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 Zutphen

z2015-00174

Openbare versie
Rapport van bevindingen

November 2015

DATUM November 2015

INHOUDSOPGAVE

SAMENVATTING

Sinds 2002 wisselen diverse overheidsorganisaties (persoons)gegevens van burgers uit in het domein werk en inkomen op basis van de Wet structuur uitvoeringsorganisatie werk en inkomen (Wet SUWI). Deze gegevensuitwisseling vindt plaats via de Gezamenlijke elektronische Voorzieningen SUWI (GeVS, ook wel Suwinet genoemd)[1].

Uit verschillende onderzoeken blijkt dat de beveiliging van Suwinet niet in alle gevallen voldoet aan de wettelijke vereisten. Recent onderzoek van het College bescherming persoonsgegevens (CBP) heeft uitgewezen dat de GeVS bij de toegang tot Suwinet voor niet-Suwipartijen onvoldoende beveiligd was, onder meer omdat raadplegingen niet adequaat werden gelogd en een beveiligingsplan ontbrak[2]. Uit twee recente onderzoeken van de Inspectie SZW kan worden geconcludeerd dat de beveiliging van Suwinet bij veel gemeenten niet voldoet aan de wettelijke vereisten[3]. Voor het CBP vormt dit mede de aanleiding om te controleren of toegang tot Suwinet en gebruik hiervan door gemeenten voldoet aan de vereisten van de Wet bescherming persoonsgegevens (Wbp).

In het kader van zijn toezichthoudende taak heeft het CBP bij een aantal gemeenten onderzoek gedaan naar de beveiliging van persoonsgegevens die via Suwinet kunnen worden geraadpleegd. Het onderzoek is gericht op de naleving van de door de Wbp en SUWI wet- en regelgeving gestelde vereisten ten aanzien van de beveiliging van persoonsgegevens die via Suwinet geraadpleegd kunnen worden. Dit rapport van bevindingen heeft betrekking op één van de onderzochte organisaties: de gemeente Zutphen .

Uit het onderzoek volgt dat de Wbp wordt overtreden. Niet is gebleken dat de gemeente Zutphen met betrekking tot raadplegingen van de afdeling Burgerzaken, meerdere keren per jaar controle op gebruik van Suwinet uitvoert. De gemeente Zutphen handelt op dit punt in strijd met norm 13.5 van het Normenkader GeVS en daarmee met artikel 13 Wbp.

[1] Suwinet wordt ook wel aangeduid als "de Gezamenlijke elektronische Voorzieningen SUWI" (of GeVS).
[2] https:/ / cbpweb.nl/ nl/ nieuws/ cbp-persoonsgegevens-suwinet-niet-goed-beveiligd
[3] http:/ / www.rijksoverheid.nl/ documenten-en-publicaties/ kamerstukken/ 2015/ 06/ 04/ kamerbrief-suwinet-veilig-omgaan-met-elkaars-gegevens.html

1 INLEIDING

1.1 Achtergrond onderzoek

Sinds 2002 wisselen diverse overheidsorganisaties (persoons)gegevens van burgers uit in het domein Werk & Inkomen via Suwinet. Suwinet beschikt over applicaties (bijvoorbeeld Suwinet-Inkijk) die toegang geven tot (persoons)gegevens van burgers. Het betreft de gegevens over onder meer inkomsten uit arbeid en uitkeringen, werkgever(s), uitkeringsaanvragen en opleidings- en beroepservaring. Suwinet-Inkijk biedt ook informatie over de status van identiteitsbewijzen en adresgegevens en contactpersonen van bedrijven.

De Suwipartijen zoals in de Wet SUWI genoemd, zijn: Gemeentelijke Sociale Diensten (GSD), het UWV en de Sociale Verzekeringsbank (SVB). Dit zijn bronhouders. Bronhouders zijn partijen die gegevens leveren via Suwinet. Naast Suwipartijen kunnen zogenaamde niet-Suwipartijen toegang krijgen tot Suwinet. Deze niet-Suwipartijen zijn onder andere de Immigratie- en Naturalisatiedienst (IND), de Inspectie SZW, gemeentelijke Belastingdeurwaarders, gemeenten in het kader van de Regionale Meld en Coördinatie punten voor voortijdig schoolverlaters (RMC) en de Stichting Netwerk Gerechtsdeurwaarders (SNG).

Zorgvuldige omgang met de persoonsgegevens die door middel van Suwinet worden uitgewisseld is essentieel voor de privacy van grote groepen burgers. Via Suwinet worden miljoenen maatschappelijk gevoelige persoonsgegevens van burgers tussen veel partijen uitgewisseld.

Uit verschillende onderzoeken blijkt dat de beveiliging van Suwinet niet in alle gevallen voldoet aan de wettelijke vereisten. Recent onderzoek van het CBP heeft uitgewezen dat toegang tot Suwinet voor niet-Suwipartijen onvoldoende beveiligd was[4]. Uit twee recente onderzoeken van de Inspectie SZW[5] kan worden geconcludeerd dat de beveiliging van Suwinet bij veel gemeenten niet voldoet aan de wettelijke vereisten. Voor het CBP vormt dit mede de aanleiding om te controleren of toegang tot Suwinet en gebruik hiervan door gemeenten voldoet aan de vereisten van de Wbp. Een goede beveiliging is van belang omdat binnen Suwinet steeds meer gegevens worden uitgewisseld[6]. Hieronder bevinden zich zeer privacygevoelige gegevens, zoals fraudevorderingen (informatie over bijstandsvorderingen betreffende fraude of recidive[7]) 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[8]. Adequate beveiligingsmaatregelen kunnen er voor zorgen dat de kans op dergelijke incidenten tot het minimum wordt beperkt.

---

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

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

[6] http://www.bkwi.nl/fileadmin/downloads/Suwinet/Factsheets/13_BK_factsheet_SUWI_Gegevensregister.pdf

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

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

Dit rapport betreft de definitieve bevindingen van het door het CBP uitgevoerde onderzoek bij de gemeente Zutphen.

1.2 Doel, reikwijdte en uitvoering onderzoek

In het kader van de toezichthoudende taak heeft het CBP op grond van artikel 60 Wbp een ambtshalve onderzoek verricht naar de naleving van de vereisten van de Wbp en SUWI wet- en regelgeving door de gemeente Zutphen met betrekking tot de beveiliging van persoonsgegevens die via Suwinet geraadpleegd kunnen worden.

De hoofdvragen van het onderzoek zijn:

- Beschikt de gemeente Zutphen over een (formeel vastgesteld) beveiligingsplan en autorisatieprocedure specifiek gericht op Suwinet?
- Hoe zijn de autorisaties tot Suwinet in de praktijk bij de gemeente Zutphen ingericht?
- Worden vereisten met betrekking tot autorisaties door de gemeente nageleefd?
- Worden de raadplegingen gecontroleerd aan de hand van logging rapportages?

Bij brief van 26 februari 2015 heeft het CBP bij de gemeente Zutphen het onderzoek aangekondigd en schriftelijke stukken (het Suwinet beveiligingsplan, de procedure voor het toekennen, wijzigen en beëindigen van autorisaties van medewerkers voor toegang tot persoonsgegevens en de controle op raadplegingen van persoonsgegevens via Suwinet, alsmede een overzicht van alle geautoriseerde medewerkers, inclusief hun functie, afdeling en de toegekende rollen bij toegang tot Suwinet) opgevraagd.

Op 26 maart 2015 heeft het CBP de gevraagde informatie van de gemeente Zutphen ontvangen. Op 14 april 2015 heeft het CBP om aanvullende informatie verzocht. De gevraagde aanvullende informatie is op 6 mei 2015 door het CBP ontvangen.

Het CBP heeft op 30 juni 2015 het Rapport van voorlopige bevindingen vastgesteld. Het CBP heeft de gemeente Zutphen 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 Zutphen vertrouwelijke (bedrijfs)gegevens bevatten. Bij brief van 30 juli 2015 heeft de gemeente Zutphen verzocht om uitstel. Het CBP heeft de gemeente Zutphen uitstel verleend tot 31 augustus 2015.
De gemeente Zutphen heeft bij brief van 31 augustus 2015 haar zienswijze, alsmede een reactie op de (bedrijfs) vertrouwelijkheidstoets, ingebracht.

1.3 Wettelijk kader

De volgende wetsartikelen vorm het juridisch kader van dit onderzoek:

- Artikel 13 Wbp
- Artikel 6.4 Regeling SUWI
- Bijlage I. , bedoeld in artikel 6.4 van de Regeling SUWI: *Stelselontwerp & Beveiliging Kaders en uitgangspunten aangaande de Gezamenlijke elektronische Voorzieningen Suwi (GeVS)* (hierna: Bijlage I Regeling SUWI).
- Het Normenkader GeVS en de Verantwoordingsrichtlijn GeVS (Gezamenlijke elektronische Voorzieningen SUWI)
- De Code voor Informatiebeveiliging (NEN-ISO/IEC 27002:2013)

De gemeente Zutphen heeft een aantal medewerkers Burgerzaken geautoriseerd tot Suwinet. De gemeente Zutphen is in het kader van dit onderzoek verantwoordelijke in de zin van artikel 1, aanhef en onder d, Wbp voor de raadplegingen van persoonsgegevens door medewerkers van de afdeling Burgerzaken.

De gemeente Zutphen heeft, samen met de gemeente Lochem, de uitvoering van de Participatiewet en andere wettelijke taken uitbesteed aan de Gemeenschappelijke regeling Het Plein, een openbaar lichaam als bedoeld in artikel 8, eerste lid, Wet gemeenschappelijke regelingen (Wgr). De Gemeenschappelijke Regeling Het Plein voert namens de gemeente Zutphen en Lochem een aantal wetten uit die te maken hebben met werk, inkomen en participatie. Omdat de gemeente Zutphen doel en middelen vaststelt voor het raadplegen van persoonsgegevens via Suwinet, is de gemeente Zutphen in het kader van dit onderzoek verantwoordelijke in de zin van artikel 1, aanhef en onder d, Wbp.

2 BEVINDINGEN ONDERZOEK

2.1 Beveiligingsplan Suwinet

2.1.1 Norm

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

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

Uit bijlage I ('Stelselontwerp & Beveiliging Gezamenlijke elektronische Voorzieningen SUWI') volgt dat de Suwipartijen onderling en gezamenlijk, met het 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.

Het normenkader GeVS stelt dat de afnemer/ registratiehouder/ beheerder de inrichting van en de taken en verantwoordelijkheden voor de beveiliging (van de eigen delen van de GeVS) heeft beschreven, vastgesteld en belegd (norm 1). De Suwipartij dient voor de Suwi-omgeving een Suwinet beveiligingsplan te hebben opgesteld dat gebaseerd is op het informatiebeveiligingsbeleid van de organisatie en afspraken in de Suwiketen (norm 1.2). Het informatiebeveiligingsbeleid en het beveiligingsplan van het Suwinet dienen te zijn goedgekeurd door het management van de Suwipartij (norm 1.3). Het informatiebeveiligingsbeleid en het beveiligingsplan

van het Suwinet worden jaarlijks geëvalueerd en indien nodig geactualiseerd (norm 1.5).

2.1.2 Bevindingen

Voor raadplegingen via Suwinet van de gemeente Zutphen door medewerkers van de afdeling Burgerzaken geldt het volgende. De gemeente heeft een door het college van burgemeester en wethouders vastgesteld Informatiebeveiligingsbeleid. Dit Informatiebeveiligingsbeleid is vastgesteld op 17 februari 2015. Dit Informatiebeveiligingsbeleid bevat een hoofdstuk (hoofdstuk 12) over de beveiliging Suwinet. Hierin wordt ingegaan op het algemeen wettelijk kader, het beschermingsniveau, de verantwoordelijkheid ten aanzien van de beveiliging van Suwinet, functies die in aanmerking komen om te worden geautoriseerd om persoonsgegevens te raadplegen via Suwinet en de controleactiviteiten op de raadplegingen van persoonsgegevens via Suwinet .

Met betrekking tot de Gemeenschappelijke regeling Het Plein heeft de gemeente Zutphen een algemeen Informatiebeveiligingsplan overgelegd. In hoofdstuk 11 van dit Informatiebeveiligingsplan wordt ingegaan op Suwinet. De Gemeenschappelijke regeling Het Plein heeft ook een Beveiligingsplan 2015 Suwinet opgesteld. Dit Beveiligingsplan 2015 is goedgekeurd door het de directie van de gemeente Zutphen. In deze beveiligingsplannen wordt eveneens ingegaan op het algemeen wettelijk kader, het beschermingsniveau, de verantwoordelijkheid ten aanzien van de beveiliging van Suwinet (algemeen Informatiebeveiligingsplan 2015), functies die in aanmerking komen om te worden geautoriseerd om persoonsgegevens te raadplegen via Suwinet en de controleactiviteiten op de raadplegingen van persoonsgegevens via Suwinet (Beveiligingsplan 2015 Suwinet).

2.1.3 Beoordeling

De gemeente Zutphen heeft een door het management vastgesteld Informatiebeveiligingsplan dat een passage bevat over Suwinet.
Het Beveiligingsplan 2015 Suwinet van de Gemeenschappelijke regeling Het Plein is vastgesteld door directie van de gemeente Zutphen.

De gemeente Zutphen handelt op dit punt conform normen 1.2 en 1.3 van het Normenkader GeVS, en daarmee eveneens conform artikel 13 Wbp.

2.2 Procedure toekenning autorisaties Suwinet

2.2.1 Norm

Zoals reeds beschreven onder paragraaf 2.1.1, kunnen Bijlage I Regeling SUWI en de Verantwoordingsrichtlijn GeVS met het daarin opgenomen Normenkader GeVS worden beschouwd als wettelijke uitwerkingen van het algemene beveiligingsvoorschrift uit artikel 13 Wbp voor de Suwiketen. Bijlage I Regeling SUWI geeft onder meer invulling aan de gezamenlijke aansturing van privacy en beveiliging. In bijlage I Regeling SUWI wordt aangegeven dat de Verantwoordingsrichtlijn GeVS een gezamenlijk product is van de Suwipartijen en de beheerder van de centrale voorziening. Het bevat de normen, criteria en vormvereisten ten aanzien van privacy en beveiliging.

De gemeente Zutphen is zowel verantwoordelijk voor de wijze waarop wordt omgegaan met autorisaties binnen de eigen organisatie (de afdeling Burgerzaken) als

de autorisaties binnen de organisatie van de Gemeenschappelijke regeling Het Plein (voor zover het de gemeente Zutphen betreft).

Ten aanzien van autorisaties stelt norm 13.1 van het Normenkader GeVS dat de Suwipartij de gebruikers die toegang hebben tot de Suwinet applicaties op basis van een formele procedure autoriseert en registreert. In deze procedure moeten de volgende zaken zijn opgenomen:

- het verlenen van toegang tot de benodigde gegevens op basis van de uit te voeren functie / taken;
- het uniek identificeren van elke gebruiker tot één persoon;
- het goedkeuren van de aanvraag voor toegangsrechten door de manager of een gemandateerde;
- het tijdig wijzigen (dus ook intrekken) van de autorisatie bij functiewijziging of vertrek;
- het benaderen van de Suwi databestanden door gebruikers mag alleen plaatsvinden via applicatieprogrammatuur (tenzij sprake is van calamiteiten).

Norm 13.2 stelt voorts dat technisch beheerders geen Suwinet account mogen hebben.

2.2.2 Bevindingen

a. Autorisatieprocedure afdeling Burgerzaken
Voor het toekennen, wijzigen en beëindigen van autorisaties van medewerkers Burgerzaken van de gemeente Zutphen wordt de procedure 'Toegangsbeveiliging en toegangsbeheer Suwinet-inkijk' gehanteerd door de gemeente Zutphen. In het document wordt stapsgewijs beschreven welke medewerker een bepaalde activiteit dient uit te voeren en op welke manier dit dient te gebeuren.

b. Autorisatieprocedure Gemeenschappelijke regeling Het Plein
Voor het toekennen, wijzigen en beëindigen van autorisaties van medewerkers binnen de organisatie van de Gemeenschappelijke regeling Het Plein wordt de procedure 'Autorisatie tot Suwinet' gehanteerd. In het document wordt eveneens stapsgewijs beschreven welke medewerker een bepaalde activiteit dient uit te voeren en op welke manier dit dient te gebeuren. Het document bevat een reeks instructies die betrekking hebben op het verlenen van toegang tot de benodigde gegevens op basis van de uit te voeren functie en taken; het uniek identificeren van elke gebruiker tot één persoon; het goedkeuren van de aanvraag voor toegangsrechten door de manager of een gemandateerde, en het tijdig wijzigen en intrekken van autorisaties bij functiewijziging of vertrek.

2.2.3 Beoordeling

Uit de overgelegde documenten blijkt dat gebruikers die toegang hebben tot Suwinet, zowel bij de afdeling Burgerzaken van de gemeente Zutphen als de Gemeenschappelijke Regeling Het Plein, op basis van een procedure worden geautoriseerd en geregistreerd. De handelwijze van de gemeente Zutphen voldoet op dit punt aan norm 13.1 van het Normenkader GeVS en daarmee met artikel 13 Wbp.

2.3 Toegangsrechten Suwinet

2.3.1 Norm

Artikel 13 Wbp bepaalt dat de verantwoordelijke maatregelen ten uitvoer legt om persoonsgegevens te beveiligen tegen enige vorm van

onrechtmatige verwerking. Onder onrechtmatige vormen van verwerking vallen de onbevoegde kennisneming, wijziging of verstrekking daarvan.[9] Er dienen procedures aanwezig te zijn om alleen bevoegde gebruikers toegang te geven tot de informatiesystemen en -diensten die zij voor de uitvoering van hun taken nodig hebben en om onbevoegde toegang tot informatiesystemen te voorkomen.

In uitgangspunt 11 van het Normenkader GeVS wordt aangegeven dat toegang tot de via GeVS uitgewisselde gegevens wordt verleend aan unieke geïdentificeerde, geauthentiseerde en geautoriseerde personen en slechts voor zover dit nodig is voor de uitvoering van de hen opgedragen taken. Norm 13.1 van het Normenkader GeVS stelt dat het verlenen van toegang tot de benodigde gegevens op basis van de uit te voeren functie en taken dient plaats te vinden.

Artikel 9.2.3 van de Code voor informatiebeveiliging (NEN-ISO-IEC 27002:2013) stelt dat het toewijzen en gebruik van speciale toegangsrechten dient te worden beperkt en beheerst. Binnen het gemeentelijke Suwidomein zijn speciale autorisaties gedefinieerd door het BKWI. Deze zware rollen mogen beperkt worden toebedeeld. Dit zijn de rollen waarvan BKWI aangeeft dat het 'risicovolle autorisaties' betreft, die onder andere bedoeld zijn om fraude mee te bestrijden . Deze mogen worden toebedeeld aan een beperkte groep gespecialiseerde medewerkers zoals de sociale recherche[10].

2.3.2 Bevindingen

In de door de gemeente Zutphen verstrekte overzichten worden zware autorisatierollen met uitgebreide zoekfunctionaliteiten beperkt en gespecificeerd toegekend aan medewerkers die deze autorisaties nodig hebben voor de uitvoering van hun specifieke taken. De verleende toegangsrechten sluiten daarmee aan op de uit te voeren functies en taken van de geautoriseerde medewerkers.

2.4.3 Beoordeling

De gemeente Zutphen heeft zware autorisatierollen met uitgebreide zoekfunctionaliteiten slechts specifiek toegekend aan een beperkte groep van gespecialiseerde medewerkers. Hiermee handelt de gemeente Zutphen conform norm 13.1 van het Normenkader GeVS en daarmee met artikel 13 Wbp.

2.4 Controle toegangsrechten en gebruik Suwinet

2.4.1 Norm

Bijlage I Regeling SUWI en de Verantwoordingsrichtlijn GeVS met het daarin opgenomen Normenkader GeVS worden beschouwd als wettelijke uitwerkingen van het algemene beveiligingsvoorschrift uit artikel 13 Wbp voor de Suwiketen. Norm 13.5 van het Normenkader GeVS schrijft voor dat de controle op verleende toegangsrechten en gebruik meerdere keren per jaar plaatsvindt. Dit is een interne controle op rechten en gebruik van Suwinet waarbij de van het BKWI verkregen informatie over het gebruik van Suwi-gegevens geanalyseerd dient te worden.

[9] Kamerstukken II 1997-1998, 25 892, nr. 3, p. 98.
[10] http:/ / www.bkwi.nl/ uploads/ media/ 20150408_Handreiking_autorisatie_op_Suwinet-Inkijk_voor_GSD_01.pdf

De gemeente Zutphen is zowel verantwoordelijk voor de wijze waarop het gebruik wordt gecontroleerd binnen de eigen organisatie (de afdeling Burgerzaken) als de organisatie van de Gemeenschappelijke regeling Het Plein (voor zover het de gemeente Zutphen betreft).

2.4.2 Bevindingen

a. Controle afdeling Burgerzaken
In de procedure 'Toegangsbeveiliging en toegangsbeheer Suwinet Inkijk' (d.d. 25 april 2014) wordt de procedure genoemd die wordt gehanteerd bij de controle van de toegekende autorisaties en de raadplegingen via Suwinet. In deze procedure wordt aangegeven dat de Security Officer van de gemeente Zutphen jaarlijks de raadplegingen via Suwinet controleert. Als daar aanleiding voor is, bespreekt de Security Officer de resultaten met de verantwoordelijke leidinggevende en rapporteert aan de proceseigenaar.

b. Controle Gemeenschappelijke regeling Het Plein
Voor de Gemeenschappelijke regeling Het Plein wordt in de procedure 'Controle gebruik Suwinet' beschreven hoe de raadplegingen via Suwinet worden gecontroleerd. In deze procedure is opgenomen dat het gebruik van Suwinet ten minste ieder kwartaal door de Security Officer geanalyseerd en gecontroleerd wordt. In 2015 zijn meerdere keren rapportages over het gebruik van Suwinet van het BKWI opgevraagd en gecontroleerd. Deze controles zijn schriftelijk vastgelegd.

2.4.3 Beoordeling

a. Controle afdeling Burgerzaken
Niet is gebleken dat de gemeente Zutphen, ten aanzien van Suwinet gegevensverwerkingen door de afdeling Burgerzaken van de gemeente Zutphen, meerdere keren per jaar controle op het gebruik van Suwinet uitvoert. De gemeente Zutphen handelt op deze punten in strijd met norm 13.5 van het Normenkader GeVS en daarmee met artikel 13 Wbp.

b. Controle Gemeenschappelijke regeling Het Plein
Ten aanzien van het gebruik van Suwinet in het kader van de Gemeenschappelijke regeling Het Plein zijn meerdere controles door de gemeente Zutphen in 2015 uitgevoerd. Deze controles zijn schriftelijk vastgelegd. Hiermee is voldoende aangetoond dat de gemeente Zutphen voor de Gemeenschappelijke regeling Het Plein meerdere keren per jaar controle op het gebruik van Suwinet uitvoert. De gemeente Zutphen handelt op dit punt conform norm 13.5 van het Normenkader GeVS en daarmee met artikel 13 Wbp.

3 CONCLUSIE

Uit het onderzoek volgt dat de Wbp wordt overtreden.

- Niet is gebleken dat de gemeente Zutphen, ten aanzien van de werkzaamheden door de afdeling Burgerzaken van de gemeente Zutphen, meerdere keren per jaar controle op gebruik van Suwinet uitvoert. De gemeente Zutphen handelt op dit punt in strijd met norm 13.5 van het Normenkader GeVS en daarmee met artikel 13 Wbp.

Het College bescherming persoonsgegevens,
Voor het College,

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

BIJLAGE I: REACTIE CBP OP ZIENSWIJZE GEMEENTEN ZUTPHEN

Zienswijze gemeente Zutphen

De gemeente Zutphen gaat in zijn zienswijze in op de volgende twee punten uit het Rapport van voorlopige bevindingen:

1. Het beveiligingsplan;
2. Procedure voor controle door middel van logging.

Ten aanzien van de bevindingen en beoordeling betreffende het beveiligingsplan 2014 merkt de gemeente Zutphen op dat deze historisch gezien (ten tijde van het onderzoek) op zichzelf genomen juist zijn.

Naar aanleiding van de bevindingen en beoordeling betreffende het Beveiligingsplan 2014 Suwinet merkt de gemeente Zutphen op dat het Beveiligingsplan 2015 Suwinet Gemeenschappelijke regeling Het Plein onlangs door de directeur van de Gemeenschappelijke regeling is vastgesteld. Voor zover het de gemeentelijke sociale dienst betreft handelt de gemeente Zutphen niet meer in strijd met artikel 13 Wbp, noch is sprake van een schending van norm 1.2 en noem 1.3 van het Normenkader GeVS. De gemeente verzoekt het CBP van deze nieuwe feitelijke situatie melding te maken in hetgeen het CBP voornemens is te publiceren. Een kopie van voornoemd document is bijgevoegd door de gemeente Zutphen. Met betrekking tot het Beveiligingsplan van de gemeente Zutphen merkt de gemeente Zutphen op dat reeds voorafgaand aan het Rapport van voorlopige bevindingen is gestart met het actualiseren van het bestaand Informatiebeveiligingsplan.

Met betrekking tot het tweede punt geeft de gemeente in haar zienswijze aan dat, in tegenstelling tot wat in het Rapport van voorlopige bevindingen wordt gesteld en geconcludeerd, meerdere keren per jaar controle op verleende toegangsrechten is uitgevoerd. Bij de controle is gebruik gemaakt van de informatie die door het BKWI is gegenereerd en beschikbaar gesteld.

Controle Burgerzaken

De verleende toegangsrechten zijn gecontroleerd op 18 december 2014 en op 19 februari 2015. Van beide controles is een rapportage opgemaakt die als bijlage is meegezonden. Een controle op het gebruik van Suwinet is uitgevoerd op 19 december 2014 en op 16 juni 2015. Van de eerstgenoemde controle is een rapportage opgemaakt die eveneens als bijlage is gevoegd bij de zienswijze.

Bij de controle is gebruik gemaakt van de Burgerzakenrapportage: gemeente Zutphen Periode: juni-november, welke door het BKWI is gegenereerd en via Suwinet is opgevraagd. Tijdens de controle is geoordeeld dat de rapportage van het BKWI geen aanleiding gaf om een specifieke rapportage op te vragen. De betreffende verantwoordelijke leidinggevende heeft die conclusie onderschreven.
In de Procedure Periodieke en specifieke rapportages gebruik Suwinet-Inkijk van het BKWI wordt volgens de gemeente Zutphen aangegeven dat de specifieke privacy- en beveiligingsrapportage een hulpmiddel is bij de steekproefsgewijze controle van mogelijk misbruik van gegevens uit Suwinet –Inkijk door een medewerker. Dat betekent naar de mening van de gemeente Zutphen dat volstaan kan worden met de

algemene periodieke rapportage als die geen aanleiding geeft om een specifieke rapportage op te vragen.

Van de controle op 16 juni 2015 is tevens een rapportage opgemaakt. Bij deze controle is gebruik gemaakt van de Burgerzaken rapportage: gemeente Zutphen Periode: november 2014- april 2015, welke door het BKWI is gegenereerd en via Suwinet is opgevraagd. Deze controle gaf aanleiding om een specifieke rapportage op te vragen bij het BKWI. Uit de bijgaande e-mail wisseling blijkt dat deze rapportage pas op 15 juli 2015 door het BKWI beschikbaar is gesteld. Aangezien dit midden in de vakantieperiode viel van de zojuist teruggekeerde Security Officer, wordt deze rapportage zo spoedig mogelijk afgerond. De opgemaakt rapportage is als bijlage bij de brief gevoegd.

Controle Gemeenschappelijke regeling Het Plein
Ten aanzien van Gemeenschappelijke regeling Het Plein merkt de gemeente Zutphen op dat de controle op de verleende toegangsrechten de facto op 4 februari 2015 heeft plaatsgevonden. Hiervan is een rapportage opgesteld op basis van de procedure Autorisatie tot Suwinet. Deze rapportage is als bijlage bij de brief gevoegd. In de maand september 2015 wordt eveneens een controle uitgevoerd op de autorisaties tot Suwinet. Daarnaast is in juni 2015 een controle uitgevoerd op het gebruik van Suwinet. Hiervan is een rapportage opgemaakt. Bij de controle is gebruik gemaakt van aanvullende informatie (specifieke rapportage) van het BKWI. Om een correcte en tijdige uitvoering van de controle te waarborgen is een procedure Controle gebruik Suwinet opgesteld en door de verantwoordelijke manager vastgesteld. De procedure en de rapportage treft u als bijlage aan.

Op basis van het bovenstaande verzoekt de gemeente Zutphen het CBP om de passages onder 3.3.2 Bevindingen en 3.3.3 Beoordeling aan te passen, temeer gelet op hetgeen de gemeente Zutphen heeft aangegeven en ook volgens de gemeente Zutphen feitelijk als vaststaand kan worden beschouwd.

De gemeente Zutphen hecht er tot slot aan te vermelden reeds voorafgaand aan de publicatie met voortvarendheid te zijn begonnen met de uitvoering van een gemeente brede privacy gap analyse door een externe specialist en het actualiseren van het beveiligingsplan.

Reactie CBP

Hieronder volgt de puntsgewijze reactie van het CBP op de ingebrachte zienswijze van de gemeente Zutphen.

1. Het beveiligingsplan

Het Beveiligingsplan 2015 Suwinet Gemeenschappelijke regeling Het Plein d.d. 15 juli 2015 is door de directeur van de Gemeenschappelijke regeling vastgesteld. De eerder geconstateerde overtreding is hiermee beëindigd. De bevindingen zullen op dit punt worden aangepast.

De gemeente Zutphen heeft ten aanzien van de werkzaamheden die buiten de Gemeenschappelijke regeling Het Plein vallen, een beveiligingsplan opgesteld dat een passage bevat dat specifiek is gericht op Suwinet. Hierdoor handelt de gemeente Zutphen op dit punt conform normen 1.2 en 1.3 van het Normenkader GeVS, en

daarmee eveneens conform artikel 13 Wbp. De bevindingen worden op dit punt niet aangepast.

2. Procedure voor controle door middel van logging

Controle Burgerzaken
De gemeente Zutphen stelt dat de verleende toegangsrechten buiten de Gemeenschappelijke regeling Het Plein, zijn gecontroleerd op 18 december 2014 en op 19 februari 2015. Van beide controles is een rapportage opgemaakt die als bijlage is meegezonden.

Het CBP heeft kopieën ontvangen van de controle rapportages d.d. 18 december 2014 en 19 februari 2015. Een controle op het gebruik van Suwinet is volgens de gemeente uitgevoerd op 19 december 2014 en op 16 juni 2015. In de overgelegde documenten ten aanzien van de autorisatie van Suwinet (de Procedure toegangsbeveiliging en toegangsbeheer Suwinet d.d. 9 december 2014) wordt aangegeven dat verleende toegangsrechten en gebruik van Suwinet *jaarlijks* wordt gecontroleerd.

Omdat in Procedure toegangsbeveiliging en toegangsbeheer Suwinet d.d. 9 december 2014) niet wordt aangegeven dat meerdere keren per jaar controle op verleende toegangsrechten en gebruik wordt uitgevoerd, en de controles in verschillende kalenderjaren hebben plaatsgevonden, is onvoldoende aannemelijk gemaakt dat de controles *jaarlijks meerdere keren* worden uitgevoerd. De bevindingen zijn op dit punt niet aangepast.

Controle Gemeenschappelijke regeling Het Plein
Ten aanzien van Gemeenschappelijke regeling Het Plein heeft controle op de verleende toegangsrechten de facto op 4 februari 2015 plaatsgevonden. Hiervan is een rapportage opgesteld op basis van de procedure Autorisatie tot Suwinet. Deze rapportage is als bijlage bij de brief gevoegd. In de maand september 2015 wordt eveneens een controle uitgevoerd op de autorisaties tot Suwinet.

In juni 2015 is een controle uitgevoerd op het gebruik van Suwinet. Hiervan is een rapportage opgemaakt. Hiervoor is een procedure 'Controle gebruik Suwinet' opgesteld en op 10 juli 2015 door de verantwoordelijke manager vastgesteld. Deze procedure is aan het CBP overgelegd.

In de procedure 'Controle gebruik Suwinet' wordt aangegeven dat de Security Officer tenminste één keer per kwartaal de rapportage over het gebruik van Suwinet opvraagt bij het BKWI en deze analyseert. Ook wordt aangegeven hoe deze analyse plaats dient te vinden. Het CBP concludeert dat op basis van deze procedure en de controle die in juni 2015 heeft plaatsgevonden, voldoende aannemelijk is gemaakt dat de gemeente Zutphen op dit punt conform norm 13.5 van het Normenkader GeVS handelt. Hiermee is op dit punt de overtreding van artikel 13 Wbp beëindigd.

Gebruikersrapportages BKWI
Uit de bijgevoegde informatie blijkt dat zowel de gemeente Zutphen als de Gemeenschappelijke regeling Het Plein bij voornoemde controles op gebruik van Suwinet, gebruikersrapportages van het BKWI betrekken. Het CBP is van oordeel dat in voldoende mate is aangetoond dat de gemeente Zutphen op dit punt conform norm

13.5 van het Normenkader GeVS en daarmee met artikel 13 Wbp handelt. De bevindingen zijn op dit punt aangepast.