COLLEGE BESCHERMING PERSOONSGEGEVENS

POSTADRES Postbus 93374, 2509 AJ Den Haag **BEZOEKADRES** Juliana van Stolberglaan 4-10

TEL 070 - 88 88 500 **FAX** 070 - 88 88 501 **INTERNET** www.cbpweb.nl

College bescherming persoonsgegevens

Onderzoek naar de beveiliging van persoonsgegevens via Suwinet Gemeente Moerdijk

z2015-00401

Openbare versie
Rapport van bevindingen

November 2015

DATUM November 2015

INHOUDSOPGAVE

SAMENVATTING

Uit het onderzoek van het College bescherming persoonsgegevens (CBP) volgt dat de Wet bescherming persoonsgegevens (Wbp) wordt overtreden, omdat de gemeente Moerdijk één norm uit het Normenkader GeVS (Gezamenlijke elektronische Voorzieningen SUWI) niet of onvoldoende naleeft: Niet is gebleken dat de Security Officer van de gemeente Moerdijk in de praktijk rechtstreeks rapporteert aan het hoogste management. De gemeente Moerdijk handelt hiermee in strijd met norm 2.3 van het Normenkader GeVS, 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 betreffende fraude of recidive[1]) 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 achterhalen[2]. Adequate beveiligingsmaatregelen kunnen er voor zorgen dat dergelijke incidenten worden voorkomen.

[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

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 ontbrak[3]. 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.

Op 4 juni 2015 is de definitieve rapportage van dit laatstbedoelde onderzoek 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 Moerdijk.

1.3 Doel en reikwijdte van het onderzoek

Het onderzoek beoogt vast te stellen of de gemeente Moerdijk, 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 (norm1.5);
4. Functiescheiding (norm 2.2);
5. De functie van Security Officer (norm 2.3);

[3] https:/ / cbpweb.nl/ nl/ nieuws/ cbp-persoonsgegevens-suwinet-niet-goed-beveiligd

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 Moerdijk 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 Moerdijk 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 Moerdijk 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 Moerdijk vertrouwelijke (bedrijfs)gegevens bevatten.
De gemeente Moerdijk heeft bij brief van 13 augustus 2015 haar zienswijze, alsmede een reactie op de (bedrijfs) vertrouwelijkheidstoets, 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 onder andere 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.

Het normenkader voor de wijze waarop verantwoording dient te worden afgelegd voor de beveiliging van de (verwerking van) persoonsgegevens via Suwinet is nader uitgewerkt in de 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 er in het informatiebeveiligingsbeleid of –plan van de gemeente Moerdijk niet specifiek op de beveiliging van Suwinet wordt ingegaan.

Uit de zienswijze van de gemeente Moerdijk blijkt dat de gemeente een Suwinet beveiligingsplan heeft dat op 16 juni 2015 door burgemeester en wethouders bij besluit is vastgesteld.

2.1.3 Beoordeling

De gemeente Moerdijk heeft een door het college van burgemeester en wethouders vastgesteld beveiligingsplan voor Suwinet. Hiermee handelt de gemeente Moerdijk op dit punt conform norm 1.3 van het Normenkader GeVS en daarmee 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 aantoonbaar moet zijn uitgedragen in de organisatie. 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 Moerdijk geen beveiligingsplan voor Suwinet heeft en dat er daarom evenmin sprake kan zijn van een beveiligingsplan dat wordt uitgedragen in de organisatie.

Uit de informatie bij de zienswijze van de gemeente Moerdijk blijkt dat in het Suwinet beveiligingsplan thans een passage is opgenomen over bewustwording. Hierin wordt aangegeven dat

- het Suwi informatiebeveiligingsbeleid en –plan voor alle medewerkers beschikbaar zijn via intranet;
- minimaal twee keer per jaar actie zal worden ondernomen om de medewerkers te attenderen op het bestaan van het informatiebeveiligingsbeleid en-plan;

- nieuwe medewerkers worden op het plan gewezen via het afdelingsmanagement met de opdracht er kennis van te nemen;
- bij functioneringsgesprekken zal bij medewerkers die Suwinet gebruiken worden ingegaan op informatiebeveiliging en Suwinet.

De gemeente Moerdijk zal blijkens het Suwinet beveiligingsplan op verschillende wijzen de aandacht van de medewerkers vragen voor het Suwinet beveiligingsplan. Ook heeft de gemeente het Suwinet beveiligingsplan centraal voor alle medewerkers toegankelijk gemaakt. Ter onderbouwing hiervan zijn diverse schermafdrukken van de mailwisseling en intranet publicaties zowel van de gemeente Moerdijk als van de Intergemeentelijke Sociale Dienst (ISD) Werkplein Hart van West-Brabant, die een aantal aan de wet SUWI gerelateerde taken voor de gemeente uitvoert, door de gemeente Moerdijk overgelegd.

2.2.3 Beoordeling

De gemeente Moerdijk handelt op dit punt conform norm 1.4 van het Normenkader GeVS en 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 Moerdijk heeft volgens de bevindingen van de Inspectie SZW niet aangetoond dat het beveiligingsplan van het Suwinet wordt geëvalueerd. De evaluatie betreft het algemene beveiligingsbeleid, niet specifiek het beveiligingsplan met betrekking tot Suwinet.

Uit de informatie bij de zienswijze van de gemeente Moerdijk blijkt dat het Suwinet beveiligingsplan op 16 juni 2015 is goedgekeurd. Hierin is opgenomen dat het plan jaarlijks zal worden geëvalueerd en indien nodig geactualiseerd.

2.3.3 Beoordeling

Gelet op de korte periode die is verstreken na de inwerkingtreding van het beveiligingsplan voor Suwinet en de indiening van de zienswijze is er nog geen reële mogelijkheid geweest voor een evaluatie. De gemeente Moerdijk handelt op dit punt thans niet in strijd met norm 1.5 van het Normenkader GeVS. Hiermee handelt de gemeente Moerdijk 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 heeft de gemeente Moerdijk de taken, verantwoordelijkheden en bevoegdheden ten aanzien van het gebruik, het beheer en de beveiliging van Suwinet gegevens niet of onvoldoende formeel beschreven. Verder heeft de gemeente de functiescheiding niet aantoonbaar geformaliseerd.

Uit de informatie bij de zienswijze van de gemeente Moerdijk blijkt dat de taken, verantwoordelijkheden en bevoegdheden ten aanzien van het gebruik, het beheer en de beveiliging van Suwinet gegevens formeel zijn beschreven en de functiescheiding aantoonbaar is geformaliseerd.

2.4.3 Beoordeling

De functiescheiding is voldoende doorgevoerd. De gemeente Moerdijk handelt hiermee conform norm 2.2. van het Normenkader GeVS. De gemeente Moerdijk 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 geen Security Officer is aangesteld, een taakomschrijving van de Security Officer ontbreekt en de Security Officer niet rechtstreeks aan het hoogste

management rapporteert. Er zijn in 2014 geen duidelijk waarneembare activiteiten van een Security Officer geweest.

Uit de opgestuurde informatie bij de zienswijze van de gemeente Moerdijk blijkt dat de gemeente Moerdijk een Security Officer heeft aangesteld en een taakomschrijving van de Security Officer in het beveiligingsplan Suwinet (d.d. 16 juni 2015) heeft opgenomen. Uit deze taakomschrijving blijkt ook dat de Security Officer rechtstreeks aan het college van burgemeester en wethouders dient te rapporteren. De gemeente heeft ook twee verslagen meegestuurd waaruit blijkt dat de Security Officer generieke rapportages over gebruik opvraagt en analyseert. De Security Officer heeft een collegevoorstel voor de vaststelling van het beleidsnotitie "Beveiliging Suwinet 2015 gemeente Moerdijk opgesteld, waarin achtergrondinformatie staat met betrekking tot het voorstel om de beleidsnotitie vast te stellen. De gemeente heeft echter geen informatie opgestuurd waaruit blijkt dat de Security Officer in de praktijk rechtstreeks aan het college van burgemeester en wethouders rapporteert (bijvoorbeeld door middel van verslagen en rapportages).

2.5.3 Beoordeling

Nu niet is gebleken dat de Security Officer rechtstreeks aan het hoogste management rapporteert, handelt de gemeente Moerdijk 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 Moerdijk heeft volgens de bevindingen van de Inspectie SZW geen formele autorisatieprocedure.

Uit de informatie bij de zienswijze van de gemeente Moerdijk blijk dat de gemeente een vastgelegde autorisatieprocedure en een autorisatiematrix heeft. Hieruit blijkt dat de gemeente de gebruikers die toegang hebben tot de Suwinet applicaties op basis van een formele procedure autoriseert en registreert.

2.6.3 Beoordeling

De gemeente Moerdijk handelt op dit punt in overeenstemming met norm 13.1 van het Normenkader GeVS daarmee tevens in overeenstemming 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 Moerdijk in 2014 geen rapportages opgevraagd bij het BKWI en heeft er geen analyse plaatsgevonden van bij het BKWI verkregen informatie over het gebruik van persoonsgegevens via Suwinet.

Uit informatie bij de zienswijze van de gemeente Moerdijk blijkt dat in 2015 rapportages zijn opgevraagd bij het BKWI, en dat de bij het BKWI verkregen informatie over het gebruik van gegevens via Suwinet is geanalyseerd.

2.7.3 Beoordeling

De gemeente Moerdijk handelt hiermee conform norm 13.5 van het Normenkader GeVS en daarmee tevens met artikel 13 Wbp.

3 CONCLUSIES

Uit het onderzoek van het CBP volgt dat de Wbp wordt overtreden, omdat de gemeente Moerdijk één norm uit het Normenkader GeVS (Gezamenlijke elektronische Voorzieningen SUWI) niet of onvoldoende naleeft: Niet is gebleken dat de Security Officer van de gemeente Moerdijk in de praktijk rechtstreeks rapporteert aan het hoogste management. De gemeente Moerdijk handelt hiermee in strijd met norm 2.3 van het Normenkader GeVS, 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 ZIENSWIJZE GEMEENTE MOERDIJK

Zienswijze gemeente Moerdijk

In haar zienswijze gaat de gemeente Moerdijk per onderzochte norm in op de acties de zijn ondernomen naar aanleiding van de bevindingen van de Inspectie SZW.

1. Norm 1.3

De gemeente geeft aan dat is besloten een apart Beveiligingsplan Suwinet vast te stellen. Ter onderbouwing hiervan zijn het beveiligingsplan Suwinet Gemeente Moerdijk en de schermafdruk van het vaststellingsbesluit bijgevoegd.

2. Norm 1.4

Inmiddels er is een specifiek voor het Suwinet opgesteld beveiligingsplan opgesteld. Dit plan is meerdere malen onder de aandacht gebracht van de medewerkers en wel op de volgende wijze:

- De medewerkers zijn persoonlijk op de hoogte gesteld;
- De medewerkers hebben via de mail het beleid toegestuurd gekregen;
- De medewerkers hebben een verklaring gebruik Suwinet getekend;
- Via intranet is melding gemaakt van vaststelling van het Suwinet beveiligingsplan. Dit plan is via intranet tevens in te zien;
- De Suwinet kalender is uitgereikt aan de medewerkers;
- De genoemde acties zijn ook uitgevoerd naar de oud-medewerkers van de gemeente Moerdijk. Dit is in nauw overleg gegaan ISD werkplein.

Ter onderbouwing hiervan zijn diverse schermafdrukken van de mailwisseling en intranet publicaties zowel van de gemeente Moerdijk als van de ISD Werkplein Hart van West-Brabant.

3. Norm 1.5

Naar aanleiding van de bevindingen van de Inspectie SZW hebben verschillende gesprekken plaatsgevonden met diverse betrokken medewerkers, teamhoofden, managers en de bestuurlijk verantwoordelijke wethouder voor informatiebeveiliging maar ook met diverse medewerkers van de ISD. Voor de gemeente Moerdijk heeft dat geleid tot het opstellen van een advies aan het college van burgemeester en wethouders om de maatregelen aan te scherpen en deze vast te leggen in een Suwinet beveiligingsplan. Met de ISD is de afspraak gemaakt dat de ISD zorg draagt voor het opstellen van een eigen Suwinet beveiligingsplan. Dit plan is recentelijk door het management van de ISD vastgesteld en zal worden aangeboden aan het college van burgemeester en wethouders van de gemeente Moerdijk en de overige aangesloten gemeenten.

Ter onderbouwing van deze reactie is het advies aan burgemeester en wethouders over de bevindingen en de te treffen maatregelen betreffende Suwinet beveiliging bijgevoegd. Dit advies is in de vergadering van het college van burgemeester en wethouders van 16 juni 2015 besproken en vastgesteld.

4. Norm 1.4

Naar aanleiding van de bevindingen van de Inspectie SZW is in het nieuw opgestelde Suwinet beveiligingsplan een beschrijving gemaakt van de taken en verantwoordelijkheden. De gemeente Moerdijk heeft een functiescheiding aangebracht voor de volgende rollen:

- Gebruikers: het gebruik van Suwinet;
- Autorisatiebeheer: toekennen van autorisaties;
- Teamhoofd/toezichthouder gebruik: aanwijzing en toekenning van bevoegdheden gebruikers.

De taken op het gebied van controle op gebruik Suwinet zijn apart beschreven onder norm 13.5 controle op toegang en gebruik.

Ter onderbouwing wordt door de gemeente Moerdijk verwezen naar het onderdeel 'Norm 2.2 Taken, verantwoordelijkheden en bevoegdheden' in het Suwinet beveiligingsplan en de bijlage bij het plan: "Overzicht gebruikers, rollen en bevoegdheden Suwinet gemeente Moerdijk". Bij het opstellen hiervan is onder meer gebruik gemaakt van het door het BKWI ontwikkelde document Toegangsrechten GSD accounts voor Suwinet.docx. Bovendien wordt verwezen naar de beschrijving van de controle op toegang en gebruik onder norm 13.5 in het Suwinet beveiligingsplan.

De formalisatie van de functiescheiding is aangetoond door vaststelling van het Suwinet beveiligingsplan met bijlagen door het college van burgemeester en wethouders.

5. Norm 2.3

In het algemene informatiebeveiligingsbeleid en -plan van de gemeente Moerdijk is de organisatie van informatiebeveiliging beschreven en ook de rol van de Security Officer (informatiebeveiligingsfunctionaris). Bevoegdheden ten aanzien van Suwinet zijn daarin niet expliciet beschreven. Naar aanleiding van de bevindingen is nu ook in het Suwinet beveiligingsplan de functiebeschrijving van de Security Officer opgenomen die daarmee ook ten aanzien van Suwinet expliciet is vastgesteld.

De bevinding dat er in 2014 geen duidelijk waarneembare activiteiten van een Security Officer zijn geweest, geldt niet in zijn algemeenheid, doch wellicht wel voor Suwinet. Als reactie op de bevindingen van de Inspectie SZW heeft de Security Officer in 2015 het initiatief genomen om verbeteracties op gang te zetten en het college te adviseren over het treffen van de nodige maatregelen. Met de toezichthouders gebruik heeft een beoordeling plaatsgevonden van de rapportage gebruik van het eerste halfjaar 2015. Dit gesprek heeft ook plaatsgevonden met een vertegenwoordiger van de ISD in verband met het gebruik van het account van Moerdijk door een aantal medewerkers van de ISD.
De Security Officer heeft zelf diverse detailrapportages opgevraagd bij de Suwinet servicedesk om zich een oordeel te vormen over het gebruik van Suwinet over het eerste halfjaar van 2015. Daarnaast heeft de Security Officer het initiatief genomen om in overleg met de ISD, om zolang men gebruik maakt van het account van Moerdijk, hierover afspraken te maken.

6. Norm 13.1

Als reactie op deze bevinding is in het Suwinet beveiligingsplan een aparte autorisatieprocedure opgenomen. Bij het toekennen van autorisaties is en wordt gebruik gemaakt van het door het BKWI ontwikkelde document 'Toegangsrechten GSD accounts voor Suwinet.docx. De toestemming voor toekenning of het intrekken van de autorisatie voor het gebruik van Suwinet geschiedt schriftelijk door de

toezichthouder/teamhoofd. Voor de autorisatieprocedure verwijst de gemeente Moerdijk naar het Suwinet beveiligingsplan, waar onder norm 13.1 de beschrijving hiervan is opgenomen. Bijgevoegd zijn toekenningen van autorisaties van de medewerkers van de ISD. Tevens is een actueel overzicht van de gebruikers en toegekende autorisaties van Suwinet Inkijk bijgevoegd.

7. Norm 13.5

Als reactie op deze bevinding is in het Suwinet beveiligingsplan de procedure voor de controle op de toegangsrechten en het gebruik beschreven. Door de teamhoofden/toezichthouders gebruik zijn de rapportages over het eerste halfjaar opgevraagd. Nadat men zelf een oordeel had gevormd, zijn de rapportages besproken met de Security Officer. De Security Officer heeft zelf diverse detailrapportages opgevraagd bij de Suwinet servicedesk om zich een oordeel te vormen over het gebruik van Suwinet over het eerste halfjaar van 2015. In verband met de bijzondere situatie dat de medewerkers van de ISD eveneens gebruik maken van het Suwinet account van de gemeente Moerdijk heeft er ook een apart gesprek plaatsgevonden met de ISD. Zowel de rapportages gebruik als de door de Security Officer opgevraagde specifieke rapportage gaven geen aanleiding tot verder onderzoek.

Ter onderbouwing van bovenstaande verwijst de gemeente Moerdijk naar het Suwinet beveiligingsplan, waar onder 13.5 de procedure is beschreven. Tevens verwijst de gemeente Moerdijk naar de Verklaring rechtmatig gebruik Suwinet waarin onder andere staat beschreven dat de activiteiten van gebruikers gelogd worden en dat er controles uitgevoerd (kunnen) worden op het rechtmatig gebruik. Deze verklaring is door alle gebruikers ondertekend. Bijgevoegd zijn ook het verslag van de analyses en bespreking hiervan met verschillende toezichthouders.

Reactie CBP

Het CBP gaat hieronder puntsgewijs in op de zienswijze van de gemeente Moerdijk.

1. Norm 1.3

De gemeente Moerdijk heeft een Suwinet beveiligingsplan dat op 16 juni 2015 door burgemeester en wethouders bij besluit is vastgesteld. De gemeente Moerdijk handelt hiermee conform norm 1.3 van het Normenkader GeVS. De overtreding van artikel 13 Wbp is op dit punt beëindigd.

2. Norm 1.4

In het Suwinet beveiligingsplan is een passage opgenomen over bewustwording. Hierin wordt aangegeven dat

- het Suwi informatiebeveiligingsbeleid en –plan voor alle medewerkers beschikbaar zijn via intranet;
- minimaal twee keer per jaar actie zal worden ondernomen om de medewerkers te attenderen op het bestaan van het informatiebeveiligingsbeleid en-plan;
- nieuwe medewerkers worden op het plan gewezen via het afdelingsmanagement met de opdracht er kennis van te nemen;
- bij functioneringsgesprekken zal bij medewerkers die Suwinet gebruiken worden ingegaan op informatiebeveiliging en Suwinet.

De gemeente Moerdijk heeft op verschillende wijzen de aandacht van de medewerkers gevraagd voor het Suwinet beveiligingsplan. Ook heeft de gemeente het Suwinet beveiligingsplan centraal voor alle medewerkers toegankelijk gemaakt. De gemeente Moerdijk handelt hiermee conform norm 1.4 van het Normenkader GeVS. De overtreding van artikel 13 Wbp is op dit punt beëindigd. De bevindingen zijn op dit punt aangepast.

3. Norm 1.5

Het Suwinet beveiligingsplan is op 16 juni 2015 goedgekeurd. Hierin is opgenomen dat het plan jaarlijks zal worden geëvalueerd en indien nodig geactualiseerd. Gelet op de korte tijd waarin het beveiligingsplan voor het Suwinet in werking zijn getreden, en de afspraken die reeds zijn gemaakt om het dit beveiligingsplan te evalueren, de gemeente Moerdijk op dit punt conform norm 1.5 van het Normenkader GeVS handelt. Op dit punt is de overtreding van artikel 13 beëindigd. De bevindingen zijn op dit punt aangepast.

4. Norm 2.2

Uit het beveiligingsplan Suwinet en het overzicht 'Gebruikers, rollen en bevoegdheden Suwinet gemeente Moerdijk blijkt dat de taken, verantwoordelijkheden en bevoegdheden ten aanzien van het gebruik, het beheer en de beveiliging van Suwinet gegevens formeel zijn beschreven en de functiescheiding aantoonbaar is geformaliseerd. Op grond hiervan kan worden geconcludeerd dat functiescheiding voldoende is doorgevoerd. De gemeente Moerdijk handelt hiermee conform norm 2.2. van het Normenkader GeVS. De gemeente Moerdijk handelt hiermee op dit punt tevens conform artikel 13 Wbp. De bevindingen zijn op dit punt aangepast[4].

5. Norm 2.3

Uit de opgestuurde informatie bij de zienswijze van de gemeente Moerdijk blijkt dat de gemeente Moerdijk een Security Officer heeft aangesteld en een taakomschrijving van de Security Officer in het beveiligingsplan Suwinet heeft opgenomen. Uit deze taakomschrijving blijkt ook dat de Security Officer rechtstreeks aan het college van burgemeester en wethouders dient te rapporteren. De gemeente heeft ook twee verslagen meegestuurd waaruit blijkt dat de Security Officer generieke rapportages over gebruik opvraagt en analyseert. De gemeente heeft echter geen informatie opgestuurd waaruit blijkt dat de Security Officer in de praktijk rechtstreeks aan het college van burgemeester en wethouders rapporteert (bijvoorbeeld door middel van verslagen en rapportages). Hoewel de gemeente Moerdijk belangrijke stappen heeft gezet, is de overtreding op dit punt nog niet beëindigd. De bevindingen worden aan de hand van bovenstaande aangepast. De overtreding van artikel 13 Wbp is echter op dit punt niet beëindigd.

6. Norm 13.1

De gemeente heeft een vastgelegde autorisatieprocedure en een autorisatiematrix overgelegd. Hieruit blijkt dat de gemeente de gebruikers die toegang hebben tot de Suwinet applicaties op basis van een formele procedure autoriseert en registreert. De gemeente Moerdijk handelt hiermee conform norm 13.1 van het Normenkader GeVS. De overtreding is hiermee op dit punt beëindigd. De bevindingen zijn op dit punt aangepast.

[4] NB de normen 2.2 en 2.3 worden in het beveiligingsplan Suwinet door elkaar gehaald op p. 4.

7. Norm 13.5

Uit informatie bij de zienswijze van de gemeente Moerdijk blijkt dat in 2015 rapportages zijn opgevraagd bij BKWI, en dat de bij het BKWI verkregen informatie over het gebruik van gegevens via Suwinet is geanalyseerd. De gemeente Moerdijk handelt hiermee conform norm 13.5 van het Normenkader GeVS. De overtreding is hiermee op dit punt beëindigd. De bevindingen zijn op dit punt aangepast.