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
www.mijnprivacy.nl

College bescherming persoonsgegevens

Onderzoek beveiliging van persoonsgegevens via Suwinet Gemeente Woudenberg

z2015-00398

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 Woudenberg één norm uit het Normenkader GeVS (Gezamenlijke elektronische Voorzieningen SUWI) niet of onvoldoende naleeft: Niet is gebleken dat de Security Officer van de gemeente Woudenberg in de praktijk rechtstreeks rapporteert aan het hoogste management. De gemeente Woudenberg 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 electronische 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.

1.2 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.

---

[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 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 gemeente Woudenberg, zijnde één van de onderzochte gemeenten.

1.3 Doel en reikwijdte van het onderzoek

Het onderzoek beoogt vast te stellen of gemeente Woudenberg, 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);
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 Woudenberg 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 Woudenberg 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 Woudenberg 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 Woudenberg vertrouwelijke (bedrijfs)gegevens bevatten.
De gemeente Woudenberg heeft bij e-mail van 17 augustus 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 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

Het CBP heeft kennisgenomen van de bevindingen van het onderzoek en de rapportage van de Inspectie SZW. In deze bevindingen wordt aangegeven dat de gemeente Woudenberg ten tijde van het onderzoek niet beschikt over een beveiligingsplan dat specifiek is betrekking heeft op het Suwinet.

Uit de zienswijze van de gemeente Woudenberg blijkt dat de gemeente Woudenberg op 22 juli 2015 een door het management van de gemeente ondertekend Informatiebeveiligingsplan heeft, waarin het Beveiligingsbeleid Suwinet is opgenomen.

2.1.3 Beoordeling

De gemeente Woudenberg heeft een door het management vastgesteld beveiligingsplan voor Suwinet. De gemeente Woudenberg handelt op dit punt thans 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

In de bevindingen van de Inspectie SZW staat dat de gemeente Woudenberg schriftelijk heeft aangegeven dat het plan (Informatiebeveiligingsbeleid van de gemeente Woudenberg, toevoeging CBP) niet wordt uitgedragen in de organisatie.

Uit de zienswijze van de gemeente Woudenberg blijkt dat het Informatiebeveiligingsplan centraal beschikbaar is gesteld voor het personeel via intranet, en dat er meerdere malen aandacht is gevraagd voor de beveiliging van Suwinet en het Informatiebeveiligingsplan door middel van e-mails aan betrokken medewerkers.

2.2.3 Beoordeling

De gemeente Woudenberg draagt het beveiligingsplan voor Suwinet uit in de organisatie. Hiermee handelt de gemeente Woudenberg 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 Woudenberg heeft volgens de bevindingen van de Inspectie SZW geen evaluatie van het SUWI beveiligingsplan uitgevoerd.

Uit de zienswijze van de gemeente Woudenberg blijkt dat het Informatiebeveiligingsplan vanaf 22 juli 2015 in werking is getreden. Hierin is een uitgebreide procedure voor de evaluatie opgenomen, waarin onder andere wordt aangegeven dat het Informatiebeveiligingsplan minimaal eenmaal per jaar wordt geëvalueerd.

2.3.3 Beoordeling

Gelet op de korte periode 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 Woudenberg handelt 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 heeft de gemeente Woudenberg taken en verantwoordelijkheden ten aanzien van Suwinet niet beschreven.

De zienswijze van de gemeente Woudenberg bevat een Informatiebeveiligingsplan dat op 22 juli 2015 in werking is getreden. In dit Informatiebeveiligingsplan 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 inmiddels gescheiden zijn belegd.

2.4.3 Beoordeling

De gemeente Woudenberg handelt conform norm 2.2 van het Normenkader GeVS. De gemeente Woudenberg 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 de taken en verantwoordelijkheden van de Security Officer niet formeel zijn beschreven. De gemeente Woudenberg heeft aangegeven dat het takenpakket van de Security Officer bestaat uit overleg met applicatiebeheerder Suwinet en het uitbrengen van verslag over gebruik en beheer Suwinet aan de eindverantwoordelijke. De Inspectie SZW heeft verslagen ontvangen, maar deze zijn niet gestuurd aan het hoogste management.

Uit de zienswijze van de gemeente Woudenberg blijkt het volgende: In het Informatiebeveiligingsplan 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. De Security Officer heeft formeel wat betreft rapportages een bijzondere rol. Deze rapporteert namelijk rechtstreeks aan de bestuurlijk verantwoordelijke.'

De gemeente Woudenberg heeft informatie overgelegd waaruit blijkt dat de Security Officer formeel is aangesteld en activiteiten uitvoert ten aanzien van de beveiliging van Suwinet. De gemeente Woudenberg heeft echter geen informatie overgelegd waaruit blijkt dat de Security Officer in de praktijk rechtstreeks aan het hoogste management rapporteert.

2.5.3 Beoordeling

Niet is gebleken dat de Security Officer van de gemeente Woudenberg in de praktijk rechtstreeks aan het hoogste management rapporteert. De gemeente Woudenberg 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 Woudenberg heeft volgens de bevindingen van de Inspectie SZW geen procedure overgelegd die betrekking heeft op de wijze waarop autorisaties worden verleend.

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.

2.6.3 Beoordeling

De gemeente Woudenberg handelt hiermee op dit punt conform norm 13.1 van het Normenkader GeVS 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 Suwinet geanalyseerd dient te worden.

2.7.2 Bevindingen

Volgens de bevindingen van de Inspectie SZW heeft de gemeente Woudenberg geen procedure voor de controle op de verleende toegangsrechten overgelegd. Evenmin is duidelijk wie deze controles uitvoert. Tot slot is onduidelijk hoe de van het BKWI verkregen informatie over het gebruik van Suwinet geanalyseerd wordt. Door de Inspectie SZW zijn bovendien opvallende raadplegingen geconstateerd die door de gemeente Woudenberg onvoldoende zijn onderzocht en waarvoor geen toereikende verklaring is gegeven.

De gemeente Woudenberg heeft bij haar zienswijze een vastgestelde procedure voor de beoordeling gebruik Suwinet meegezonden. Hierin wordt aangegeven dat een daartoe aangewezen medewerker de taak heeft twee keer per jaar een adequaat onderzoek te doen naar het rechtmatig gebruik van de Suwinet applicatie aan de hand van door het BKWI beschikbaar gestelde half jaarlijkse rapportages en daarover te rapporteren aan de Security Officer en het management. De procedure bevat een stappenplan, criteria aan de hand waarvan de rapportage wordt beoordeeld en een format voor verslaglegging.
De gemeente Woudenberg heeft één verslag inzake halfjaar controle gebruik Suwinet van 22 juli 2015 bijgevoegd. Uit dit verslag blijkt dat de door het BKWI beschikbaar gestelde half jaarlijkse rapportage is geanalyseerd.

2.7.3 Beoordeling

Gebleken is dat de gemeente Woudenberg de van het BKWI verkregen informatie over het gebruik van Suwinet niet in strijd met norm 13.5 van het Normenkader GeVS analyseert. Dit is evenmin in strijd met artikel 13 Wbp.

CONCLUSIES

Uit het onderzoek van het CBP volgt dat de Wbp wordt overtreden, omdat de gemeente Woudenberg één norm uit het Normenkader GeVS (Gezamenlijke elektronische Voorzieningen SUWI) niet of onvoldoende naleeft: Niet is gebleken dat de Security Officer van de gemeente Woudenberg in de praktijk rechtstreeks rapporteert aan het hoogste management. De gemeente Woudenberg 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 VAN DE GEMEENTE WOUDENBERG

Zienswijze gemeente Woudenberg

Het CBP-rapport van voorlopige bevindingen is, net als dat van de inspectie SZW eind vorig jaar, voor de gemeente Woudenberg aanleiding geweest de informatiebeveiliging integraal op te pakken.

Begin maart is onderkend dat de gemeente onvoldoende expertise in huis heeft om (op korte termijn) eigenhandig gevolg te kunnen geven aan de eisen ten behoeve van informatiebeveiliging, waaronder het veilig gebruik Suwinet. Met de focus op het verantwoord gebruik van Suwinet heeft de gemeente Woudenberg geïnvesteerd in een oplossing van een expertisebureau. Met behulp van dit bureau is een aanvang gemaakt om de gemeentelijke informatiebeveiliging ten behoeve van GBA, BAG, DigiD en SUWI op orde te brengen.

Zoals aangegeven ligt de focus nu op het veilig gebruik van Suwinet. Met betrekking tot de normen waarop is gerapporteerd zijn diverse acties ondernomen. De gemeente verwijst hiervoor naar de bijlagen bij de zienswijze.

Reactie CBP

Het CBP reageert hieronder puntsgewijs op de zienswijze van de gemeente Woudenberg.

1. Het beveiligingsplan

De gemeente Woudenberg heeft een op 22 juli 2015 door het management van de gemeente ondertekend Informatiebeveiligingsplan, waarin het Beveiligingsbeleid Suwinet is opgenomen. De gemeente Woudenberg 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 Woudenberg bij de zienswijze heeft gevoegd, blijkt dat het Informatiebeveiligingsplan centraal beschikbaar is gesteld voor het personeel via intranet, en dat er meerdere malen aandacht is gevraagd voor de beveiliging van Suwinet en het Informatiebeveiligingsplan door middel van e-mails aan betrokken medewerkers. De gemeente Woudenberg 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 Informatiebeveiligingsplan en de uitgebreide procedure voor de evaluatie in het Informatiebeveiligingsplan, waarin onder andere wordt aangegeven dat het Informatiebeveiligingsplan minimaal eenmaal per jaar wordt geëvalueerd, kan worden geconcludeerd dat de gemeente Woudenberg 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 Informatiebeveiligingsplan 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 Woudenberg 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 Informatiebeveiligingsplan 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. De Security Officer heeft formeel wat betreft rapportages een bijzondere rol. Deze rapporteert namelijk rechtstreeks aan de bestuurlijk verantwoordelijke.

Verder heeft de gemeente Woudenberg informatie overgelegd waaruit blijkt dat de Security Officer formeel is aangesteld en activiteiten uitvoert ten aanzien van de beveiliging van Suwinet. De gemeente Woudenberg 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 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 Woudenberg voldoet op dit punt aan norm 13.1 van het Normenkader GeVS. De overtreding van artikel 13 Wbp is hiermee beëindigd. De bevindingen zijn op dit punt aangepast.

7. Controle op autorisaties en gebruik

De gemeente Woudenberg heeft een vastgestelde procedure voor de beoordeling gebruik Suwinet. Hierin wordt aangegeven dat een daartoe aangewezen medewerker de taak heeft twee keer per jaar een adequaat onderzoek te doen naar het rechtmatig gebruik van de Suwinet applicatie aan de hand van door het BKWI beschikbaar gestelde half jaarlijkse rapportages en daarover te rapporteren aan de Security Officer en het management. De procedure bevat een stappenplan, criteria aan de hand waarvan de rapportage wordt beoordeeld en een format voor verslaglegging.
De gemeente Woudenberg heeft één verslag inzake halfjaar controle gebruik Suwinet van 22 juli 2015 bijgevoegd.

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