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 Werkendam

z2015-00399

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 Werkendam drie normen uit het Normenkader GeVS (Gezamenlijke elektronische Voorzieningen SUWI) niet of onvoldoende naleeft.

1. Niet is gebleken dat de gemeente Werkendam het beveiligingsplan voor Suwinet uitdraagt in de organisatie. Hiermee handelt de gemeente Werkendam in strijd met norm 1.4 van het Normenkader GeVS en daarmee tevens met artikel 13 Wbp;
2. Niet is gebleken dat de Security Officer van de gemeente Werkendam rechtstreeks rapporteert aan het hoogste management. De gemeente Werkendam handelt hiermee in strijd met norm 2.3 van het Normenkader GeVS, en daarmee tevens met artikel 13 Wbp;
3. De controle op verleende toegangsrechten vindt niet plaats conform norm 13.5 van het Normenkader GeVS, waardoor artikel 13 Wbp wordt overtreden.

1 INLEIDING

1.1 Achtergrond

Sinds 2002 wisselen diverse overheidsorganisaties (persoons)gegevens van burgers uit in het domein Werk & Inkomen via de Gemeenschappelijke elektronische Voorziengen 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 Wet (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 tot het minimum 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 naleven. 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 Werkendam.

1.3 Doel en reikwijdte van het onderzoek

Het onderzoek beoogt vast te stellen of de gemeente Werkendam, 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 Werkendam 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 Werkendam 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 Werkendam 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 Werkendam vertrouwelijke (bedrijfs)gegevens bevatten.
De gemeente Werkendam heeft op 25 september 2015 per email een zienswijze ingebracht, waarbij tevens een reactie met betrekking tot de (bedrijfs) vertrouwelijkheidstoets, is 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 de gemeente Werkendam niet over een beveiligingsplan beschikt dat is gericht op Suwinet en dat ook is goedgekeurd door het management.

Uit de zienswijze van de gemeente Werkendam blijkt dat het college van burgemeester en wethouders van de gemeente Werkendam op 30 juni 2015 het Informatiebeveiligingsplan Wet werk en bijstand / Participatiewet heeft vastgesteld.

2.1.3 Beoordeling

De gemeente Werkendam heeft een door het college van burgemeester en wethouders vastgesteld beveiligingsplan voor Suwinet. Hiermee handelt de gemeente Werkendam op dit punt conform norm 1.3 van het Normenkader GeVS en 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 van Suwinet. 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 Werkendam geen beveiligingsplan voor Suwinet heeft dat wordt uitgedragen in de organisatie.

De gemeente Werkendam geeft in haar zienswijze aan dat het veilig gebruik van Suwinet een vast agendapunt is in het maandelijks werkoverleg van het taakveld Participatiewet. Bij het herhaling worden de medewerkers van dit taakveld gewezen op het gebruik van Suwinet. Het CBP heeft echter geen (schriftelijke) stukken ontvangen waaruit blijkt dat het Informatiebeveiligingsplan Wet werk en bijstand / Participatiewet wordt uitgedragen binnen de organisatie.

2.2.3 Beoordeling

Niet is gebleken dat de gemeente Werkendam het beveiligingsplan voor Suwinet voldoende uitdraagt in de organisatie. Hiermee handelt de gemeente Werkendam in strijd met norm 1.4 van het Normenkader GeVS en daarmee tevens met 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 Werkendam 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 Werkendam blijkt dat het beveiligingsplan voor Suwinet vanaf 30 juni 2015 in werking is getreden. Hierin wordt onder andere aangegeven dat het beveiligingsplan van het Suwinet minimaal eenmaal per jaar wordt geëvalueerd.

2.3.3 Beoordeling

De korte periode na de inwerkingtreding van het beveiligingsplan voor Suwinet in acht genomen, en omdat afspraken zijn gemaakt om dit beveiligingsplan jaarlijks te evalueren, handelt de gemeente Werkendam op dit punt thans niet in strijd met norm 1.5 van het Normenkader GeVS en daarmee 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.

Uit de zienswijze van de gemeente Werkendam blijkt dat in het Informatiebeveiligingsplan WWB/Participatiewet een uitgebreide beschrijving van taken, verantwoordelijkheden en bevoegdheden ten

aanzien van het gebruik van Suwinet is opgenomen. Hierin zijn de verantwoordelijkheid voor de uitvoering van taken, borging van rechtmatig gebruik, de controle op het gebruik van Suwinet en het toebedelen en beheer van autorisaties gescheiden belegd.

2.4.3 Beoordeling

De gemeente Werkendam handelt conform norm 2.2. van het Normenkader GeVS. De gemeente Werkendam 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 op basis van de beschikbaar gestelde informatie de taken van de Security Officer gedurende de onderzoeksperiode niet kunnen worden vastgesteld.
Er is door de Security Officer niet gerapporteerd over de beveiliging van Suwinet aan het hoogste management.

Ook uit de zienswijze van de gemeente Werkendam blijkt niet dat de Security Officer rechtstreeks aan het hoogste management rapporteert.

2.5.3 Beoordeling

Niet is gebleken dat de Security Officer rechtstreeks aan het hoogste management rapporteert. De gemeente Werkendam 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 Werkendam heeft volgens de bevindingen van de Inspectie SZW geen formele autorisatieprocedure.

De gemeente heeft bij haar zienswijze een autorisatieprocedure en een autorisatiematrix overgelegd. Hieruit blijkt dat de gemeente Werkendam de gebruikers die toegang hebben tot de Suwinet applicaties op basis van een formele procedure autoriseert en registreert. Het verlenen van toegang tot de benodigde gegevens gebeurt op basis van de uit te voeren functie en taken. Elke gebruiker wordt tot één persoon herleid. Het goedkeuren van de aanvraag voor toegangsrechten gebeurt door de manager. Bij functiewijziging of vertrek wordt de autorisatie aangepast of gewijzigd.

2.6.3 Beoordeling

De gemeente Werkendam handelt hiermee niet in strijd met norm 13.1 van het Normenkader en daarmee evenmin in strijd 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 Werkendam niet aangetoond op welke wijze de controle plaatsvindt en welke criteria hierbij worden gehanteerd. Er is evenmin verslag opgemaakt van de controle en analyse.

Uit de zienswijze van de gemeente Werkendam blijkt het volgende. In het Informatiebeveiligingsplan van de gemeente Werkendam wordt aangegeven dat de Security Officer minimaal eenmaal per jaar gegevens over het gebruik van Suwinet opvraagt. De gemeente Werkendam heeft verder geen informatie opgestuurd waaruit blijkt dat het gebruik van persoonsgegevens via Suwinet meerdere keren per jaar met behulp van de informatie van het BKWI wordt gecontroleerd.

2.7.3 Beoordeling

Niet is gebleken dat de gemeente Werkendam het gebruik van persoonsgegevens via Suwinet meerdere keren per jaar controleert en analyseert met behulp van de van het BKWI verkregen informatie. Dit is in strijd met 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 Werkendam drie normen uit het Normenkader GeVS (Gezamenlijke elektronische Voorzieningen SUWI) niet of onvoldoende naleeft.

1. Niet is gebleken dat de gemeente Werkendam het SUWI Beveiligingsplan uitdraagt in de organisatie. Hiermee handelt de gemeente Werkendam in strijd met norm 1.4 van het Normenkader GeVS en daarmee tevens met artikel 13 Wbp;
2. Niet is gebleken dat de Security Officer van de gemeente Werkendam rechtstreeks rapporteert aan het hoogste management. De gemeente Werkendam handelt hiermee in strijd met norm 2.3 van het Normenkader GeVS, en daarmee tevens met artikel 13 Wbp;
3. De controle op verleende toegangsrechten vindt niet plaats conform norm 13.5 van het Normenkader GeVS, waardoor artikel 13 Wbp wordt overtreden.

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 WERKENDAM

Zienswijze gemeente Werkendam

Naar aanleiding van de brief van het CBP van 8 juli 2015, waarbij het "Onderzoek naar beveiliging van Suwinet / Rapport van voorlopige bevindingen"(kenmerk z2015-00339)" aan de gemeente Werkendam is gezonden deelt de gemeente Werkendam het volgende mee.

1. Naar aanleiding van de brief

Gezien het feit, dat de informatie in de rapportage volgens de gemeente Werkendam al eerder is gepubliceerd in de rapportage van de Inspectie SZW en in dat opzicht niets nieuws bevat, maakt de gemeente Werkendam tegen publicatie geen bezwaar.

2. Naar aanleiding van het rapport van voorlopige bevindingen

Voor zover de gemeente Werkendam uit het Rapport van voorlopige bevindingen heeft kunnen opmaken betreft de uitkomst van uw onderzoek het één op één overnemen van de uitkomsten van de door de Inspectie SZW in haar rapportage van 6 maart 2015 neergelegde uitkomsten. Het schetst volgens de gemeente Werkendam dan ook geen verbazing dat de conclusie op pagina 12 als volgt is geformuleerd: "Uit het onderzoek volgt dat de Wbp wordt overtreden omdat de gemeente Werkendam zeven normen uit het Normenkader GeVS niet of onvoldoende naleeft."
De gemeente Werkendam hecht er waarde aan dat de uitkomsten van het onderzoek door de Inspectie SZW een momentopname is van medio 2014, en de tijd sindsdien niet heeft stilgestaan.

De gemeente Werkendam geeft in haar zienswijze aan dat het college van burgemeester en wethouders van Werkendam in haar brief van 11 februari 2015 aan de Inspectie SZW heeft laten weten, dat de door de Inspectie getrokken conclusie geen recht doet aan de aandacht die de gemeente Werkendam de laatste jaren heeft besteed aan het veilig gebruik van Suwinet. De Inspectie heeft om haar moverende redenen geen aanleiding gezien om haar conceptrapportage inzake Veilig gebruik Suwinet naar aanleiding van de reactie van het college te herzien.

De gemeente Werkendam geeft in haar zienswijze vervolgens een korte reactie van de zeven normen.

1. Norm 1.3 Informatiebeveiligingsplan

Het college van Werkendam heeft op 30 juni 2015 het Informatiebeveiligingsplan Wet werk en bijstand / Participatiewet vastgesteld. Het collegebesluit en beveiligingsplan treft u bijgaand aan.

2. Norm 1.4 Uitdragen van beveiligingsplan in de organisatie

Het veilig gebruik van Suwinet is een vast agendapunt in het maandelijks werkoverleg van het taakveld Participatiewet. Bij herhaling worden de medewerkers van dit taakveld gewezen op het gebruik van Suwinet.

3. Norm 1.5 Jaarlijkse evaluatie

Het plan is op 30 juni 2015 definitief door het college van Werkendam vastgesteld. De eerste jaarlijkse evaluatie op basis van dit plan kan dan ook pas eerst in het voorjaar

2016 worden opgesteld. De opdracht hiertoe zal worden verstrekt aan de Interne Controleur van het taakveld Participatiewet.

4. Norm 2.2 Functiescheiding
Dit is geregeld is het Informatiebeveiligingsplan WWB/PW.

5. Norm 2.3 Werkwijze Security Officer
De werkwijze is beschreven in het Informatiebeveiligingsplan WWB/PW en de invoering van deze werkwijze is inmiddels in volle gang.

6. Norm 13.1 Autorisatie gebruik Suwinet
Ten tijde van het onderzoek van de Inspectie werden de mutaties niet schriftelijk vastgelegd. Dit is inmiddels wel ter hand genomen.

7. Norm 13.5 Controle op rechten en gebruik van Suwinet
Zie opmerking onder 6.

Reactie CBP
Hieronder gaat het CBP puntsgewijs in op de zienswijze van de gemeente Werkendam.

1. Norm 1.3 Informatiebeveiligingsplan
Het college van Werkendam heeft op 30 juni 2015 het Informatiebeveiligingsplan Wet werk en bijstand / Participatiewet vastgesteld. Het collegebesluit en beveiligingsplan zijn bijgevoegd. De gemeente Werkendam handelt hiermee conform norm 1.3 van het Normenkader GeVS. De overtreding van artikel 13 Wbp is hiermee beëindigd. De bevindingen zijn op dit punt aangepast.

2. Norm 1.4 Uitdragen van beveiligingsplan in de organisatie
De gemeente Werkendam geeft aan dat het veilig gebruik van Suwinet een vast agendapunt is in het maandelijks werkoverleg van het taakveld Participatiewet. Bij herhaling worden de medewerkers van dit taakveld gewezen op het gebruik van Suwinet. Het CBP heeft echter geen (schriftelijke) stukken ontvangen waaruit blijkt dat het Informatiebeveiligingsplan Wet werk en bijstand / Participatiewet wordt uitgedragen binnen de organisatie. De overtreding is hiermee niet beëindigd.

3. Norm 1.5 Jaarlijkse evaluatie
Gezien de korte periode na de inwerkingtreding van het Informatiebeveiligingsplan en het gegeven dat een jaarlijkse evaluatie in het Informatiebeveiligingsplan is opgenomen, kan worden geconcludeerd dat de gemeente Werkendam op dit punt voldoet aan norm 1.5 van het Normenkader GeVS. De gemeente Werkendam handelt daarmee op dit punt tevens conform artikel 13 Wbp. De bevindingen zijn op dit punt aangepast.

4. Norm 2.2 Functiescheiding
In het Informatiebeveiligingsplan WWB/Participatiewet 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 toebedelen en beheer van autorisaties gescheiden is belegd. De gemeente Werkendam handelt conform norm 2.2. van het Normenkader GeVS. De gemeente Werkendam handelt hiermee op dit punt tevens conform artikel 13 Wbp. De bevindingen zijn op dit punt aangepast.

5. Norm 2.3 Werkwijze Security Officer

Uit de toegezonden informatie blijkt niet dat de Security Officer rechtstreeks aan het hoogste management rapporteert. Dit is niet conform norm 2.3 van het Normenkader GeVS. De overtreding is op dit punt niet beëindigd.

6. Norm 13.1 Autorisatie gebruik Suwinet

De gemeente heeft bij haar zienswijze een autorisatieprocedure en een autorisatiematrix overgelegd. Hieruit blijkt dat de gemeente Woudenberg de gebruikers die toegang hebben tot de Suwinet applicaties op basis van een formele procedure autoriseert en registreert. Het verlenen van toegang tot de benodigde gegevens gebeurt op basis van de uit te voeren functie en taken. Elke gebruiker wordt tot één persoon herleid. Het goedkeuren van de aanvraag voor toegangsrechten gebeurt door de manager. Bij functiewijziging of vertrek wordt de autorisatie aangepast of gewijzigd. De gemeente Werkendam voldoet op dit punt aan norm 13.1 van het Normenkader GeVS. De overtreding van artikel 13 Wbp is op dit punt beëindigd. De bevindingen zijn op dit punt aangepast.

7. Norm 13.5 Controle op rechten en gebruik van Suwinet

In het Informatiebeveiligingsplan van de gemeente Werkendam wordt aangegeven dat de Security Officer minimaal eenmaal per jaar gegevens over het gebruik van Suwinet opvraagt. De gemeente Werkendam heeft verder geen informatie opgestuurd waaruit blijkt dat het gebruik meerdere keren per jaar met behulp van de informatie van het BKWI wordt gecontroleerd. Dit is niet conform norm 13.5 van het Normenkader GeVS, die vereist dat deze controle meerdere keren per jaar wordt uitgevoerd. De overtreding van artikel 13 Wbp is op dit punt niet beëindigd.