COLLEGE BESCHERMING PERSOONSGEGEVENS

College bescherming persoonsgegevens

Onderzoek naar de beveiliging van persoonsgegevens via Suwinet Gemeente Brielle

z2015-00404

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

1. Niet is gebleken dat de gemeente Brielle het beveiligingsplan voor Suwinet uitdraagt. Hierdoor handelt de gemeente Brielle in strijd met norm 1.4 van het Normenkader GeVS, en daarmee tevens in strijd met artikel 13 Wbp;
2. Niet is gebleken dat het beveiligingsplan voor Suwinet geëvalueerd wordt door de gemeente Brielle. Hierdoor handelt de gemeente Brielle in strijd met norm 1.5 van het Normenkader GeVS, en daarmee tevens in strijd met artikel 13 Wbp;
3. De functiescheiding voor de Suwi-omgeving is onvoldoende beschreven. Hierdoor handelt de gemeente Brielle in strijd met norm 2.2 van het Normenkader GeVS, en daarmee tevens in strijd met artikel 13 Wbp;
4. Niet is gebleken dat de gemeente Brielle een Security Officer heeft aangesteld die in de praktijk rechtstreeks aan het hoogste management rapporteert. De gemeente Brielle handelt hiermee in strijd met norm 2.3 van het Normenkader GeVS, en daarmee tevens met artikel 13 Wbp;
5. De toegang tot Suwinet wordt niet beperkt tot de medewerkers die gegevens via Suwinet op basis van de uit te voeren functie en taken mogen inzien. De gemeente Brielle handelt hiermee in strijd met norm 13.1 van het Normenkader GeVS en daarmee tevens met artikel 13 Wbp.
6. De controle op verleende toegangsrechten vindt niet plaats conform norm 13.5, 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 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. Een goede beveiliging is van belang omdat binnen Suwinet steeds meer verschillende gegevens 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] http://www.bkwi.nl/uploads/media/20150408_Handreiking_autorisatie_op_Suwinet-Inkijk_voor_GSD_01.pdf

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

1.2 Aanleiding

Uit verschillende onderzoeken blijkt dat de beveiliging van Suwinet niet in alle gevallen voldoet aan de wettelijke vereisten. Recent onderzoek van het College bescherming persoonsgegevens (CBP) heeft uitgewezen dat de GeVS bij de toegang tot Suwinet voor niet-Suwipartijen onvoldoende beveiligd was, onder meer omdat raadplegingen niet adequaat werden gelogd en een beveiligingsplan ontbrak[3]. In 2013 heeft de Inspectie SZW onderzoek gedaan naar de beveiliging van Suwinet. In dit onderzoek bleek dat slechts 4% van de gemeenten bij het gebruik van Suwinet voldoende maatregelen had getroffen om de vertrouwelijkheid van uitgewisselde gegevens te waarborgen. Gezien de uitkomsten van dat onderzoek heeft de Inspectie SZW dit onderzoek in 2014 bij een groot aantal gemeenten herhaald.

Op 4 juni 2015 is de definitieve rapportage van dit laatstbedoelde onderzoek zoals opgesteld door de Inspectie SZW (verder: rapportage) aangeboden aan de Tweede Kamer. Uit de rapportage blijkt onder meer dat negen gemeenten geen van de zeven onderzochte beveiligingsnormen naleeft. Het CBP heeft besloten onderzoek in te stellen naar acht van deze negen gemeenten.

Dit rapport betreft de bevindingen van het onderzoek aangaande de gemeente Brielle, zijnde één van de bovenbedoelde gemeenten.

1.3 Doel en reikwijdte van het onderzoek

Het onderzoek beoogt vast te stellen of de gemeente Brielle, zijnde de 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);

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

6. Een formele autorisatieprocedure (norm 13.1);
7. Controle op verleende toegangsrechten (norm 13.5).

1.5 Werkwijze

In de rapportage heeft de Inspectie SZW aangegeven dat de gemeente Brielle 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 Brielle 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 Brielle 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 Brielle vertrouwelijke (bedrijfs)gegevens bevatten.
De gemeente Brielle heeft bij brief van 11 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.

1.7 Verantwoordelijke en bewerker

Het begrip 'verantwoordelijke' betekent in de zin van de Wbp degene die alleen of tezamen met anderen het doel en de middelen van de gegevensverwerkingen bepaalt. Omdat de gemeente Brielle de formeel-juridische bevoegdheid heeft om doel en middelen van de gegevensverwerkingen via Suwinet te bepalen, is de gemeente Brielle, ook in materiele zin, verantwoordelijk voor gegevensverwerkingen door middel van Suwinet. De gemeente Nissewaard is aangesloten op Suwinet en raadpleegt Suwinet mede namens de gemeente Brielle. Dit betekent dat de gemeente Nissewaard is aan te merken als bewerker in de zin van de Wbp. De gemeente Nissewaard dient zich als op het Suwinet aangesloten partij te houden aan het Normenkader GeVS.
Op grond van artikel 14 Wbp dient de gemeente Brielle zorg te dragen voor voldoende waarborgen ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerkingen. Ingevolge artikel 14 Wbp dient de gemeente Brielle erop toe te zien dat de gemeente Nissewaard, zich als aangesloten partij, ten aanzien van de verwerkingen van persoonsgegevens via Suwinet die zij voor de gemeente Brielle uitvoert, houdt aan het Normenkader GeVS.

2 BEVINDINGEN

2.1 Beveiligingsbeleid en beveiligingsplan

2.1.1 Norm

Volgens het Normenkader GeVS dient onder meer het beveiligingsplan van het Suwinet te zijn goedgekeurd door het management van de Suwipartij (norm 1.3). Omdat de gemeente Nissewaard in dit geval optreedt als bewerker voor de gemeente Brielle, dient de gemeente Brielle aan te tonen dat de gemeente Nissewaard voor de werkzaamheden die de gemeente Nissewaard ten behoeve van de gemeente Brielle uitvoert, een beveiligingsplan van het Suwinet heeft, dat is goedgekeurd door het management.

2.1.2 Bevindingen

In de bevindingen van de Inspectie SZW wordt aangegeven dat ten tijde van het onderzoek het beveiligingsplan van het Suwinet niet is goedgekeurd door het management of de leiding van de gemeente Brielle.

In haar zienswijze heeft de gemeente Brielle aangegeven dat de gemeente Nissewaard, die de uitvoering van Suwi gerelateerde onderwerpen voor de gemeente Brielle verzorgd, sinds 9 december 2014 beschikt over een vastgesteld beveiligingsplan Suwinet.

2.1.3 Beoordeling

De gemeente Brielle beschikt over een vastgesteld beveiligingsplan voor Suwinet. De gemeente Brielle handelt hiermee 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 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 Brielle geen informatie heeft verstrekt waaruit blijkt dat het beveiligingsplan voor Suwinet van de gemeente Brielle wordt uitgedragen in de organisatie.

In de zienswijze van de gemeente Brielle en het beveiligingsplan Suwinet van de gemeente Nissewaard wordt aangegeven dat de communicatie rondom informatiebeveiliging is belegd bij de Security Officer. Het CBP

heeft verder geen informatie van de gemeente Brielle ontvangen waaruit blijkt dat beveiligingsplan voor Suwinet wordt uitgedragen.

2.2.3 Beoordeling

Niet is gebleken dat de gemeente Brielle het beveiligingsplan voor Suwinet uitdraagt in de organisatie. Hiermee handelt de gemeente Brielle op dit punt 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 worden geëvalueerd.

2.3.2 Bevindingen

De gemeente Brielle heeft volgens de bevindingen van de Inspectie SZW niet aangetoond dat het beveiligingsplan voor Suwinet wordt geëvalueerd.

Het CBP heeft geen informatie van de gemeente Brielle ontvangen waaruit blijkt dat het beveiligingsplan voor Suwinet jaarlijks wordt geëvalueerd.

2.3.3 Beoordeling

Niet is gebleken dat het beveiligingsplan voor het Suwinet geëvalueerd wordt door de gemeente Brielle. Hierdoor handelt de gemeente Brielle in strijd met norm1.5 van het Normenkader GeVS, en daarmee tevens 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 Brielle de wijze waarop taken, verantwoordelijkheden en bevoegdheden ten aanzien van het gebruik, de inrichting, het beheer en de beveiliging van Suwinet gegevens, applicaties, processen en infrastructuur zijn belegd, beschreven in een Beveiligingsplan van het Suwinet dat niet is goedgekeurd.

De zienswijze van de gemeente Brielle geeft aanleiding om de bevindingen als volgt aan te vullen. Ten aanzien van functiescheiding voor de Suwi-

omgeving zijn in het beveiligingsplan Suwinet vier functies weliswaar gescheiden vastgelegd, maar er wordt hierbij geen onderscheid gemaakt tussen de functie van de medewerker die autorisaties verstrekt en de medewerker die de autorisaties controleert.

2.4.3 Beoordeling

De functiescheiding is onvoldoende beschreven, omdat de functies onvoldoende gescheiden zijn belegd. Er wordt geen onderscheid gemaakt tussen de functie van de medewerker die autorisaties verstrekt en de medewerker die de autorisaties controleert. Op grond hiervan kan worden geconcludeerd dat in strijd met norm 2.2. gehandeld wordt door de gemeente Brielle. De gemeente Brielle handelt hiermee op dit punt tevens in strijd met 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 er ten tijde van het onderzoek bij de gemeente Brielle geen Security Officer is aangesteld.

De zienswijze van de gemeente Brielle geeft aanleiding om de bevindingen als volgt aan te vullen. In het beveiligingsplan is een functieomschrijving van de Security Officer opgenomen. Uit de functieomschrijving blijkt dat de Security Officer periodiek rechtstreeks aan het college van burgemeester en wethouders dient te rapporteren. De gemeente Brielle geeft voorts in haar zienswijze aan dat de gemeente Nissewaard inmiddels een Security Offcer heeft aangesteld die de gehele informatiebeveiliging, inclusief de evaluaties aanstuurt. De gemeente Brielle heeft hier geen ondersteunende informatie of bewijs voor aangedragen. Evenmin is uit de zienswijze van de gemeente Brielle gebleken dat de Security Officer in de praktijk rechtstreeks aan het hoogste management heeft gerapporteerd (door middel van verslagen of rapportages).

2.5.3 Beoordeling

Niet is gebleken dat de gemeente Brielle een Security Officer heeft aangesteld, noch dat die in de praktijk rechtstreeks aan het hoogste management rapporteert. De gemeente Brielle 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).

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[4]. Deze mogen worden toebedeeld aan een beperkte groep gespecialiseerde medewerkers zoals de sociale recherche.

2.6.2 Bevindingen

De gemeente Brielle heeft volgens de bevindingen van de Inspectie SZW geen informatie overgelegd waaruit blijkt dat autorisaties worden toegekend, aangepast en gewijzigd volgens een vastgestelde formele procedure. Er is geen antwoord gekomen op de vraag van de Inspectie SZW naar een verschil in de opgave van Brielle over het aantal zware rollen, en eenzelfde opgave van het BKWI. Vastgesteld is dat er gedurende tenminste de eerste drie kwartalen van 2014 sprake is geweest van een groot aantal inactieve accounts zonder dat daar actie op is ondernomen door de gemeente Brielle.

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

De zienswijze van de gemeente Brielle geeft aanleiding om de bevindingen als volgt aan te vullen. Bijlage I van het beveiligingsplan Suwinet betreft de autorisatieprocedure Suwinet. Hierin wordt aangeven dat maandelijks wordt gecontroleerd of de gebruikers op basis van hun functie nog toegang moeten hebben tot Suwinet en of de toegekende rollen nog in overeenstemming zijn met hun functie. Deze controles worden gearchiveerd.

De gemeente heeft ook een autorisatiematrix overgelegd waaruit blijkt dat de applicatiebeheerder toegang heeft tot alle rollen, inclusief de zware rollen als Fraudevorderingen, RDW Fraude, GBA zoeken en GBA zoeken uitgebreid. Uit deze matrix blijkt ook dat alle medewerkers, afgezien van de Security Officer en de medewerker inburgering, toegang hebben tot Fraudevorderingen.

2.6.3 Beoordeling

De gemeente Brielle autoriseert en registreert de gebruikers die toegang hebben tot de Suwinet applicaties op basis van een formele procedure. Omdat vrijwel alle medewerkers toegang hebben tot Fraudevorderingen, is de toegang niet beperkt tot de medewerkers die gegevens op basis van de uit te voeren functie en taken mogen inzien. De gemeente Brielle handelt hiermee in strijd met norm 13.1 van het Normenkader GeVS 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 Brielle geen procedure voor de controle op de verleende toegangsrechten overgelegd. Er is geen bewijs aangeleverd van de beoordelingen en rapportages over de controle van de rapportages van BKWI, er is geen standaardprocedure voor deze controles vastgelegd.

De zienswijze van de gemeente Brielle geeft aanleiding om de bevindingen als volgt aan te vullen. De gemeente Brielle 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 door een medewerker geanalyseerd dient te worden.

Er zijn geen nadere stukken overgelegd waaruit blijkt dat het gebruik van Suwinet in de praktijk wordt gecontroleerd. De gemeente Brielle heeft geen controleverslagen of rapportages overgelegd. Er zijn evenmin generieke of specifieke rapportages bijgevoegd door de gemeente Brielle.

2.7.3 Beoordeling

Niet is gebleken dat de gemeente Brielle de van het BKWI verkregen informatie over het gebruik van persoonsgegevens via Suwinet meerdere keren per jaar opvraagt en controleert. Dit is in strijd met norm 13.5 van het Normenkader GeVS en daarmee tevens met artikel 13 Wbp.

3 CONCLUSIES

Uit het onderzoek van het CBP volgt dat de Wbp wordt overtreden, omdat de gemeente Brielle zes normen uit het Normenkader GeVS (Gezamenlijke elektronische Voorzieningen SUWI) niet of onvoldoende naleeft.

1. Niet is gebleken dat de gemeente Brielle het beveiligingsplan SUWI uitdraagt. Hierdoor handelt de gemeente Brielle in strijd met norm 1.4 van het Normenkader GeVS, en daarmee tevens in strijd met artikel 13 Wbp;
2. Niet is gebleken dat het SUWI beveiligingsplan geëvalueerd wordt door de gemeente Brielle. Hierdoor handelt de gemeente Brielle in strijd met norm1.5 van het Normenkader GeVS, en daarmee tevens in strijd met artikel 13 Wbp;
3. De functiescheiding voor de Suwi-omgeving is onvoldoende beschreven. Hierdoor handelt de gemeente Brielle in strijd met norm 2.2 van het Normenkader GeVS, en daarmee tevens in strijd met artikel 13 Wbp;
4. Niet is gebleken dat de gemeente Brielle een Security Officer heeft aangesteld die in de praktijk rechtstreeks aan het hoogste management rapporteert. De gemeente Brielle handelt hiermee in strijd met norm 2.3 van het Normenkader GeVS, en daarmee tevens met artikel 13 Wbp;
5. De toegang tot Suwinet wordt niet beperkt tot de medewerkers die gegevens via Suwinet op basis van de uit te voeren functie en taken mogen inzien. De gemeente Brielle handelt hiermee in strijd met norm 13.1 van het Normenkader GeVS en daarmee tevens met artikel 13 Wbp.
6. De controle op verleende toegangsrechten vindt niet plaats conform norm 13.5, 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 BRIELLE

Zienswijze gemeente Brielle

De gemeente Brielle stelt in haar zienswijze dat de bevindingen in het Rapport van voorlopige bevindingen inmiddels achterhaald zijn en daardoor niet meer correct. In de zienswijze zet de gemeente per norm uiteen wat de actuele stand van zaken is.

In haar zienswijze geeft de gemeente aan dat de zij zelf niet is aangesloten op het Suwinet. Binnen haar organisatie zijn dan ook geen medewerkers werkzaam die toegang hebben tot Suwinet. Alle taken die zijn gerelateerd aan het gebruik van Suwinet zijn belegd bij de gemeente Nissewaard. Hier ligt ook de aansturing op het veilig gebruik van Suwinet. De gemeente Nissewaard is, binnen een Gemeenschappelijke regeling met centrumgemeente constructie, uitvoerder van alle aan gemeenten opgedragen taken op het gebied van werk, inkomen en zorg.

Het onderzoek van de Inspectie SZW naar het veilig gebruik van Suwinet over 2014, heeft zich, aldus de gemeente Brielle, als verantwoordelijke voor de in onze gemeente woonachtige bijstandsgerechtigden, gericht op de gemeente Brielle, maar heeft materieel betrekking op de uitvoeringssituatie in Nissewaard. Inmiddels zijn verbeteringen gerealiseerd waarvan onderstaande overzicht wordt gegeven.

1. Norm 1.3

Sinds 9 december 2014 beschikt de gemeente Nissewaard over een geldig beveiligingsplan Suwinet. Deze is bijgevoegd bij de zienswijze.

2. Norm 1.4

Zoals aangegeven kent de gemeente Brielle geen (gebruikers van het) Suwinet. Binnen de gemeente Nissewaard geldt dat alle gebruikers bij de mailwisseling met betrekking tot Suwinet standaard geïnformeerd worden over de regels en de privacyaspecten betreffende Suwinet.

3. Norm 1.5

De gemeente Nisserwaard heeft inmiddels een Security Officer aangesteld die de gehele informatiebeveiliging, inclusief de evaluaties, aanstuurt.

4. Norm 2.2

Door de aanstelling van de Security Officer konden de verantwoordelijkheden rondom de informatiebeveiliging worden geoptimaliseerd. De Security Officer is eindverantwoordelijke die buiten dát deel van de organisatie is geplaatst waarin de operationele bevragingen van Suwinet worden uitgevoerd. Hiermee is de verantwoordelijkheid rondom de Suwinet informatiebeveiliging in lijn met wat het rijk beoogd.

5. Norm 2.3
Evaluaties en rapportages zijn onderdeel van het takenpakket van de Security Officer en worden conform uitgevoerd.

6. Norm 13.1
Ook de nieuwe autorisatieprocedure is inmiddels vastgesteld en geïmplementeerd door de gemeente Nissewaard. Maandelijks wordt gecontroleerd of de gebruikers (binnen de gemeente Nissewaard) op basis van hun functie nog toegang moeten hebben tot Suwinet en of de toegekende rollen nog in overeenstemming zijn met hun functie. Deze controles worden gearchiveerd. Zoals aangegeven zijn er binnen de gemeente Brielle geen gebruikers van Suwinet.

7. Norm 13.5
De Security Officer van de gemeente Nissewaard heeft de controle van het gebruik ter hand genomen en deze belegd en geborgd in de eigen organisatie.

Reactie CBP
Alvorens puntsgewijs in te gaan op de zienswijze van de gemeente Brielle op het Rapport van voorlopige bevindingen, gaat het CBP in op het begrip 'verantwoordelijke' uit de Wbp.

De gemeente Brielle geeft in haar zienswijze aan dat het onderzoek van de Inspectie SZW naar het veilig gebruik van Suwinet over 2014, gericht was op de gemeente Brielle, maar materieel betrekking heeft op de uitvoeringssituatie in Nissewaard.

Het begrip 'verantwoordelijke' betekent in de zin van de Wbp degene die alleen of tezamen met anderen het doel en de middelen van de gegevensverwerkingen bepaalt. Omdat de gemeente Brielle de formeel-juridische bevoegdheid heeft om doel en middelen van de gegevensverwerkingen via Suwinet te bepalen, is de gemeente Brielle, ook in materiele zin, verantwoordelijk voor gegevensverwerkingen door middel van Suwinet. De gemeente Nissewaard is aangesloten op Suwinet en raadpleegt Suwinet mede namens de gemeente Brielle. Dit betekent dat de gemeente Nissewaard is aan te merken als bewerker in de zin van de Wbp. De gemeente Nissewaard dient zich als op het Suwinet aangesloten partij te houden aan het Normenkader GeVS.
Op grond van artikel 14 Wbp dient de gemeente Brielle zorg te dragen voor voldoende waarborgen ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerkingen. Ingevolge artikel 14 Wbp dient de gemeente Brielle erop toe te zien dat de

gemeente Nissewaard, zich als aangesloten partij houdt aan het Normenkader GeVS.

Hieronder zal het CBP puntsgewijs ingaan op de zienswijze van de gemeente Brielle.

1. Norm 1.3

Het CBP heeft geconstateerd dat de gemeente Nissewaard, die de uitvoering van Suwi gerelateerde onderwerpen voor de gemeente Brielle verzorgd, sinds 9 december 2014 beschikt over een goedgekeurd beveiligingsplan Suwinet. Hiermee handelt de gemeente Brielle conform norm 1.3 van het Normenkader GeVS. De overtreding van artikel 13 Wbp is hiermee beëindigd. De bevindingen zijn op dit punt aangepast.

2. Norm 1.4

In het beveiligingsplan Suwinet wordt de communicatie rondom informatiebeveiliging belegd bij de Security Officer. Het CBP heeft verder geen informatie van de gemeente Brielle ontvangen waaruit blijkt dat het beveiligingsplan Suwinet worden uitgedragen binnen de organisatie. De bevindingen zijn op dit punt niet aangepast.

3. Norm 1.5

Het CBP heeft geen informatie van de gemeente Brielle ontvangen waaruit blijkt dat beveiligingsplan Suwinet jaarlijks worden geëvalueerd en geactualiseerd. De bevindingen zijn op dit punt niet aangepast.

4. Norm 2.2

Ten aanzien van functiescheiding voor de Suwi-omgeving zijn in het beveiligingsplan Suwinet vier functies weliswaar gescheiden vastgelegd, maar er wordt hierbij geen onderscheid gemaakt tussen de functie van de medewerker die autorisaties verstrekt en de medewerker die de autorisaties controleert. Dit is strijdig met norm 2.2 omdat de functies onvoldoende gescheiden zijn belegd. De gemeente heeft hierin stappen gemaakt, maar nog onvoldoende om volledig aan norm 2.2 van het Normenkader GeVS te voldoen. De bevindingen zijn op dit punt aangepast, echter de juridische conclusie dat op dit punt artikel 13 Wbp wordt overtreden, blijft ongewijzigd.

5. Norm 2.3

In het beveiligingsplan is een functieomschrijving van de Security Officer opgenomen. Uit de functieomschrijving blijkt dat de Security Officer periodiek rechtstreeks aan het college van burgemeester en wethouders dient te rapporteren. Het CBP heeft geen informatie ontvangen van de gemeente Brielle waaruit blijkt dat de Security Officer in de praktijk

rechtstreeks aan het hoogste management heeft gerapporteerd (door middel van verslagen of rapportages).
Op dit punt zijn duidelijk stappen gemaakt, maar nog onvoldoende om te kunnen concluderen dat volledig aan norm 2.3 van het Normenkader GeVS wordt voldaan. De bevindingen zijn op dit punt aangepast.

6. Norm 13.1

Bijlage I van het beveiligingsplan Suwinet betreft de autorisatieprocedure Suwinet. Hierin wordt aangeven dat maandelijks wordt gecontroleerd of de gebruikers (binnen de gemeente Nissewaard) op basis van hun functie nog toegang moeten hebben tot Suwinet en of de toegekende rollen nog in overeenstemming zijn met hun functie. Deze controles worden gearchiveerd. De gemeente heeft ook een autorisatiematrix overgelegd waaruit blijkt dat de applicatiebeheerder toegang heeft tot alle rollen, inclusief de zware rollen als Fraudevorderingen, RDW Fraude, GBA zoeken en GBA zoeken uitgebreid. Uit deze matrix blijkt ook dat alle medewerkers, afgezien van de Security Officer en de medewerker inburgering, toegang hebben tot Fraudevorderingen.

De gemeente Brielle autoriseert en registreert de gebruikers die toegang hebben tot de Suwinet applicaties op basis van een formele procedure. Omdat de applicatiebeheerder toegang heeft tot vrijwel alle (zware) rollen en vrijwel alle medewerkers toegang hebben tot Fraudevorderingen, is de toegang niet beperkt tot de medewerkers die gegevens op basis van de uit te voeren functie en taken mogen inzien De gemeente Brielle handelt hiermee in strijd met norm 13.1 van het Normenkader GeVS en artikel 13 Wbp. De bevindingen zijn op basis van bovenstaande aangevuld. De overtreding van artikel 13 is echter niet beëindigd.

7. Norm 13.5

De gemeente Brielle 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 door een medewerker geanalyseerd dient te worden.

Er is geen informatie aangeleverd waaruit blijkt dat het gebruik van Suwinet in de praktijk wordt gecontroleerd. De gemeente Brielle heeft geen controleverslagen overgelegd. Er zijn evenmin generieke of specifieke rapportages bijgevoegd door de gemeente Brielle.

Hoewel de gemeente Brielle een procedure voor de controle voor op het gebruik heeft overgelegd, kan niet worden geconcludeerd dat de gemeente Brielle volledig conform 13.5 van het Normenkader GeVS handelt. De overtreding van artikel 13 Wbp is niet beëindigd. De bevindingen worden op dit punt aangepast, echter de juridische beoordeling van de feiten blijft ongewijzigd.