



SUWI net / Wet Bescherming Privacy

Vragen art 33 Regl.

Geacht College, voorzitter,

De fractie van D66 heeft kennis genomen van het onderzoek van De Autoriteit Persoonsgegevens. Zij heeft onderzocht of de gemeente voldoet aan de belangrijkste beveiligingsnormen.

Uit dit onderzoek blijkt dat Midden Drenthe (nog) niet voldoet aan alle onderzochte vereisten.

Na een eerste onderzoek heeft Midden Drenthe een aantal constateringën aangepast echter hoe positief de ontwikkeling ook is, volgens de fractie van D66 blijft het onacceptabel dat het risico blijft bestaan dat gegevens in verkeerde handen komen. De autoriteit waarschuwt dat bij geen verandering dat zij zal gaan handhaven.

Onze fractie heeft hierover aan aantal vragen.

- 1 Hoe groot is het risico dat gegevens in verkeerde handen vallen door deze openstaande constateringën?
- 2 Waarom zijn alle constateringën niet adequaat opgepakt bij het eerste onderzoek?
- 3 Wanneer denkt het College de twee openstaande constateringën opgelost te hebben?
- 4 Wanneer we niet voldoen aan de vereisten en de Autoriteit Persoonsgegevens over zal gaan tot handhaving wat kunnen de consequenties dan zijn voor de gemeente?

Namens de fractie van D66 Midden Drenthe

Harma van der Roest

Fractievoorzitter

College bescherming persoonsgegevens

Onderzoek naar de beveiliging van persoonsgegevens via Suwinet
Gemeente Midden-Drenthe

z2015-00402

Openbare versie
Rapport van bevindingen

November 2015

INHOUDSOPGAVE

Samenvatting	4
1 Inleiding	5
1.1 Achtergrond	5
1.2 Aanleiding	5
1.3 Doel en reikwijdte van het onderzoek.....	6
1.4 Onderzoeksvraag	6
1.5 Werkwijze.....	6
1.6 Juridisch kader	7
2 Bevindingen	8
2.1 Beveiligingsbeleid en beveiligingsplan	8
2.1.1 Norm.....	8
2.1.2 Bevindingen	8
2.1.3 Beoordeling.....	8
2.2 Uitdragen informatiebeveiligingsbeleid en beveiligingsplan	8
2.2.1 Norm	8
2.2.2 Bevindingen	8
2.2.3 Beoordeling	8
2.3 Evaluatie Informatiebeveiligingsbeleid en SUWI beveiligingsplan	8
2.3.1 Norm	8
2.3.2 Bevindingen	9
2.3.3 Beoordeling	9
2.4 Functiescheiding.....	9
2.4.1 Norm	9
2.4.2 Bevindingen	9
2.4.3 Beoordeling	9
2.5 De Security Officer	10
2.5.1 Norm	10
2.5.2 Bevindingen	10
2.5.3 Beoordeling	10
2.6 Autorisatieprocedure	10
2.6.1 Norm	10
2.6.2 Bevindingen	11
2.6.3 Beoordeling	11
2.7 Controle op verleende toegangsrechten	11
2.7.1 Norm	11
2.7.2 Bevindingen	11
2.7.3 Beoordeling	11
3 Conclusies	13
Bijlage I: Reactie CBP op de zienswijze van de gemeente Midden-Drenthe.....	14
Zienswijze gemeente Midden-Drenthe.....	14
Reactie CBP	14

SAMENVATTING

Uit het onderzoek van het College bescherming persoonsgegevens (CBP) volgt dat de Wet bescherming persoonsgegevens (Wbp) wordt overtreden, omdat de gemeente Midden-Drenthe twee normen uit het Normenkader GeVS (Gezamenlijke elektronische Voorzieningen SUWI) niet of onvoldoende naleeft.

1. Niet is gebleken dat de Security Officer van de gemeente Midden-Drenthe rechtstreeks aan het hoogste management rapporteert. De gemeente Midden-Drenthe handelt hiermee in strijd met norm 2.3 van het Normenkader GeVS, en daarmee tevens met artikel 13 Wbp;
2. Niet is gebleken dat de gemeente Midden-Drenthe over een formele procedure beschikt op basis waarvan de gebruikers die toegang hebben tot de Suwinet applicaties worden geautoriseerd en geregistreerd. De gemeente Midden-Drenthe handelt hiermee in strijd met norm 13.1 van het Normenkader en daarmee tevens met artikel 13 Wbp.

1 INLEIDING

1.1 Achtergrond

Sinds 2002 wisselen diverse overheidsorganisaties (persoons)gegevens van burgers uit in het domein Werk & Inkomen via de Gemeenschappelijke elektronische Voorzieningen SUWI (GeVS, ook wel Suwinet genoemd). Suwinet beschikt over diverse applicaties (bijvoorbeeld Suwinet-Inkijk) die toegang geven tot (persoons)gegevens van burgers. Het betreft de gegevens over onder meer inkomsten uit arbeid en uitkeringen, werkgever(s), uitkeringsaanvragen en opleidings- en beroepservaring. Suwinet-Inkijk biedt ook informatie over de status van identiteitsbewijzen en adresgegevens en contactpersonen van bedrijven.

De Suwipartijen zoals in de Wet structuur uitvoeringsorganisatie werk en inkomen (SUWI) genoemd, zijn: Gemeentelijke Sociale Diensten (GSD), het UWV en de Sociale Verzekeringsbank (SVB). Dit zijn bronhouders. Bronhouders zijn partijen die gegevens leveren via Suwinet. Naast Suwipartijen kunnen zogenaamde niet-Suwipartijen toegang krijgen tot Suwinet. Deze niet-Suwipartijen zijn onder andere de Immigratie- en Naturalisatiedienst (IND), de Inspectie SZW, gemeentelijke Belastingdeurwaarders, gemeenten in het kader van de Regionale Meld en Coördinatie punten voor voortijdig schoolverlaters (RMC) en de Stichting Netwerk Gerechtsdeurwaarders (SNG).

Zorgvuldige omgang met de persoonsgegevens die door middel van Suwinet worden uitgewisseld is essentieel voor grote groepen burgers. Via Suwinet worden miljoenen maatschappelijk gevoelige persoonsgegevens van burgers tussen veel partijen uitgewisseld. Hieronder bevinden zich zeer privacygevoelige gegevens, zoals fraudevorderingen (informatie over bijstandsvorderingen met betrekking tot fraude en recidive¹) en informatie over arbeidsongeschiktheid.

De schade door misbruik van Suwinet kan bovendien vergaande gevolgen hebben. In het verleden hebben zich incidenten voorgedaan rond blijf-van-mijn-lijf huizen, waarbij de (ex) partner de verblijfplaats van zijn (ex)vrouw via Suwinet heeft kunnen achterhalen². Adequate beveiligingsmaatregelen kunnen er voor zorgen dat dergelijke incidenten worden voorkomen.

1.2 Aanleiding

Uit verschillende onderzoeken blijkt dat de beveiliging van Suwinet niet in alle gevallen voldoet aan de wettelijke vereisten. Recent onderzoek van het College bescherming persoonsgegevens (CBP) heeft uitgewezen dat de GeVS bij de toegang tot Suwinet voor niet-Suwipartijen onvoldoende beveiligd was, onder meer omdat raadplegingen niet adequaat werden gelogd en een beveiligingsplan ontbrak³. In 2013 heeft de Inspectie SZW onderzoek gedaan naar de beveiliging van Suwinet. In dit onderzoek bleek dat slechts 4% van de gemeenten bij het gebruik van Suwinet voldoende maatregelen had getroffen om de vertrouwelijkheid van uitgewisselde gegevens te waarborgen. Gezien de uitkomsten van dat onderzoek heeft de Inspectie SZW dit onderzoek in 2014 bij een groot aantal gemeenten herhaald.

¹ http://www.bkwi.nl/uploads/media/20150408_Handreiking_autorisatie_op_Suwinet-Inkijk_voor_GSD_01.pdf

² <http://www.helmond.nl/BIS/2014/Notities%20en%20kaarten/Commissies/CN%20Integriteitbeleid-risicoanalyse%20afd%20werk%20en%20Inkomen%20gemeente%20Helmond.pdf>

³ <https://cbpweb.nl/nl/nieuws/cbp-persoonsgegevens-suwinet-niet-goed-beveiligd>

Op 4 juni 2015 is de definitieve rapportage zoals opgesteld door de Inspectie SZW (verder: rapportage) aangeboden aan de Tweede Kamer. Uit de rapportage blijkt onder meer dat negen gemeenten geen van de zeven onderzochte beveiligingsnormen naleeft. Het CBP heeft besloten onderzoek in te stellen naar acht van deze negen gemeenten.

Dit rapport betreft de bevindingen van het onderzoek aangaande de gemeente Midden-Drenthe, zijnde één van de bovenbedoelde gemeenten.

1.3 Doel en reikwijdte van het onderzoek

Het onderzoek beoogt vast te stellen of de gemeente Midden-Drenthe, zijnde de verantwoordelijke voor de verwerkingen van persoonsgegevens via Suwinet in de zin van de Wbp, passende technische en organisatorische maatregelen heeft getroffen om deze persoonsgegevens te beveiligen.

1.4 Onderzoeksvraag

Onderzocht is of de verantwoordelijke passende technische en organisatorische maatregelen ten uitvoer heeft gelegd teneinde persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking, zoals bedoeld in artikel 13 Wbp. Het onderzoek richt zich in dit kader op de volgende zeven normen uit het Normenkader GeVS:

1. Een beveiligingsplan specifiek voor de Suwi-omgeving (norm 1.3);
2. Het uitdragen van het beveiligingsplan (norm 1.4);
3. Evaluatie van het beveiligingsplan (norm 1.5);
4. Functiescheiding (norm 2.2);
5. De functie van Security Officer (norm 2.3);
6. Een formele autorisatieprocedure (norm 13.1);
7. Controle op verleende toegangsrechten (norm 13.5).

1.5 Werkwijze

In de rapportage heeft de inspectie SZW aangegeven dat de gemeente Midden-Drenthe aan geen van de zeven normen voldoet zoals omschreven in het Normenkader GeVS. Nadat het daarvan door de Inspectie SZW in kennis is gesteld, heeft het CBP de rapportage bestudeerd. Het CBP heeft kennis genomen van de bevindingen die daarin zijn opgenomen en deze beoordeeld. Op basis hiervan is de rapportage van voorlopige bevindingen opgesteld.

Het college van burgemeester en wethouders van de gemeente Midden-Drenthe is bij brief van 4 juni 2015 door het CBP ingelicht over de gehanteerde werkwijze.

Het CBP heeft op 30 juni 2015 het Rapport van voorlopige bevindingen vastgesteld. Het CBP heeft de gemeente Midden-Drenthe bij brief van 8 juli 2015 in de gelegenheid gesteld om haar zienswijze op het Rapport van voorlopige bevindingen te geven. Het CBP heeft daarbij tevens verzocht aan te geven of en zo ja welke onderdelen daarvan, volgens de gemeente Midden-Drenthe vertrouwelijke (bedrijfs)gegevens bevatten. De gemeente Midden-Drenthe heeft bij email van 17 september 2015 haar zienswijze ingebracht.

1.6 Juridisch kader

Artikel 13 Wbp bepaalt, voor zover thans van belang, dat de verantwoordelijke passende technische en organisatorische maatregelen ten uitvoer legt om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen. Onder onrechtmatige vormen van verwerking vallen de aantasting van gegevens, onbevoegde kennisneming, wijziging of verstrekking daarvan.

Artikel 13 Wbp behelst het algemeen beveiligingsvoorschrift. Artikel 6.4 Regeling SUWI bevat bepalingen met betrekking tot de inhoud van een verplicht gesteld beveiligingsplan en kan op dit punt worden beschouwd als een wettelijke uitwerking van artikel 13 Wbp. Artikel 6.4, eerste lid, Regeling SUWI stelt onder meer dat de colleges van burgemeester en wethouders zorg dragen voor de beveiliging van de gegevensuitwisselingen die plaatsvinden in het kader van de gezamenlijke elektronische voorzieningen SUWI, tegen inbreuk op de beschikbaarheid, integriteit en vertrouwelijkheid, overeenkomstig hetgeen voor het stelsel van maatregelen en procedures te hanteren normen is bepaald in bijlage I ('Stelselontwerp & Beveiliging Gezamenlijke elektronische Voorzieningen SUWI'). Artikel 6.4, tweede lid, Regeling Suwi bepaalt onder meer dat de colleges van burgemeester en wethouders in een beveiligingsplan aan dienen te geven op welke wijze zij invulling geven aan het eerste lid.

Uit bijlage I ('Stelselontwerp & Beveiliging Gezamenlijke elektronische Voorzieningen SUWI') volgt dat de Suwipartijen onderling en gezamenlijk, met het Bureau Keteninformatisering Werk en Inkomen (BKWI), afspraken maken op de verschillende deelgebieden van informatie-uitwisseling binnen de Suwiketen. De afspraken vinden hun weerslag in diverse concrete producten, onder meer de Keten Service Level Agreement, het SUWI-Gegevens Register, de SUWI-Ketenarchitectuur en de Verantwoordingsrichtlijn Privacy & Beveiliging GeVS.

De verantwoording voor de beveiliging van de (verwerking van) persoonsgegevens via Suwinet is nader uitgewerkt in deze verantwoordingsrichtlijn. Het in de verantwoordingsrichtlijn opgenomen Normenkader GeVS bevat de eisen die gelden als leidraad voor het operationeel management bij het inrichten, de werking en de controleerbaarheid van de organisatorische en technische infrastructuur voor de risicobeheersing van de gegevenshuishouding.

2 BEVINDINGEN

2.1 Beveiligingsbeleid en beveiligingsplan

2.1.1 Norm

Volgens het Normenkader GeVS dient onder meer het beveiligingsplan voor Suwinet te zijn goedgekeurd door het management van de Suwipartij (norm 1.3).

2.1.2 Bevindingen

In de bevindingen van de Inspectie SZW wordt aangegeven dat de gemeente Midden-Drenthe niet beschikt over een beveiligingsplan voor Suwinet dat ook is goedgekeurd door het management. In het huidige informatiebeveiligingsbeleid of –plan wordt niet specifiek op de beveiliging van Suwinet ingegaan.

De gemeente Midden-Drenthe heeft bij haar zienswijze een op 30 juni 2015 door het college van burgemeester en wethouders vastgesteld beveiligingsplan voor Suwinet Midden-Drenthe overgelegd.

2.1.3 Beoordeling

De gemeente Midden-Drenthe heeft een door het college van burgemeester en wethouders vastgesteld beveiligingsplan voor Suwinet. De gemeente Midden-Drenthe handelt hiermee conform norm 1.3 uit het Normenkader GeVS en daarmee op dit punt tevens conform artikel 13 Wbp.

2.2 Uitdragen informatiebeveiligingsbeleid en beveiligingsplan

2.2.1 Norm

Norm 1.4 van het Normenkader GeVS bepaalt onder meer dat het beveiligingsplan voor Suwinet moet worden uitgedragen in de organisatie. Dit betekent dat het beveiligingsplan kenbaar moet zijn voor de (potentiële) gebruikers. Dit kan door middel van bijeenkomsten, workshops, berichtgeving op intranet en e-mails.

2.2.2 Bevindingen

Uit de bevindingen van de Inspectie SZW blijkt dat de gemeente Midden-Drenthe geen beveiligingsplan voor Suwinet heeft dat wordt uitgedragen in de organisatie.

Uit de informatie die de gemeente Midden-Drenthe bij de zienswijze heeft gevoegd, blijkt dat het beveiligingsplan Suwinet Midden-Drenthe centraal beschikbaar is gesteld voor het personeel via intranet, en dat door middel van een presentatie aandacht is gevraagd voor de beveiliging van Suwinet en het Beveiligingsplan Suwinet Midden-Drenthe.

2.2.3 Beoordeling

De gemeente Midden-Drenthe het SUWI draagt het beveiligingsplan voor Suwinet uit in de organisatie. Hiermee handelt de gemeente Midden-Drenthe conform norm 1.4 van het Normenkader GeVS en daarmee tevens conform artikel 13 Wbp.

2.3 Evaluatie Informatiebeveiligingsbeleid en SUWI beveiligingsplan

2.3.1 Norm

Norm 1.5 van het Normenkader GeVS bepaalt onder meer dat het beveiligingsplan voor Suwinet jaarlijks wordt geëvalueerd.

2.3.2 Bevindingen

De gemeente Midden-Drenthe voert volgens de bevindingen van de Inspectie SZW geen evaluatie uit op de werking van het beveiligingsplan voor Suwinet.

Uit de zienswijze van de gemeente Midden-Drenthe blijkt dat het beveiligingsplan Suwinet Midden-Drenthe minder dan één jaar geleden in werking is getreden. De Security Officer heeft volgens het beveiligingsplan Suwinet Midden-Drenthe de taak om jaarlijks een evaluatie uit te voeren.

2.3.3 Beoordeling

Gelet op de korte periode die is verstreken na de inwerkingtreding van het beveiligingsplan voor Suwinet is er nog geen reële mogelijkheid geweest voor een evaluatie. De gemeente Midden-Drenthe handelt op dit punt thans niet in strijd met norm 1.5 van het Normenkader GeVS. Hiermee handelt de gemeente Midden-Drenthe evenmin in strijd met artikel 13 Wbp.

2.4 Functiescheiding

2.4.1 Norm

De taken, verantwoordelijkheden en bevoegdheden ten aanzien van het gebruik, de inrichting, het beheer en de beveiliging van Suwinet gegevens, applicaties, processen en infrastructuur moeten volgens norm 2.2 van het Normenkader GeVS zijn beschreven en duidelijk en afhankelijk van de schaalomvang van de organisatie gescheiden zijn belegd.

2.4.2 Bevindingen

Volgens de bevindingen van de Inspectie SZW kan de functiescheiding op basis van de beschikbaar gestelde informatie gedurende de onderzoeksperiode niet worden vastgesteld. De gemeente maakt gebruik van generieke functiebeschrijvingen die voor het gehele gemeentelijke apparaat gelden. Hierin past volgens de gemeente niet een specifieke toevoeging voor bevoegdheden binnen Suwinet. Verder heeft de gemeente geen informatie verstrekt over de wijze waarop de taken, verantwoordelijkheden en bevoegdheden ten aanzien van het gebruik, de inrichting, het beheer en de beveiliging van Suwinet gegevens, applicaties, processen en infrastructuur zijn beschreven en zijn belegd.

Uit de zienswijze van de gemeente Midden-Drenthe blijkt dat een uitgebreide beschrijving van taken, verantwoordelijkheden en bevoegdheden ten aanzien van het gebruik van Suwinet in het Beveiligingsplan Suwinet is opgenomen. Hieruit blijkt onder meer dat de verantwoordelijkheid voor de uitvoering van taken, borging van rechtmatig gebruik, de controle op het gebruik van Suwinet en het beheer van autorisaties gescheiden is belegd.

2.4.3 Beoordeling

Omdat de taken, verantwoordelijkheden en bevoegdheden ten aanzien van het gebruik, het beheer en de beveiliging van Suwinet gegevens zijn beschreven en vastgesteld, kan worden geconcludeerd dat de gemeente Midden-Drenthe conform norm 2.2 van het Normenkader GeVS handelt. De gemeente Midden-Drenthe handelt hiermee op dit punt tevens conform artikel 13 Wbp.

2.5 De Security Officer

2.5.1 Norm

De Security Officer dient volgens norm 2.3 van het Normenkader GeVS in het kader van Suwinet beveiligingsprocedures en –maatregelen te beheren. De Security Officer beheerst maatregelen in het kader van Suwinet, zodanig dat de beveiliging van Suwinet overeenkomstig wettelijke eisen is geïmplementeerd, bevordert en adviseert over de beveiliging van Suwinet, verzorgt rapportages over de status, controleert of met betrekking tot de beveiliging van Suwinet de maatregelen worden nageleefd, evalueert de uitkomsten en doet voorstellen tot implementatie c.q. aanpassing van plannen op het gebied van de beveiliging van Suwinet. De Security Officer rapporteert rechtstreeks aan het hoogste management.

2.5.2 Bevindingen

In de bevindingen van de Inspectie SZW wordt aangegeven dat bij besluit van 7 januari 2014 door het college van burgemeester en wethouders een Security Officer ten behoeve van het gebruik van Suwinet is aangesteld. Deze is formeel gemandateerd om specifieke rapportages op te vragen bij het BKWI. Een specifieke functiebeschrijving van de Security Officer ontbreekt. Hierdoor is zijn takenpakket niet verder uitgewerkt en vastgesteld. Het is onduidelijk of de Security Officer direct over de beveiliging van Suwinet heeft gerapporteerd aan het hoogste management.

Uit de zienswijze van de gemeente Midden-Drenthe blijkt dat de Security Officer (CISO) beveiligingsprocedures en -maatregelen in het kader van Suwinet beheert, zodanig dat de beveiliging van Suwinet overeenkomstig wettelijke eisen is geïmplementeerd. De Security Officer bevordert en adviseert over de beveiliging van Suwinet, verzorgt rapportages over de status, controleert dat, met betrekking tot de beveiliging van Suwinet, de maatregelen worden nageleefd, evalueert de uitkomsten en adviseert en doet voorstellen tot implementatie c.q. aanpassing van plannen op het gebied van de beveiliging van Suwinet. Verder heeft de gemeente Midden-Drenthe informatie (rapportages) overgelegd waaruit blijkt dat de Security Officer activiteiten uitvoert ten aanzien van de beveiliging van Suwinet. De gemeente Midden-Drenthe heeft echter geen informatie overgelegd waaruit blijkt dat de Security Officer rechtstreeks aan het hoogste management rapporteert.

2.5.3 Beoordeling

Niet is gebleken dat de Security Officer van de gemeente Midden-Drenthe rechtstreeks aan het hoogste management rapporteert. De gemeente Midden-Drenthe handelt hiermee in strijd met norm 2.3 van het Normenkader GeVS, en daarmee tevens met artikel 13 Wbp.

2.6 Autorisatieprocedure

2.6.1 Norm

Norm 13.1 van het Normenkader bepaalt dat de Suwipartij op basis van een formele procedure de gebruikers die toegang hebben tot de Suwinet applicaties autoriseert en registreert. In deze procedure moeten de volgende elementen zijn opgenomen.

- Het verlenen van toegang tot de benodigde gegevens op basis van de uit te voeren functie / taken;
- Het uniek identificeren van elke gebruiker tot één persoon;

- Het goedkeuren van de aanvraag voor toegangsrechten door de manager of een gemandateerde;
- Het tijdig aanpassen of wijzigen van de autorisatie bij functiewijziging of vertrek;
- Het benaderen van de Suwi-databestanden door gebruikers mag alleen plaatsvinden via applicatieprogrammatuur (tenzij sprake is van calamiteiten).

2.6.2 Bevindingen

De gemeente Midden-Drenthe heeft volgens de bevindingen van de Inspectie SZW geen formele autorisatieprocedure.

De gemeente heeft bij haar zienswijze een autorisatiematrix overgelegd aan de hand waarvan autorisaties worden gekoppeld aan specifieke rollen. De gemeente heeft echter geen autorisatieprocedure overgelegd.

2.6.3 Beoordeling

Niet is gebleken dat de gemeente Midden-Drenthe over een formele procedure beschikt op basis waarvan de gebruikers die toegang hebben tot de Suwinet applicaties worden geautoriseerd en geregistreerd. De gemeente Midden-Drenthe handelt hiermee in strijd met norm 13.1 van het Normenkader en daarmee tevens met artikel 13 Wbp.

2.7 Controle op verleende toegangsrechten

2.7.1 Norm

Norm 13.5 van het Normenkader GeVS bepaalt dat de controle op verleende toegangsrechten en gebruik meerdere keren per jaar plaats dient te vinden. Deze controle betreft een interne controle op rechten en gebruik van Suwinet, waarbij de van het BKWI verkregen informatie over het gebruik van persoonsgegevens via Suwinet geanalyseerd dient te worden.

2.7.2 Bevindingen

Volgens de bevindingen van de Inspectie SZW heeft de gemeente Midden-Drenthe niet aangetoond op welke wijze de controle plaatsvindt en welke criteria hierbij worden gehanteerd. Er is evenmin verslag opgemaakt van de controle en analyse.

Naar aanleiding van de zienswijze kan worden vastgesteld dat de gemeente Midden-Drenthe een procedure voor de beoordeling gebruik Suwinet heeft. Hierin wordt onder meer aangegeven dat de afdeling Samenlevingszaken eens per maand een standaard generieke en een specifieke BKWI rapportage opvraagt. Over de BKWI rapportages wordt ieder kwartaal gerapporteerd. Deze rapportages worden voorgelegd aan het afdelingshoofd.

De gemeente Midden-Drenthe heeft verschillende verslagen met betrekking tot de controle op het gebruik van Suwinet over de eerste helft van 2015 bijgevoegd. Omdat meerdere verslagen zijn meegezonden, heeft de gemeente Midden-Drenthe aangetoond dat de controle op het gebruik meerdere keren per jaar plaatsvindt.

2.7.3 Beoordeling

De gemeente Midden-Drenthe heeft aangetoond dat de van het BKWI verkregen informatie over het gebruik van persoonsgegevens via Suwinet wordt gecontroleerd

en geanalyseerd. Dit is conform norm 13.5 van het Normenkader GeVS en daarmee op dit punt tevens conform artikel 13 Wbp.

3 CONCLUSIES

Uit het onderzoek van het CBP volgt dat de Wbp wordt overtreden, omdat de gemeente Midden-Drenthe twee normen uit het Normenkader GeVS (Gezamenlijke elektronische Voorzieningen SUWI) niet of onvoldoende naleeft.

1. Niet is gebleken dat de Security Officer van de gemeente Midden-Drenthe rechtstreeks aan het hoogste management rapporteert. De gemeente Midden-Drenthe handelt hiermee in strijd met norm 2.3 van het Normenkader GeVS, en daarmee tevens met artikel 13 Wbp;
2. Niet is gebleken dat de gemeente Midden-Drenthe over een formele procedure beschikt op basis waarvan de gebruikers die toegang hebben tot de Suwinet applicaties worden geautoriseerd en geregistreerd. De gemeente Midden-Drenthe handelt hiermee in strijd met norm 13.1 van het Normenkader en daarmee tevens met artikel 13 Wbp.

Het College bescherming persoonsgegevens,
Voor het College,

Mr. W.B.M. Tomesen
Lid van het College

BIJLAGE I: REACTIE CBP OP DE ZIENSWIJZE VAN DE GEMEENTE MIDDEN-DRENTHE

Zienswijze gemeente Midden-Drenthe

De gemeente Midden-Drenthe heeft per email verschillende documenten opgestuurd, zonder nadere motivering.

Reactie CBP

Het CBP zal hieronder puntsgewijze reageren op de zienswijze van de gemeente Midden-Drenthe.

1. Het beveiligingsplan

De gemeente Midden-Drenthe heeft een op 30 juni 2015 door het college van burgemeester en wethouders van de gemeente vastgestelde Beveiligingsplan Suwinet Midden-Drenthe overgelegd. De gemeente Midden-Drenthe voldoet hiermee aan norm 1.3 van het Normenkader GeVS. De overtreding van artikel 13 Wbp is hiermee beëindigd. De bevindingen zijn op dit punt aangepast.

2. Uitdragen beveiligingsplan

Uit de informatie die de gemeente Midden-Drenthe bij de zienswijze heeft gevoegd, blijkt dat het Beveiligingsplan Suwinet Midden-Drenthe centraal beschikbaar is gesteld voor het personeel via intranet, en dat door middel van een presentatie aandacht is gevraagd voor de beveiliging van Suwinet en het beveiligingsplan Suwinet Midden-Drenthe. De gemeente Midden-Drenthe voldoet hiermee aan norm 1.4 van het Normenkader GeVS. De overtreding van artikel 13 Wbp is hiermee beëindigd. De bevindingen zijn op dit punt aangepast.

3. Evaluatie beveiligingsplan

Gezien de korte periode na de inwerkingtreding van het beveiligingsplan Suwinet Midden-Drenthe en de bij de Security Officer belegde taak om jaarlijks een evaluatie uit te voeren, kan worden geconcludeerd dat de gemeente Midden-Drenthe op dit punt voldoet aan norm 1.5 van het Normenkader GeVS. De overtreding van artikel 13 Wbp is hiermee beëindigd. De bevindingen zijn op dit punt aangepast.

4. Functiescheiding

In het beveiligingsplan Suwinet Midden-Drenthe is een uitgebreide beschrijving van taken, verantwoordelijkheden en bevoegdheden ten aanzien van het gebruik van Suwinet opgenomen. Hieruit blijkt onder meer dat de verantwoordelijkheid voor de uitvoering van taken, borging van rechtmatig gebruik, de controle op het gebruik van Suwinet en het beheer van autorisaties gescheiden is belegd. De gemeente Midden-Drenthe voldoet op dit punt aan norm 1.5 van het Normenkader GeVS. De overtreding van artikel 13 Wbp is hiermee beëindigd. De bevindingen zijn op dit punt aangepast.

5. Security Officer

In het beveiligingsplan Suwinet Midden-Drenthe wordt aangegeven dat de Security Officer (CISO) beveiligingsprocedures en -maatregelen in het kader van Suwinet beheert, zodanig dat de beveiliging van Suwinet overeenkomstig wettelijke eisen is geïmplementeerd. De Security Officer bevordert en adviseert over de beveiliging van Suwinet, verzorgt rapportages over de status, controleert dat, met betrekking tot de beveiliging van Suwinet, de maatregelen worden nageleefd, evalueert de uitkomsten

en adviseert en doet voorstellen tot implementatie c.q. aanpassing van plannen op het gebied van de beveiliging van Suwinet. Verder heeft de gemeente Midden-Drenthe informatie (rapportages) overgelegd waaruit blijkt dat de Security Officer activiteiten uitvoert ten aanzien van de beveiliging van Suwinet. De gemeente Midden-Drenthe heeft echter geen informatie overgelegd waaruit blijkt dat de Security Officer rechtstreeks aan het hoogste management rapporteert. Dit laatste is niet conform norm 2.3 van het Normenkader GeVS. De overtreding van artikel 13 is op dit punt niet beëindigd. De bevindingen zijn naar aanleiding van bovenstaande aangepast.

6. Autorisatieprocedure

De gemeente heeft bij haar zienswijze een autorisatiematrix overgelegd aan de hand waarvan autorisaties worden gekoppeld aan specifieke rollen. De gemeente heeft echter geen autorisatieprocedure en overgelegd. De gemeente Midden-Drenthe voldoet op dit punt niet aan norm 13.1 van het Normenkader GeVS. De overtreding van artikel 13 Wbp is hiermee niet beëindigd. De bevindingen zijn op dit punt aangepast.

7. Controle op autorisaties en gebruik

De gemeente Midden-Drenthe heeft een vastgestelde procedure voor de beoordeling gebruik Suwinet. Hierin wordt onder meer aangegeven dat de afdeling Samenlevingszaken eens per maand een standaard generieke en een specifieke BKWI rapportage opvraagt. Over de BKWI rapportages wordt ieder kwartaal gerapporteerd. Deze rapportages worden voorgelegd aan het afdelingshoofd.

De gemeente Midden-Drenthe heeft verschillende verslagen met betrekking tot de controle op het gebruik van Suwinet over de eerste helft van 2015 bijgevoegd. Omdat er meerdere verslagen zijn meegezonden, heeft de gemeente Midden-Drenthe aangetoond dat de controle op het gebruik meerdere keren per jaar plaatsvindt.

De gemeente Midden-Drenthe voldoet op dit punt aan norm 13.5 van het Normenkader GeVS. De overtreding van artikel 13 Wbp is hiermee beëindigd.