COLLEGE BESCHERMING PERSOONSGEGEVENS

College bescherming persoonsgegevens

Onderzoek naar de beveiliging van persoonsgegevens via Suwinet Gemeente Brummen

z2015-00403

Openbare versie
Rapport van bevindingen

November 2015

DATUM November 2015

INHOUDSOPGAVE

Samenvatting **4**

1 Inleiding **6**
1.1 Achtergrond 6
1.2 Aanleiding 6
1.3 Doel en reikwijdte van het onderzoek 7
1.4 Onderzoeksvraag 7
1.5 Werkwijze 7
1.6 Juridisch kader 8
1.7 Verantwoordelijke en bewerker 8

2 Bevindingen **10**
2.1 Beveiligingsbeleid en beveiligingsplan 10
2.1.1 Norm 10
2.1.2 Bevindingen 10
2.1.3 Beoordeling 10
2.2 Uitdragen informatiebeveiligingsbeleid en beveiligingsplan 11
2.2.1 Norm 11
2.2.2 Bevindingen 11
2.2.3 Beoordeling 11
2.3 Evaluatie Informatiebeveiligingsbeleid en SUWI beveiligingsplan 12
2.3.1 Norm 12
2.3.2 Bevindingen 12
2.3.3 Beoordeling 12
2.4 Functiescheiding 12
2.4.1 Norm 12
2.4.2 Bevindingen 12
2.4.3 Beoordeling 13
2.5 De Security Officer 13
2.5.1 Norm 13
2.5.2 Bevindingen 13
2.5.3 Beoordeling 13
2.6 Autorisatieprocedure 14
2.6.1 Norm 14
2.6.2 Bevindingen 14
2.6.3 Beoordeling 14
2.7 Controle op verleende toegangsrechten 15
2.7.1 Norm 15
2.7.2 Bevindingen 15
2.7.3 Beoordeling 15

3 Conclusies **16**

Bijlage I: Reactie CBP op de zienswijze van de gemeente Brummen **17**
Zienswijze gemeente Brummen 17
Reactie CBP 20

SAMENVATTING

Uit het onderzoek van het College bescherming persoonsgegevens (CBP) volgt dat de Wet bescherming persoonsgegevens (Wbp) wordt overtreden, omdat de gemeente Brummen zeven normen uit het Normenkader GeVS (Gezamenlijke elektronische Voorzieningen SUWI) niet of onvoldoende naleeft.

1. Niet is gebleken dat de gemeente Brummen beschikt over een (goedgekeurd) beveiligingsplan voor Suwinet. De gemeente Brummen handelt hiermee in strijd met norm 1.3 uit het Normenkader GeVS en daarmee tevens met artikel 13 Wbp;
2. Niet is gebleken dat het beveiligingsplan voor Suwinet wordt uitgedragen in de organisatie. De gemeente Brummen handelt hiermee in strijd met norm 1.4 van het Normenkader GeVS en daarmee tevens met artikel 13 Wbp;
3. Niet is gebleken dat de gemeente Brummen een evaluatie heeft uitgevoerd op het beveiligingsplan voor Suwinet. Hierdoor handelt de gemeente Brummen in strijd met norm 1.5 van het Normenkader GeVS en daarmee tevens met artikel 13 Wbp;
4. Niet is gebleken dat functiescheiding is doorgevoerd. De gemeente Brummen handelt hiermee in strijd met norm 2.2 van het Normenkader GeVS en op dit punt tevens in strijd met artikel 13 Wbp;
5. De taken en verantwoordelijkheden van de Security Officer zijn onvoldoende beschreven en niet is gebleken dat zij in de in de praktijk zijn gebracht. Hierdoor handelt de gemeente Brummen in strijd met norm 2.3 van het Normenkader GeVS, en daarmee in strijd met artikel 13 Wbp;
6. Niet is gebleken dat de gebruikers die toegang hebben tot de Suwinet applicaties op basis van een formele procedure worden geautoriseerd en geregistreerd. De gemeente Brummen handelt hiermee in strijd met norm 13.1 van het Normenkader en daarmee tevens met artikel 13 Wbp;
7. 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. 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.

1.2 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

[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

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 Brummen, zijnde één van de bovenbedoelde gemeenten.

1.3 Doel en reikwijdte van het onderzoek

Het onderzoek beoogt vast te stellen of de gemeente Brummen, zijnde de verantwoordelijke voor verwerkingen van persoonsgegevens via Suwinet in de zin van de Wbp, passende technische en organisatorische maatregelen heeft getroffen om deze persoonsgegevens te beveiligen.

1.4 Onderzoeksvraag

Onderzocht is of de verantwoordelijke passende technische en organisatorische maatregelen ten uitvoer heeft gelegd teneinde persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking, zoals bedoeld in artikel 13 Wet bescherming persoonsgegevens (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 Brummen 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 Brummen 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 Brummen 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 Brummen vertrouwelijke (bedrijfs)gegevens bevatten.

De gemeente Brummen heeft bij brief van 11 augustus 2015 haar zienswijze ingebracht. De gemeente Brummen heeft geen reactie ingebracht ten aanzien van de bedrijfsvertrouwelijkheid.

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.

De verantwoording 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 Brummen de formeel-juridische bevoegdheid heeft om doel en middelen van de gegevensverwerkingen via Suwinet te bepalen, is de gemeente Brummen, ook in materiele zin, verantwoordelijk voor gegevensverwerkingen door

middel van Suwinet. De gemeente Apeldoorn is aangesloten op Suwinet en raadpleegt Suwinet mede namens de gemeente Brummen. Dit betekent dat de gemeente Apeldoorn is aan te merken als bewerker in de zin van de Wbp. De gemeente Apeldoorn dient zich als op het Suwinet aangesloten partij te houden aan het Normenkader GeVS.
Op grond van artikel 14 Wbp dient de gemeente Brummen 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 Brummen erop toe te zien dat de gemeente Apeldoorn, zich, als aangesloten partij, ten aanzien van de verwerkingen van persoonsgegevens via Suwinet die zij voor de gemeente Brummen 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 Apeldoorn in dit geval optreedt als bewerker voor de gemeente Brummen, dient de gemeente Brummen aan te tonen dat de gemeente Apeldoorn voor de werkzaamheden die de gemeente Apeldoorn ten behoeve van de gemeente Brummen uitvoert, een beveiligingsplan voor 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 voor Suwinet niet is overgelegd door de gemeente Brummen.

De gemeente Brummen heeft bij haar zienswijze op het Rapport van voorlopige bevindingen een document gevoegd getiteld 'ICT Beveiligingsdocument (inclusief Suwinet)', ondertekend op 19 juni 2015. Dit document bevat een passage over de beveiliging van Suwinet.
De gehele uitvoering van het domein Werk en Inkomen is door de gemeente Brummen uitbesteed aan de gemeente Apeldoorn. De gemeente Apeldoorn maakt hierbij gebruik van Suwinet. Het 'ICT Beveiligingsdocument' van de gemeente Brummen bevat een passage over de beveiliging voor Suwinet bij de gemeente Apeldoorn. De zienswijze bevat geen specifiek beveiligingsplan voor Suwinet van de gemeente Apeldoorn.
De gemeente Brummen heeft ook toegang tot Suwinet voor de uitvoering van werkzaamheden door de afdeling Burgerzaken. Hiervoor heeft de gemeente evenmin een beveiligingsplan voor Suwinet overgelegd.

2.1.3 Beoordeling

De gemeente Brummen heeft aangegeven dat er voor de uitvoering van het domein Werk en Inkomen gebruik wordt gemaakt van het beveiligingsplan voor Suwinet van de gemeente Apeldoorn. Echter het beveiligingsplan van de gemeente Apeldoorn is niet bij de zienswijze gevoegd. Hierdoor heeft de gemeente Brummen niet aangetoond dat de gemeente Apeldoorn ten aanzien van de uitvoering van het domein Werk en Inkomen, beschikt over een goedgekeurd beveiligingsplan voor Suwinet. De gemeente Brummen heeft evenmin een beveiligingsplan overgelegd voor de toegang die de gemeente Brummen heeft voor de afdeling Burgerzaken.

Nu niet is gebleken dat de gemeente Brummen, noch voor de afdeling Burgerzaken, noch voor de werkzaamheden die worden uitgevoerd door de gemeente Apeldoorn, over een (goedgekeurd) Beveiligingsplan voor Suwinet te beschikken, handelt de gemeente Brummen in strijd met norm 1.3 uit het Normenkader GeVS. Hiermee wordt op dit punt tevens artikel 13 Wbp overtreden.

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 Brummen geen informatie heeft verstrekt waaruit blijkt dat het beveiligingsplan voor Suwinet van de gemeente Brummen worden uitgedragen in de organisatie.

In de zienswijze van de gemeente Brummen op het rapport van voorlopige bevindingen wordt het volgende aangegeven:

De gemeente Brummen is bezig de BIG (Baseline Informatiebeveiliging Gemeenten) te implementeren in de organisatie. Dit project wordt in 2015 afgerond en dient jaarlijks te worden geëvalueerd. Suwinet maakt hier onderdeel van uit.

Het informatiebeveiligingsbeleid is verder voor alle gebruikers centraal beschikbaar. Op intranet staat het informatiebeveiligingsplan gepubliceerd. Alle medewerkers kunnen hierop de gegevens raadplegen betreffende beveiligingseisen.

Daarnaast worden volgens de gemeente Brummen regelmatig acties uitgevoerd om de medewerkers te attenderen op het bestaan van het beveiligingsbeleid, plan of passage, zoals bijvoorbeeld phishingmails en mysteryguests. Daarnaast is er ook een online quiz over informatiebeveiliging geweest waarbij iets kon worden gewonnen. Verder is informatiebeveiliging een vast te bespreken onderwerp geweest tijdens de jaarlijkse functioneringsgesprekken en wordt het om de zoveel tijd geagendeerd tijdens de teamoverleggen.

Alle medewerkers leggen een eed of belofte af waarin tevens een geheimhoudingsverklaring is opgenomen. Medewerkers die geen aanstelling bij de gemeente Brummen hebben, maar zijn ingehuurd, ondertekenen een geheimhoudingsverklaring, waarin zij beloven vertrouwelijk om te gaan met de informatie die zij bij de gemeente Brummen onder ogen krijgen.

Hoewel de gemeente Brummen in haar zienswijze heeft aangegeven aandacht te besteden aan het onderwerp informatiebeveiliging, heeft de gemeente Brummen, noch voor de gemeente Brummen, noch voor de gemeente Apeldoorn, informatie (bewijs) overgelegd waaruit blijkt dat het beveiligingsplan voor Suwinet wordt uitgedragen.

2.2.3 Beoordeling

Nu niet is gebleken dat de gemeente Brummen, zowel voor de afdeling Burgerzaken en voor de werkzaamheden die worden uitgevoerd door de gemeente Apeldoorn, over een Beveiligingsplan voor Suwinet beschikt, kan worden geconcludeerd dat, noch door de gemeente Apeldoorn, noch door de gemeente Brummen beveiligingsplannen voor Suwinet worden uitgedragen. In aanmerking genomen dat er geen feiten en omstandigheden zijn waaruit blijkt dat beveiligingsplannen voor

Suwinet worden uitgedragen door de gemeente Brummen en de gemeente Apeldoorn, handelt de gemeente Brummen 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 wordt geëvalueerd.

2.3.2 Bevindingen

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

De gemeente Brummen heeft in haar zienswijze op het Rapport van voorlopige bevindingen geen beveiligingsplan voor Suwinet overgelegd. Hieruit volgt dat niet kan worden vastgesteld dat de gemeente Brummen voor zowel de eigen toegang tot Suwinet als voor de toegang van de gemeente Apeldoorn een beveiligingsplan heeft dat jaarlijks wordt geëvalueerd.

2.3.3 Beoordeling

Niet is gebleken dat de gemeente Brummen een evaluatie heeft uitgevoerd op het beveiligingsplan voor Suwinet. Hierdoor handelt de gemeente Brummen in strijd met norm 1.5 van het Normenkader GeVS en daarmee tevens 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 Brummen geen informatie overgelegd aan de Inspectie SZW over 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 beschreven en belegd.

De gemeente Brummen geeft in haar zienswijze aan dat de volledige uitvoering van Suwinet voor wat betreft het domein werk en inkomen is uitbesteed aan de gemeente Apeldoorn. De gemeente Brummen conformeert zich aan het Informatiebeveiligingsplan Dienst Samenleving. Daarin zijn de verschillende functies en de bijbehorende taken vastgelegd.

De functiescheiding van alle personen die zijn betrokken bij Suwinet zijn volgens de gemeente Brummen duidelijk. Er zijn medewerkers die Suwinet kunnen inzien. Het functioneel beheer ligt bij degene die de accounts aanmaakt en Suwinet beheert. Daarnaast is het team betrokken bij de controle op het gebruik van Suwinet en is er

sprake van een management die beslissingen neemt over wie wel of geen gebruik mag maken van Suwinet en beslissingen neemt bij eventueel oneigenlijk gebruik.

Hoewel de gemeente Brummen aangeeft dat de functiescheiding van alle personen die zijn betrokken bij Suwinet volgens de gemeente Brummen duidelijk zijn, heeft het CBP, noch voor de werkzaamheden die de gemeente Apeldoorn uitvoert ten behoeve van de gemeente Brummen, noch voor de afdeling Burgerzaken van de gemeente Brummen, stukken ontvangen waaruit blijkt dat functiescheiding voor de Suwi-omgeving is doorgevoerd binnen de betreffende organisaties. Het CBP heeft wel om dergelijke stukken verzocht.

2.4.3 Beoordeling

Niet is gebleken dat functiescheiding is doorgevoerd. De gemeente Brummen handelt hiermee in strijd met norm 2.2 van het Normenkader GeVS en 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 de taken en verantwoordelijkheden van de Security Officer niet zijn ontvangen.

In haar zienswijze geeft de gemeente Brummen aan dat er binnen de gemeente Brummen een Security Officer functioneert. Echter, deze is niet formeel benoemd. De gemeente Brummen geeft aan op korte termijn een Security Officer aan te zullen stellen. Deze Security Officer zal verantwoordelijk worden voor de uit te voeren actiepunten, waaronder:

- Invullen zelfevaluatie SUWI;
- Verdere implementatie BIG;
- Contact met Security Officer van de gemeente Apeldoorn om alsnog de gegevens aan de Inspectie te kunnen zenden.

De Security Officer beheert volgens de gemeente Brummen de beveiligingsprocedures en rapporteert hierover aan het management en het college van burgemeester en wethouders.

2.5.3 Beoordeling

Niet is gebleken dat het tot het takenpakket van de Security Officer van Brummen of Apeldoorn behoort om beveiligingsprocedures te beheren en maatregelen in het

kader van Suwinet te beheersen, zodanig dat de beveiliging van Suwinet overeenkomstig wettelijke eisen is geïmplementeerd. Evenmin is gebleken dat de Security Officer van Brummen of Apeldoorn adviseert over de beveiliging van Suwinet, controleert dat met betrekking tot de beveiliging van Suwinet de maatregelen worden nageleefd en voorstellen doet tot implementatie of aanpassing van plannen op het gebied van de beveiliging van Suwinet. Tot slot heeft de gemeente Brummen niet aangetoond dat de Security Officer van Brummen of Apeldoorn rechtstreeks aan het hoogste management rapporteert.

De taken en verantwoordelijkheden van de Security Officer zijn onvoldoende beschreven en niet is gebleken dat zij in de in de praktijk zijn gebracht. Hierdoor handelt de gemeente Brummen in strijd met norm 2.3 van het Normenkader GeVS, en daarmee 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 Brummen heeft volgens de bevindingen van de Inspectie SZW geen procedure overgelegd die betrekking heeft op de wijze waarop autorisaties worden verleend.

In haar zienswijze verwijst de gemeente Brummen naar het informatiebeveiligingsplan Dienst samenleving en heeft de gemeente Brummen het 'ICT Beveiligingsdocument' bijgevoegd. Hierin wordt verwezen naar de wijze waarop medewerkers worden geautoriseerd voor toegang tot Suwinet. Het CBP heeft van de gemeente Brummen echter geen formele autorisatieprocedure voor toegang tot Suwinet ontvangen die betrekking heeft op de voor de werkzaamheden die de gemeente Apeldoorn ten behoeve van de gemeente Brummen uitvoert. Het CBP heeft evenmin een formele autorisatieprocedure voor toegang tot Suwinet ontvangen voor de uitvoering van werkzaamheden door de afdeling Burgerzaken.

2.6.3 Beoordeling

Niet is gebleken dat de gebruikers die toegang hebben tot de Suwinet applicaties op basis van een formele procedure worden geautoriseerd en geregistreerd. De gemeente Brummen handelt hiermee in strijd met 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 Brummen geen procedure voor de controle voor op de verleende toegangsrechten overgelegd. Evenmin is duidelijk wie deze controles uitvoert. Tot slot is onduidelijk hoe de van het BKWI verkregen informatie over het gebruik van gegevens die via Suwinet zijn geraadpleegd, geanalyseerd wordt en op welke wijze deze analyse plaatsvindt.

De gemeente Brummen geeft in haar zienswijze aan dat elke vier maanden een gebruiksrapportage via Suwinet-Inkijk wordt opgevraagd en onderzocht. Ook wordt volgens de gemeente Brummen aanvullende informatie opgevraagd als dit nodig is. Dit wordt ook aangegeven in het 'ICT Beveiligingsdocument'. De gemeente Brummen heeft echter geen informatie overgelegd waaruit blijkt of waarmee wordt aangetoond dat de door BKWI opgestelde rapportages over het gebruik van persoonsgegevens via Suwinet zijn opgevraagd en worden geanalyseerd.

2.7.3 Beoordeling

Niet is gebleken dat de door BKWI opgestelde rapportages over het gebruik van persoonsgegevens via Suwinet zijn opgevraagd en worden geanalyseerd. 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 Brummen zeven normen uit het Normenkader GeVS (Gezamenlijke elektronische Voorzieningen SUWI) niet of onvoldoende naleeft.

1. Niet is gebleken dat de gemeente Brummen beschikt over een (goedgekeurd) beveiligingsplan van het Suwinet. De gemeente Brummen handelt hiermee in strijd met norm 1.3 uit het Normenkader GeVS en daarmee tevens met artikel 13 Wbp;
2. Niet is gebleken dat het beveiligingsplan van het Suwinet wordt uitgedragen in de organisatie. De gemeente Brummen handelt hiermee in strijd met norm 1.4 van het Normenkader GeVS en daarmee tevens met artikel 13 Wbp;
3. Niet is gebleken dat de gemeente Brummen een evaluatie heeft uitgevoerd op het beveiligingsplan van het Suwinet. Hierdoor handelt de gemeente Brummen in strijd met norm 1.5 van het Normenkader GeVS en daarmee tevens met artikel 13 Wbp;
4. Niet is gebleken dat functiescheiding is doorgevoerd. De gemeente Brummen handelt hiermee in strijd met norm 2.2 van het Normenkader GeVS en op dit punt tevens in strijd met artikel 13 Wbp;
5. De taken en verantwoordelijkheden van de Security Officer zijn onvoldoende beschreven en niet is gebleken dat zij in de in de praktijk zijn gebracht. Hierdoor handelt de gemeente Brummen in strijd met norm 2.3 van het Normenkader GeVS, en daarmee in strijd met artikel 13 Wbp;
6. Niet is gebleken dat de gebruikers die toegang hebben tot de Suwinet applicaties op basis van een formele procedure worden geautoriseerd en geregistreerd. De gemeente Brummen handelt hiermee in strijd met norm 13.1 van het Normenkader en daarmee tevens met artikel 13 Wbp;
7. 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 DE ZIENSWIJZE VAN DE GEMEENTE BRUMMEN

Zienswijze gemeente Brummen

Voordat de gemeente Brummen ingaat op het Rapport van voorlopige bevindingen, geeft de gemeente in haar zienswijze aan dat de gehele uitvoering van het domein Werk en Inkomen is uitbesteed aan de gemeente Apeldoorn. Omdat tussen de gemeente Apeldoorn en de gemeente Brummen enige tijd onduidelijkheid heeft bestaan over de verantwoordelijkheid voor de informatievoorziening en de informatieverstrekking, is vanuit de gemeente Brummen niet tijdig gereageerd op de uitgezette vragen door de inspectie. Uit het definitieve verslag van de bevindingen Veilig Gebruik Suwinet 2014 bleek dan ook dat de gemeente niet voldeed aan de gestelde eisen.

De gemeente gaat vervolgens puntsgewijs in op het Rapport van voorlopige bevindingen.

1. Niet is gebleken dat de gemeente Brummen beschikt over een (goedgekeurd) Informatiebeveiligingsbeleid en een beveiligingsplan. De gemeente Brummen handelt hiermee in strijd met norm 1.3 uit het Normenkader GeVS en daarmee tevens met artikel 13 Wbp

De gemeente Brummen geeft aan dat er een informatiebeveiligingsplan 2014-2017 is, door het college goedgekeurd en vastgesteld op 26 augustus 2014. Dit informatiebeveiligingsplan is gericht op de gehele gemeente. Dit plan is conform de BIG (Baseline Informatiebeveiliging Gemeenten).

Zoals hierboven vermeld is de gehele uitvoering van het domein Werk en Inkomen uitbesteed aan de gemeente Apeldoorn. Gemeente Apeldoorn heeft daarnaast een goedgekeurd plan Informatiebeveiliging Dienst Samenleving, gericht op het werkplein Activerium. In het beveiligingsplan van het werkplein Activerium wordt specifiek aandacht besteed aan het onderdeel Suwinet. Omdat door de gemeente Apeldoorn ook werkzaamheden worden uitgevoerd voor regio gemeenten, waaronder de gemeente Brummen, is de gemeente Brummen ook in het plan opgenomen en is deze tevens op de gemeente Brummen van toepassing. Door de gemeente Brummen is schriftelijk bevestigd akkoord te zijn met het inzien van Suwinet door de bewoners van de gemeente Brummen.

2. Omdat niet is gebleken dat het Informatiebeveiligingsbeleid en het Beveiligingsplan van het Suwinet worden uitgedragen in de organisatie, handelt de gemeente Brummen in strijd met norm 1.4 van het Normenkader GeVS en daarmee tevens met artikel 13 Wbp

De gemeente Brummen is bezig om de BIG te implementeren in de organisatie. Dit project wordt in 2015 afgerond en dient jaarlijks te worden geëvalueerd. Suwinet maakt hier onderdeel van uit.

Het informatiebeveiligingsbeleid is verder voor alle gebruikers centraal beschikbaar. Op intranet staat het informatiebeveiligingsplan gepubliceerd. Alle medewerkers kunnen hierop de gegevens raadplegen betreffende beveiligingseisen.

Daarnaast worden regelmatig acties uitgevoerd om de medewerkers te attenderen op het bestaan van het beveiligingsbeleid, plan of passage, zoals bijvoorbeeld phishingmails en mysteryguests. Daarnaast is er ook een online quiz over informatiebeveiliging geweest waarbij iets kon worden gewonnen. Verder is informatiebeveiliging een vast te bespreken onderwerp geweest tijdens de jaarlijkse functioneringsgesprekken en wordt het om de zoveel tijd geagendeerd tijdens de teamoverleggen.

Uiteraard leggen alle medewerkers een eed of belofte af waarin tevens een geheimhoudingsverklaring is opgenomen. Medewerkers die geen aanstelling bij de gemeente Brummen hebben, maar zijn ingehuurd, ondertekenen een geheimhoudingsverklaring, waarin zij beloven vertrouwelijk om te gaan met de informatie die zij bij de gemeente Brummen onder ogen krijgen.

3. Niet is gebleken dat de gemeente Brummen een evaluatie heeft uitgevoerd op het Informatiebeveiligingsbeleid en het SUWI beveiligingsplan. Hierdoor handelt de gemeente Brummen in strijd met norm 1.5 van het Normenkader GeVS en daarmee tevens met artikel 13 Wbp

Tussen de gemeente Apeldoorn en de gemeente Brummen heeft onduidelijkheid bestaan over de verantwoordelijkheid voor het invullen van de zelfevaluatie. Inmiddels is dit opgehelderd. Helaas hebben wij de zelfevaluatie te laat ingevuld, zodat deze niet meer kon worden meegenomen met het conceptverslag van de Inspectie SZW.

4. De functiescheiding voor de Suwi-omgeving is niet of onvoldoende aangetoond. Hierdoor handelt de gemeente Brummen in strijd met norm 2.2 van het Normenkader GeVS, en daarmee in strijd met artikel 13 Wbp

Omdat de volledige uitvoering van Suwinet voor wat betreft het domein werk en inkomen is uitbesteed aan de gemeente Apeldoorn conformeert de gemeente Brummen aan het Informatiebeveiligingsplan Dienst Samenleving. Daarin zijn de verschillende functies en de bijbehorende taken vastgelegd.
Daarnaast is door de gemeente Apeldoorn een matrix opgesteld met daarin de functies van de medewerkers en de groepen waarin ze worden verdeeld. Ook is er een matrix opgesteld waarin vermeld wordt welke autorisatie er per groep binnen Suwinet is. Aan de hand hiervan wordt iemand aangemeld voor het gebruik van Suwinet.

De functiescheiding van alle personen die zijn betrokken bij Suwinet zijn duidelijk. Er zijn medewerkers die Suwinet kunnen inzien. Het functioneel beheer ligt bij degene die de accounts aanmaakt en Suwinet beheert. Daarnaast is het team betrokken bij de controle op het gebruik van Suwinet en is er sprake van een management die beslissingen neemt over wie wel of geen gebruik mag maken van Suwinet en beslissingen neemt bij eventueel oneigenlijk gebruik.

5. De taken en verantwoordelijkheden van de Security Officer zijn onvoldoende beschreven. Hierdoor handelt de gemeente Brummen in strijd met norm 2.3 van het Normenkader GeVS, en daarmee in strijd met artikel 13 Wbp

Binnen de gemeente Brummen is een Security Officer. Echter, deze is niet formeel benoemd. De gemeente Brummen geeft aan op korte termijn een Security Officer aan te zullen stellen. Deze Security Officer zal verantwoordelijk worden voor de uit te voeren actiepunten, waaronder:
- Invullen zelfevaluatie SUWI;
- Verdere implementatie BIG;
- Contact met Security Officer van de gemeente Apeldoorn om alsnog de gegevens aan de Inspectie te kunnen zenden.

De Security Officer beheert de beveiligingsprocedures en rapporteert hierover aan het management en het college van burgemeester en wethouders.

6. Niet is gebleken dat de gebruikers die toegang hebben tot de Suwinet applicaties op basis van een formele procedure worden geautoriseerd en geregistreerd. De gemeente Brummen handelt hiermee in strijd met norm 13.1 van het Normenkader en daarmee tevens met artikel 13 Wbp

Conform het informatiebeveiligingsplan Dienst samenleving wordt er, wanneer een medewerker Suwinet wil gaan gebruiken, bij het team Functioneel Beheer een account aangevraagd. Door de teamleider wordt hier toestemming voor gegeven en aan de hand van de matrix/functie medewerker wordt de rol van Suwinet bepaald. Per rol zijn autorisaties schriftelijk vastgelegd.

Een keer per kwartaal controleert Functioneel Beheer welke accounts geblokkeerd staan. Wanneer ze langer dan zes maanden geblokkeerd staan worden ze verwijderd. Wanneer medewerkers uit dienst zijn, worden de accounts ook beëindigd.

Daarnaast maakt het Team Burgerzaken gebruik van Suwinet. Hiervoor is een apart contract afgesloten.

7. De controle op verleende toegangsrechten vindt niet plaats conform norm 13.5, waardoor artikel 13 Wbp wordt overtreden.

Elke vier maanden vraagt de medewerker Kwaliteitszorg van het Team Functioneel Beheer een gebruiksrapportage op via Suwinet-Inkijk. Deze taak staat beschreven in het Informatiebeveiligingsplan van de Dienst Samenleving.
Daarnaast wordt elke vier maanden de resultaten van het onderzoek vastgelegd in het interne controleplan. Deze wordt per periode besproken in het MT en vastgesteld. Wanneer uit de gebruikersrapportage blijkt dat er nader onderzoek noodzakelijk is, vraagt de medewerker Kwaliteitszorg via de Security Officer aanvullende informatie op bij het BKWI. Door middel van een CD-ROM wordt aanvullende informatie aangeleverd (namen medewerkers). Naar aanleiding van deze informatie wordt nader onderzoek uitgevoerd en worden teammanagers geraadpleegd voor nadere toelichting. Wanneer uit onderzoek blijkt dat er sprake is van oneigenlijk gebruik, dan worden er maatregelen getroffen.

De gemeente Brummen concludeert dat er, door een intern communicatieprobleem, een onjuist beeld is ontstaan over de beveiliging van persoonsgegevens in het domein Werk en Inkomen die via Suwinet kunnen worden ingezien. Gezien bovenstaande komt de gemeente Brummen tot de conclusie dat de gemeente Brummen aan de belangrijkste veiligheidseisen voldoet. Een aantal actiepunten zijn opgepakt en worden geïmplementeerd. Gestreefd wordt om dit in 2015 gereed te hebben.

Reactie CBP

Het CBP gaat hieronder puntsgewijs in op de zienswijze van de gemeente Brummen.

1. Beveiligingsplan

De gehele uitvoering van het domein Werk en Inkomen is door de gemeente Brummen uitbesteed aan de gemeente Apeldoorn. De gemeente Apeldoorn maakt hierbij gebruik van Suwinet. Het op 19 juni 2015 ondertekende 'ICT Beveiligingsdocument' van de gemeente Brummen, bevat een passage over de beveiliging van Suwinet bij de gemeente Apeldoorn. De zienswijze bevat echter geen beveiligingsplan voor het Suwinet van de gemeente Apeldoorn. De gemeente Brummen heeft derhalve niet aangetoond dat een beveiligingsplan voor het Suwinet is goedgekeurd en wordt gehanteerd voor de werkzaamheden die de gemeente Apeldoorn ten behoeve van de gemeente Brummen uitvoert. De bevindingen blijven op dit punt ongewijzigd.

De gemeente Brummen heeft ook toegang tot Suwinet voor de uitvoering van werkzaamheden door de afdeling Burgerzaken. Hiervoor heeft de gemeente geen beveiligingsplan overgelegd. Dit houdt in dat de gemeente op dit punt in strijd met norm 1.3 handelt. Dit betekent tevens een overtreding van artikel 13 Wbp.

De bevindingen zijn op basis van bovenstaande aangepast.

2. Uitdragen van het beveiligingsplan

Het CBP heeft geen informatie (bewijs) ontvangen waaruit blijkt dat het beveiligingsplan wordt uitgedragen binnen de organisatie. De bevindingen zijn op dit punt niet gewijzigd.

3. Evaluatie en actualisatie van het beveiligingsplan

Niet is gebleken dat het beveiligingsplan Suwinet, ten aanzien van de werkzaamheden die de gemeente Apeldoorn ten behoeve van de gemeente Brummen uitvoert, wordt voldaan aan norm 1.5 van het Normenkader GeVS en artikel 13 Wbp.

Voor het gebruik van Suwinet door de gemeente Brummen is geen beveiligingsplan overgelegd. Hieruit volgt dat niet kan worden vastgesteld dat de gemeente Brummen voor de eigen toegang tot Suwinet een beveiligingsplan heeft dat jaarlijks wordt geëvalueerd en indien nodig wordt geactualiseerd. Dit houdt in dat de gemeente op dit punt eveneens in strijd met norm 1.5 handelt.
Dit betekent tevens een overtreding van artikel 13 Wbp.

4. Functiescheiding

Het CBP heeft geen informatie (bewijs) ontvangen waaruit blijkt dat functiescheiding voor de Suwi-omgeving is doorgevoerd binnen de organisatie. De bevindingen zijn op dit punt niet gewijzigd.

5. Security Officer

Het CBP heeft van de gemeente Brummen geen informatie (bewijs) ontvangen waaruit blijkt dat er een Security Officer is aangesteld die taken uitvoert en verantwoordelijkheden heeft zoals bedoeld in 2.3 van het Normenkader GeVS. De bevindingen zijn op dit punt niet gewijzigd.

6. Autorisatieprocedure

In het 'ICT beveiligingsdocument' wordt verwezen naar de wijze waarop medewerkers worden geautoriseerd voor toegang tot Suwinet. Het CBP heeft van de gemeente Brummen echter geen formele autorisatieprocedure voor toegang tot Suwinet ontvangen die betrekking hebben op de voor de werkzaamheden die de gemeente Apeldoorn ten behoeve van de gemeente Brummen uitvoert. De bevindingen blijven op dit punt ongewijzigd.

Het CBP heeft evenmin een formele autorisatieprocedure voor toegang tot Suwinet ontvangen voor de uitvoering van werkzaamheden door de afdeling Burgerzaken. De bevindingen blijven op dit punt ongewijzigd.

7. Controle op gebruik

De gemeente Brummen geeft in haar zienswijze aan dat elke vier maanden een gebruiksrapportage via Suwinet-Inkijk wordt opgevraagd en onderzocht. Ook wordt volgens de gemeente Brummen aanvullende informatie opgevraagd als dit nodig is. Dit wordt ook aangegeven in het 'ICT Beveiligingsplan'. De gemeente Brummen heeft echter geen informatie overgelegd waaruit blijkt of wordt aangetoond dat de door BKWI opgestelde rapportages over het gebruik van persoonsgegevens via Suwinet zijn opgevraagd en geanalyseerd worden. De bevindingen blijven op dit punt ongewijzigd.