

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 Delft

z2015-00172

Openbare versie
Rapport van bevindingen

November 2015

INHOUDSOPGAVE

Samenvatting	3
1. Inleiding.....	4
1.1 Achtergrond onderzoek	4
1.2 Doel, reikwijdte en uitvoering onderzoek	5
1.3 Wettelijk kader.....	5
2 Bevindingen	7
2.1 Beveiligingsplan Suwinet	7
2.1.1 Norm	7
2.1.2 Bevindingen	8
2.1.3 Beoordeling	8
2.2 Procedure toekenning autorisaties Suwinet	8
2.2.1 Norm	8
2.2.2 Bevindingen	8
2.2.3 Beoordeling	9
2.3 Toegangsrechten Suwinet	9
2.3.1 Norm	9
2.3.2 Bevindingen	9
2.3.3 Beoordeling	10
2.4 Controle toegangsrechten en gebruik Suwinet	10
2.4.1 Norm	10
2.4.2 Bevindingen	10
2.4.3 Beoordeling	10
3 Conclusie.....	11
Bijlage I: Reactie CBP op zienswijze gemeente Delft.....	12
Zienswijze gemeente Delft	12
Reactie CBP	12

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 ontbrak². Uit twee recente onderzoeken van de Inspectie SZW bleek dat de beveiliging van Suwinet bij veel gemeenten niet voldeed aan de wettelijke vereisten³. 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 Delft.

Uit het onderzoek volgt dat de Wbp op de onderzochte punten niet wordt overtreden.

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 met 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 was⁴. Uit twee recente onderzoeken van de Inspectie SZW⁵ 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 uitgewisseld⁶. Hieronder bevinden zich zeer privacygevoelige gegevens, zoals fraudevorderingen (informatie over bijstandsvorderingen betreffende fraude of recidive⁷) 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 achterhalen⁸. Adequate beveiligingsmaatregelen kunnen er voor zorgen dat dergelijke incidenten worden voorkomen.

⁴ <https://cbpweb.nl/nl/nieuws/cbp-persoonsgegevens-suwinet-niet-goed-beveiligd>

⁵ <http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2015/06/04/kamerbrief-suwinet-veilig-omgaan-met-elkaars-gegevens.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 Delft.

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 Delft met betrekking tot de beveiliging van persoonsgegevens die via Suwinet geraadpleegd kunnen worden.

De hoofdvragen van het onderzoek zijn:

- Beschikt de gemeente Delft over een (formeel vastgesteld) beveiligingsplan en autorisatieprocedure specifiek gericht op Suwinet?
- Hoe zijn de autorisaties tot Suwinet in de praktijk bij de gemeente Delft 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 Delft 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 16 maart heeft het CBP de gevraagde informatie van de gemeente Delft ontvangen. Op 2 april 2015 heeft het CBP een verzoek om aanvullende informatie verstuurd. Op 22 april 2015 heeft het CBP de gevraagde informatie van de gemeente Delft ontvangen.

Het CBP heeft op 30 juni 2015 het Rapport van voorlopige bevindingen vastgesteld. Het CBP heeft de gemeente Delft 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 Delft vertrouwelijke (bedrijfs)gegevens bevatten. De gemeente Delft heeft bij brief van 12 augustus 2015 haar zienswijze, alsmede een reactie op de (bedrijfs) vertrouwelijkheidstoets, ingebracht.

1.3 Wettelijk kader

De volgende wetsartikelen vormen 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)
- Artikel 9.2.3 van de Code voor informatiebeveiliging (NEN-ISO-IEC 27002:2013)

De gemeente Delft 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 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 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 Delft heeft een Informatiebeveiligingsbeleid overgelegd dat op 9 september 2014 is vastgesteld door het College van burgemeester en wethouders. De gemeente Delft heeft tevens een in juli 2015 door het management vastgesteld beveiligingsplan Suwi 2015 aan het CBP overgelegd.

2.1.3 Beoordeling

De gemeente Delft heeft een Informatiebeveiligingsbeleid dat is goedgekeurd door het management. Op dit punt handelt de gemeente Delft conform norm 1.3 van het Normenkader GeVS en daarmee met artikel 13 Wbp.

Het beveiligingsplan is specifiek opgesteld voor de Suwi-omgeving en is gebaseerd op het Informatiebeveiligingsbeleid. Het beveiligingsplan voor Suwinet is goedgekeurd door het management van de gemeente Delft. Het beveiligingsplan is door het management vastgesteld ten tijde van het onderzoek. De gemeente Delft handelt op dit punt niet meer in strijd met norm 1.3 van het Normenkader GeVS en daarmee evenmin in strijd met artikel 13 Wbp.

2.2 Procedure toekenning autorisaties Suwinet

2.2.1 Norm

Zoals reeds beschreven onder paragraaf 3.1.1, 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 Delft heeft een document overgelegd getiteld 'Procesbeschrijving aanvragen Suwinet Inlijk account', dat een beschrijving bevat van de gang van zaken

bij het toekennen, wijzigen en beëindigen van autorisaties. In het document wordt stapsgewijs beschreven welke medewerker een bepaalde activiteit dient uit te voeren en op welke manier dit dient te gebeuren. Het document bevat een reeks instructies die betrekking hebben op het verlenen van toegang tot de benodigde gegevens op basis van de uit te voeren functie en taken, het uniek identificeren van elke gebruiker tot één persoon, het goedkeuren van de aanvraag voor toegangsrechten door de manager of een gemandateerde en het tijdig wijzigen en intrekken van autorisaties bij functiewijziging of vertrek.

2.2.3 Beoordeling

Uit het overgelegde document blijkt dat gebruikers die toegang hebben tot Suwinet, op basis van een procedure worden geautoriseerd en geregistreerd.

De handelwijze van de gemeente Delft voldoet op dit punt aan norm 13.1 van het Normenkader GeVS en daarmee 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 recherche¹⁰.

2.3.2 Bevindingen

Uit de door de gemeente Delft verstrekte overzichten blijkt dat zogenaamde zware¹¹ autorisatirollen met uitgebreide zoekfunctionaliteiten, zoals 'Zoeken in GBA' en 'Zoeken+ in GBA' beperkt en gespecificeerd worden toegekend aan medewerkers die deze autorisaties nodig hebben voor de uitvoering van hun specifieke taken. De

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

verleende toegangsrechten sluiten daarmee aan op de uit te voeren functies en taken van de geautoriseerde medewerkers.

2.3.3 Beoordeling

De gemeente Delft heeft zware autorisatie rollen met uitgebreide zoekfunctionaliteiten specifiek toegekend aan een beperkte groep van gespecialiseerde medewerkers. De gemeente Delft handelt op dit punt conform norm 13.1 van het Normenkader GeVS en daarmee met artikel 13 Wbp.

2.4 Controle toegangsrechten en gebruik Suwinet

2.3.1 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 2015 van de gemeente Delft bevat een onderdeel getiteld: 'Controle op gebruik Suwinet Inkijk'. In dit onderdeel van het Informatiebeveiligingsplan Suwinet 2014 wordt aangegeven dat maandelijks een generieke gebruikersrapportage door het Bureau Keteninformatisering Werk en Inkomen (BKWI) wordt verstrekt aan de gemeente Delft. Deze generieke maandrapportage wordt maandelijks geanalyseerd. Indien daartoe behoefte bestaat, worden specifieke gebruikersrapportages opgevraagd bij het BKWI waarmee het gebruik verder kan worden geanalyseerd.

Bij geconstateerde gebreken worden de verantwoordelijke lijnmanager, de proceseigenaar en de security officer geïnformeerd. De verantwoordelijke lijnmanager onderneemt actie tot verbetering van gedrag of procedure of het treffen van sancties.

Voorts wordt in het 'Protocol Suwinet-Inkijk' aangegeven dat tenminste een keer per drie maanden specifieke gebruikersrapportages worden opgevraagd en geanalyseerd.

De gemeente Delft heeft twee generieke rapportages over het gebruik van Suwinet in de periodes juli 2014- december 2014 en augustus 2014- januari 2015 aan het CBP overgelegd. In de overgelegde rapportages zijn aantekeningen zichtbaar die met pen zijn aangebracht. Hieruit maakt het CBP op dat de toegestuurde rapportages door de gemeente Delft worden geanalyseerd.

2.4.3 Beoordeling

Uit de door de gemeente Delft overgelegde informatie blijkt dat de gemeente Delft 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 Delft handelt op deze punten conform norm 13.5 van het Normenkader GeVS.

3 CONCLUSIE

Uit het onderzoek volgt dat de Wbp op de onderzochte punten niet wordt overtreden.

Het College bescherming persoonsgegevens,
Voor het College,

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

BIJLAGE I: REACTIE CBP OP ZIENSWIJZE GEMEENTE DELFT

Zienswijze gemeente Delft

De gemeente Delft gaat in haar zienswijze op het Rapport van voorlopige bevindingen in op de volgende twee punten:

1. Het beveiligingsplan Suwi is niet goedgekeurd door het management;
2. Een groot aantal medewerkers heeft een te ruime autorisatie voor de zoekfunctie in GBA.

Ten aanzien van het eerste punt geeft de gemeente aan dat het beveiligingsplan inmiddels is goedgekeurd door het management en ondertekend door de gemeente secretaris. De gemeente Delft heeft hiervan een afschrift meegezonden.

Ten aanzien van het tweede punt geeft de gemeente aan dat de autorisaties op dit punt zijn herzien. Naar aanleiding hiervan heeft de gemeente Delft besloten uitsluitend aan de medewerkers die zich met fraudebestrijding en bijzondere onderzoeken bezighouden, zware autorisatie rollen toe te kennen met uitgebreide zoekfunctionaliteiten zoals 'Zoeken in GBA' en/of 'Zoeken+ in GBA'. De gemeente Delft heeft tevens een recente versie van de autorisatiematrix aan het CBP toegezonden.

Reactie CBP

Het CBP heeft het door het management goedgekeurde en door de gemeentesecretaris ondertekende beveiligingsplan Suwi ontvangen. Doordat het beveiligingsplan Suwi is goedgekeurd door het management van de gemeente Delft is er geen sprake meer van een overtreding van norm 1.3 van het Normenkader GeVS. Hiermee is tevens de overtreding van artikel 13 Wbp op dit punt opgeheven. Het rapport van bevindingen is op dit punt aangepast.

De autorisatiematrix is eveneens ontvangen door het CBP. Hieruit blijkt dat uitsluitend aan de medewerkers die zich met fraudebestrijding en bijzonder onderzoeken bezighouden, zware autorisatie rollen met uitgebreide zoekfunctionaliteiten zijn toegekend. Op dit punt is de overtreding van norm 13.1 van het Normenkader GeVS, artikel 9.2.3 van de Code voor informatiebeveiliging en artikel 13 Wbp opgeheven. Het rapport van bevindingen is op dit punt aangepast.