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 Baarle-Nassau

z2015-00400

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 Baarle-Nassau twee normen uit het Normenkader GeVS (Gezamenlijke elektronische Voorzieningen SUWI) niet of onvoldoende naleeft.

1. Niet is gebleken dat de gemeente Baarle-Nassau het beveiligingsplan voor Suwinet voldoende uitdraagt in de organisatie. Omdat de gemeente niet heeft kunnen aantonen dat het Beveiligingsplan van het Suwinet voldoende wordt uitgedragen in de organisatie, handelt de gemeente Baarle-Nassau in strijd met norm 1.4 van het Normenkader GeVS en daarmee tevens met artikel 13 Wbp.
2. 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 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 CBP heeft uitgewezen dat 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 Baarle-Nassau, zijnde één van de onderzochte gemeenten.

1.3 Doel en reikwijdte van het onderzoek

Het onderzoek beoogt vast te stellen of de gemeente Baarle-Nassau, zijnde verantwoordelijke in de zin van de Wbp voor de verwerkingen van persoonsgegevens via Suwinet, 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 Baarle-Nassau 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 grond hiervan is de rapportage van voorlopige
bevindingen opgesteld.

Het college van burgemeester en wethouders van de gemeente Baarle-Nassau 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 Baarle-Nassau 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 Baarle-Nassau vertrouwelijke (bedrijfs)gegevens bevatten.
De gemeente Baarle-Nassau heeft bij brief van 13 augustus 2015 haar zienswijze, alsmede een reactie op de (bedrijfs)vertrouwelijkheidstoets, ingebracht.

1.6 Juridisch kader

Artikel 13 Wbp bepaalt, voor zover thans van belang, dat de verantwoordelijke passende technische en organisatorische maatregelen ten uitvoer legt om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen. Onder onrechtmatige vormen van verwerking vallen onder andere de aantasting van gegevens, onbevoegde kennisneming, wijziging of verstrekking daarvan.

Artikel 13 Wbp behelst het algemeen beveiligingsvoorschrift. Artikel 6.4 Regeling SUWI bevat bepalingen met betrekking tot de inhoud van een verplicht gesteld beveiligingsplan en kan op dit punt worden beschouwd als een wettelijke uitwerking van artikel 13 Wbp. Artikel 6.4, eerste lid, Regeling SUWI stelt onder meer dat de colleges van burgemeester en wethouders zorg dragen voor de beveiliging van de gegevensuitwisselingen die plaatsvinden in het kader van de gezamenlijke elektronische voorzieningen SUWI, tegen inbreuk op de beschikbaarheid, integriteit en vertrouwelijkheid, overeenkomstig hetgeen voor het stelsel van maatregelen en procedures te hanteren normen, is bepaald in bijlage I ('Stelselontwerp & Beveiliging Gezamenlijke elektronische Voorzieningen SUWI'). Artikel 6.4, tweede lid, Regeling Suwi bepaalt onder meer dat de colleges van burgemeester en wethouders in een beveiligingsplan aan dienen te geven op welke wijze zij invulling geven aan het eerste lid.

Uit bijlage I ('Stelselontwerp & Beveiliging Gezamenlijke elektronische Voorzieningen SUWI') volgt dat de Suwipartijen onderling en gezamenlijk, met het Bureau Keteninformatisering Werk en Inkomen (BKWI), afspraken maken op de verschillende deelgebieden van informatie-uitwisseling binnen de Suwiketen. De afspraken vinden hun weerslag in diverse concrete producten, onder meer de Keten Service Level Agreement, het SUWI-Gegevens Register, de SUWI-Ketenarchitectuur en de Verantwoordingsrichtlijn Privacy & Beveiliging GeVS.

Het normenkader voor de wijze waarop verantwoording dient te worden afgelegd voor de beveiliging van de (verwerking van) persoonsgegevens via Suwinet is nader uitgewerkt in de Verantwoordingsrichtlijn. Het in de Verantwoordingsrichtlijn opgenomen Normenkader GeVS bevat de eisen die gelden als leidraad voor het operationeel management bij het inrichten, de werking en de controleerbaarheid van de organisatorische en technische infrastructuur voor de risicobeheersing van de gegevenshuishouding.

2 BEVINDINGEN

2.1 Beveiligingsbeleid en beveiligingsplan

2.1.1 Norm

Volgens het Normenkader GeVS dient onder meer het beveiligingsplan voor Suwinet te zijn goedgekeurd door het management van de Suwipartij (norm 1.3).

2.1.2 Bevindingen

In de bevindingen van de Inspectie SZW wordt aangegeven dat ten tijde van het onderzoek geen specifiek op Suwinet gericht, vastgesteld beveiligingsplan is overlegd door de gemeente Baarle-Nassau.

Naar aanleiding van de zienswijze van de gemeente Baarle-Nassau kan het volgende aan de bevindingen worden toegevoegd. De gemeente Baarle-Nassau heeft een beveiligingsplan Suwinet opgestuurd dat op 11 augustus 2015 is goedgekeurd door het college van burgemeester en wethouders van de gemeente Baarle-Nassau.

2.1.3 Beoordeling

De gemeente Baarle-Nassau heeft een door het college van burgemeester en wethouders vastgesteld beveiligingsplan voor Suwinet. De gemeente Baarle-Nassau handelt hiermee op dit punt thans conform norm 1.3 uit het Normenkader GeVS en daarmee tevens met artikel 13 Wbp.

2.2 Uitdragen informatiebeveiligingsbeleid en beveiligingsplan

2.2.1 Norm

Norm 1.4 van het Normenkader GeVS bepaalt onder meer dat 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 Baarle-Nassau geen informatie heeft verstrekt waaruit blijkt dat het beveiligingsplan voor Suwinet van de gemeente Baarle-Nassau wordt uitgedragen in de organisatie.

Naar aanleiding van de zienswijze van de gemeente Baarle-Nassau kan het volgende aan de bevindingen worden toegevoegd. In het beveiligingsplan Suwinet is opgenomen dat er binnen de gemeente gecommuniceerd wordt over het beveiligingsproces. Dit gebeurt door middel van periodiek werkoverleg en functioneringsgesprekken. Ook is beveiliging een onderwerp bij informatieverstrekking om het beveiligingsbewustzijn van het eigen personeel te verhogen.

2.2.3 Beoordeling

Het onderwerp beveiliging komt aan de orde tijdens werkoverleggen en functioneringsgesprekken, maar het is onduidelijk of specifiek het beveiligingsplan Suwi tijdens de werkoverleggen en functioneringsgesprekken aan de orde komt. Nu niet is gebleken dat het beveiligingsplan voor Suwinet wordt uitgedragen in de organisatie, handelt de gemeente Baarle-Nassau 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 Baarle-Nassau heeft volgens de bevindingen van de Inspectie SZW niet aangetoond dat het beveiligingsplan voor Suwinet wordt geëvalueerd.

Naar aanleiding van de zienswijze van de gemeente Baarle-Nassau kan het volgende aan de bevindingen worden toegevoegd. Het beveiligingsplan voor Suwinet is kort geleden in werking getreden, en er is een passage hierover in het beveiligingsplan Suwi opgenomen, inhoudende dat het beveiligingsplan Suwi jaarlijks wordt geëvalueerd.

2.3.3 Beoordeling

Gelet op de korte periode die is verstreken na de inwerkingtreding van het beveiligingsplan voor Suwinet is er nog geen reële mogelijkheid geweest voor een evaluatie. De gemeente Baarle-Nassau handelt op dit punt thans niet in strijd met norm 1.5 van het Normenkader GeVS. Hiermee handelt de gemeente Baarle-Nassau 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 Baarle-Nassau geen functiebeschrijvingen met betrekking tot het gebruik van Suwinet opgesteld. Er is geen scheiding aangebracht tussen de functies van de medewerker die autorisaties verstrekt, de medewerker die hiertoe opdracht verleent en de medewerker die de autorisaties controleert.

Naar aanleiding van de zienswijze van de gemeente Baarle-Nassau kan het volgende worden toegevoegd aan de bevindingen. Ten aanzien van functiescheiding voor de Suwi-omgeving zijn in bijlage I van het beveiligingsplan Suwinet, getiteld Autorisaties Suwinet, vier functies gescheiden vastgelegd. Er wordt onderscheid gemaakt tussen de functies van de medewerker die autorisaties verstrekt, de medewerker die hiertoe opdracht verleent en de medewerker die de autorisaties controleert. Er is tevens een eindverantwoordelijke aangewezen.

2.4.3 Beoordeling

Omdat op 11 augustus 2015 functiebeschrijvingen zijn vastgesteld met betrekking tot het gebruik van Suwinet en er een scheiding is aangebracht tussen de functies van de medewerker die autorisaties verstrekt, de medewerker die hiertoe opdracht verleent en de medewerker die de autorisaties controleert en er een eindverantwoordelijke is

aangewezen, kan worden geconcludeerd dat functiescheiding voldoende is doorgevoerd. De gemeente Baarle-Nassau handelt hiermee conform norm 2.2 van het Normenkader GeVS. De gemeente Baarle-Nassau handelt hiermee 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 een taakomschrijving van de Security Officer ontbreekt en de Security Officer niet rechtstreeks aan het hoogste management heeft gerapporteerd.

Naar aanleiding van de zienswijze van de gemeente Baarle-Nassau kan het volgende worden toegevoegd aan de bevindingen. De gemeente Baarle-Nassau heeft een taakomschrijving van de Security Officer opgesteld die deel uitmaakt van het beveiligingsplan Suwinet. Hieruit kan worden opgemaakt dat het tot de taken van de Security Officer behoort om rechtstreeks naar het college van burgemeester en wethouders te rapporteren. Uit de verstrekte informatie is gebleken dat de gemeente Baarle-Nassau een Security Officer bij besluit van 11 augustus 2015 heeft aangesteld.

2.5.3 Beoordeling

De korte periode tussen de aanstelling van de Security Officer (11 augustus 2015) en de indiening van de zienswijze (13 augustus 2015) in acht genomen, heeft de gemeente Baarle-Nassau geen reële mogelijkheid gehad om aan te tonen dat de Security Officer ook in de praktijk aan het hoogste management rapporteert. De gemeente Baarle-Nassau handelt thans niet in strijd met norm 2.3 van het Normenkader GeVS, en op dit punt evenmin in strijd 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 Baarle-Nassau heeft volgens de bevindingen van de Inspectie SZW geen formele autorisatieprocedure overlegd.

Naar aanleiding van de zienswijze van de gemeente Baarle-Nassau kan het volgende worden toegevoegd aan de bevindingen. De gemeente Baarle-Nassau heeft een autorisatieprocedure opgesteld die deel uitmaakt van het beveiligingsplan Suwinet. Hieruit blijkt dat de gemeente Baarle-Nassau gebruikers die toegang hebben tot de Suwinet applicaties, op basis van een formele procedure autoriseert en registreert.

2.6.3 Beoordeling

De gemeente Baarle-Nassau handelt hiermee conform norm 13.1 van het Normenkader en daarmee tevens 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 Baarle-Nassau niet aangetoond dat de controle op verleende toegangsrechten plaatsvindt en welke criteria hierbij worden gehanteerd. Er is geen verslaggeving van de controle en analyse aangetroffen.

Naar aanleiding van de zienswijze van de gemeente Baarle-Nassau kan het volgende worden toegevoegd aan de bevindingen. De gemeente Baarle-Nassau heeft een procedure voor het gebruik van Suwinet opgesteld die deel uitmaakt van het beveiligingsplan Suwinet. Hieruit blijkt dat de controle op verleende toegangsrechten en gebruik meerdere keren per jaar plaats dient te vinden. De gemeente Baarle-Nassau heeft geen verslagen van deze controles overgelegd of in haar zienswijze generieke of specifieke rapportages van het BKWI bijgevoegd.

De gemeente heeft een procedure overgelegd getiteld ‘Procedure autorisatie’, die onderdeel uitmaakt van het beveiligingsplan Suwinet. Hierin wordt aangegeven dat de Security Officer jaarlijks de actualiteit en rechtmatigheid van de ingevoerde autorisaties controleert.

Er is geen informatie of bewijs overgelegd waaruit blijkt dat in de praktijk rapportages worden opgevraagd bij het BKWI. Er is geen verslaggeving van de controle en analyse ontvangen door het CBP.

2.7.3 Beoordeling

Niet is gebleken dat in de praktijk rapportages worden opgevraagd bij het BKWI. Niet is gebleken dat de gemeente Baarle-Nassau de van het BKWI verkregen informatie over het gebruik van persoonsgegevens via Suwinet analyseert. 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 College bescherming persoonsgegevens (CBP) volgt dat de Wet bescherming persoonsgegevens (Wbp) wordt overtreden, omdat de gemeente Baarle-Nassau twee normen uit het Normenkader GeVS (Gezamenlijke elektronische Voorzieningen SUWI) niet of onvoldoende naleeft.

1. Niet is gebleken dat de gemeente Baarle-Nassau het SUWI beveiligingsplan voldoende uitdraagt in de organisatie. Omdat de gemeente niet heeft kunnen aantonen dat het Beveiligingsplan van het Suwinet voldoende wordt uitgedragen in de organisatie, handelt de gemeente Baarle-Nassau in strijd met norm 1.4 van het Normenkader GeVS en daarmee tevens met artikel 13 Wbp.
2. 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 ZIENSWIJZE GEMEENTE BAARLE-NASSAU

Zienswijze gemeente Baarle Nassau

Bij haar zienswijze heeft de gemeente Baarle-Nassau een door burgemeester en wethouders goedgekeurd beveiligingsplan Suwinet gevoegd. Verder is als bijlage bij de zienswijze een vastgesteld besluit van burgemeester en wethouders tot benoeming van een Security Officer. Deze benoeming is volgens de gemeente Baarle-Nassau tijdelijk omdat per 1 september 2015 de centraal bij het SSC gestationeerde Security Officer in dienst zal treden die naast alle BIG onderdelen ook de Suwinet-beveiliging overneemt.

Naar aanleiding van norm 1.4 (het uitdragen van het beveiligingsplan) geeft de gemeente Baarle-Nassau aan dat de eerste mogelijkheid om het beveiligingsplan en de controles te bespreken in het managementteam op dinsdag 18 augustus 2015 is. De gemeente Baarle-Nassau geeft aan dat het verslag van deze vergadering niet tijdig geleverd kan worden, in verband met de reactietermijn die eveneens 18 augustus 2015 verloopt. De gemeente Baarle-Nassau geeft aan deze aanvullende informatie zo snel mogelijk te leveren.

Reactie CBP

Het CBP zal hieronder per onderzochte norm reageren op de zienswijze van de gemeente Baarle-Nassau.

1. De gemeente Baarle-Nassau heeft een beveiligingsplan Suwinet opgestuurd dat op 11 augustus 2015 is goedgekeurd door het college van burgemeester en wethouders van de gemeente Baarle-Nassau. De gemeente Baarle Nassau handelt hiermee conform norm 1.3 van het Normenkader GeVS. De geconstateerde overtreding van artikel 13 Wbp is hiermee beëindigd. De bevindingen zijn op dit punt aangepast.
2. In het beveiligingsplan Suwinet is opgenomen dat er binnen de gemeente gecommuniceerd wordt over het beveiligingsproces. Dit gebeurt door middel van periodiek werkoverleg en functioneringsgesprekken. Ook is beveiliging een onderwerp bij informatieverstrekking om het beveiligingsbewustzijn van het eigen personeel te verhogen. Hoewel het onderwerp beveiliging aan de orde komt tijdens werkoverleggen en functioneringsgesprekken, is onvoldoende gebleken dat het beveiligingsbeleid en het beveiligingsplan Suwinet worden uitgedragen in de organisatie. De gemeente Baarle-Nassau handelt hiermee in strijd met norm 1.4 van het Normenkader GeVS. De geconstateerde overtreding van artikel 13 Wbp is hiermee niet beëindigd. De bevindingen zijn op dit punt niet aangepast.
3. Het CBP is van oordeel dat, gelet op de korte tijd waarin het beveiligingsplan voor het Suwinet in werking is getreden (minder dan een jaar), en de passage die hierover in het beveiligingsplan Suwi is opgenomen, de gemeente Baarle-Nassau op dit punt conform norm 1.5 van het Normenkader GeVS handelt. Op dit punt is de overtreding van artikel 13 beëindigd. De bevindingen zijn op dit punt aangepast.
4. Ten aanzien van functiescheiding voor de Suwi-omgeving zijn in bijlage I van het beveiligingsplan Suwinet, getiteld Autorisaties Suwinet, vier functies gescheiden vastgelegd. De gemeente Baarle-Nassau handelt hiermee conform norm 2.2 van het Normenkader GeVS. De overtreding van artikel 13 Wbp is op dit punt beëindigd. De bevindingen zijn op dit punt aangepast.

5. De gemeente Baarle-Nassau heeft een taakomschrijving van de Security Officer opgesteld die deel uitmaakt van het beveiligingsplan Suwinet. Hieruit kan worden opgemaakt dat het tot de taken van de Security Officer behoort om rechtstreeks naar het college van burgemeester en wethouders te rapporteren. Uit de verstrekte informatie is gebleken dat de gemeente Baarle-Nassau een Security Officer heeft aangesteld die in de praktijk ook rechtstreeks aan het hoogste management dient te rapporteren. De korte periode tussen de aanstelling van de Security Officer (11 augustus 2015) en de indiening van de zienswijze (13 augustus 2015) in acht genomen, heeft de gemeente Baarle-Nassau onvoldoende tijd gehad om aan te tonen dat de Security Officer ook in de praktijk aan het hoogste management rapporteert. De gemeente Baarle-Nassau handelt niet in strijd met norm 2.3 van het Normenkader GeVS, en op dit punt evenmin in strijd met artikel 13 Wbp.
6. De gemeente Baarle-Nassau heeft een autorisatieprocedure opgesteld die deel uitmaakt van het beveiligingsplan Suwinet. Hieruit blijkt dat de gemeente Baarle-Nassau gebruikers die toegang hebben tot de Suwinet applicaties, op basis van een formele procedure autoriseert en registreert. De gemeente Baarle-Nassau handelt hiermee conform 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. De gemeente Baarle-Nassau heeft een procedure voor het gebruik van Suwinet opgesteld die deel uitmaakt van het beveiligingsplan Suwinet. Hieruit blijkt 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. De Security Officer controleert de rapportages. De gemeente Baarle-Nassau heeft geen verslagen van deze controles overgelegd of haar zienswijze generieke of specifieke rapportages van het BKWI bijgevoegd.

   Er is geen informatie of bewijs overgelegd waaruit blijkt dat in de praktijk rapportages worden opgevraagd bij het BKWI. Er is geen verslaggeving van de controle en analyse ontvangen door het CBP.

   Op basis van bovenstaande concludeert het CBP dat de gemeente Baarle-Nassau naar aanleiding van het rapport stappen heeft gezet, maar dat deze stappen nog niet hebben geleid tot een werkwijze conform norm 13.1 van het Normenkader. De overtreding van artikel 13 Wbp is op dit punt derhalve nog niet beëindigd. De verbeterpunten zullen worden meegenomen in de bevindingen, de juridische beoordeling blijft echter ongewijzigd.