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 Enschede

z2015-00173

Openbare versie
Rapport van bevindingen

November2015

DATUM November 2015

INHOUDSOPGAVE

SAMENVATTING

Sinds 2002 wisselen diverse overheidsorganisaties (persoons)gegevens van burgers uit in het domein Werk en Inkomen op basis van de Wet structuur uitvoeringsorganisatie werk en inkomen (Wet SUWI). Deze gegevensuitwisseling vindt plaats via de Gezamenlijke elektronische Voorzieningen SUWI (GeVS, ook wel Suwinet genoemd)[1].

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[2]. Uit twee recente onderzoeken van de Inspectie SZW kan worden geconcludeerd dat de beveiliging van Suwinet bij veel gemeenten niet voldoet aan de wettelijke vereisten[3]. Voor het CBP vormt dit mede de aanleiding om te controleren of toegang tot Suwinet en gebruik hiervan door gemeenten voldoet aan de vereisten van de Wet bescherming persoonsgegevens (Wbp).

In het kader van zijn toezichthoudende taak heeft het CBP bij een aantal gemeenten onderzoek gedaan naar de beveiliging van persoonsgegevens die via Suwinet kunnen worden geraadpleegd. Het onderzoek is gericht op de naleving van de door de Wbp en SUWI wet- en regelgeving gestelde vereisten ten aanzien van de beveiliging van persoonsgegevens die via Suwinet geraadpleegd kunnen worden. Dit rapport van bevindingen heeft betrekking op één van de onderzochte organisaties: de gemeente Enschede.

Uit het onderzoek volgt dat de Wbp wordt overtreden. Het beëindigen van autorisaties is onvoldoende beschreven omdat niet duidelijk is welke functionarissen hierbij betrokken zijn en welke activiteiten zij hierbij dienen uit te voeren. Er is geen procedurestap met betrekking tot het wijzigen van autorisaties. De handelwijze van de gemeente Enschede voldoet op dit punt niet aan norm 13.1 van het Normenkader GeVS en is daarmee in strijd met artikel 13 Wbp.

[1] Suwinet wordt ook wel aangeduid als "de Gezamenlijke elektronische Voorzieningen SUWI" (of GeVS).
[2] https:/ / cbpweb.nl/ nl/ nieuws/ cbp-persoonsgegevens-suwinet-niet-goed-beveiligd
[3] http:/ / www.rijksoverheid.nl/ documenten-en-publicaties/ kamerstukken/ 2015/ 06/ 04/ kamerbrief-suwinet-veilig-omgaan-met-elkaars-gegevens.html

1 INLEIDING

1.1 Achtergrond onderzoek

Sinds 2002 wisselen diverse overheidsorganisaties (persoons)gegevens van burgers uit in het domein Werk & Inkomen via Suwinet. Suwinet beschikt over 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 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.

Uit verschillende onderzoeken blijkt dat de beveiliging van Suwinet niet in alle gevallen voldoet aan de wettelijke vereisten. Recent onderzoek van het CBP heeft uitgewezen dat toegang tot Suwinet voor niet-Suwipartijen onvoldoende beveiligd was[4]. Uit twee recente onderzoeken van de Inspectie SZW[5] kan worden geconcludeerd dat de beveiliging van Suwinet bij veel gemeenten niet voldoet aan de wettelijke vereisten. Voor het CBP vormt dit mede de aanleiding om te controleren of toegang tot Suwinet en gebruik hiervan door gemeenten voldoet aan de vereisten van de Wbp. Een goede beveiliging is van belang omdat binnen Suwinet steeds meer gegevens worden uitgewisseld[6]. Hieronder bevinden zich zeer privacygevoelige gegevens, zoals fraudevorderingen (informatie over bijstandsvorderingen betreffende fraude of recidive[7]) 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[8]. Adequate beveiligingsmaatregelen kunnen er voor zorgen dat de kans op dergelijke incidenten tot het minimum wordt beperkt.

---

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

[5] Programmarapportage 'De burger bediend in 2013', Inspectie SZW, 8 november 2013, http:/ / www.rijksoverheid.nl/ documenten-en-publicaties/ rapporten/ 2013/ 11/ 08/ programmarapportage-de-burger-bediend-in-2013.html

[6] http:/ / www.bkwi.nl/ fileadmin/ downloads/ Suwinet/ Factsheets/ 13_BK_factsheet_SUWI_Gegevensregister.pdf

[7] http:/ / www.bkwi.nl/ uploads/ media/ 20150408_Handreiking_autorisatie_op_Suwinet-Inkijk_voor_GSD_01.pdf

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

Dit rapport betreft de definitieve bevindingen van het door het CBP uitgevoerde onderzoek bij de gemeente Enschede.

1.2 Doel, reikwijdte en uitvoering onderzoek

In het kader van de toezichthoudende taak heeft het CBP op grond van artikel 60 Wbp een ambtshalve onderzoek verricht naar de naleving van de vereisten van de Wbp en SUWI wet- en regelgeving door de gemeente Enschede met betrekking tot de beveiliging van persoonsgegevens die via Suwinet geraadpleegd kunnen worden.

De hoofdvragen van het onderzoek zijn:

- Beschikt de gemeente Enschede over een (formeel vastgesteld) beveiligingsplan en autorisatieprocedure specifiek gericht op Suwinet?
- Hoe zijn de autorisaties tot Suwinet in de praktijk bij de gemeente Enschede ingericht?
- Worden vereisten met betrekking tot autorisaties door de gemeente nageleefd?
- Worden de raadplegingen gecontroleerd aan de hand van logging rapportages?

Bij brief van 26 februari 2015 heeft het CBP bij de gemeente Enschede het onderzoek aangekondigd en schriftelijke stukken (het Suwinet beveiligingsplan, de procedure voor het toekennen, wijzigen en beëindigen van autorisaties van medewerkers voor toegang tot persoonsgegevens en de controle op raadplegingen van persoonsgegevens via Suwinet, alsmede een overzicht van alle geautoriseerde medewerkers, inclusief hun functie, afdeling en de toegekende rollen bij toegang tot Suwinet) opgevraagd.

Op 12 maart 2015 heeft het CBP de gevraagde informatie van de gemeente Enschede ontvangen. Op 2 april 2015 heeft het CBP om aanvullende informatie verzocht. De gevraagde aanvullende informatie is op 9 april 2015 door het CBP ontvangen.

Het CBP heeft op 30 juni 2015 het Rapport van voorlopige bevindingen vastgesteld. Het CBP heeft de gemeente Enschede bij brief van 8 juli 2015 in de gelegenheid gesteld om haar zienswijze op het Rapport van voorlopige bevindingen naar voren te brengen. Het CBP heeft daarbij tevens verzocht aan te geven of en zo ja welke onderdelen daarvan, volgens de gemeente Enschede vertrouwelijke (bedrijfs)gegevens bevatten.
De gemeente Enschede heeft bij email van 7 augustus 2015 haar zienswijze, alsmede een reactie op de (bedrijfs) vertrouwelijkheidstoets, ingebracht.

1.3 Wettelijk kader

De volgende wetsartikelen vorm het juridisch kader van dit onderzoek:

- Artikel 13 Wbp
- Artikel 6.4 Regeling SUWI
- Bijlage I. , bedoeld in artikel 6.4 van de Regeling SUWI: *Stelselontwerp & Beveiliging Kaders en uitgangspunten aangaande de Gezamenlijke elektronische Voorzieningen Suwi (GeVS)* (hierna: Bijlage I Regeling SUWI).
- Het Normenkader GeVS en de Verantwoordingsrichtlijn GeVS (Gezamenlijke elektronische Voorzieningen SUWI)
- De Code voor Informatiebeveiliging (NEN-ISO/IEC 27002:2013)

De gemeente Enschede is in het kader van dit onderzoek verantwoordelijke in de zin van artikel 1, aanhef en onder d, Wbp.

2 BEVINDINGEN

2.1 Beveiligingsplan Suwinet

2.1.1 Norm

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 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.

Het normenkader GeVS stelt dat de afnemer/ registratiehouder/ beheerder de inrichting van en de taken en verantwoordelijkheden voor de beveiliging (van de eigen delen van de GeVS) heeft beschreven, vastgesteld en belegd (norm 1). De Suwipartij dient voor de Suwi-omgeving een Suwinet beveiligingsplan te hebben opgesteld dat gebaseerd is op het informatiebeveiligingsbeleid van de organisatie en afspraken in de Suwiketen (norm 1.2). Het informatiebeveiligingsbeleid en het beveiligingsplan van het Suwinet dienen te zijn goedgekeurd door het management van de Suwipartij (norm 1.3). Het informatiebeveiligingsbeleid en het beveiligingsplan van het Suwinet worden jaarlijks geëvalueerd en indien nodig geactualiseerd (norm 1.5).

2.1.2 Bevindingen

De gemeente Enschede heeft een Beveiligingsplan Suwinet-Inkijk overgelegd. Het betreft een versie van september 2014. Het Beveiligingsplan Suwinet Inkijk is op 9 december 2014 goedgekeurd door het managementteam Economie en Werk van de gemeente Enschede.

2.1.3 Beoordeling

Het Beveiligingsplan Suwinet-Inkijk is vastgesteld door het management van de gemeente Enschede. Dit is conform norm 1.3 van het Normenkader GeVS en daarmee ook conform artikel 13 Wbp.

2.2 Procedure toekenning autorisaties Suwinet

2.2.1 Norm

Zoals reeds beschreven onder paragraaf 2.1.1, kunnen Bijlage I Regeling SUWI en de Verantwoordingsrichtlijn GeVS met het daarin opgenomen Normenkader GeVS worden beschouwd als wettelijke uitwerkingen van het algemene beveiligingsvoorschrift uit artikel 13 Wbp voor de Suwiketen. Bijlage I Regeling SUWI geeft onder meer invulling aan de gezamenlijke aansturing van privacy en beveiliging. In bijlage I Regeling SUWI wordt aangegeven dat de Verantwoordingsrichtlijn GeVS een gezamenlijk product is van de Suwipartijen en de beheerder van de centrale voorziening. Het bevat de normen, criteria en vormvereisten ten aanzien van privacy en beveiliging.

Ten aanzien van autorisaties stelt norm 13.1 van het Normenkader GeVS dat de Suwipartij de gebruikers die toegang hebben tot de Suwinet applicaties op basis van een formele procedure autoriseert en registreert. In deze procedure moeten de volgende zaken 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 wijzigen (dus ook intrekken) 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).

Norm 13.2 stelt voorts dat technisch beheerders geen Suwinet account mogen hebben.

2.2.2 Bevindingen

De gemeente Enschede beschrijft onder paragraaf 4.1.1 ('Toegangsbeheersing en –autorisatie voor informatiesystemen') in het Beveiligingsplan Suwinet Inkijk de wijze waarop autorisaties voor Suwinet worden toegekend en beëindigd. In deze paragraaf wordt beschreven dat autorisaties op aanvraag van de betreffende leidinggevende, ter beoordeling en goedkeuring van de systeemeigenaren, worden verleend op basis van de uit te voeren werkzaamheden. Accounts van medewerkers die uit dienst gaan, worden op de datum van uitdiensttreding afgesloten en na drie maanden uitdiensttreding verwijderd. Niet duidelijk is welke functionarissen hierbij betrokken zijn en welke activiteiten zij hierbij dienen uit te voeren. Voorts bevat de paragraaf

geen beschrijving van de wijze waarop wordt omgegaan met wijzigingen in functies of hoe autorisaties worden gewijzigd.

2.2.3 Beoordeling

Uit paragraaf 4.1.1 van het Beveiligingsplan Suwinet Inkijk blijkt dat gebruikers die toegang hebben tot Suwinet, op basis van een procedure worden geautoriseerd. Het beëindigen van autorisaties is onvoldoende beschreven omdat niet duidelijk is welke functionarissen hierbij betrokken zijn en welke activiteiten zij hierbij dienen uit te voeren. De paragraaf bevat voorts geen procedurestap met betrekking tot het wijzigen van autorisaties.
De handelwijze van de gemeente Enschede voldoet op dit punt niet aan norm 13.1 van het Normenkader GeVS en is daarmee in strijd met artikel 13 Wbp.

2.3 Toegangsrechten Suwinet

2.3.1 Norm

Artikel 13 Wbp bepaalt dat de verantwoordelijke maatregelen ten uitvoer legt om persoonsgegevens te beveiligen tegen enige vorm van onrechtmatige verwerking. Onder onrechtmatige vormen van verwerking vallen de onbevoegde kennisneming, wijziging of verstrekking daarvan.[9] Er dienen procedures aanwezig te zijn om alleen bevoegde gebruikers toegang te geven tot de informatiesystemen en -diensten die zij voor de uitvoering van hun taken nodig hebben en om onbevoegde toegang tot informatiesystemen te voorkomen.

In uitgangspunt 11 van het Normenkader GeVS wordt aangegeven dat toegang tot de via GeVS uitgewisselde gegevens wordt verleend aan unieke geïdentificeerde, geauthentiseerde en geautoriseerde personen en slechts voor zover dit nodig is voor de uitvoering van de hen opgedragen taken. Norm 13.1 van het Normenkader GeVS stelt dat het verlenen van toegang tot de benodigde gegevens op basis van de uit te voeren functie en taken dient plaats te vinden.

Artikel 9.2.3 van de Code voor informatiebeveiliging (NEN-ISO-IEC 27002:2013) stelt dat het toewijzen en gebruik van speciale toegangsrechten dient te worden beperkt en beheerst. Binnen het gemeentelijke Suwidomein zijn speciale autorisaties gedefinieerd door het BKWI. Deze zware rollen mogen beperkt worden toebedeeld. Dit zijn de rollen waarvan BKWI aangeeft dat het 'risicovolle autorisaties' betreft, die onder andere bedoeld zijn om fraude mee te bestrijden . Deze mogen worden toebedeeld aan een beperkte groep gespecialiseerde medewerkers zoals de sociale recherche[10].

2.3.2 Bevindingen

In de door de gemeente Enschede verstrekte overzichten worden zware[11] autorisatierollen beperkt en gespecificeerd toegekend aan medewerkers die deze autorisaties nodig hebben voor de uitvoering van hun specifieke taken. De verleende toegangsrechten sluiten daarmee aan op de uit te voeren functies en taken van de geautoriseerde medewerkers. De autorisaties sluiten aan op de uit te voeren functies en taken van de geautoriseerde medewerkers.

---

[9] Kamerstukken II 1997-1998, 25 892, nr. 3, p. 98.
[10] http:/ / www.bkwi.nl/ uploads/ media/ 20150408_Handreiking_autorisatie_op_Suwinet-Inkijk_voor_GSD_01.pdf
[11] Idem

2.3.3 Beoordeling

De gemeente Enschede heeft zware autorisatierollen specifiek toegekend aan een beperkte groep van gespecialiseerde medewerkers. De gemeente Enschede handelt hiermee thans conform norm 13.1 van het Normenkader GeVS en daarmee met artikel 13 Wbp.

2.4 Controle toegangsrechten en gebruik Suwinet

2.4.1 Norm

Bijlage I Regeling SUWI en de Verantwoordingsrichtlijn GeVS met het daarin opgenomen Normenkader GeVS worden beschouwd als wettelijke uitwerkingen van het algemene beveiligingsvoorschrift uit artikel 13 Wbp voor de Suwiketen. Norm 13.5 van het Normenkader GeVS schrijft voor dat de controle op verleende toegangsrechten en gebruik meerdere keren per jaar plaatsvindt. Dit is een interne controle op rechten en gebruik van Suwinet waarbij de van het BKWI verkregen informatie over het gebruik van Suwi-gegevens geanalyseerd dient te worden.

2.4.2 Bevindingen

Het Beveiligingsplan Suwinet Inkijk van de gemeente Enschede beschrijft onder paragraaf 5.1 de controle door middel van logging. In dit onderdeel van het Beveiligingsplan Suwinet Inkijk wordt aangegeven dat maandelijks een generieke gebruiksrapportage door het Bureau Keteninformatisering Werk en Inkomen (BKWI) wordt verstrekt aan de gemeente Enschede. De Security Officer beoordeelt deze generieke maandrapportage. Bij vermoedens van onjuist, onrechtmatig of oneigenlijk gebruik worden specifieke gebruiksrapportages opgevraagd bij het BKWI.

De specifieke rapportages worden door de Security Officer nader onderzocht. Bij vaststelling van onrechtmatig gebruik zal de proceseigenaar in overleg met de leidinggevende de benodigde maatregelen treffen.

De gemeente Enschede heeft het laatste verslag over het gebruik van Suwinet in 2014 aan het CBP overgelegd.

2.4.3 Beoordeling

Uit de door de gemeente Enschede overgelegde informatie blijkt dat de gemeente Enschede meerdere keren per jaar controle op verleende toegangsrechten tot en gebruik van Suwinet uitvoert. Interne controle op rechten en gebruik van Suwinet vindt plaats waarbij de van het BKWI verkregen informatie over het gebruik van Suwi-gegevens wordt geanalyseerd. De gemeente Enschede handelt op deze punten conform norm 13.5 van het Normenkader GeVS.

3 CONCLUSIE

Uit het onderzoek volgt dat de Wbp wordt overtreden. Het beëindigen van autorisaties is onvoldoende beschreven omdat niet duidelijk is welke functionarissen hierbij betrokken zijn en welke activiteiten zij hierbij dienen uit te voeren. Er is geen procedurestap met betrekking tot het wijzigen van autorisaties. De handelwijze van de gemeente Enschede voldoet op dit punt niet aan norm 13.1 van het Normenkader GeVS en is daarmee in strijd 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 ENSCHEDE

Zienswijze gemeente Enschede

De gemeente Enschede heeft op 7 augustus 2015 per email haar zienswijze ingebracht. De gemeente Enschede stelt in haar zienswijze te hebben kennisgenomen van de voorlopige bevindingen naar aanleiding van het onderzoek naar de beveiliging van Suwinet.

De gemeente Enschede geeft aan te hebben besloten de voorlopige bevindingen te accepteren en daartegen geen formeel bezwaar te maken, hoewel de gemeente van mening is dat één van de bevindingen niet terecht is, zijnde de brede autorisatie voor de rol "Fraudevorderingen", waaronder consulenten bestandsbeheer.
De gemeente Enschede geeft aan dat deze rol is bedoeld voor medewerkers die:

- Sociaal rechercheur zijn of althans bij de Sociale Recherche werkzaam zijn
- Recidive beoordelen
- Boetes beoordelen.

De gemeente Enschede geeft in haar zienswijze aan dat het de bestaande werkwijze is dat consulenten bestandsbeheer beoordelingen van boetes uitvoeren en daarover advies uitbrengen. Vanuit die taak beschikken zij dan ook volgens de gemeente Enschede terecht over de betreffende autorisatie. Gebleken is echter, aldus de gemeente Enschede, dat ook bij een beperkte autorisatie consulenten bestandsbeheer voldoende informatie tot hun beschikking hebben om de beoordeling te kunnen doen. De gemeente Enschede geeft aan dat inmiddels de toegang tot Suwinet via de rol "Fraudevorderingen" beperkt is tot consulenten handhaving.

De beschrijving van beëindiging of wijziging van autorisaties in geval van uitdiensttreding of wijziging van functie wordt door de gemeente Enschede aangepast in het beveiligingsplan SUWI. Dit zal worden meegenomen in de jaarlijkse update daarvan.

Reactie CBP

Hoewel de gemeente Enschede de voorlopige bevindingen accepteert en geen formeel bezwaar maakt, geeft zij aan van mening te zijn dat één van de bevindingen niet juist is. Het gaat hier om de autorisatierol 'Fraudevorderingen' voor consulenten bestandsbeheer. Volgens de gemeente beschikken consulenten bestandsbeheer terecht over de betreffende autorisatie, omdat deze consulenten beoordelingen van boetes uitvoeren en daarover advies uitbrengen. Tegelijkertijd geeft de gemeente aan dat ook bij een beperkte autorisatie consulenten bestandsbeheer voldoende informatie tot hun beschikking hebben om de beoordeling te kunnen doen.

De gemeente Enschede heeft echter inmiddels de toegang tot Suwinet via de autorisatierol 'Fraudevorderingen' beperkt tot consulenten handhaving.

Omdat de gemeente de toegang tot Suwinet via de autorisatierol 'Fraudevorderingen' heeft beperkt tot consulenten handhaving, handelt de gemeente Enschede conform norm 13.1 van het Normenkader GeVS en artikel 9.2.3 van de Code voor informatiebeveiliging. Hiermee is tevens de overtreding van artikel 13 Wbp beëindigd. De bevindingen zijn op dit punt aangepast.

Overigens blijft het CBP van oordeel dat de constatering ten aanzien van de autorisatierol 'Fraudevorderingen' uit het rapport van voorlopige bevindingen terecht is. De betreffende (zware) autorisatierol gaat gepaard met brede toegangsrechten tot Suwinet via uitgebreide zoekfunctionaliteiten. Deze rol was niet beperkt tot de medewerkers die de genoemde toegangsrechten nodig hebben voor de uit te voeren taken. De gemeente Enschede heeft immers ook zelf aangegeven dat bij een beperktere autorisatie consulenten bestandsbeheer voldoende informatie tot hun beschikking hebben om hun taak uit te kunnen voeren.