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 Heerenveen

z2015-00397

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

1. De functiescheiding voor de Suwi-omgeving is onvoldoende beschreven. Hierdoor handelt de gemeente Heerenveen in strijd met norm 2.2 van het Normenkader GeVS, en daarmee in strijd met artikel 13 Wbp;
2. De controle op verleende toegangsrechten vindt niet plaats conform norm 13.5 van het Normenkader GeVS, waardoor in strijd met artikel 13 Wbp wordt gehandeld.

1 INLEIDING

1.1 Achtergrond

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

---

[1] http:/ / www.bkwi.nl/ fileadmin/ downloads/ Suwinet/ Suwinet-Autorisatie/ 20150408_Handreiking_autorisatie_op_Suwinet-Inkijk_voor_GSD.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 de gemeente Heerenveen.

1.3 Doel en reikwijdte van het onderzoek

Het onderzoek beoogt vast te stellen of de gemeente Heerenveen, zijnde de verantwoordelijke voor de 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 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 Heerenveen 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 Heerenveen 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 Heerenveen 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 Heerenveen vertrouwelijke (bedrijfs)gegevens bevatten.
Bij brief van 3 augustus 2015 heeft de gemeente Heerenveen verzocht om uitstel. Het CBP heeft de gemeente Heerenveen uitstel verleend tot 31 augustus 2015. De gemeente Heerenveen heeft bij brief van 27 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 van het Suwinet te zijn goedgekeurd door het management van de Suwipartij (norm 1.3).

2.1.2 Bevindingen

Het CBP heeft kennisgenomen van de bevindingen van het onderzoek en de rapportage van de Inspectie SZW. In deze bevindingen wordt aangegeven dat ten tijde van het onderzoek het beveiligingsplan dat specifiek betrekking heeft op het Suwinet niet is goedgekeurd door het management van de gemeente Heerenveen.

In haar zienswijze heeft de gemeente Heerenveen aangegeven dat een beveiligingsplan Suwinet op 24 maart 2015 is goedgekeurd door het college van burgemeester en wethouders.

2.1.3 Beoordeling

De gemeente Heerenveen heeft een door het college van burgemeester en wethouders vastgesteld beveiligingsplan voor Suwinet. Hiermee handelt de gemeente Heerenveen conform norm 1.3 van het Normenkader GeVS. Op dit punt handelt de gemeente tevens thans conform 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 aantoonbaar moet zijn uitgedragen in de organisatie. 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 Heerenveen schriftelijk heeft aangegeven dat het beveiligingsplan via intranet en workshops wordt uitgedragen in de organisatie. De bevindingen van de Inspectie SZW wijzen uit dat hiervoor echter geen dan wel onvoldoende bewijs is verstrekt door de gemeente Heerenveen.

De gemeente Heerenveen heeft in reactie op het Rapport van voorlopige bevindingen documenten aangedragen die aantonen dat de gemeente een aantal activiteiten heeft ondernomen. Er zijn presentaties gegeven over informatiebeveiliging waarin het beveiligingsplan van Suwinet een punt van aandacht is. Ook zijn Suwinet kalenders aangeboden op werkplekken waar gebruik wordt gemaakt van Suwinet. Het CBP heeft eveneens geconstateerd dat de gemeente het beveiligingsplan voor Suwinet op Intranet heeft gepubliceerd.

2.2.3 Beoordeling

De gemeente Heerenveen heeft aangetoond dat het beveiligingsplan voor Suwinet wordt uitgedragen in de organisatie. Nu de gemeente dit heeft kunnen aantonen , handelt zij conform norm 1.4 van het Normenkader GeVS en daarmee tevens conform 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 Heerenveen heeft volgens de bevindingen van de Inspectie SZW geen evaluatie van het Informatiebeveiligingsbeleid en het beveiligingsplan voor Suwinet uitgevoerd.

De gemeente Heerenveen heeft in zijn zienswijze aangegeven dat het beveiligingsplan voor Suwinet in 2015 is goedgekeurd. In september en oktober van 2015 staan evaluatie overleggen gepland ten aanzien van het beveiligingsplan.

2.3.3 Beoordeling

Gelet op de korte periode die is verstreken na de inwerkingtreding van het beveiligingsplan voor Suwinet en de indiening van de zienswijze is er nog geen reële mogelijkheid geweest voor een evaluatie. De gemeente Heerenveen handelt op dit punt thans niet in strijd met norm 1.5 van het Normenkader GeVS. Hiermee handelt de gemeente Heerenveen 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. Dit onderzoek is beperkt tot vier gescheiden functies. In principe zijn minimaal de volgende functies bij verschillende personen belegd:

- uitvoering van taken (het gebruik van Suwinet zoals de klantmanager);
- het beheer van autorisaties (toegang verlenen tot Suwinet, de applicatiebeheerder van Suwinet);
- kwaliteitszorg en borging van rechtmatig gebruik (controle op gebruik van Suwinet, bijvoorbeeld de Security Officer);
- management (beslissen over bevoegdheden van functiegroepen, en/of individuele medewerkers, uitdragen belang goed gebruik, bijsturen na oneigenlijk gebruik, optreden na misbruik Suwinet).

2.4.2 Bevindingen

Volgens de bevindingen van de Inspectie SZW heeft de gemeente Heerenveen aan de Inspectie SZW een concept SUWI beveiligingsplan overgelegd. Hierin wordt gesproken over de Security Officer (controle), klantmanager (uitvoering) en over autorisaties door de beherende afdelingen. Het afdelingshoofd is volgens dit concept Informatiebeveiligingsbeleid verantwoordelijk voor het bepalen welke autorisaties een medewerker nodig heeft. Tevens wordt in hoofdstuk 6 van dit concept verwezen naar de bijlage ‘Autorisaties Suwinet-Inkijk’. In deze bijlage worden de zeven verschillende functies binnen de afdeling Werk, inkomen en maatschappelijke ondersteuning (WIMO) beschreven.

De gemeente Heerenveen heeft volgens de ingediende zienswijze inmiddels een door burgemeester en wethouders goedgekeurd beveiligingsplan voor het Suwinet. In bijlage 2 van dit beveiligingsplan wordt de functiescheiding beschreven.

- De uitvoering van de verschillende taken is belegd bij de klantmanagers, leidinggevenden en uitvoerend personeel;
- Het beheer van autorisaties (toegang verlenen tot Suwinet) is belegd bij de Security Officer, via de applicatiebeheerder Suwinet. De functie van applicatiebeheerder Suwinet wordt niet beschreven in deze bijlage;
- De kwaliteitszorg en borging van rechtmatig gebruik (controle op gebruik van Suwinet) is tevens belegd bij de Security Officer;
- Het management is eindverantwoordelijk over het gebruik en de beveiliging van Suwinet. De eindverantwoordelijke (het afdelingshoofd beslist hoe wordt gehandeld in geval van ongeoorloofd gebruik door medewerkers.

2.4.3 Beoordeling

Het beheer van de autorisaties en de borging van rechtmatig gebruik is belegd bij de Security Officer. Deze twee taken dienen volgens norm 2.2 gescheiden te worden belegd. De functiescheiding is hierdoor onvoldoende beschreven. Op grond hiervan kan worden geconcludeerd dat in strijd met norm 2.2 gehandeld wordt door de gemeente Heerenveen. De gemeente Heerenveen handelt hiermee 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. De gemeente Heerenveen heeft aangegeven dat het takenpakket van de Security Officer bestaat uit controle rapportage BKWI en dat bij twijfel de detailrapportage wordt opgevraagd. Verder wordt genoemd dat hij regelmatig overleg heeft met de consulent applicaties sociaal domein.

In haar zienswijze heeft de gemeente Heerenveen het volgende aangegeven. De gemeente Heerenveen heeft een Security Officer benoemd bij besluit van 25 augustus 2015, die specifiek naar de beveiliging van Suwinet moet kijken. Er is een functieomschrijving van de Security Officer. Hierin in vastgelegd is dat de Security Officer minimaal 2 keer per jaar de beveiliging van Suwinet controleert. Vastgelegd is ook dat de Security Officer periodiek rechtstreeks rapporteert aan het afdelingsmanagement en via de directie aan het college van burgemeester en wethouders. De Security Officer dient volgens de functieomschrijving ten minste een

keer in de drie maanden een logging rapportage opvragen bij het BKWI. Er zijn een procedure en een formulier ontwikkeld die de Security Officer voor de controle dient te gebruiken.

2.5.3 Beoordeling

De korte periode na de aanstelling van de Security Officer (25 augustus 2015) en de indiening van de zienswijze (31 augustus 2015) in acht genomen, heeft de gemeente Heerenveen onvoldoende tijd gehad om aan te tonen dat de Security Officer ook in de praktijk aan het hoogste management rapporteert. De gemeente Heerenveen handelt niet in strijd met norm 2.3 van het Normenkader GeVS, en daarmee 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 Heerenveen heeft volgens de bevindingen van de Inspectie SZW geen procedure overgelegd die betrekking heeft op de wijze waarop autorisaties worden verleend.

De gemeente Heerenveen heeft in haar zienswijze een autorisatieprocedure en een autorisatiematrix overgelegd. Hieruit blijkt dat accounts en de toewijzing van rechten voor medewerkers kunnen worden herleid tot individuele medewerkers. Uit de autorisatieprocedure blijkt dat alleen afdelingshoofden bevoegdheden kunnen toewijzen. Controle op autorisaties wordt uitgevoerd door de Security Officer. Volgens de procedure worden autorisaties tijdig aanpast of gewijzigd bij functiewijziging of vertrek.

2.6.3 Beoordeling

De gemeente Heerenveen handelt hiermee op dit punt niet in strijd met norm 13.1 van het Normenkader GeVS en evenmin in strijd 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 Suwinet geanalyseerd dient te worden.

2.7.2 Bevindingen

Volgens de bevindingen van de Inspectie SZW heeft de gemeente Heerenveen geen procedure voor de controle 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 Suwinet geanalyseerd wordt. Door de Inspectie SZW zijn bovendien opvallende raadplegingen geconstateerd die door de gemeente Heerenveen onvoldoende zijn onderzocht en waarvoor geen toereikende verklaring is gegeven.

De gemeente Heerenveen heeft een procedure overgelegd aan de hand waarvan generieke rapportages worden opgevraagd en beoordeeld door de Security Officer. De gemeente Heerenveen heeft in haar zienswijze geen generieke of specifieke rapportage van het BKWI bijgevoegd.

2.7.3 Beoordeling

Niet is aangetoond dat meerdere keren per jaar rapportages worden opgevraagd bij het BKWI. Dit is in strijd met norm 13.5 van het Normenkader GeVS en daarmee tevens met artikel 13 Wbp.

3 CONCLUSIES

Uit het onderzoek volgt dat de Wbp wordt overtreden omdat de gemeente Heerenveen twee normen uit het Normenkader GeVS niet of onvoldoende naleeft.

1. De functiescheiding voor de Suwi-omgeving is onvoldoende beschreven. Hierdoor handelt de gemeente Heerenveen in strijd met norm 2.2 van het Normenkader GeVS, en daarmee in strijd 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 DE ZIENSWIJZE VAN DE GEMEENTE HEERENVEEN

Zienswijze gemeente Heerenveen

De gemeente Heerenveen zegt in haar zienswijze de conclusies op pagina 13 van het Rapport van voorlopige bevindingen te kunnen delen. Hier wordt door de gemeente Heerenveen aan toegevoegd dat deze situatie gold op de datum waarop het inspectieonderzoek werd uitgevoerd (juli 2014). Inmiddels is de situatie volgens de gemeente Heerenveen aanmerkelijk verbeterd.

Na het eerdere rapport van de Inspectie SZW heeft de gemeente Heerenveen meteen acties in gang gezet. Inmiddels heeft zij een Beveiligingsplan Suwinet vastgesteld, dat ook ter kennis is gebracht van de gemeenteraad. Ook is er een actieplan in uitvoering dat voortvloeit uit dit beveiligingsplan, waarbij het doel is om de betreffende acties voor 1 oktober 2015 af te hebben gerond.

De gemeente Heerenveen gaat vervolgens in haar zienswijze in op de zeven punten waarop volgens het Rapport van voorlopige bevindingen de Wbp wordt overtreden.

1. Een beveiligingsplan specifiek voor de Suwi-omgeving (norm 1.3)

Sinds maart 2015 is er een goedgekeurd beveiligingsplan Suwinet bij de gemeente Heerenveen. Dit beveiligingsplan is door de gemeente bijgevoegd.

2. Het uitdragen van het beveiligingsplan (norm 1.4)

Sinds maart 2015 zijn er diverse presentaties gegeven binnen de gemeente over i-bewustzijn waar Suwinet in wordt meegenomen. Op diverse werkplekken waar Suwinet wordt gebruikt zijn Suwinet kalenders geplaatst, met handige tips over het gebruik van Suwinet. Het beveiligingsplan van Suwinet staat op Intranet gepubliceerd. Overleg is er minimaal twee keer per jaar met de betreffende afdelingshoofden of indien nodig op afspraak. Bewijsstukken hiervoor zijn door de gemeente bijgevoegd.

3. Evaluatie van het beveiligingsplan (norm 1.5)

In september en oktober van 2015 staan evaluatie overleggen gepland ten aanzien van het beveiligingsplan. De afspraken in outlook zijn door de gemeente bijgevoegd.

4. Functiescheiding (norm 2.2)

In het beveiligingsplan Suwinet staat in bijlage 2 een stuk over autorisatie en de hiermee bereikte controle technische functiescheidingen. Tevens is er een autorisatiematrix gemaakt waar per functie de rollen zijn aangegeven. Medewerkers krijgen op basis van hun functies automatisch de juiste rol. Bewijsstukken hiervoor zijn door de gemeente bijgevoegd.

5. De functie van Security Officer (norm 2.3)

Taken en werkzaamheden worden beschreven in bijlage 2 van het beveiligingsplan. Deze is door de gemeente bij de zienswijze gevoegd.

6. Een formele autorisatieprocedure (norm 13.1)

In bijlage 4 van het beveiligingsplan staat beschreven hoe de autorisaties worden geregeld. Deze is eveneens door de gemeente bijgevoegd.

7. Controle op de verleende toegangsrechten en gebruik (norm 13.5)

Tijdens de maandelijkse controles via de rapportages vanuit BKWI, wordt er ook gekeken en gesproken over de toegangsrechten en autorisaties. Dit wordt gelogd met een document dat ook geparafeerd wordt. De gemeente heeft een voorbeeld van een dergelijk document bijgevoegd.

Reactie CBP

Het CBP zal hieronder puntsgewijs gemotiveerd aangeven hoe er wordt omgegaan met de zienswijze van de gemeente Heerenveen.

1. Een beveiligingsplan specifiek voor de Suwi-omgeving (norm 1.3)

Het CBP heeft kennis genomen van het beveiligingsplan Suwinet, dat op 24 maart 2015 door het college van burgemeester en wethouders is goedgekeurd. Dit beveiligingsplan is sindsdien twee maal (in mei en juli 2015) aangepast, waarbij goedkeuring is gegeven door het afdelingshoofd. Het CBP is van oordeel dat de gemeente Heerenveen op dit punt conform Norm 1.3 van het Normenkader GeVS handelt. De overtreding van artikel 13 Wbp is op dit punt beëindigd. De bevindingen zijn op dit punt aangepast.

2. Het uitdragen van het beveiligingsplan (norm 1.4)

Het CBP heeft kennisgenomen van de presentaties ten aanzien van informatiebeveiliging waarin het beveiligingsplan van Suwinet een punt van aandacht is. Ook heeft het CBP kennisgenomen van de bewijsstukken ten aanzien van het aanbieden van Suwinet kalenders op werkplekken waar gebruik wordt gemaakt van Suwinet. Het CBP heeft eveneens geconstateerd dat de gemeente het beveiligingsplan van Suwinet op Intranet heeft gepubliceerd. Overleg is er minimaal twee keer per jaar met de betreffende afdelingshoofden of indien nodig op afspraak. Bewijsstukken hiervoor zijn door de gemeente bijgevoegd.

Op grond van bovenstaande is het CBP is van oordeel dat het Informatiebeveiligingsbeleid en het beveiligingsplan van het Suwinet conform norm 1.4 van het Normenkader GeVS worden uitgedragen. Dit betekent dat de overtreding van artikel 13 Wbp is beëindigd. De bevindingen zijn op dit punt aangepast.

3. Evaluatie van het beveiligingsplan (norm 1.5)

In september en oktober van 2015 staan evaluatie overleggen gepland ten aanzien van het beveiligingsplan. De afspraken in outlook zijn door de gemeente bijgevoegd. Volgens de gemeente zal het Informatiebeveiligingsbeleid in oktober geëvalueerd en geactualiseerd worden.

Gezien de korte periode na de inwerkingtreding van het beveiligingsplan voor het Suwinet en de afspraken die reeds zijn gemaakt om het dit beveiligingsplan te evalueren, de gemeente Heerenveen 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.

Ten aanzien van het Informatiebeveiligingsbeleid is niet gebleken dat jaarlijks wordt geëvalueerd en geactualiseerd. Dit is niet conform norm 1.5 van het Normenkader GeVS. De overtreding van artikel 13 Wbp is op dit punt niet beëindigd. De bevindingen zijn op dit punt niet aangepast.

4. Functiescheiding (norm 2.2)

De gemeente Heerenveen heeft volgens de ingediende zienswijze inmiddels een door burgemeester en wethouders goedgekeurd beveiligingsplan voor het Suwinet. In bijlage 2 van dit beveiligingsplan wordt de functiescheiding beschreven.

Het beheer van de autorisaties en de borging van rechtmatig gebruik is belegd bij de Security Officer. Deze twee taken dienen volgens norm 2.2 gescheiden te worden belegd. De functiescheiding is hierdoor onvoldoende beschreven. Op grond hiervan kan worden geconcludeerd dat in strijd met norm 2.2 gehandeld wordt door de gemeente Heerenveen. De gemeente Heerenveen handelt hiermee tevens in strijd met artikel 13 Wbp. De verbeterpunten zullen worden meegenomen in de bevindingen, de juridische beoordeling blijft echter ongewijzigd.

5. De functie van Security Officer (norm 2.3)

De gemeente Heerenveen heeft een Security Officer bij besluit van 25 augustus 2015 benoemd binnen de gemeente, die specifiek naar de beveiliging van Suwinet moet kijken. Er is een functieomschrijving van de Security Officer. Hierin in vastgelegd is dat de Security Officer minimaal 2 keer per jaar de beveiliging van Suwinet controleert. Vastgelegd is ook dat de Security Officer periodiek rapporteert aan het hoogtste management. De Security Officer dient ten minste een keer in de drie maanden een loggingrapportage opvragen bij het BKWI. Er zijn een procedure en een formulier ontwikkeld die de Security Officer voor de controle die niet te gebruiken.

Het CBP concludeert dat de functie van Security Officer is vastgelegd conform norm 2.3 van het Normenkader GeVS. De korte periode na de aanstelling van de Security Officer (25 augustus 2015) en de indiening van de zienswijze (31 augustus 2015) in acht genomen, heeft de gemeente Heerenveen onvoldoende tijd gehad om aan te tonen dat de Security Officer ook in de praktijk aan het hoogste management rapporteert. De gemeente Heerenveen handelt niet in strijd met norm 2.3 van het Normenkader GeVS, en daarmee op dit punt evenmin in strijd met artikel 13 Wbp.

6. Een formele autorisatieprocedure (norm 13.1)

De gemeente Heerenveen heeft een autorisatieprocedure en een autorisatiematrix overgelegd. Hieruit blijkt dat accounts en de toewijzing van rechten voor medewerkers kunnen worden herleid. De gemeente moet kunnen aantonen dat medewerkers daadwerkelijk conform hun functie de rollen en de daarbij horende autorisaties toegewezen hebben gekregen (autorisatieoverzicht nog opvragen bij de gemeente). Uit de autorisatieprocedure blijkt dat alleen afdelingshoofden bevoegdheden kunnen toewijzen. Controle op autorisaties wordt uitgevoerd door de Security Officer. Volgens de procedure worden autorisaties tijdig aanpast of gewijzigd van bij functiewijziging of vertrek.

Het CBP is van oordeel dat de gemeente Heerenveen hiermee handelt conform norm 13.1 van het Normenkader GeVS en daarmee de overtreding van artikel 13 Wbp heeft beëindigd. De bevindingen zijn op dit punt aangepast.

7. Controle op de verleende toegangsrechten en gebruik (norm 13.5)

De gemeente Heerenveen heeft een procedure overgelegd aan de hand waarvan generieke rapportages worden opgevraagd en beoordeeld door de Security Officer. Deze procedure is afgestemd met het management, en er is een format aan de hand

waarvan een verslag kan worden opgesteld. De criteria in deze procedure zijn niet concreet uitgewerkt. Er wordt bijvoorbeeld niet aantoonbaar standaard gekeken naar grote verschuivingen, hoge aantallen en verschillen met vergelijkbare gemeenten. De gemeente Heerenveen heeft in haar zienswijze geen generieke of specifieke rapportage van het BKWI bijgevoegd. Niet is gebleken dat in de praktijk rapportages worden opgevraagd bij het BKWI.

Op basis van bovenstaande concludeert het CBP dat de gemeente Heerenveen 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.