DPIA in het eerste kwartaal van 2019 zou worden uitgevoerd.
- **Functionaris voor de Gegevensbescherming:** De benoeming heeft voor 25 mei 2018 al plaatsgevonden.
- **Meldplicht datalekken:** Tussen 25 mei en 2 oktober 2018 zijn er vier datalekken gemeld bij de FG, daarvan is er één gemeld bij de Autoriteit Persoonsgegevens (AP). De overige drie zijn intern als datalek genoteerd.
- **Verwerkersovereenkomsten:** Het sluiten van verwerkersovereenkomsten blijft een punt van aandacht volgens de FG. Het sluiten van deze overeenkomsten is uitgezet bij contractmanagers, de beoordeling ervan is de verantwoordelijkheid van de FG of Juridische zaken. Bij voorkeur gebruikt de gemeente Dronten het model dat zij heeft overgenomen van de Informatiebeveiligingsdienst (IBD) voor gemeenten.
- **Leidende toezichthouder:** Omdat de gemeente Dronten al haar gegevens binnen Nederland verwerkt en gevestigd is in Nederland, is en blijft de leidend toezichthouder voor de gemeente Dronten de AP.
- **Toestemming:** Bij elke gegevensverwerking waar eerder gebruik werd gemaakt van de rechtmatigheidsgrond toestemming, bekijkt de gemeente Dronten of dit de enige mogelijke grond voor het verwerken van gegevensverwerking is, of dat er andere gronden beschikbaar zijn.

---

[21] Op de datum van schrijven, 1 maart 2019, is een dergelijk aanvraagformulier niet beschikbaar via de website. Wel worden inwoners voor vragen over inzage doorverwezen naar de FG. Zie: https://www.dronten.nl/mozard/!suite86.scherm0325?mVrg=3288

[22] Rapportage Q2 en Q3 Memo (2 oktober 2018)

[23] Rapportage Q2 en Q3 Memo (2 oktober 2018)

[24] De uitkomsten hiervan zijn (nog) niet bekend bij de onderzoekers

[25] Ook wel genoemd: gegevensbeschermingseffect beoordeling (GEB)

Tijdens de interviews werd hierbij opgemerkt dat het proces ten aanzien van de implementatie van de AVG nog niet is geëvalueerd.

Externe samenwerkingspartners uit het sociaal domein betrokken bij voorbereiding AVG

De gemeente Dronten heeft samenwerkingspartners uit het sociaal domein betrokken bij de voorbereiding op de AVG. De samenwerkingspartners werden tijdens bijeenkomsten geïnformeerd over mogelijke wijzigingen in de samenwerking of de werkwijze van de gemeente in het algemeen.

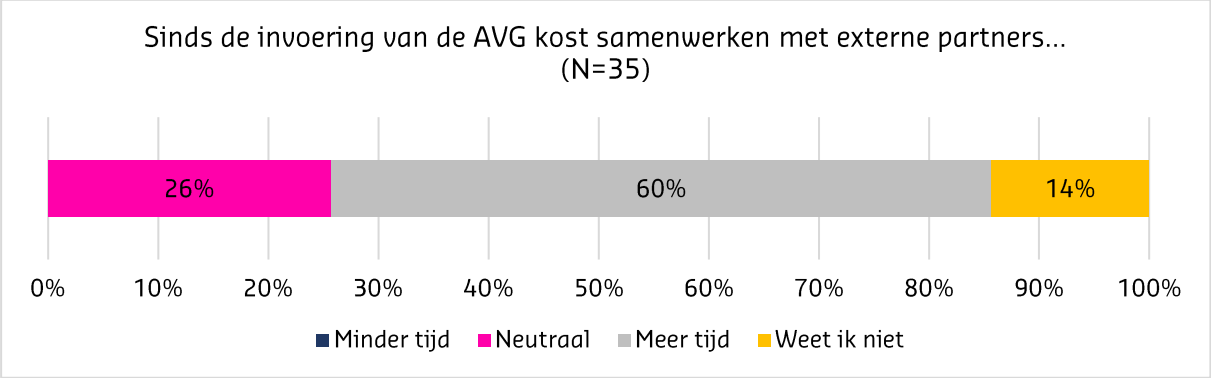
2.2 / Ervaren werkbaarheid AVG en effecten op doorlooptijden

Doorlooptijden zijn landelijk langer en taken worden omvangrijker door de AVG

In het algemeen wordt verwacht dat door de invoering van de AVG doorlooptijden langer en taken omvangrijker worden, zo blijkt onder meer uit de nationale privacy benchmark[26] en de ICT benchmark gemeenten.[27] De nationale privacy benchmark laat zien dat het afhandelen van rechten van betrokkenen (denk aan inzage/correctie/verwijdering) de nodige tijd gaat vragen van organisaties. Ook de ICT benchmark gemeenten komt tot de bevinding dat de AVG een toenemend beroep doet op de ICT-formatie.

Deze algemene trends worden gestaafd door de bevindingen uit de enquête: 38% van de medewerkers geeft aan dat afstemming met collega's meer tijd kost dan voor de invoering van de AVG en 52% geeft aan dat er meer handelingen moeten worden verricht om het takenpakket uit te voeren. Daarnaast kost samenwerking met externe partners volgens de respondenten meer tijd sinds de invoering van de AVG (60% van de ondervraagden geeft dit aan, figuur 2). In de gesprekken werd aangegeven dat met name de extra handelingen voor de eigen werkzaamheden weliswaar meer tijd kosten, maar dat het niet om veel tijd gaat. Slechts 8% van de mensen schat in dat er na invoering van de AVG meer medewerkers nodig zijn op de afdeling sociaal domein in Dronten.

Figuur 2 Doorlooptijd in samenwerking met externe partners



Geen negatieve signalen over werkbaarheid bij FG/CISO

De invoering van de AVG vroeg van de uitvoerend medewerkers in het sociaal domein niet al te veel aanpassingen: zij hadden altijd al te maken met privacywetgeving. Zo wordt bijvoorbeeld standaard in rapportages alleen de nodige informatie meegestuurd, en worden overbodige gegevens achterwege gelaten. Medewerkers die verantwoordelijk zijn voor privacy en informatieveiligheid horen dan ook weinig tot geen klachten van hun collega's uit het sociaal domein met betrekking tot de werkbaarheid van wet- en regelgeving sinds de invoering van de AVG. Medewerkers stellen bij onduidelijkheden vragen, bijvoorbeeld aan de privacycoördinator sociaal domein, de FG of de CISO, maar de algemene instelling lijkt te zijn dat 'het is zoals het is'.

[26] Rapport Nationale Privacy Benchmark, Verdonck, Klooster & Associates, 2017

[27] Conclusie ICT benchmark gemeenten 2018

Externe samenwerkingspartners uit het sociaal domein ervaren weinig verandering door de AVG

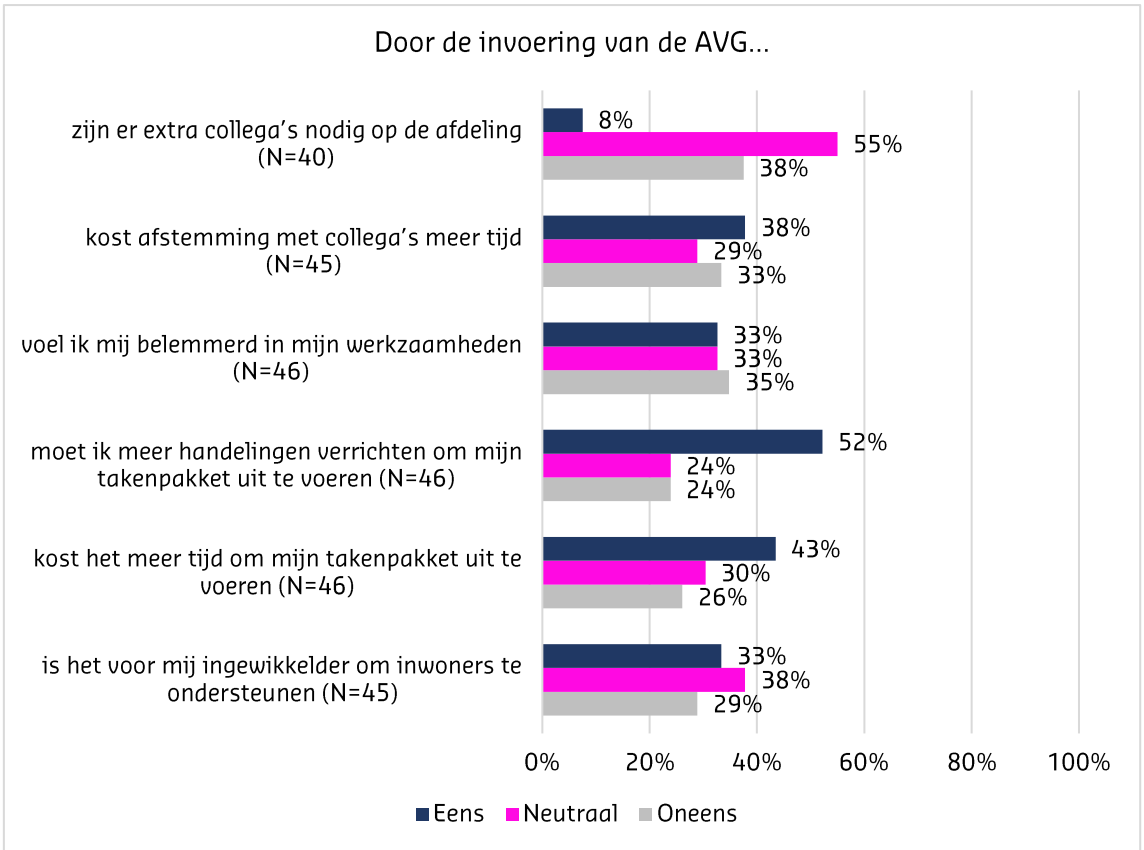
Externe partners uit het sociaal domein geven aan dat er weinig veranderd is in de samenwerking door de invoering van de AVG. Er was wel sprake van een aanpassingsperiode van ongeveer een half jaar. Hierin werden voornamelijk praktische en technische aanpassingen doorgevoerd door de samenwerkingspartners. Dit had geen grote of negatieve gevolgen voor de samenwerkingsrelatie. De afspraken tussen externe partners en de gemeente zijn wel veranderd. Hoewel er reeds voor de AVG afspraken over gegevensuitwisseling bestonden, zijn deze bij de invoering van de AVG aangescherpt. Ook zijn er meer afspraken gemaakt op bestuurlijk niveau, die gelden voor de hele organisatie. Dit beperkt de ruimte voor individuele medewerkers van zorgpartners of medewerkers uit het sociaal domein van de gemeente om onderling afspraken te maken en bevordert de eenduidigheid.

Medewerkers constateren knelpunten privacywetgeving en negatieve gevolgen voor inwoners in de dagelijkse praktijk

De enquête geeft een minder rooskleurig beeld over de gevolgen van de AVG. . Zo geven respondenten aan dat het werk meer tijd kost, dat mensen soms -onterecht- geen informatie meer durven delen (intern en extern), en dat processen soms stagneren. De werkzaamheden van bijvoorbeeld de 'Gidsen' in de gemeente zouden makkelijker uit te voeren zijn als zij direct volledige dossiers kunnen inzien van inwoners die ondersteuning ontvangen van de gemeente, vanuit alle disciplines. Nu kan het voorkomen dat bijvoorbeeld vanuit Jeugd een koers wordt ingezet met het gezin, die tegengesteld is aan het plan van de afdeling Participatie. Externe partners uit het sociaal domein herkennen zich ten dele in dit beeld. Het voornaamste voorbeeld van een maatregel waardoor extra stappen in het proces nodig zijn is beveiligd mailen, ten opzichte van gewoon mailen.

Ten aanzien van een deel van de stellingen (figuur 3) over de invoering van de AVG zijn de meningen gelijkmatig verdeeld. Het betreft hier de stellingen dat onderlinge afstemming meer tijd kost, dat medewerkers zich door de AVG belemmerd voelen in hun werkzaamheden en dat het ingewikkelder is geworden om inwoners te ondersteunen.

Figuur 3 Stellingen ten aanzien van werkbaarheid



Doorlooptijden uitvoeringspraktijk lijken in praktijk niet beïnvloed door de AVG

Naast het feit dat er geen signalen bekend zijn bij de gemeente ten aanzien van de doorlooptijden in het sociaal domein, zijn hiervoor ook op andere vlakken geen aanwijzingen aangetroffen in het onderzoek. De klachten over afhandelingsduur binnen het sociaal domein ontwikkelden zich in de jaren 2016-2019 als volgt[28]:

Tabel 2 Klachten afhandelingsduur 2016-2019 (tot en met februari)

Jaartal	Aantal klachten	Onderwerp
2016	3	Aanvraag bijzondere bijstand, Wmo-procedure (2x)
2017	1	Wmo-procedure
2018	2	Uitbetaling bijstandsuitkeringen, niet betaalde facturen
2019	1	Aanvraag pas regiotaxi en huishoudelijke hulp

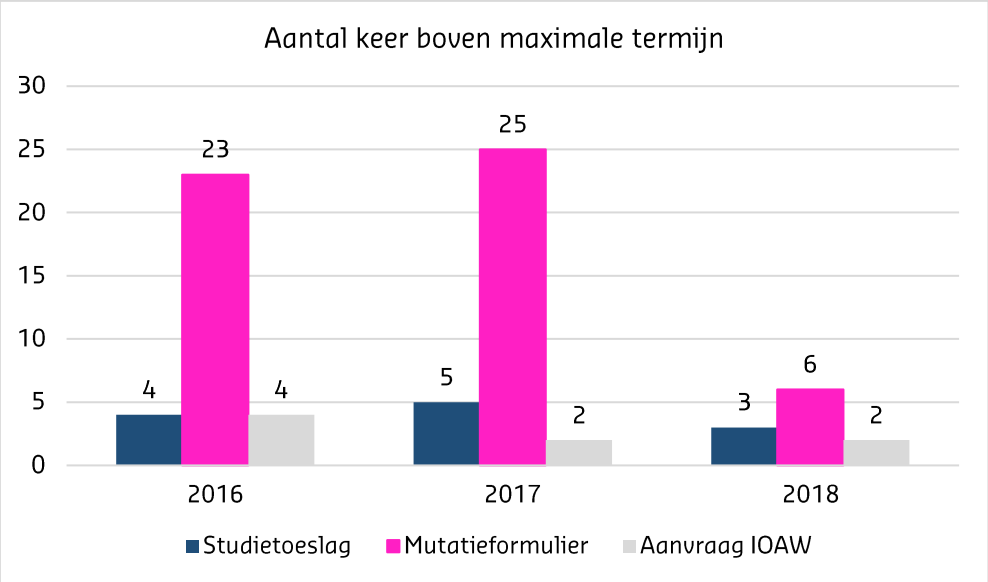
De gemeente Dronten registreert voor de procedures binnen de domeinen Jeugd en Wmo niet wat de doorlooptijden zijn. Voor een aantal procedures binnen de Participatiewet wordt dit wel geregistreerd. In dit onderzoek zijn de doorlooptijden van het aanvragen van studietoeslag, het indienen van een mutatieformulier en het aanvragen van IOAW beoordeeld. De frequenties waarin deze procedures worden doorlopen, lopen uiteen. Dit is van belang om in gedachten te houden bij het lezen van onderstaande grafiek: er zijn meer gevallen van overschrijding bij het mutatieformulier, maar deze procedure wordt ook veel vaker doorlopen.

Tabel 3 Aantal verschillende handelingen 2016-2019 (tot en met februari)

Jaar	Studietoeslag	Mutatieformulier	IOAW
2016	5	1939	19
2017	5	1895	13
2018	4	1731	20
2019	X	331	6

Op basis van deze gegevens kan (nog) geen trend geconstateerd worden ten aanzien van de doorlooptijden in relatie tot de inwerkingtreding van de AVG. Wel is het interessant dat de termijnen voor het aanvragen van studietoeslag en het mutatieformulier in 2018 minder vaak werden overschreden (figuur 4), omdat dit haaks staat op de verwachting dat de doorlooptijden zouden toenemen. Hierbij moet gezegd worden dat dit, ten aanzien van het grote aantal processen dat de gemeente binnen het sociaal domein kent, een zeer beperkte steekproef is.

Figuur 4 Aantal keer dat handelingen langer duren dan de maximale termijn 2016-2018



[28] Informatie is verstrekt door de klachtencoördinator

2.3 / Kosten

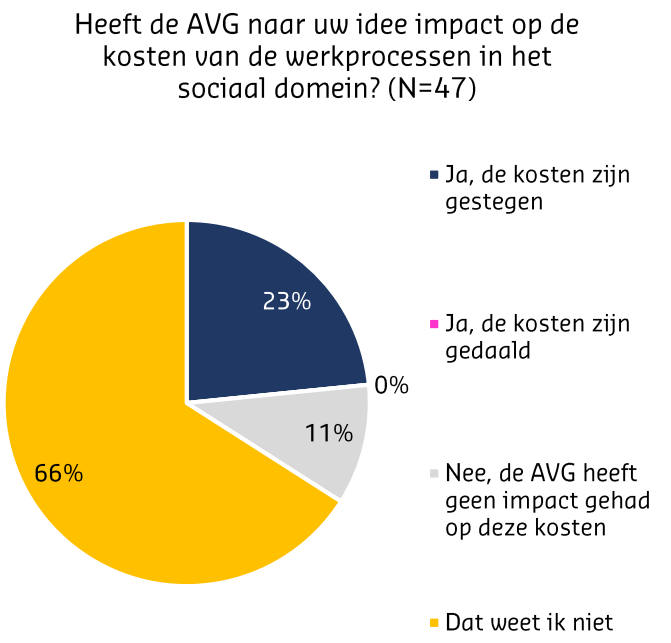
De invoering van de AVG heeft landelijk naar verwachting een kostenverhogend effect (ca. 1,1%)

Uit de nationale privacy benchmark[29] blijkt dat de respondenten verwachten dat met name de kosten die gemoeid zijn met technische beveiliging (75%) en de kosten (trainingen) voor medewerkers (70%) zullen toenemen. Een kleine minderheid van de respondenten verwacht dat de kosten voor de afhandeling van klantvragen zullen toenemen.

De ICT benchmark voor gemeenten concludeert dat de ICT-kosten van gemeenten inmiddels zijn gestegen van € 72,- per inwoner in 2015 naar € 82,- per inwoner over boekjaar 2017.[30] Deze kostenstijging wordt toegeschreven aan de trendmatig steeds verdergaande digitalisering en aan de invoering van de AVG. Het laatste jaar in de benchmark laat een kostenstijging van 3,8% zien. Deze kan worden onderverdeeld in een trendmatige stijging van 1,5% en een jaar-specifieke kostenstijging van 2,3%. De jaar-specifieke kostenstijging kan mede worden toegeschreven aan de invoering van de AVG. Ook blijkt in de benchmark dat deze kostenstijging voor gemeente voor 49% een kostenstijging voor personeelskosten betreft. Met andere woorden: van het kostenverhogend effect van 2,3% kan 1,1% worden toegeschreven aan extra kosten die voor personeel worden gemaakt.

Dit beeld is in lijn met wat naar voren komt in de gemeentebegrotingen van de gemeente Dronten voor 2018 en 2019.[31] Uit de gemeentebegrotingen voor 2018 en 2019 inzake het sociaal domein zijn geen kostenstijgingen als gevolg van de invoering van de AVG direct te herleiden. De programmabegroting voor het sociaal domein laat een lastenstijging in 2017 van 2,0% zien (rekening 2017/2016). In de begroting voor 2018 wordt een lastenstijging van 6,6% geraamd en voor de begroting 2019 wordt een bedrag aan lasten in het sociaal domein geraamd dat op hetzelfde niveau ligt als 2017. Er is dus sprake van een jaar-specifieke kostenstijging voor 2018 van ongeveer 4,6%. We vermoeden dat de geraamde lastenstijging voor het sociaal domein in 2018 mede wordt bepaald vanwege een (landelijk gemeten) kostenstijgend effect van 1,1% als gevolg van de invoering van de AVG. In de enquête bij de ambtelijke organisatie blijkt dat 23% van de respondenten denkt dat de kosten zijn gestegen sinds de invoering van de AVG (figuur 5). De verklaring 'het duurt langer, dus kost het meer' wordt hier het vaakst voor aangedragen, evenals de kosten voor de cursussen en trainingen.

Figuur 5 Kostenimpact volgens medewerkers gemeente Dronten



Onbekend of nieuwe privacyregelgeving de kosten beïnvloedt

Al met al is het onduidelijk of de nieuwe privacyregelgeving direct heeft geleid tot hogere kosten voor de gemeente Dronten. De gemeente Dronten heeft namelijk niet geanalyseerd of de uitvoeringskosten voor informatieveiligheid en privacy zijn toegenomen door nieuwe regelgeving zoals de AVG. Ten aanzien van de directe en indirecte kosten geldt het volgende:

- De *directe* kosten die bekend zijn, zijn de kosten voor het aannemen van de FG en het inhuren van een externe expert.

[29] Rapport Nationale Privacy Benchmark, pag. 24 e.v., Verdonck, Klooster & Associates, 2017

[30] Conclusie ICT benchmark gemeenten 2018 (over boekjaar 2017)

[31] Zie gemeentebegrotingen gemeente Dronten 2018 en 2019, onderdeel programmabegroting sociaal domein

- De gemeente schat in dat de *indirecte* kosten zullen stijgen, bijvoorbeeld omdat gemeenschappelijke regelingen zelf moeten investeren in het AVG-proof maken van de organisatie.
- *Overige* kosten zijn gemaakt voor een aantal veiligheidsmaatregelen die niet direct gekoppeld zijn aan de AVG. Zo is het programma Zorgmail twee jaar geleden aangeschaft in het kader van de BIG, om veilig te kunnen mailen en hebben medewerkers een trainingsprogramma doorlopen.
- *Mogelijke* toegenomen kosten ziet de gemeente in het werk van de medewerkers, omdat er meer handelingen nodig zijn (anonimiseren documenten en rapporten).

3 Uitvoeringspraktijk, bewustzijn medewerkers en samenwerking

De werkbaarheid in de praktijk van het sociaal domein wordt op verschillende vlakken bepaald: de gehanteerde werkwijze, de werkplek, de samenwerking met externen en het bewustzijn van medewerkers. Dit hoofdstuk beschrijft die praktijk, in aansluiting bij de hoofdvraag en bij de volgende deelvraag:

5. In hoeverre komt de werkwijze van medewerkers overeen met vastgestelde processen/werkwijzen rondom informatiebeveiliging en privacy (in het sociaal domein)?

3.1 / Werkwijze

De Leertuinmethode: werkbaarheid staat centraal

De gemeente Dronten heeft een specifieke methode gekozen voor het verwerken en uitwisselen van persoonsgegevens in het sociaal domein: de Leertuinmethode. De gemeente heeft ook haar samenwerkingspartners geïnformeerd over het werken volgens de Leertuin, middels een presentatiebijeenkomst. De Leertuinmethode is ontwikkeld door Jolanda van Boven en Peter Gunst.[32]

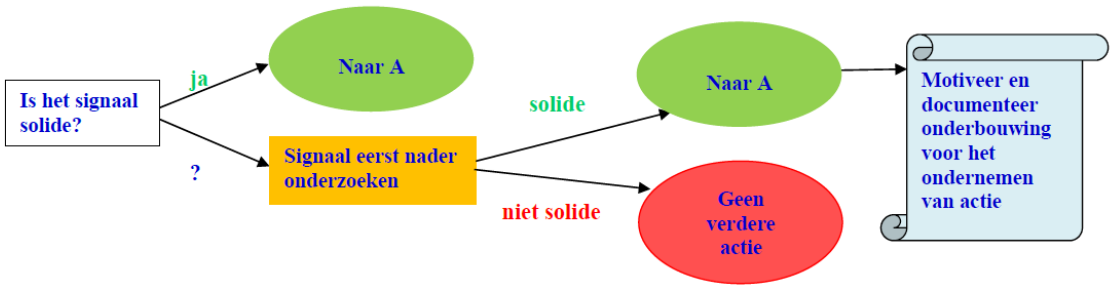
De werkwijze is sterk gebaseerd op de begrippen proportionaliteit (staat het middel in verhouding tot het doel?) en subsidiariteit (is er een mogelijk minder zwaar middel in te zetten?). Er wordt niet gewerkt met toestemmingsverklaringen, maar de medewerkers van de gemeente moete kunnen beargumenteren waarom zij gegevens willen delen. De Leertuinmethode wordt door de auteurs als volgt beschreven:

"De Leertuinmethode bevat drie stappen en drie 'zorgvuldigheidskleppen' en ziet er in de praktijk als volgt uit. De eerste stap is het bepalen van het doel en de daarbij behorende zorgvuldigheidsklep is het bepalen van de noodzaak om gegevens te delen. De tweede stap is overleg met de cliënt en - indien deze bezwaar heeft tegen informatiedeling - de daarbij behorende zorgvuldigheidsklep is het afwegen van de argumenten van de professional tegen de argumenten van de cliënt. De derde stap en de daarbij behorende zorgvuldigheidsklep is het toetsen van de argumentatie op basis van het 'juridisch Zwitsers zakmes'. Van groot belang is om de overwegingen goed in het dossier vast te leggen."[33]

[32] Uitwisselen van persoonsgegevens in een sociaal wijkteam – handboek 'Werken in de wijk', p. 165

[33] Handboek 'Werken in de wijk', p. 173

Figuur 6 Stroomschema Leertuinmethode



Medewerkers kunnen keuzes omtrent gegevensdeling (mede)bepalen op basis van aangeboden keuzeschema's zoals bijvoorbeeld het bovenstaande. Daarnaast zijn er ook stroomschema's geboden voor de beoordeling:[34]

- van het doel om informatie uit te wisselen met ketenpartners;
- van de weging om en welke informatie uit te wisselen;
- van de weging om betrokkenen te informeren over het delen van hun gegevens met ketenpartners.

Medewerkers geven aan dat zij met deze methode goed uit de voeten kunnen. De methode is praktisch en voorkomt veel administratieve handelingen. In Dronten zijn trainingen aangeboden voor de Leertuinmethode. Niet alle afdelingen van het sociaal domein waren hierbij vertegenwoordigd: zo waren er volgens betrokkenen relatief weinig aanwezigen van het team 'Jeugd'.

3.2 / Werkplekken

Schouw van de afdeling: niet zomaar naar binnen

In het kader van dit onderzoek voerden de onderzoekers een schouw van de afdeling uit (zie bijlage II voor de checklist). De onderzoekers waren op dinsdag 23 april een halve dag aanwezig bij de gemeente Dronten. De onderzoekers hebben ten eerste in de centrale ontvangstruimte van de gemeente gewerkt, naast de balies van het klantencontactcentrum (KCC). In deze ruimte werden door de medewerkers van het KCC geen, althans niet hoorbaar, persoonsgegevens besproken. De onderzoekers meldden zich vervolgens bij de welkomstbalie met de boodschap dat zij vandaag werken bij de afdeling sociaal domein. Het verzoek om zelf naar binnen te mogen werd afgewezen, hiervoor was een afspraak nodig. Een contactpersoon uit het sociaal domein heeft de onderzoekers binnengelaten. Zonder afspraak is het voor externen dus niet mogelijk om op deze manier op de werklocatie van de medewerkers uit het sociaal domein te komen.

Schouw van de afdeling: niet alle faciliteiten ten volle benut

Binnen de afdeling sociaal domein werkten de onderzoekers in een eigen ruimte. De telefoons en computers waren alleen toegankelijk met inlogcode van de gemeente. De onderzoekers constateerden bovendien dat de medewerkers uit het sociaal domein hun scherm meestal vergrendelen wanneer zij niet aanwezig zijn. De onderzoekers hebben niet gehoord dat medewerkers onderling of telefonisch persoonsgegevens bespraken. Verder werden er op de dag van het onderzoek geen achtergebleven documenten aangetroffen bij de printer. Direct naast de printer staat een papierversnipperaar. Onnodig uitgeprinte informatie kan daardoor snel worden vernietigd. Dat zijn positieve signalen. Bij een aantal zaken kunnen kanttekeningen geplaatst worden:

- Ten eerste was er op de kamer, en in meerdere andere ruimten, een archiefkast met slot aanwezig. Deze kasten bleken niet in alle ruimtes afgesloten, en in één archiefkast zat de sleutel nog in het slot.
- Daarnaast waren er niet afsluitbare kasten. Ook hierin worden mappen opgeslagen. In de kamer van de onderzoekers stonden mappen met gegevens over externe inhuur van een aantal jaren geleden.
- In de werkruimte van de onderzoekers bevond zich het centrale postverzamelpunt van de afdeling. Medewerkers leggen hier hun post met externe bestemming in een niet afgesloten verzamelbak. Deze post wordt dagelijks opgehaald om verstuurd te worden naar adressen buiten het gemeentehuis.

[34] Leertuin Stroomschema

/ Er zijn telefoons aanwezig op de werkplekken. Het betreft telefoons met draadverbinding, hierdoor is het niet mogelijk om de telefoon mee te nemen en te bellen in een afgesloten ruimte om mogelijk persoonsgegevens te bespreken. Wel zijn medewerkers uit het sociaal domein veelal ook mobiel bereikbaar, en zitten er maar weinig medewerkers in iedere ruimte.

Bij bovenstaande bevindingen is het belangrijk op te merken dat de betreffende informatie binnen de afdeling vrij toegankelijk is, maar dat deze ruimtes alleen bereikt kunnen worden met een toegangspas van de gemeente. Buitenstaanders, bijvoorbeeld inwoners van de gemeente, kunnen niet zomaar deze ruimten betreden.

3.3 / Beveiliging

Teammanager verantwoordelijk voor aanvragen autorisatie

Bij indiensttreding van nieuwe medewerkers moet de toegang tot systemen en applicaties veilig geregeld worden. De teammanager dient ten eerste een verzoek in bij Personeelszaken voor toegang tot het netwerk van de gemeente Dronten. Vervolgens stuurt de teammanager een verzoek naar de functioneel beheerders van de betreffende afdeling, zodat de nieuwe medewerkers geautoriseerd worden voor de benodigde applicaties. Dit proces is hetzelfde voor nieuwe medewerkers, extern ingehuurde capaciteit en stagiairs.

Als een medewerker uit dienst treedt, of langdurig geen gebruikmaakt van een applicatie, dan verloopt de toegang automatisch. Daarnaast blokkeren functioneel beheerders in het sociaal domein het account van de inactieve gebruiker wanneer zij de controle op autorisaties uitvoeren.

Autorisatie van medewerkers gebaseerd op rol en functie medewerker

De gemeente Dronten baseert de autorisaties van medewerkers in de verschillende systemen op rollen, posities en het team waar de medewerker onder valt. Zo is er een onderscheid in wat leden van de teams Jeugd, Inkomen en Wmo kunnen zien. Bijvoorbeeld: als een inwoner door het team Jeugd behandeld wordt, en een medewerker van het team Wmo dit dossier wil inzien, dan kan de medewerker van Wmo wel zien dat de inwoner in contact staat met team Jeugd, maar niet wat de details zijn. De verantwoordelijk medewerker uit team Jeugd kan de collega van team Wmo toevoegen aan het dossier, dan kan deze de details van de behandeling ook inzien. Medewerkers uit het sociaal domein maken zelf de beslissing om collega's al dan niet toe te voegen. Daarnaast is het mogelijk dat medewerkers uit de verschillende teams deze informatie over inwoners mondeling delen.

Periodieke controle niet uitgevoerd door drukte bij functioneel beheerders; verkeerde autorisaties niet opgespoord

Op het gebruik van de applicaties in het sociaal domein vindt geen periodieke controle plaats. De laatste jaren hebben de functioneel beheerders een ruimer takenpakket gekregen. Als uitvloeisel van deze werkdruk, voeren zij de controles alleen uit als hun agenda het toelaat of als een applicatie geüpdatet wordt. In de gesprekken werd aangegeven dat het voorkomt dat men meer informatie kan inzien dan strikt noodzakelijk is. Dit zou met een controle van de applicaties wellicht voorkomen kunnen worden.

Alle acties die medewerkers uitvoeren in de applicaties in het sociaal domein worden automatisch bijgehouden in een logbestand. Met uitzondering van de applicatie Suwinet, worden op deze logbestanden ook geen periodieke controles uitgevoerd. De functioneel beheerders krijgen een melding wanneer een applicatie onjuist wordt gebruikt. Bijvoorbeeld wanneer een medewerker een dossier probeert te openen waar hij of zij geen toegang toe heeft. De functioneel beheerders koppelen een dergelijke melding zowel terug aan de betreffende medewerker als aan de teammanager.

3.4 / Informatievoorziening over privacy aan inwoners

Inwoners geïnformeerd over privacy via de gemeentelijke website; uitgangspunten niet in lijn met de Leertuinmethode

Inwoners kunnen op de website van de gemeente Dronten informatie vinden over de wijze waarop met hun gegevens wordt omgegaan, zowel in het sociaal domein als op de website van de gemeente. Op depagina over

privacy bij websitebezoek[35] staat dat 'de bescherming van persoonsgegevens is geregeld in de Algemene Verordening Gegevensbescherming (AVG), die ook voor de gemeente Dronten van toepassing is'. Tevens staat aangegeven dat verstrekte gegevens alleen door de gemeente Dronten worden gebruikt, tenzij expliciet toestemming wordt gegeven voor het delen van de gegevens. Dit is opvallend, omdat er ook situaties zijn – zeker in het sociaal domein – waarbij dit niet het uitgangspunt is van de Leertuinmethode (zie paragraaf 3.1). Op de webpagina over het domein 'Jeugd' staat wel beschreven dat de gids in bespreking treedt met ouders op het moment dat 'het nodig is om informatie over het kind uit te wisselen'.

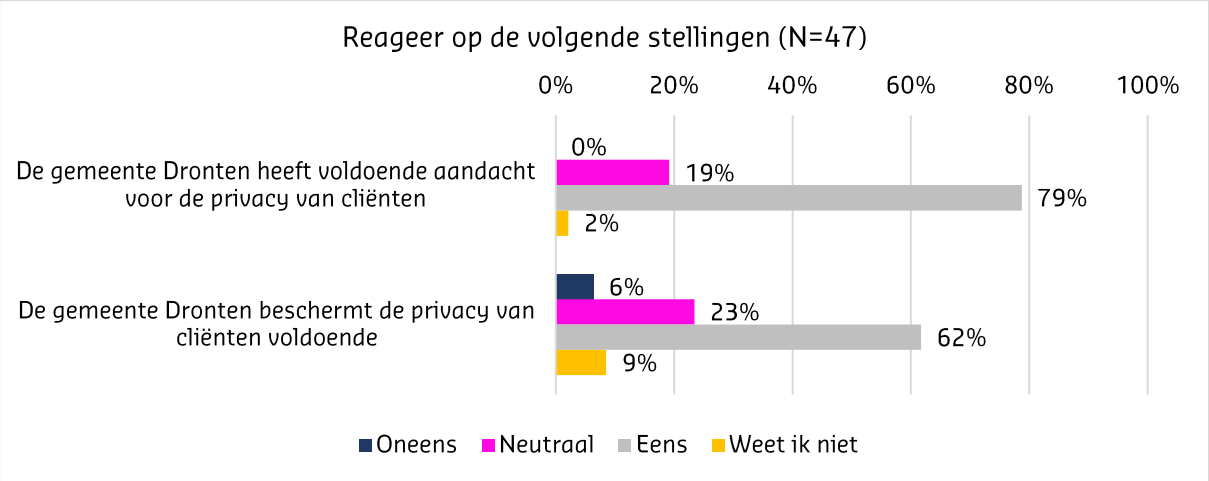
Gemeente Dronten heeft brochure voor inwoners ten aanzien van privacy

De gemeente Dronten heeft een brochure voor haar inwoners opgesteld ten aanzien van privacy.[36] Hierin worden inwoners geïnformeerd over welke gegevens de gemeente verwerkt en wat de rechten zijn van inwoners. Tevens staat beschreven hoe de behandelend ambtenaar (in Dronten: gids) alleen gegevens deelt na toestemming, tenzij sprake is van een uitzonderlijk geval. Een uitzonderlijk geval is bijvoorbeeld kindermishandeling of huiselijk geweld.[37] Voor verdere informatie over privacy verwijst de brochure naar www.rijksoverheid.nl.

Geen beeld over effectiviteit communicatie over privacy

Of de bovenstaande aanpak effectief genoeg is, is onduidelijk volgens de respondenten uit het sociaal domein. 43% van de invullers gaf namelijk 'weet ik niet' aan op de stelling dat cliënten van de gemeente Dronten voldoende zijn geïnformeerd over de wijze waarop hun gegevens worden gedeeld met externe partners. Bovendien gaf ook 21% van de invullers aan neutraal te denken over de stelling. Verder was 13% het hiermee oneens, en een grotere groep (23%) was het eens met deze stelling. Van de medewerkers geeft 79% aan van mening te zijn dat de gemeente Dronten voldoende aandacht heeft voor de privacy van cliënten. 62% vindt daarnaast dat de gemeente Dronten de privacy van inwoners voldoende beschermt (figuur 7). Gezien de tevredenheid van de medewerkers zelf, is er weinig urgentie voor medewerkers om actief met de thema's bezig te zijn.

Figuur 7 Waardering medewerkers voor de borging van privacy en informatieveiligheid



3.5 / Bewustzijn

Invoering AVG leidt volgens respondenten tot bewustzijn in het handelen van medewerkers uit het sociaal domein

In de vragenlijst is medewerkers uit het sociaal domein van de gemeente Dronten gevraagd te reageren op een aantal stellingen over de verandering van werkzaamheden sinds de invoering van de AVG (zie onderstaande

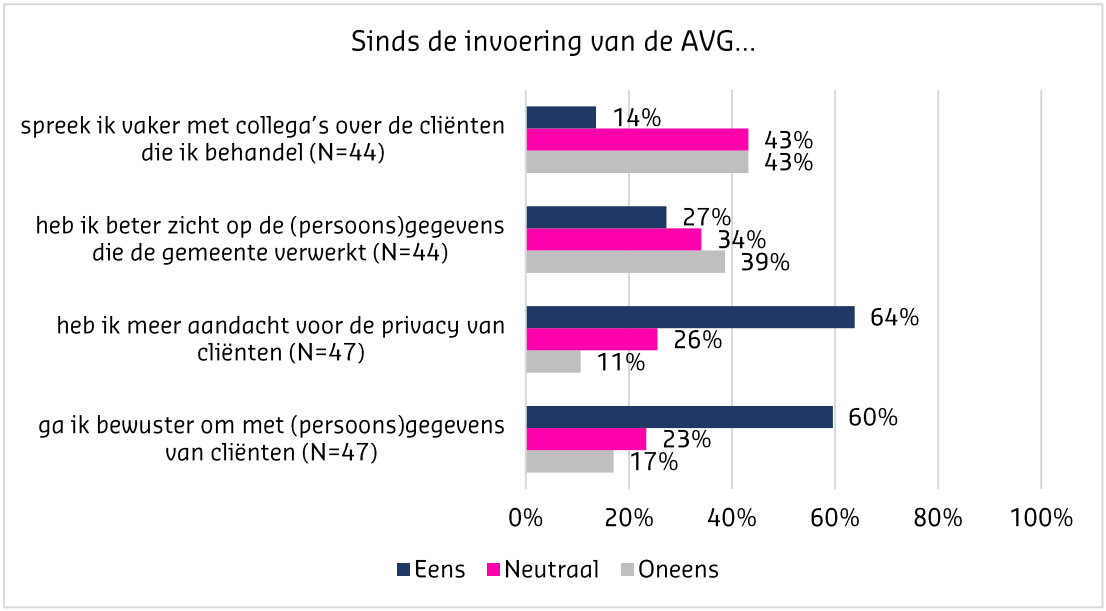
[35] https://www.dronten.nl/mozard/!suite86.scherm0325?mVrg=1082&mNch=ulxn7wqslv

[36] Brochure privacy inwoners

[37] Brochure privacy inwoners

figuur 8). In het algemeen geven medewerkers aan bewuster te handelen ten aanzien van privacy en informatiebeveiliging. Zo geeft bijna twee derde (64%) van de respondenten aan nu meer aandacht te hebben voor de privacy van cliënten. Daarnaast zegt 60% bewuster om te gaan met de gegevens van cliënten. Ook geeft 43% van de respondenten aan niet vaker met collega's over cliënten te spreken en doet slechts 14% dit wel. Opvallend is de uitkomst bij de vraag 'heb ik beter zicht op de gegevens die de gemeente verwerkt'. De grootste groep (39%) geeft aan het hier niet mee eens te zijn (figuur 8).

Figuur 8 Stellingen ten aanzien van bewustzijn in handelingen



Externe partners uit het sociaal domein geven aan dit beeld te herkennen. Volgens hen zorgt het toegenomen bewustzijn bovendien voor scherpere afspraken en dat medewerkers van de gemeente en externe partners elkaar onderling corrigeren.

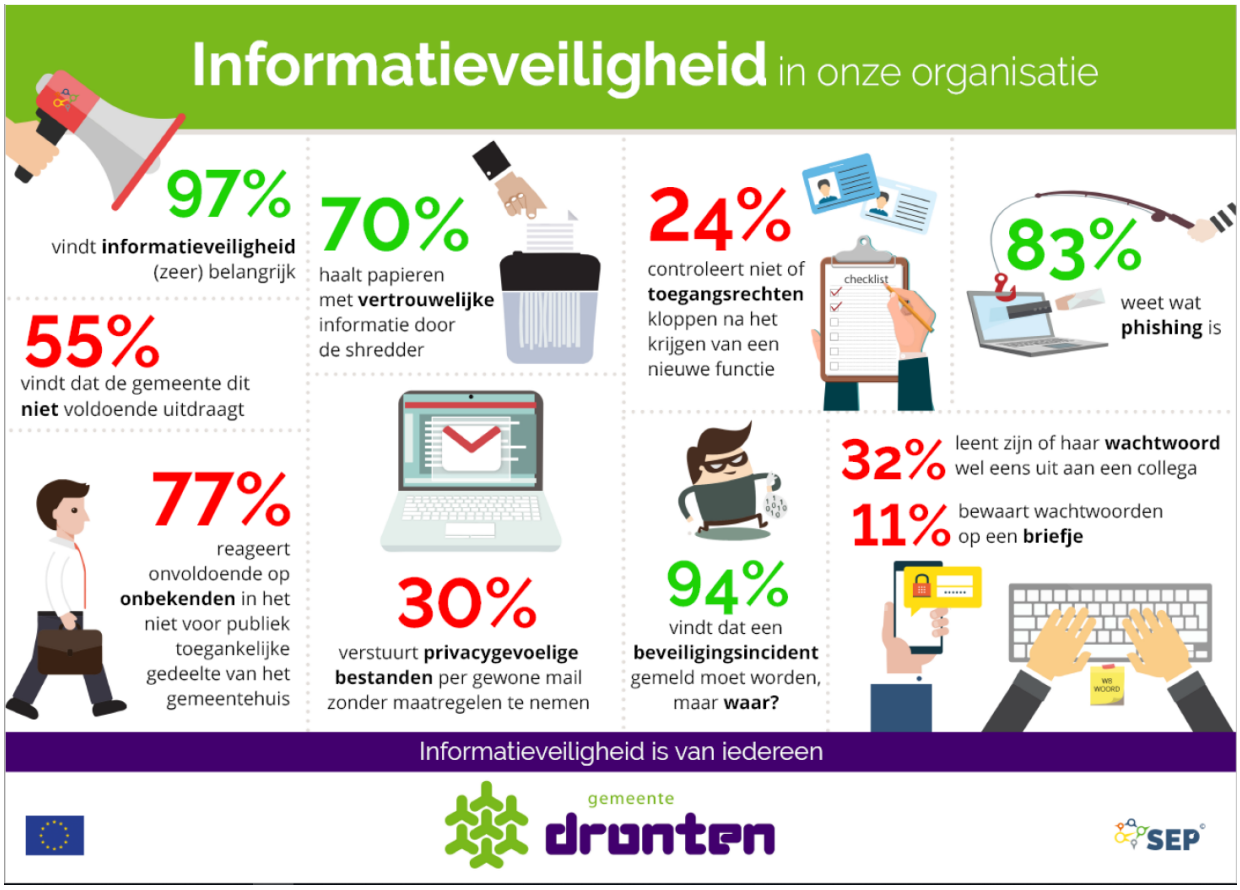
I-bewustwordingsprogramma georganiseerd in de gemeente Dronten

De gemeente Dronten heeft een I-bewustwordingsprogramma georganiseerd, gericht op het bewustzijn van medewerkers. Het I-bewustwordingsprogramma vond plaats tussen maart 2017 en april 2018. Het programma bestond uit een cyclus van meting van iBewustzijn onder medewerkers, het opstellen van leerdoelen, focus in iBewustzijnsplan, kennis aanbieden aan medewerkers en afsluiting met toetsen in diverse vormen. De E-learning krijgt een vervolg, maar er is momenteel geen geld beschikbaar voor het uitvoeren/opstarten van een bewustwordingsprogramma.

Nulmeting I-bewustzijn: weinig medewerkers deden mee

In het kader van het I-bewustwordingsprogramma is tussen 6 en 21 juni 2017 een enquête uitgezet onder medewerkers van de gemeente Dronten. In totaal zijn hiervoor 462 medewerkers uitgenodigd, waarvan 48% is begonnen aan de vragenlijst en 43% de enquête heeft afgerond. De highlights van de nulmeting zijn in de infographic (figuur 9) hieronder weergegeven:

Figuur 9 Infograhpic belangrijkste resultaten nulmeting[38]



Verbeterde alertheid op phishingmail: 11% en 6% van de ontvangers liet gegevens achter

Een aantal medewerkers van de gemeente Dronten ontving tweemaal een phishingmail. Een phishingmail probeert de ontvanger te verleiden om gegevens in te vullen onder valse voorwaarden.

De gemeente Dronten verzond een eerste phishingmail op 13 maart 2017 naar 412 medewerkers van de gemeente. Hiervan klikten 91 personen op de link in de mail, 48 personen lieten vervolgens gegevens achter op de website waar zij naartoe werden gelinkt. De tweede phishingmail werd verzonden op 27 november 2017. Van de 451 genodigden klikten er toen 38 op de link en 27 medewerkers van de gemeente Dronten lieten gegevens achter.[39] Na het doorlopen van het bewustwordingsprogramma behalen de medewerkers dus betere resultaten.

E-learning module: weinig deelnemers

Op 29 januari 2018 startte de gemeente Dronten een E-learning module onder medewerkers. 459 medewerkers werden uitgenodigd. Opvallend is dat bijna de helft (44%) van de ontvangers nooit is ingelogd in de module en dat slechts 28,5% van de ontvangers de E-learning module voltooide. Dat betekent dat een groot deel van de medewerkers geen gebruik heeft gemaakt van de module. Wel is het zo dat bijna iedereen die de E-learning voltooide, ook slaagde: 131 personen voltooiden de module, 130 zijn geslaagd.[40]

[38] Evaluatie iBewustzijn Dronten – presentatie 29-08-2018, p. 8

[39] Evaluatie iBewustzijn Dronten – presentatie 29-08-2018, p. 9

[40] Evaluatie iBewustzijn Dronten – presentatie 29-08-2018, p. 13

3.6 / Samenwerking met externe partijen

Externe partners uit het sociaal domein zijn positief over de samenwerking met de gemeente Dronten

Samenwerkingspartners uit het sociaal domein geven aan dat de samenwerking met de gemeente Dronten goed bevalt, ook in vergelijking met andere gemeenten. Dit komt met name door de communicatie via korte lijnen en de inzet van de medewerkers uit het sociaal domein die sterk betrokken zijn bij de inwoner.

Samenwerkingspartners uit het sociaal domein ontvangen bovendien geen signalen van inwoners dat zij niet willen dat de organisatie gegevens deelt met de gemeente Dronten. Daarbij dient de opmerkingen te worden gemaakt dat deze cliënten vaak door de gemeente zijn doorverwezen, en dus al bekend zijn bij de gemeente.

Samenwerking kost volgens medewerkers meer tijd; frustraties over beveiligd mailen

De samenwerking met externe partners is volgens medewerkers van de gemeente Dronten veranderd door de invoering van de AVG. Maar liefst zestig procent van de respondenten geeft aan dat het samenwerken lastiger is geworden, geen enkele respondent geeft aan dat het gemakkelijker is geworden. Een verschil van interpretatie van de regels van de AVG wordt als reden voor de lastigere samenwerking aangegeven, evenals een verhoogde mate van terughoudendheid bij het delen van informatie. Van de respondenten die werkzaam zijn bij externe partners geeft 39% aan dat het samenwerken met de gemeente Dronten lastiger is geworden, 56% staat neutraal tegenover de stelling of weet het niet. Zowel in de enquête als in de interviews is een verklaring die hiervoor wordt genoemd, het gebruik van beveiligde mailsystemen. De gemeente gebruikt Zorgmail om beveiligd te mailen. De applicatie Zorgmail werkt via een tweestaps- authenticatie. Eerst ontvangt de ontvanger een mail met het wachtwoord, vervolgens ontvangt de ontvanger de mail met beveiligde bijlage. Om beveiligd te mailen hebben medewerkers -over en weer- hun telefoon nodig om een mailtje te kunnen lezen. Dat kost tijd, en het gaat soms mis, bijvoorbeeld als de code voor een groepsmail door één persoon wordt gebruikt. Daarnaast hebben verschillende organisaties verschillende werkwijzen, wat samenwerking bemoeilijkt (zie paragraaf 1.2). Overigens wordt dit beeld niet door iedereen gedeeld: zowel in de enquête als in de gesprekken hebben verschillende personen ook aangegeven dat het beveiligd mailen voor hen geen probleem vormt.

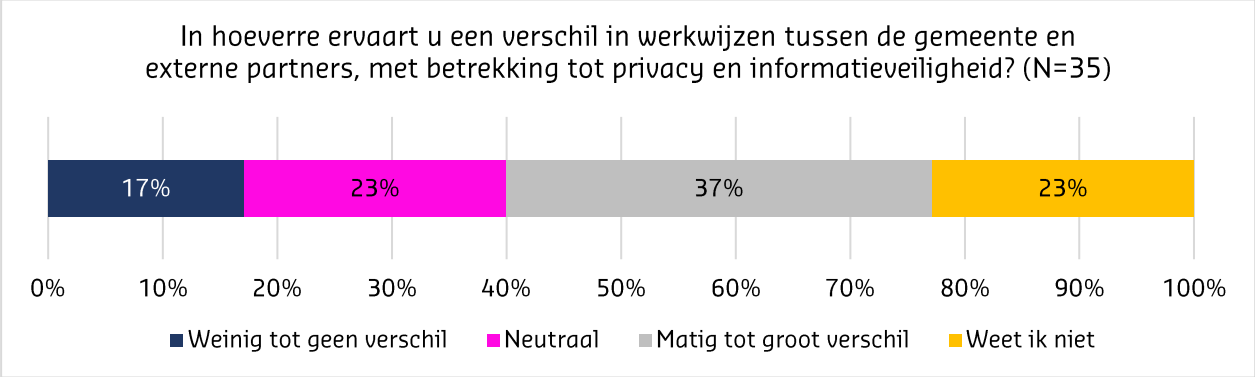
Veertig procent van de gemeentelijke respondenten geeft aan dat er sinds de invoering van de AVG minder informatie wordt gedeeld met externe partners, eveneens veertig procent staat neutraal tegenover deze stelling, terwijl geen enkele respondent aangeeft dat er meer informatie wordt gedeeld. Opvallenderwijs ligt deze stelling een stuk genuanceerder bij externe partners. Daarvan geeft slechts 13% aan dat er minder informatie gedeeld wordt. Een verklaring voor dit verschil is niet gevonden.

Tot slot geven respondenten aan dat de samenwerking met externe partners naar aanleiding van de AVG meer tijd kost dan voorheen. Zestig procent is het eens met deze stelling, terwijl geen enkele respondent aangeeft dat het samenwerken minder tijdsintensief is geworden. Onder externe partners wordt dit beeld (in mindere mate) bevestigd; daarvan geeft 43% aan dat de samenwerking met de gemeente sinds de invoering van de AVG meer tijd kost, geen enkele respondent geeft aan dat dit nu minder tijd kost.

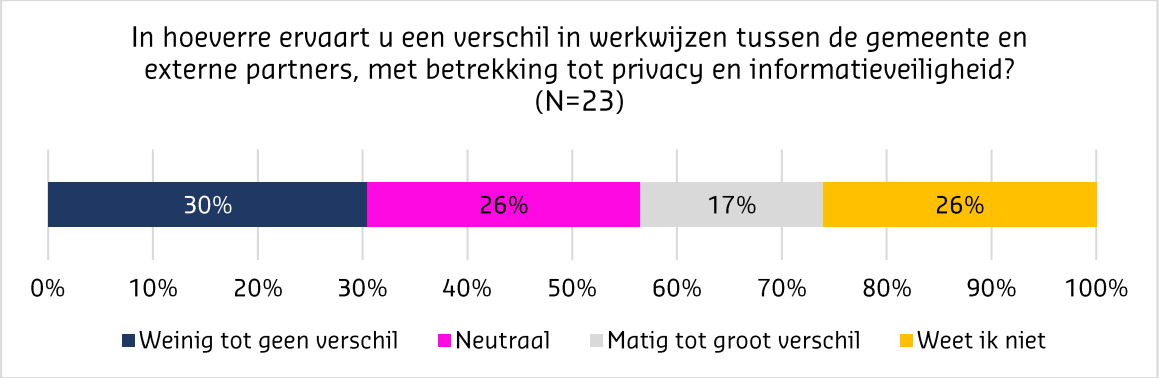
Medewerkers gemeente zien vaker verschil met werkwijze externe partijen dan andersom

Zoals aangegeven merken de medewerkers in het sociaal domein soms dat organisaties op een andere manier omgaan met gegevensdeling. In de vragenlijst werd dit voorgelegd aan zowel medewerkers van de gemeente als medewerkers van externe partijen. Het grootste deel van de medewerkers van de gemeente (37%) geeft aan dat er een matig tot groot verschil is tussen de werkwijzen omtrent gegevensdeling van de gemeente en haar externe partners, tegenover 17% die weinig tot geen verschil ziet (zie figuur 10). In de open antwoorden gaven de invullers aan dat dit lastig is in te schatten, omdat de werkwijzen van externe partners uiteenlopen. Externe partners zien het verschil in werkwijzen in mindere mate. Slechts 17% geeft aan een matig tot groot verschil te zien, 30% ziet weinig tot geen verschil (zie figuur 11). Ook de externe partners gaven aan dat dit lastig in te schatten is, zij weten niet precies hoe medewerkers van de gemeente te werk gaan. Bovendien geven zij aan dat dit ook ligt aan de situatie en de specifieke medewerker van de gemeente waarmee wordt samengewerkt.

Figuur 10 Verschil in werkwijzen, zoals gezien door medewerkers uit het sociaal domein



Figuur 11 Verschil in werkwijzen, zoals gezien door medewerkers van externe partners

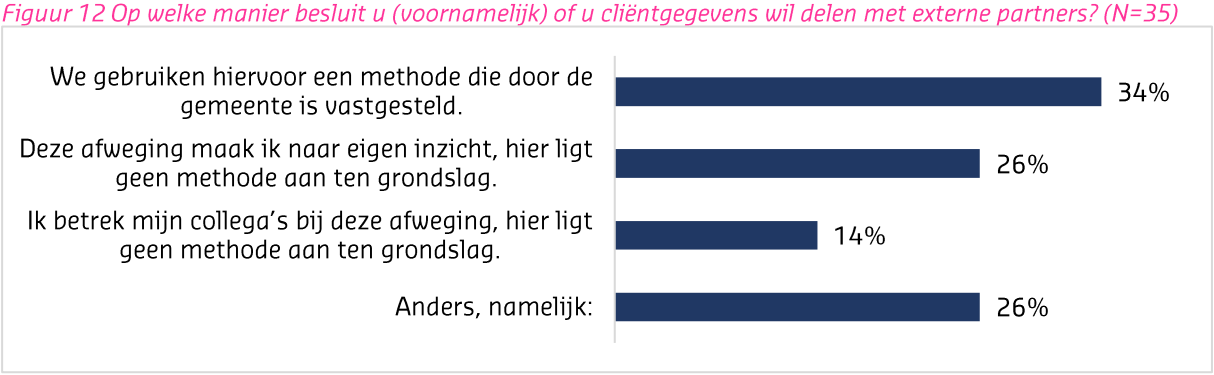


Het gebruik van verschillende werkwijzen hoeft geen belemmering te zijn voor het uitvoeren van de werkzaamheden, maar het kan wel problemen opleveren (zie bijvoorbeeld de passages over mailgebruik in deze paragraaf, of over de werkbaarheid van de AVG in paragraaf 2.2).

Veelal methode ten grondslag aan keuze tot gegevensdeling

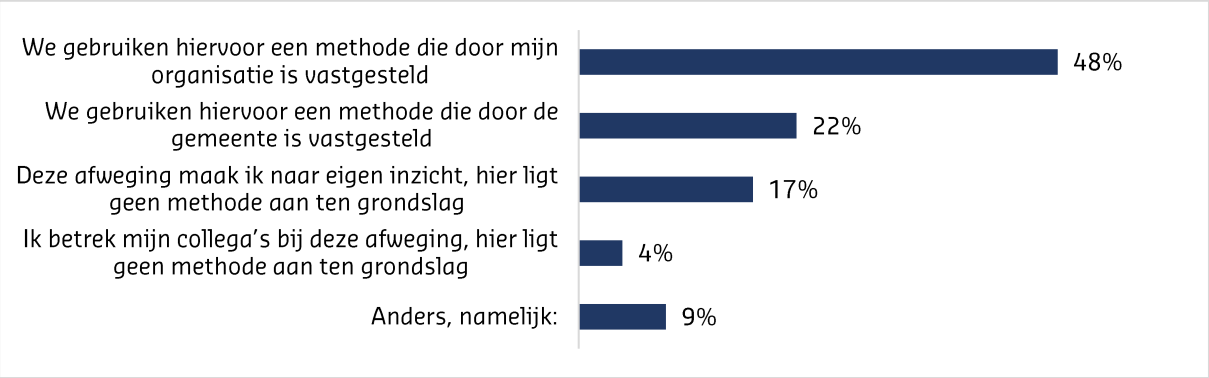
Medewerkers van de gemeente geven veelal aan te kiezen om gegevens te delen op basis van een door de gemeente vastgestelde methode (figuur 12).

Figuur 12 Op welke manier besluit u (voornamelijk) of u cliëntgegevens wil delen met externe partners? (N=35)



Opvallend is dat de beslissing over het delen van gegevens bij externe partners vaker via een vaste methode verloopt (zie figuur 13). De medewerkers van de gemeente gaan dus pragmatischer om met gegevensdeling dan hun contactpersonen bij externe partners. Bijna de helft (48%) van de externe partijen geeft aan dat ze beslissen aan de hand van een methode die door hun organisatie is vastgelegd, nog eens 22% geeft aan dit te doen aan de hand van een methode die door de gemeente is vastgelegd.

Figuur 13 Op welke manier besluit u (voornamelijk) of u cliëntgegevens wil delen met de gemeente Dronten? (N=23)



Privacy speelt dus een (negatieve) rol in de samenwerking tussen gemeente en externe partijen. Het gebruik van verschillende, niet altijd vastliggende methodes, is hier één van de verklaringen voor. Zoals in paragraaf 2.1 is beschreven, heeft de gemeente geprobeerd om dit te harmoniseren, maar dat bleek niet mogelijk.

Bijlage I - Bronnen & respondenten

Documenten

Op basis van een informatie-uitvraag en een aanvullend informatieverzoek heeft de gemeente Dronten het volgende bronmateriaal aangeleverd (indien bekend bij de onderzoekers is de datum genoemd):[41]

/ Afspraken privacy – Huisarts en POH
/ AVG plan van aanpak gemeente Dronten (juni 2014)
/ Benoeming Functionaris voor de Gegevensbescherming (11 maart 2018)
/ Beschikbare links en documentatie ten aanzien van privacybeleid
/ Bijlage 1. Uitvoeringsplan implementatie privacyprotocol
/ Bijlage 1. Werkwijze Leertuin Zorg en Veiligheid
/ Bijlage 2. Handreiking privacy in Dronten (concept) (15 november 2016)
/ Bijlage 2. Juridische visie Leertuin (deel van het boek: Werken in de wijk)
/ Brief en notitie aan gemeenteraad 'Lokaal persoonsgerichte aanpak in Dronten' (3 november 2017)
/ Brochure privacy inwoners
/ Collegeverklaring ENSIA 2017 inzake Informatiebeveiliging DigiD en Suwinet (24 april 2018)
/ Conceptinformatieveiligheidsbeleid gemeente Dronten 2019-2021 (onder embargo)
/ Conceptofferte gemeente Dronten voor hoorcollege en trainingen gegevens delen
/ Doorlooptijden handeling aanvraag IOAW
/ Doorlooptijden handeling mutatieformulier
/ Doorlooptijden handeling studietoeslag
/ ENSIA BIG rapportage 2017 – verbeterplan 2018
/ Evaluatie iBewustzijn Dronten, presentatie (29 augustus 2018)
/ Gebruikersrapportages Suwinet 2017 (januari, april, juli, oktober)
/ Gebruikersrapportages Suwinet 2018 (per maand)
/ Handboek: Werken in de wijk – Hoofdstuk 13
/ Handreiking privacy sociaal domein
/ Informatiebeleidsplan 2017-2021 – v1.1 (april 2017)
/ Informatieveiligheidsbeleid gemeente Dronten – v1.0 (1 juli 2014)
/ Leertuin eisen aan dossiervoering
/ Leertuin Stroomschema (najaar 2017)
/ Model verwerkersovereenkomst Dronten
/ Motie privacy (23 juni 2016)
/ Overeenkomst omtrent persoonsgegevens gemeente Dronten (9 november 2018)
/ Presentatie 'privacy in de keten' door Jolanda van Boven (2018)
/ Privacyprotocol sociaal domein
/ Proces informatieveiligheid incidentenmelding gemeente Dronten
/ Rapportage 3e kwartaal (overzicht kosten, opgesteld voor rekenkamer)
/ Rapportage BIG zelfevaluatie informatiebeveiliging ENSIA 2017
/ Rapportage FG Q2 en Q3 (2 oktober 2018)
/ Rapportage FG Q2 en Q3, gericht aan gemeenteraad (5 december 2018)

[41] Dit zijn de namen zoals aan de documenten gekoppeld tijdens aanlevering bij de onderzoekers. Op deze wijze zijn de documenten gemakkelijk te traceren bij de gemeente Dronten. De namen zijn alleen in hoge uitzondering aangepast of aangevuld indien onderzoekers opheldering nodig achtten.

/ Sheets Hoorcollege Peter Gunst (presentatie Leertuinmethode)
/ Sociaal domein – register van verwerkingen
/ Veiligheidsplan Suwinet 4.1 (21 november 2018)
/ Zelfscan privacy sociaal domein (20 juli 2016)

Open Bronnen

Ter verdieping van het onderzoek zijn er aanvullende gegevens gebruikt uit de volgende open bronnen en documenten:

/ Conclusie ICT benchmark gemeenten 2018
/ Gemeentebegrotingen 2018 en 2019 Dronten (onderdeel programmabegroting sociaal domein)
/ Rapport Nationale Privacy Benchmark, Verdonck, Klooster & Associates, 2017
/ Strategische Baseline Informatiebeveiliging Nederlandse gemeenten – v.1.02
/ Tactische Baseline Informatiebeveiliging Nederlandse gemeenten – v.1.02
/ Website Autoriteit Persoonsgegevens (https://www.autoriteitpersoonsgegevens.nl/)
/ Website gemeente Dronten (https://www.dronten.nl/)
/ Website IBD (https://www.informatiebeveiligingsdienst.nl/)
/ Website Vereniging van Nederlandse Gemeenten (https://vng.nl/)

Gesprekspartners

Ter verdieping van dit onderzoek zijn vier (groeps)interviews gehouden. De gespreksverslagen van deze interviews zijn ter verificatie aan de gesprekspartners voorgelegd en geaccordeerd. De verslagen dienen als achtergrondinformatie voor de Nota van bevindingen.

Datum	Naam	Functie
21 januari 2019	De heer A. van Amerongen	Wethouder (o.a. portefeuilles ICT & informatiseringsbeleid)
	De heer P. van Bergen	Wethouder (o.a. portefeuilles Jeugdzorg, Wmo & Participatiewet)
	Mevrouw M. Wessels	Juridisch Kwaliteitsmedewerker
21 januari 2019	Mevrouw N. van Oort	Functionaris voor de Gegevensbescherming (FG)
	De heer J. de Jonge	Chief Information Security Officer (CISO)
21 januari 2019	Mevrouw L. van den Brink	Griffier (a.i.)
23 april 2019	De heer C. Pot	Functioneel beheerder in het sociaal domein
	De heer V. Datema	Functioneel beheerder in het sociaal domein
8 mei 2019	De heer O. Wong	Wmo gids in het sociaal domein
	De heer J. Vos	Participatiegids in het sociaal domein
	Mevrouw E. de Groot	Participatiegids in het sociaal domein
	Mevrouw J. Bruijnes	Inkomensconsulent in het sociaal domein
	Mevrouw I. Kool	Participatiegids in het sociaal domein
13 mei 2019	Mevrouw L. Kuk	Teamcoördinator specialistische begeleiding bij Allerzorg
14 mei 2019	Mevrouw E. van Berkum	Manager dienstverlening bij Philadelphia Werk & Begeleiding Noord Nederland B.V
14 mei 2019	Mevrouw B. van Veldhuizen	Zelfstandig therapeut bij Praktijk de Eik

Bijlage II – Schouw van de afdeling

Schouw van de afdeling

De onderzoekers zijn op dinsdag 23 april een halve dag aanwezig geweest bij de gemeente Dronten. De onderzoekers hebben ten eerste in de centrale ontvangstruimte van de gemeente gewerkt, naast de balies van het klantencontactcentrum. Vervolgens hebben de onderzoekers in een eigen ruimte op de afdeling sociaal domein gewerkt. Vanaf die locatie hadden de onderzoekers toegang tot het werkgebied van de medewerkers uit het sociaal domein. Relevante observaties van de onderzoekers zijn opgenomen in het onderzoeksrapport. Hieronder vindt u de (niet uitputtende) checklist van de onderzoekers.

Handeling	Uitkomst	Toelichting (indien nodig)
Afdeling zonder controle toegankelijk?	nee	Onderzoekers konden niet bij de afdeling komen zonder begeleiding.
Beveiliging vaste telefoons?	ja	Er moet een wachtwoord ingevoerd worden om te kunnen bellen.
Beschikbaarheid afgeschermde belfaciliteiten?	nee	Er zijn voornamelijk vaste telefoons beschikbaar. Privé-bellen is daarmee niet mogelijk. Er werkt echter een klein aantal medewerkers per kamer, dus gesprekken worden niet ruim gedeeld.
Medewerkers vergrendelen scherm bij afwezigheid?	ja	
Uitgeprinte documenten blijven liggen in de printer?	nee	
Onnodige documenten beschikbaar?	ja	Er is één locatie voor externe post, deze is binnen de afdeling vrij toegankelijk. De 'postbus' is niet afgesloten. In de kamer waar de onderzoekers zaten stonden ook mappen met gegevens over externe inhuur.
Sleutelkasten aanwezig?	ja, met kanttekening	Er staan sleutelkasten in verschillende ruimten, in de kamer waar de onderzoekers zaten was deze echter niet op slot. In een andere kamer zat de sleutel in het slot.
Persoonsgegevens worden hoorbaar besproken?	nee	
Afgesloten ruimtes voor overleg?	ja	Er zijn verschillende kamers die kunnen worden afgesloten. Daarin kunnen medewerkers besloten overleggen.
Wachtwoorden zichtbaar bewaard?	nee	
Medewerkers zijn alert op niet bekende gezichten?	deels	Bij ontvangst in de aangewezen ruimte stelde de medewerker zich voor met de vraag wie wij waren. Tijdens een wandeling door de gangen werd dit niet aan de onderzoekers gevraagd.

Bijlage III – Begrippen- en verklaringenlijst

AP – Autoriteit Persoonsgegevens (tot 1 januari 2016 College bescherming persoonsgegevens). De AP houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens en adviseert over nieuwe regelgeving.

AVG – Algemene Verordening Gegevensbescherming: een Europese verordening (dus met rechtstreekse werking) die de regels voor de verwerking van persoonsgegevens door particuliere bedrijven en overheidsinstanties in de hele Europese Unie standaardiseert.

BIG – Baseline Informatiebeveiliging Nederlandse Gemeenten; gemeentelijk basisnormenkader voor informatieveiligheid.

BIO – Baseline Informatiebeveiliging Overheid; basisnormenkader voor informatieveiligheid voor overheden.

BRP – Basisregistratie personen.

CISO – Chief Information Security Officer; specialist op het gebied van de Informatie Beveiligingsfunctie, genoemd in de Baseline Informatiebeveiliging Nederlandse Gemeenten.

DigiD - Een systeem waarmee Nederlandse overheden op internet iemands identiteit kunnen verifiëren.

DPIA – Data Privacy Impact Assessment: Een instrument waarmee de risico's op het gebied van privacy in kaart kunnen worden gebracht.

ENSIA – Eenduidige Normatiek Single Information Audit: Systematiek voor verantwoording over informatieveiligheid. Het proces bestaat uit een voorbereiding, zelfevaluatie, horizontale verantwoording, verticale verantwoording en een evaluatie.

ESAR – Beveiligd internetsysteem voor professionals die werken met jongeren tot 23 jaar, dat wordt gebruikt door (overheids)instanties, waaronder de gemeente Dronten.

FG – Functionaris voor de Gegevensbescherming. Functionaris die binnen de organisatie toezicht houdt op de toepassing en naleving van de Algemene Verordening Gegevensbescherming (AVG).

GEB – Gegevensbeschermingseffect beoordelingen.

Leertuinmethode – Methode welke handvatten biedt voor medewerkers van de gemeente Dronten om gegevens te verwerken binnen de geldende privacyregelgeving.

IBD – Informatiebeveiligingsdienst voor gemeenten.

Phishingmail - In een phishingmail staat altijd een link waarop geklikt moet worden, zodat de gebruiker wordt doorverwezen naar een valse website die lijkt op de echte website van een bekend en betrouwbaar bedrijf. Daar vraagt de verzender naar gegevens zoals creditcardinformatie en/of sofinummer.

Proportionaliteit – Beginsel: een middel mag alleen gebruikt worden wanneer het in verhouding staat tot het doel.

Register van verwerkingen – Dit register bevat informatie over de persoonsgegevens die worden verwerkt. Het vervangt de bestaande verplichting uit de Wet bescherming persoonsgegevens om gegevensverwerkingen bij de Autoriteit Persoonsgegevens te melden.

Subsidiariteit – Beginsel: een middel is alleen toegestaan wanneer geen minder zwaarwegend middel hetzelfde doel kan bereiken.

Suwi – Wet Structuur uitvoeringsorganisatie werk en inkomen.

Suwinet – Registratiesysteem; systeem van informatie-uitwisseling in de keten van werk en inkomen. Uitvloeisel van de Wet structuur uitvoeringsorganisatie werk en inkomen.

Transparantie – In de context van politiek en bestuurszaken duidt dit begrip op openheid binnen een bestuurlijk of juridisch orgaan, zoals een overheid of een internationale instelling.

Vier V's van de gemeente Dronten - Vertrouwen, Verbinding, Vakmanschap en Vernieuwingskracht

VNG – Vereniging van Nederlandse gemeenten.

Wbp – Wet bescherming persoonsgegevens. Deze wet is na de invoering van de Algemene Verordening Gegevensbescherming op 25 mei 2018 niet meer van toepassing.

Wmo – Wet maatschappelijke ondersteuning; Gemeenten moeten ervoor zorgen dat mensen zo lang mogelijk thuis kunnen blijven wonen. De gemeente geeft ondersteuning thuis via de Wmo. Officieel heet deze wet Wmo 2015.

Bijlage IV – Infographic

WERKBAARHEID IN HET SOCIAAL DOMEIN

Gevolgen van de AVG in Dronten

gemeente dronten

Gevolgen AVG – beleid & governance

- Informatieveiligheidsbeleid op orde; beleidsstukken privacy niet aanwezig of in ontwikkeling.
- Duidelijke gecentraliseerde taken maar verantwoordelijkheidsgevoel bij individuele medewerkers kan beter.

Gevolgen AVG – kosten

- Landelijke verwachting: kosten stijgen.
- Dronten: onduidelijk, gemeente monitort dit ook niet.

Gevolgen AVG – samenwerken met externen

- 37% van de ambtenaren en 17% van de externe partners ziet een verschil in werkwijzen binnen en buiten de gemeentelijke organisatie. Externe partners zijn desondanks positief over de samenwerking met de gemeente Dronten.

Gevolgen AVG – ervaren werkbaarheid

52% van de medewerkers zegt meer handelingen te moeten verrichten om zijn/haar takenpakket uit te voeren.

43% van de medewerkers zegt dat het meer tijd kost om het takenpakket uit te voeren.

60% van de medewerkers gaat bewuster om met (persoons) gegevens van cliënten.

Onderzoeksperiode:	december 2018 – maart 2019
Geïnterviewde personen:	2 bestuurders, 1 griffier, 5 medewerkers privacy en informatieveiligheid, 5 medewerkers sociaal domein, 3 externe partners
Enquête:	47 medewerkers (31,5% respons) en 30 externe partners (62,5% respons)

CONCLUSIES

- Werkbaarheid staat centraal in keuzes rondom privacy en informatieveiligheid.
- Urgentie en noodzaak privacy en informatieveiligheid wordt niet breed gevoeld.

Necker van Naem

Bijlage V – Reactie van het college

gemeente dronten

Dronten	: 9 juli 2019
Verzonden	: 9 juli 2019
Kenmerk	: U19.007650/DIR/AL
Uw brief van	:
Uw kenmerk	:
Inlichtingen	: heer Lahyi

Onderwerp: Reactie college B&W inzake rekenkameronderzoek 'Privacy in het sociaal domein'

Geachte leden van de rekenkamer,

Het college heeft met veel interesse kennisgenomen van het door u uitgebrachte concept-rapport 'Privacy in het sociaal domein' en de daarbij behorende conclusies en aanbevelingen. Informatiebeveiliging is een belangrijk onderwerp voor gemeenten. De privacygevoelige informatie in het sociaal domein maakt dit onderwerp nog eens extra relevant en gewichtig. Het college heeft uw rapportage bestudeerd en heeft daarop de volgende reactie.

Reactie op de conclusies

- Uit het onderzoek komt naar voren dat binnen de gemeente, het accent ligt op werkbaarheid en pragmatiek. Voor de uitvoer van de taken in het sociaal domein wordt de Leertuinmethode gebruikt. Dit verschaft de mogelijkheid om, op een verantwoorde manier, informatie te delen in en tussen verschillende domeinen. Binnen de kaders van de Leertuin kan men ervaring opdoen met de nieuwe werkwijze en vervolgens deze werkwijze formaliseren. Dit proces wenst het college aan te houden als leidraad, omdat hiermee het accent komt te liggen op de feitelijke werkzaamheden en in mindere mate het uitvoeren van administratieve handelingen.

- Het gevoel voor de urgentie en noodzaak op het gebied van privacy en informatieveiligheid heeft binnen het onderzoek een reactief karakter. Het college onderschrijft dit en daarom is structureel budget aangevraagd in de kadernota. Voorbeelden uit uw onderzoek wijzen naar het opstellen van het privacyconvenant en het AVG-bestendig maken van de gemeente in aanloop naar de toepassing daarvan in 2018. Het college betreurt de bevinding dat op strategisch en uitvoerend niveau de urgentie niet adequaat is geweest. Wij staan achter de ambitie om bewuster en urgenter te anticiperen op nieuwe ontwikkelingen binnen dit thema.

Bijlage(n): --

De Rede 1
8251 ER Dronten

Postbus 100
8250 AC Dronten

Telefoon:
14 0321

www.dronten.nl
gemeente@dronten.nl

Ten tijde van het convenant en de AVG-implementatie, bleken de werkzaamheden meer tijd te kosten dan vooraf was ingeschat. Wij onderschrijven dat gegevensbescherming meer aandacht verdient. In de kadernota 2020 wordt door het college voorgesteld om in te zetten op informatieveiligheid en privacy bewustwording. Concreet zet het college in op bewustwording, kwaliteit en continuïteit in de bedrijfsvoerings- en dienstverleningsprocessen. Bewustwording wordt onder andere verhoogd via e-learning. Het volgen ervan was tijdens de laatste module vrijwillig, maar is inmiddels verplicht gesteld. Het college gaat zich inzetten om het aandeel in de participatie ervan te verhogen.

- De gemeenteraad speelt met haar kaderstellende en controlerende functie een belangrijke rol bij het interpreteren van AVG-normen. De AVG is een kaderwet met algemene normen die geïnterpreteerd dient te worden met het oog op de dagelijkse praktijk van de gemeente. In die vertaalslag van algemene normen naar gemeentebeleid is een vitale rol voor de gemeenteraad toebedeeld. Het college stelt voor om samen met de gemeenteraad die vertaalslag met kaders en sturing concreter te maken voor de dagelijkse praktijk in Dronten. Daarmee stelt het college dat de doorontwikkeling van het gegevensbeschermingsbeleid kan worden gewaarborgd. Aanvullend adviseert het college om waakzaam te zijn voor herhalingen van algemene en reeds bestaande AVG-normen, wet- en regelgeving.

- Het college heeft met tevredenheid kennisgenomen dat op het gebied van uitvoering, de AVG en de gevolgen daarvan bekend zijn binnen de organisatie. Uw onderzoek geeft daarnaast aan dat privacy op sturingsniveau beter verankerd dient te worden, door bijvoorbeeld het opstellen van beleid in het geval van een incident. Kaders zouden kunnen voorkomen als een incident plaatsvindt of aanpassingen nodig zouden zijn. Het college erkent dat zij daarin een sturende rol heeft. Wij zetten ons in om de hoeveelheid incidenten tot het minimum te beperken. Dat gezegd hebbende blijkt uit de informatiebeveiliging dat het 100% voorkomen van alle incidenten niet mogelijk is en dat de menselijke factor hierin een belangrijke rol speelt. Zoals eerder aangegeven zal het college zich op dit onderdeel inzetten op de bewustwording en de kwaliteit bij medewerkers. Het waarborgen van kwaliteit is evengoed van belang bij de bevinding over tegenstrijdige adviezen aan inwoners vanuit verschillende afdelingen. Wij zetten ons in om zoveel als mogelijk tegenstrijdige adviezen te voorkomen.

  Tot slot deelt het college de bevinding dat een goede grip op kosten en doorlooptijden bij de AVG-implementatie en de doorontwikkeling daarvan een prioriteit is. Uw onderzoek stelt dat op dit moment, het niet mogelijk is om kosten en doorlooptijden in kaart te brengen door de wijze waarop het administratief systeem binnen onze gemeente is ingericht. Het college stelt voor om dit beter in kaart te brengen door een evaluatie van het administratieve systeem en een nauwere samenwerking met de ambtelijke organisatie om dit op te lossen.

Reactie op de aanbevelingen (aan de raad)

- De gemeenteraad heeft naast het kaderen ook een controlerende taakstelling. Ook op dit vlak is het college bereid intensiever samen te werken ter bevordering van de onderwerpen, die binnen dit thema langskomen. Zoals eerder genoemd zou het mogelijk kunnen zijn om dit tweemaal per jaar te agenderen tijdens het fractievoorzittersoverleg.

Het college staat achter een doorontwikkeling van de bestaande rol van de raad omtrent privacy en informatieveiligheid. Over informatieveiligheid wordt de raad sinds 2017 met de voor verschillende ministeries verplicht uit te voeren Eenduidige Normatiek Single Information Audit (ENSIA) jaarlijks uitgebreid geïnformeerd over stand van zaken bij Dronten. Kennisgeving en besluitvorming hierover valt via het college onder het horizontale toezicht en de controlefunctie van de raad. De rapportage bevat onder andere gesignaleerde veiligheidsrisico's en de daarop te nemen maatregelen. Incidenten gerelateerd aan privacy en veiligheidsrisico's worden op dit moment nog niet in de P&C-cyclus opgenomen. Het college adviseert daarom om incidenten en kosten voor het waarborgen van privacy en informatieveiligheid een onderdeel te maken binnen de P&C-cyclus.

Reactie op de aanbevelingen (aan het college)

- Het college is van mening dat sturing op de ambtelijke organisatie van belang is om binnen de organisatie eigenaarschap en bewustwording verder in te bedden. In het verlengde daarvan streeft het college ernaar dit onderdeel binnen de bestaande sturingsstructuren mee te nemen en te internaliseren. Een nuancering hierin is dat het voor de meeste medewerkers duidelijk is waar de vragen over privacy gesteld kunnen worden. Voor het sociaal domein is hiervoor een ander proces ingericht via de juridische kwaliteitsmedewerkers van het sociaal domein. Op de overige plekken in de organisatie is de positie van de FG bij minstens één persoon van het team bekend en zodoende komen de vragen dan ook op de juiste plek binnen. Het afronden en implementeren van het privacybeleid heeft een hoge prioriteit. Het beleid betreft de hele organisatie, niet alleen het sociaal domein. Voor volgend jaar staat er wederom een e-learning op de planning, ditmaal gericht op de combinatie van informatiebeveiliging én privacy.

  In het kader van eigenaarschap zijn een aantal belangrijke stappen gezet. Zo is er wekelijks een contactmoment tussen de functionaris gegevensbeheer en de juridische kwaliteitsmedewerker sociaal domein, met als prioriteit alle gebeurtenissen rondom privacy binnen het sociaal domein. De functionaris gegevensbeheer wordt betrokken bij onduidelijkheden in werkwijze. Naar aanleiding van een signaal wordt vervolgens gekeken naar de werkafspraken. Er wordt gezocht naar werkbare oplossing om strijdigheden met de AVG te voorkomen. Na een bezoek van een *Mystery Guest* in de organisatie hebben CISO en de functionaris gegevensbeheer onlangs samen een presentatie gegeven aan de leden van het MT over de bevindingen. Hierin zijn de 6 gouden regels op het gebied van informatieveiligheid (privacy en informatiebeveiliging) geïntroduceerd. Ook is aan de leden van het managementteam gevraagd om privacy en informatiebeveiliging mee te nemen tijdens 'Het Goede Gesprek' met de medewerkers en de teamoverleggen.

  Verder zijn beoogde doelen het opstarten en uitvoeren van gegevensbeschermingseffectbeoordeling (GEB's) of Data Protection Impact Assessment (DPIA's). De informatiebeveiligingsdienst (IBD) heeft in september vorig jaar aangekondigd een instrument te leveren voor het uitvoeren van de DPIA's. Deze is gebaseerd op model van de Franse Autoriteit. Met het model moet het mogelijk zijn voor gemeentes om de verschillende DPIA's onderling te delen. Aangezien de processen binnen de overheid grotendeels overeenkomen, bespaart dit deels werk en deelt men de kennis onderling. Op het gebied van informatieveiligheid ligt er bij de

gemeente dronten

Datum : 9 juli 2019
Bladnr. : 4
Kenmerk : U19.007650/ DIR/ AL
Geadresseerde :

organisatie een verplichting om eens in de drie jaar het geldende Informatieveiligheidsbeleid te evalueren en te actualiseren. Dit geldt echter niet voor de toepassing en effecten van de AVG. Het college adviseert om dit eenmaal per jaar intern te evalueren. Het college staat achter de ambitie om eigenaarschap en de urgentie voor het thema op verschillende niveaus door te ontwikkelen.

- Het college onderschrijft de verantwoordelijkheid om privacy en informatieveiligheid vaker onder de aandacht te brengen van de organisatie en richting de raad. De belegging in het fractievoorzittersoverleg en het collegeoverleg kan daar eventueel een belangrijke rol in spelen. Het college is in het verleden betrokken geweest bij bewustwordingsprogramma's over dit onderwerp met een tijdspanne van meerdere maanden, gelanceerd in 2017 en begin 2018 respectievelijk. De resultaten van het bewustwordingsprogramma zijn met directie en het MT-breed geëvalueerd, waarbij er is geadviseerd om de programma's van een verplicht karakter te voorzien, in plaats van een vrijwillige deelname. Hiermee is toen akkoord gegaan, met de wens om bewustwording blijvend te agenderen binnen de gemeentelijke organisatie. Wel werd geconstateerd dat structureel budget voor een vervolg ontbrak, hetgeen nu middels de kadernota is aangevraagd.

Het college hoopt met deze reactie een bijdrage te leveren aan uw onderzoek en ziet de eindrapportage en presentatie aan de gemeenteraad van Dronten met veel belangstelling tegemoet.

Het college wil nogmaals haar waardering uitspreken voor de Rekenkamer en wenst haar veel succes bij de toekomstige onderzoeken die zij voor Dronten zal uitvoeren.

Als u naar aanleiding van deze brief nog vragen of opmerkingen hebben, dan kunt u vanzelfsprekend contact opnemen met onze gemeentesecretaris, mevrouw T. van Lenthe.

Met vriendelijke groet,

het college van Dronten

mr. E.J. Kruijswijk Jansen
loco secretaris

drs. J.P. Gebben
burgemeester

De Rede 1
8251 ER Dronten

Postbus 100
8250 AC Dronten

Telefoon:
14 0321

www.dronten.nl
gemeente@dronten.nl