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

AAN Het College van burgemeester en wethouders
van de gemeente 's-Hertogenbosch
Wolvenhoek 1
5200 GZ 's-Hertogenbosch

AANGETEKEND

DATUM 12 november 2014
ONS KENMERK z2014-00238
CONTACTPERSOON Dupon, drs. K. (CBP)
070-8888500

UW BRIEF VAN 26 augustus 2014
UW KENMERK 3958229

ONDERWERP Openbaarmakingsbesluit bevindingen CBP

Geachte College,

Op 5 juli 2013 heeft het College bescherming persoonsgegevens (CBP) ingevolge artikel 60 van de Wet bescherming persoonsgegevens (Wbp) een ambtshalve onderzoek ingesteld naar het gebruik van de Gezamenlijke elektronische Voorzieningen SUWI (GeVS/Suwinet) voor niet-Suwipartijen door de gemeente 's-Hertogenbosch. Het onderzoek is op 4 november 2014 afgerond met het vaststellen van het rapport van definitieve bevindingen (verder: bevindingen).

Besluit
Het CBP heeft tijdens het Collegeoverleg van 11 november 2014 op grond van artikel 8, eerste lid, Wet openbaarheid bestuur (Wob) en de Beleidsregels actieve openbaarmaking door het CBP (Staatscourant 14 november 2013, nr. 31433) besloten om de openbare versie van het rapport van bevindingen openbaar te maken.

Voorafgaand aan dit besluit is getoetst in hoeverre het openbaar maken van de informatie in de bevindingen achterwege dient te blijven vanwege een uitzonderingsgrond als bedoeld in artikel 10 van de Wob.

Beoordeling
Het CBP komt tot de volgende beoordeling inzake de openbaarmaking van de bevindingen .

Reactie van de gemeente 's-Hertogenbosch op het voornemen tot openbaarmaking van de bevindingen
De gemeente 's-Hertogenbosch is tot 2 september 2014 in de gelegenheid gesteld schriftelijk en gemotiveerd aan het CBP mede te delen of het bezwaren heeft tegen het voornemen tot openbaarmaking. Tevens is de gemeente 's-Hertogenbosch in de gelegenheid gesteld om aan te geven of het rapport van voorlopige bevindingen, en zo ja welke onderdelen daarvan, (bedrijfs) vertrouwelijke informatie bevatten als bedoeld in artikel 10 Wet openbaarheid van bestuur.

De gemeente 's-Hertogenbosch heeft op 26 augustus 2014 een zienswijze op het rapport van voorlopige bevindingen ingediend. De gemeente 's-Hertogenbosch heeft in deze zienswijze geen bezwaar gemaakt tegen openbaarmaking van de bevindingen door het CBP.

Bedrijfs- en fabricagegegevens
De gemeente 's-Hertogenbosch heeft niet aangegeven dat de bevindingen (bedrijfs) vertrouwelijke informatie bevatten als bedoeld in artikel 10 Wet openbaarheid van bestuur.

Persoonsgegevens
De gemeente 's-Hertogenbosch heeft niet aangegeven dat de bevindingen persoonsgegevens bevatten.

Beoordeling reactie gemeente 's-Hertogenbosch
Allereerst merkt het CBP op dat met openbaarmaking van de bevindingen het publieke belang van openbaarheid wordt gediend, en hiermee verantwoording wordt afgelegd over de manier waarop het CBP zijn bevoegdheden ter vervulling van zijn toezichthoudende taak aanwendt. In dat kader dienen de belangen van de gemeente 's-Hertogenbosch te worden afgewogen tegen voornoemd publieke belang.

Bedrijfs- en fabricagegegevens
In geval van openbaarmaking houdt het CBP rekening met de bedrijfsvertrouwelijkheid van de te publiceren informatie op grond van het bepaalde in artikel 10, eerste lid, aanhef en onder c, Wob.

Desgevraagd heeft gemeente 's-Hertogenbosch in de zienswijze van 26 augustus 2014 niet aangegeven dat de bevindingen vertrouwelijke bedrijfs- en fabricagegegevens bevatten.

Persoonsgegevens
Daarnaast houdt het CBP bij het publiceren van informatie rekening met de vraag of sprake is van persoonsgegevens, tenzij publicatie daarvan geen inbreuk maakt op de persoonlijke levenssfeer, zoals bepaald in artikel 10, eerste lid, aanhef en onder d, Wob. Het CBP stelt vast dat de passage uit voorlopige bevindingen met betrekking tot de security officer een persoonsgegeven is. Het CBP heeft de bevindingen op dit punt aangepast opdat deze passage geen persoonsgegeven meer bevat.

Het CBP merkt op dat de bevindingen een feitelijke en neutrale weergave bevatten van de onderzoeksresultaten en de gemeente 's-Hertogenbosch voorafgaande aan het opstellen van de bevindingen in de gelegenheid is gesteld om daarop een zienswijze te geven. Deze zienswijze, gegeven op 26 augustus 2014 is – zakelijk weergegeven – eveneens in de bevindingen opgenomen. Nu met de bevindingen ook de zakelijke weergave van de zienswijze van de gemeente 's-Hertogenbosch openbaar wordt gemaakt, is er sprake van een weergave van de relevante standpunten van zowel de gemeente 's-Hertogenbosch als het CBP, waarvan een ieder kennis kan nemen. Deze weergave leidt op zichzelf niet tot een onevenredige benadeling van het de gemeente 's-Hertogenbosch, zoals uit vaste jurisprudentie blijkt.

DATUM 12 november 2014
ONS KENMERK z2014-00238

Voorts heeft de gemeente 's-Hertogenbosch in zijn zienswijze niet aangegeven bezwaar te maken tegen de publicatie.

Gezien het bovenstaande concludeert het CBP dat de gemeente 's-Hertogenbosch geen bezwaar heeft gemaakt tegen openbaarmaking of dat openbaarmaking zal leiden tot onevenredige benadeling en dit tot schade voor de gemeente 's-Hertogenbosch zal leiden.

Publicatie
Het CBP gaat niet eerder over tot publicatie van de bevindingen dan veertien kalenderdagen na dagtekening van dit besluit. Het CBP publiceert derhalve de bevindingen niet eerder dan 26 november 2014.

Rechtsmiddelenclausule
Indien u het niet eens bent met dit besluit tot openbaarmaking van de openbare versie van het rapport van bevindingen, kunt u hiertegen op grond van artikel 7:1 van de Algemene wet bestuursrecht (Awb) binnen zes weken na de dag waarop dit besluit is verzonden bezwaar maken door het indienen van een gemotiveerd bezwaarschrift, gericht aan het CBP, Postbus 93374, 2509 AJ Den Haag, onder vermelding van "Awb-bezwaar" op de enveloppe. Het indienen van een bezwaarschrift schort de werking van dit besluit niet op. Indien onverwijlde spoed – gelet op de betrokken belangen – dat vereist kunt u de voorzieningenrechter van de rechtbank verzoeken een voorlopige voorziening te treffen.

Hoogachtend,
Het College bescherming persoonsgegevens,

I.O.

mr. W.B.M. Tomesen
Plv. voorzitter

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

AAN Het College van burgemeester en wethouders
van de gemeente 's-Hertogenbosch
Wolvenhoek 1
5200 GZ 's-Hertogenbosch

DATUM 12 november 2014
ONS KENMERK z2014-00238
CONTACTPERSOON Dupon, drs. K. (CBP)
070-8888500

UW BRIEF VAN
UW KENMERK 3958229

ONDERWERP Definitieve bevindingen onderzoek gemeente 's-Hertogenbosch gebruik Suwinet door niet-Suwipartijen

Geacht College,

Het College bescherming persoonsgegevens (CBP) heeft in het kader van zijn toezichthoudende taak op grond van artikel 60 Wet bescherming persoonsgegevens (Wbp) onderzoek verricht naar het gebruik van de Gezamenlijke elektronische Voorzieningen SUWI (GeVS/Suwinet) door niet-Suwipartijen van de gemeente 's-Hertogenbosch.

Zoals in artikel 60, tweede lid Wbp is bepaald, bent u in de gelegenheid gesteld uw reactie te geven op de voorlopige bevindingen. Uw reactie op de voorlopige bevindingen heeft het CBP bij brief van 26 augustus 2014 ontvangen. Hierbij ontvangt u het rapport van definitieve bevindingen (verder: bevindingen) dat op 4 november 2014 is vastgesteld.

Uw reactie heeft geleid tot aanpassing van de bevindingen ten aanzien van de toegang tot Suwinet in het kader van de Wet Maatschappelijke Ondersteuning (WMO) en de beveiliging van inloggegevens en daarmee samenhangende wijzigingen in de conclusies. Tevens zijn de bevindingen ten aanzien van de controle van rechten en gebruik van Suwinet aangepast en enkele tekstuele wijzigingen doorgevoerd. Voor het overige heeft de reactie niet geleid tot wijziging van de bevindingen en de conclusies. De rapportage van bevindingen is aldus vastgesteld.

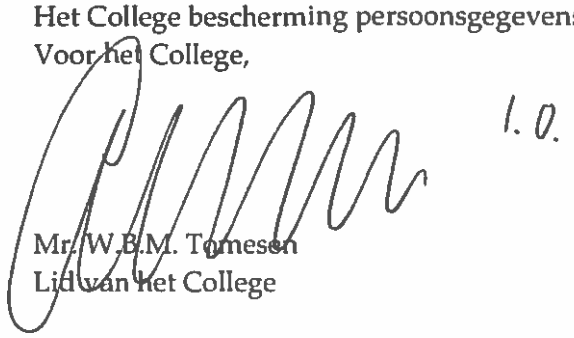
Conclusie
Bij het onderzoek naar de verwerking van persoonsgegevens van de gemeente 's-Hertogenbosch bij de toegang tot de Gezamenlijke elektronische Voorzieningen SUWI (GeVS/Suwinet) voor niet-Suwipartijen zijn overtredingen van de artikelen 6 en 13 Wbp geconstateerd.

DATUM 12 november 2014
ONS KENMERK z2014-00238

Handhaving
U ontvangt nader bericht indien het CBP zijn handhavende bevoegdheden inzet.

Indien u naar aanleiding van deze brief nog vragen heeft, kunt u contact opnemen met de bovengenoemde contactpersoon.

Hoogachtend,
Het College bescherming persoonsgegevens,
Voor het College,



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

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 gebruik Suwinet door niet-Suwipartijen Gemeente 's-Hertogenbosch

z2014-00238

Rapport van bevindingen

November 2014

DATUM 4 november 2014

INHOUDSOPGAVE

SAMENVATTING

Sinds 2002 wisselen diverse overheidsorganisaties persoonsgegevens van burgers uit in het domein Werk en Inkomen op basis van de Wet structuur uitvoeringsorganisatie werk en inkomen (SUWI). Dit vindt plaats door middel van de Gezamenlijke elektronische Voorzieningen SUWI (GeVS/Suwinet)[1].

In het kader van de toezichthoudende taak heeft het College bescherming persoonsgegevens (CBP) bij twee organisaties onderzoek gedaan naar toegang tot Suwinet voor niet-Suwipartijen. Het onderzoek is gericht op de naleving van de door de Wet bescherming persoonsgegevens (Wbp) en SUWI wet- en regelgeving gestelde vereisten. Dit rapport van bevindingen heeft betrekking op één van de onderzochte organisaties: de gemeente 's-Hertogenbosch.

Uit het onderzoek volgt dat de Wbp wordt overtreden.

- Ten aanzien van het aansluiten van niet-Suwipartijen op Suwinet wordt door de gemeente 's-Hertogenbosch op meerdere punten (uitwerking Wbp-vereisten, rollen en autorisaties) niet gewerkt volgens het aansluitprotocol uit bijlage III van de Regeling SUWI. Dit betekent dat op deze punten artikel 6 Wbp wordt overtreden.

- Medewerkers van de gemeente 's-Hertogenbosch hebben in hoedanigheid van WMO-consulent toegang tot Suwinet. De gemeente 's-Hertogenbosch handelt hiermee in strijd met artikel 13 Wbp.

- Voorts voldoet de gemeente 's-Hertogenbosch op verschillende punten (toekennen en controle autorisaties, beveiligingsplan, audit, beveiligingsincidenten, beveiliging inloggegevens RMC-taak) niet aan de vereisten uit bijlage I van de Regeling SUWI, het in de Verantwoordingsrichtlijn opgenomen Normenkader GeVS en de Code voor Informatiebeveiliging waardoor de gemeente 's-Hertogenbosch artikel 13 Wbp overtreedt.

- Tot slot wordt de wettelijke informatieplicht van artikel 34 Wbp niet nageleefd door de gemeente 's-Hertogenbosch.

[1] Suwinet wordt ook wel aangeduid als "de Gezamenlijke elektronische Voorzieningen SUWI" (of GeVS).

1 Inleiding

1.1 Achtergrond onderzoek

Sinds 2002 wisselen diverse overheidsorganisaties persoonsgegevens van burgers uit in het domein Werk & Inkomen via Suwinet. Suwinet is een besloten netwerk dat wordt ondersteund, beheerd en verder (technisch) ontwikkeld door het Bureau Keteninformatisering Werk en Inkomen (BKWI), formeel onderdeel van het Uitvoeringsinstituut werknemersverzekeringen (UWV). Suwinet beschikt over diverse applicaties (bijvoorbeeld Suwinet Inkijk) die toegang geven tot (persoons)gegevens van burgers. Het betreft de gegevens over onder andere 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)-taak en Stichting Netwerk Gerechtsdeurwaarders (SNG).

Zorgvuldige omgang met de persoonsgegevens die door middel van Suwinet worden uitgewisseld is essentieel voor de privacy van grote groepen kwetsbare burgers. Met Suwinet worden miljoenen maatschappelijk gevoelige persoonsgegevens van burgers met veel partijen uitgewisseld. Uit onderzoek van de Inspectie SZW is gebleken dat de beveiliging van Suwinet bij veel gemeenten niet voldoet aan de wettelijke vereisten[2]. Voor het CBP vormt dit de aanleiding om te controleren in hoeverre de Wbp bij het verschaffen van toegang tot Suwinet door niet-Suwipartijen nageleefd wordt.

Dit rapport betreft de bevindingen van het onderzoek dat het CBP heeft verricht bij de gemeente 's-Hertogenbosch. Zoals in artikel 60 lid 2 Wbp is bepaald, is de gemeente 's-Hertogenbosch in de gelegenheid gesteld zijn zienswijze te geven op de voorlopige bevindingen. Het CBP heeft de reactie van de gemeente 's-Hertogenbosch bij brief van 26 augustus 2014 ontvangen en heeft de definitieve bevindingen vastgesteld, waarbij rekening is gehouden met voornoemde reactie.

1.2 Doel, reikwijdte en uitvoering onderzoek

In het kader van de toezichthoudende taak heeft het CBP een ambtshalve onderzoek verricht conform artikel 60 Wbp naar de naleving van de vereisten van de Wbp en SUWI wet- en regelgeving door de gemeente 's-Hertogenbosch met betrekking tot het gebruik van Suwinet in het kader van niet-Suwi taken. De oorspronkelijke reikwijdte van het onderzoek was beperkt tot de RCM-taak. Tijdens het onderzoek zijn de taken betrokken die de gemeente 's-Hertogenbosch uitvoert in het kader van de Wet Maatschappelijke Ondersteuning (WMO).

[2] http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2013/11/08/programmarapportage-de-burger-bediend-in-2013.html

Hierbij zijn de volgende onderzoeksvragen leidend geweest:

1. Heeft de gemeente 's-Hertogenbosch een overeenkomst ondertekend inzake verwerking gegevens afkomstig van Suwinet?
2. Welke concrete afspraken zijn gemaakt met betrekking tot de naleving van de Wbp?
3. Worden vereisten met betrekking tot toegang en beveiliging van Suwinet (bijvoorbeeld beveiligingsplan Suwinet, toekenning en beheer van autorisaties tot Suwinet, logging gebruik Suwinet en beveiligingsincidenten) door de gemeente 's-Hertogenbosch nageleefd?
4. Worden de Wbp-vereisten met betrekking tot de wettelijke informatieplicht door de gemeente 's-Hertogenbosch nageleefd?

Bij brief van 18 maart 2014 heeft het CBP bij de gemeente 's-Hertogenbosch het onderzoek aangekondigd. Per email (d.d. 21 maart 2014) zijn enkele relevante schriftelijke stukken (waaronder het beveiligingsbeleid, het beveiligingsplan en de procedure voor het verlenen van autorisaties toegang Suwinet) opgevraagd.
Op 3 april 2014 heeft een onderzoek ter plaatse bij de gemeente 's-Hertogenbosch plaatsgevonden, waarbij het CBP interviews heeft gehouden met diverse medewerkers van de gemeente en kennis heeft genomen van de wijze waarop medewerkers toegang krijgen tot Suwinet. Tijdens het onderzoek ter plaatse heeft het CBP relevante documentatie (o.a. beveiligingsplan Suwinet, autorisatieprocedure Suwinet, overzicht medewerkers die toegang tot Suwinet hebben, printscreens Suwinet) opgevraagd. Een deel van deze documentatie heeft de gemeente 's-Hertogenbosch later, te weten op 4 april 2014 per emailbericht aan het CBP overgelegd.

Het CBP heeft op 15 juli 2014 het Rapport voorlopige bevindingen vastgesteld.
Het CBP heeft de gemeente 's-Hertogenbosch bij brief van 17 juli 2014 in de gelegenheid gesteld om haar zienswijze op het Rapport voorlopige bevindingen naar voren te brengen. Het CBP heeft daarbij tevens verzocht aan te geven of en zo ja welke onderdelen daarvan, volgens de gemeente 's-Hertogenbosch vertrouwelijke (bedrijfs)gegevens bevatten. De gemeente 's-Hertogenbosch heeft bij brief van 24 juli 2014 verzocht om uitstel van de termijn voor het geven van een zienswijze tot en met 15 september 2014. Het CBP heeft per brief van 1 augustus 2014 uitstel verleend tot en met 1 september 2014. De gemeente 's-Hertogenbosch heeft zijn zienswijze, alsmede een reactie op de (bedrijfs) vertrouwelijkheidstoets, op 26 augustus 2014 schriftelijk ingebracht.

1.3 Wettelijk kader

De volgende wetsartikelen en voorschriften vormen het juridisch kader van dit onderzoek:

- Artikel 6 Wbp
- Artikel 13 Wbp
- Artikel 34 Wbp
- Artikel 62 Wet SUWI
- Artikel 5.23 Besluit SUWI
- Artikel 6.5 Regeling SUWI
- Bijlage I. , bedoeld in artikel 6.3 van de Regeling SUWI (*Stelselontwerp & Beveiliging Kaders en uitgangspunten aangaande de Gezamenlijke elektronische Voorzieningen Suwi (GeVS)*)

- Bijlage III. Regeling SUWI (Aansluitprotocol GeVS)
- Het Normenkader GeVS en de Verantwoordingsrichtlijn GeVS (Gezamenlijke elektronische Voorzieningen SUWI)
- De Code voor Informatiebeveiliging (NEN-ISO/IEC 27002:2013)

2 Organisatie

Het Ministerie van Onderwijs, Cultuur en Wetenschappen (OC&W) richtte de RMC op om voortijdige schoolverlaters een betere uitgangspositie te geven in de maatschappij. De RMC is er sinds 1994. In 2001 is de functie uitgewerkt in de Regionale Meld- en Coördinatiewetgeving (RMC-wetgeving). Nederland kent 39 RMC-regio's. De kerntaken van de RMC-regio zijn:

- een sluitende melding en registratie, doorverwijzing en herplaatsing van voortijdig schoolverlaters;
- het bevorderen van een goede samenwerking tussen alle partijen in de regio die te maken hebben met jongeren tot 27 jaar;
- het realiseren van een sluitende aanpak met een zo goed mogelijk traject op maat.

Per regio is een contactgemeente aangewezen om de kerntaken uit te voeren. Voor de regio Noord-Oost-Brabant is de gemeente 's-Hertogenbosch de contactgemeente.

2.1 Verantwoordelijke

De gemeente 's-Hertogenbosch is in het kader van dit onderzoek de verantwoordelijke in de zin van artikel 1, aanhef en onder d, Wbp. Formeel het College van burgemeester en wethouders van de gemeente 's-Hertogenbosch.

3 Bevindingen Onderzoek

3.1 Toegang Suwinet

3.1.1 Norm

Artikel 6 Wbp bepaalt dat persoonsgegevens in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze moeten worden verwerkt. In de wet is uitgewerkt dat de aansluiting van niet-Suwipartijen volgens artikel 5.23, eerste lid, van het Besluit SUWI bij overeenkomst dient te zijn geregeld. Artikel 5: 23 Besluit SUWI bepaalt dat bij ministeriële regeling nadere regels kunnen worden gesteld over de overeenkomst, bedoeld in het eerste lid. Het in bijlage III van de Regeling SUWI opgenomen protocol – het zogenaamde aansluitprotocol– bevat nadere regels ten aanzien van de overeenkomst. Volgens dit protocol spreken de contractpartijen in de overeenkomst onder meer de volgende zaken af:

a) hoe aan de voorwaarden van het aansluitprotocol wordt voldaan;
b) welke rollen en autorisaties benodigd zijn;
c) op welke wijze de eisen voortvloeiend uit de Wbp worden nageleefd.

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.
De verantwoordelijke dient dus 'passende technische en organisatorische maatregelen' te treffen om de persoonsgegevens die via Suwinet worden verwerkt te

beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Onder onrechtmatige vormen van verwerking vallen de aantasting van gegevens, onbevoegde kennisneming, wijziging of verstrekking daarvan[3].

Bijlage I van de Regeling SUWI (Stelselontwerp & Beveiliging Kaders en uitgangspunten aangaande de Gezamenlijke elektronische Voorzieningen SUWI (GeVS)) en de Verantwoordingsrichtlijn GeVS met het daarin opgenomen Normenkader GeVS kunnen worden beschouwd als wettelijke uitwerkingen van het algemene beveiligingsvoorschrift uit artikel 13 Wbp voor de Suwiketen. Bijlage I van de Regeling SUWI geeft onder meer invulling aan de gezamenlijke *governance* van privacy en beveiliging. In bijlage I van de Regeling SUWI wordt onder meer aangegeven dat de Verantwoordingsrichtlijn (privacy en beveiliging van de 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.

Ten aanzien van autorisaties stelt norm 13.1 van het Normenkader GeVS dat de Suwipartij de gebruikers autoriseert en registreert die toegang hebben tot de Suwinet applicaties op basis van een formele procedure.

3.1.2 Bevindingen

A. Overeenkomsten inzake toegang Suwinet door niet-Suwipartijen

Het CBP heeft de overeenkomst die de RMC Noord-Oost-Brabant met het UWV heeft gesloten, opgevraagd. De overeenkomst werd in juni 2011 gesloten. In de overeenkomst wordt niet aangegeven op welke wijze de Wbp-vereisten met betrekking tot bewaartermijnen (artikel 10 Wbp), de bovenmatigheid (artikel 11 Wbp) en de informatieplicht (artikel 34 Wbp) worden ingevuld. De overeenkomsten bevatten geen passages over de benodigde rollen en de wijze waarop autorisaties worden toegekend, beheerd en gecontroleerd.

B. Toekenning en controle van autorisaties Suwinet

Het CBP heeft voorafgaand aan het onderzoek ter plaatse een autorisatieprocedure opgevraagd. De gemeente 's-Hertogenbosch heeft een document getiteld *'Protocol m.b.t. het gebruik van gegevens van Suwinet'* aan het CBP toegestuurd. Het document is geschreven als een interne notitie, waarin naar de bestaande algemene autorisatieprocedure van de gemeente 's-Hertogenbosch wordt verwezen. Het protocol bevat regels ten aanzien toekenning en controle van autorisaties. Het document is door het MT van de afdeling Arbeidsmarkt en Sociale Zaken (AmSZ) vastgesteld. Het bevat geen datum en historie, en is nog niet geëvalueerd.

Medewerkers van verschillende afdelingen van de gemeente 's-Hertogenbosch maken gebruik van gegevens via Suwinet. In het kader van de RMC-taak zijn medewerkers van meerdere gemeenten geautoriseerd om gebruik te maken van gegevens via Suwinet. Het genoemde protocol bevat geen bepalingen ten aanzien van medewerkers van andere afdelingen van de gemeente 's-Hertogenbosch. Het protocol bevat evenmin bepalingen ten aanzien van RMC-medewerkers van andere gemeenten.

[3] Kamerstukken II, 1997/1998, 25 892, nr. 3, blz. 98.

De gemeente 's-Hertogenbosch beschikt verder niet over een formeel vastgestelde en gedocumenteerde autorisatieprocedure met betrekking tot toegang Suwinet. Een autorisatieprocedure gericht op de RMC onderliggende gemeenten is evenmin beschikbaar.

Tijdens het onderzoek ter plaatse werd de werkwijze bij het verlenen van de toegang tot Suwinet mondeling toegelicht. Het BKWI autoriseert de gemeente 's-Hertogenbosch op verzoek van een Suwipartij (UWV) die gegevens levert. Nadat de administrator bij de gemeente 's-Hertogenbosch door het BKWI is geautoriseerd, worden alle individuele accounts op medewerkersniveau lokaal door de gemeente zelf verdeeld. De administrator autoriseert in opdracht van een leidinggevende andere medewerkers in de eigen organisatie. De leidinggevende bepaalt op basis van de functie van de medewerker de toe te kennen rol. Binnen RMC zijn twee rollen te onderscheiden: die van gebruikers met een raadpleegaccount en die van de *administrator* zonder gebruikersaccount.

Drie gemeenten uit de RMC-regio hebben een aansluiting op Suwinet in het kader van RMC-taken gekregen. De gemeente 's-Hertogenbosch heeft met deze gemeenten een aparte overeenkomst gesloten.[4] In totaal hebben acht RMC medewerkers toegang tot Suwinet: twee medewerkers bij de gemeente 's-Hertogenbosch en zes bij de 'onderliggende' gemeenten. De administrator autoriseert ook de RMC medewerkers van de andere gemeenten binnen de RMC-regio. Hiervoor is geen procedure aanwezig bij de gemeente 's-Hertogenbosch. Er is ook geen procedure bij de gemeente 's-Hertogenbosch aanwezig voor de controle op autorisaties bij de aangesloten gemeenten. Voorts heeft de gemeente 's-Hertogenbosch aangegeven dat zij geen formeel vastgestelde en gedocumenteerde procedure heeft die specifiek gericht is op de controle van verleende autorisaties Suwinet lokaal en bij de RMC onderliggende gemeenten.

In het *'Protocol m.b.t. het gebruik van gegevens van Suwinet'* (ongedateerde interne notitie) dat aan het CBP is overgelegd, staat vermeld dat er wekelijks een e-mailbericht aan het applicatiebeheer van de afdeling Arbeidsmarkt en Sociale Zaken (AmSZ) wordt verstuurd met een overzicht van medewerkers van de gemeente 's-Hertogenbosch die uit dienst zijn getreden. Bij functiewijziging van een medewerker dient de desbetreffende manager de applicatiebeheerder van AmSZ in te lichten. Bij vertrek van een medewerker wordt de algehele account, inclusief toegang tot alle applicaties afgesloten. De gemeente 's-Hertogenbosch heeft tevens een document getiteld 'Autorisatie intrekken bij vertrek medewerkers (bron SG beheergroep; update 7-3-2012 TIEE)' aan het CBP toegestuurd. Het betreft een interne notitie waarin de werkwijze inzake intrekken autorisaties is beschreven. Het document is niet vastgesteld door de directie of het MT.

3.1.3 Beoordeling

A. Overeenkomst inzake toegang Suwinet door niet-Suwipartijen

In de overeenkomst wordt niet aangegeven op welke wijze de vereisten uit de artikelen 10, 11 en 34 Wbp worden nageleefd. Nu op dit punt het aansluitprotocol uit bijlage III van de Regeling SUWI niet wordt gevolgd, vindt de verwerking van

[4] Deze overeenkomsten worden in dit rapport niet inhoudelijk beoordeeld.

persoonsgegevens niet in overeenstemming met de wet plaats. Deze verwerking is derhalve in strijd met artikel 6 Wbp.

De benodigde rollen en autorisaties worden niet in de overeenkomst als bedoeld in artikel 5.23, eerste lid, van het Besluit SUWI geregeld. Rollen en autorisaties worden, vooraf en buiten de overeenkomst om, met het BKWI afgestemd en besproken. Voormelde is niet conform het aansluitprotocol, zoals opgenomen in bijlage III van de Regeling SUWI, hetgeen betekent dat deze verwerking van persoonsgegevens in strijd is met artikel 6 Wbp.

B. Toekenning en controle autorisaties Suwinet
Uit de overlegde stukken blijkt niet dat de gebruikers die toegang hebben tot de Suwinet applicaties op basis van een formele procedure worden geautoriseerd en geregistreerd. Dit houdt in dat de handelwijze van de gemeente 's-Hertogenbosch op dit punt niet voldoet aan norm 13.1 uit het Normenkader GeVS.

3.2 Toegang tot Suwinet in het kader van de Wet maatschappelijke ondersteuning (WMO)

3.2.1 Norm

Voor het SUWI-stelsel geldt een gesloten verstrekkingenregime. Daarmee wordt bedoeld dat verstrekking van persoonsgegevens aan organisaties buiten SUWI slechts mogelijk is indien daarvoor een wettelijke grondslag bestaat (paragraaf 4.2 van de Memorie van Toelichting bij de Wet SUWI). Voor het raadplegen van gegevens via Suwinet voor de WMO-taak van gemeenten is geen wettelijke grondslag aanwezig.

Artikel 13 Wbp vereist onder meer dat maatregelen ten uitvoer worden gelegd om onrechtmatige verwerking en onbevoegde kennisneming van persoonsgegevens tegen te gaan. 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. Voorts schrijft norm 2.2 van het Normenkader GeVS voor dat 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 zijn beschreven en duidelijk gescheiden zijn belegd. 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. De Code voor informatiebeveiliging is een algemeen geaccepteerde technologie-neutrale beveiligingsstandaard binnen de praktijk van de informatiebeveiliging, die breed wordt toegepast bij het formuleren en implementeren van beveiligingsmaatregelen en kan worden beschouwd als een algemene en gezaghebbende uitwerking van het beveiligingsvoorschrift uit artikel 13 Wbp. De code voor informatiebeveiliging stelt voorts dat gebruikers verantwoordelijk gesteld moeten kunnen worden voor hun handelingen[5].

3.2.2 Bevindingen

Om de scheiding van de functies en bevoegdheden inzake toegang Suwinet te controleren heeft het CBP ten tijde van het onderzoek ter plaatse een actueel overzicht van alle geautoriseerde medewerkers van de gemeente 's-Hertogenbosch opgevraagd, inclusief hun rollen en afdeling. De gemeente 's-Hertogenbosch heeft enkele dagen na

[5] NEN-ISO/IEC 27002:2013, 9.2.1. a)

afloop van het onderzoek ter plaatse dit overzicht aan het CBP overgelegd. Uit het overzicht blijkt dat bij de Gemeentelijke Sociale Dienst (GSD) diverse medewerkers toegang tot Suwinet hebben met een rol van 'WMO consulent'.

Uit de zienswijze op de voorlopige bevindingen, die de gemeente 's-Hertogenbosch op 26 augustus 2014 heeft gegeven, blijkt dat deze medewerkers een dubbele uitvoerende taak hebben. Naast WMO aanvragen behandelen zij ook aanvragen op het gebied van het bijzondere bijstand (WWB). Voor de taakuitoefening van bijzondere bijstand vallen zij, aldus de gemeente, onder de Wet SUWI. Voor deze bijzondere situatie is vooraf met het BKWI afgesproken dat de rol WMO-consulent gebruikt wordt. Het doel hiervan is volgens de gemeente 's-Hertogenbosch 'juist transparantie én gerichte controle bij audits'. Deze medewerkers hebben volgens de gemeente 's-Hertogenbosch al enige tijd geen toegang gezocht tot Suwinet, waardoor hun account is geblokkeerd.

3.2.3 Beoordeling

WMO-consulenten mogen, gelet op het gesloten verstrekkingenregime van de SUWI wet- en regelgeving en gezien de aard van hun werkzaamheden, geen toegang krijgen tot Suwinet. Dit betekent dat de gemeente 's-Hertogenbosch ervoor moet zorgen dat er voor bepaalde functies, zoals de functie van WMO-consulent, geen autorisaties worden gecreëerd voor Suwinet.

Het CBP heeft tijdens het onderzoek vastgesteld dat WMO consulenten geautoriseerd zijn voor toegang tot Suwinet. Uit de toelichting van de gemeente 's-Hertogenbosch blijkt dat deze medewerkers een dubbele uitvoerende taak hebben. Naast WMO aanvragen behandelen zij ook aanvragen op het gebied van het bijzondere bijstand (WWB). Gezien het gesloten verstrekkingenregime mag het Suwinet niet worden ontsloten voor WMO doeleinden. Autorisaties voor gebruik van Suwinet mogen slechts verleend worden voor de uitvoering van de bijzondere bijstand taak.

In haar zienswijze op de voorlopige bevindingen heeft de gemeente 's-Hertogenbosch naar voren gebracht dat WMO-consulenten juist geautoriseerd zijn voor het doel van transparantie en gerichte controle bij audits. Hierover merkt het CBP het volgende op.

WMO-consulenten mogen in de rol van WMO-consulent toegang krijgen tot de informatiesystemen en diensten die ze voor de uitvoering van hun taken nodig hebben. Hiertoe behoort, gelet op het gesloten verstrekkingenregime van de SUWI wet en regelgeving, niet het Suwinet. Op het moment dat deze medewerkers in het kader van bepaalde WWB taken worden geautoriseerd voor toegang tot Suwinet dient dit, mede met het oog op transparantie en controleerbaarheid, op heldere wijze te worden weergegeven in een autorisatieoverzicht. Dit houdt in dat de rol op basis waarvan deze medewerkers toegang mogen krijgen tot Suwinet gebaseerd dient te zijn op de feitelijke taken die zij uitvoeren als medewerker bijzondere bijstand WWB. Dit sluit aan op norm 13.1 van het Normenkader GeVS, die stelt dat het verlenen van toegang tot de benodigde gegevens op basis van de uit te voeren functie en taken dient plaats te vinden.

Voorts dient te worden aangegeven dat in dit geval sprake is van twee uitvoerende taken die op gespannen voet met elkaar staan (conflicterende taken) omdat de gegevens via Suwinet slechts mogen worden ontsloten voor de WWB taak en niet

voor de WMO taak. Hierbij dient tevens te worden aangegeven welke beheersmaatregelen zijn genomen. Op deze wijze is sprake van autorisaties die transparant zijn belegd en die controleerbaar zijn. In dit geval dient de gemeente in ieder geval te controleren of de persoonsgegevens via Suwinet niet zijn geraadpleegd voor het uitvoeren van WMO taken.

Gelet op het feit dat diverse medewerkers van de gemeente 's-Hertogenbosch op grond van hun rol als WMO consulent geautoriseerd zijn om gegevens via Suwinet te raadplegen ten behoeve van taken ten aanzien van bijzondere bijstandsaanvragen, concludeert het CBP dat de gemeente 's-Hertogenbosch onvoldoende in staat is om de handelingen van de betreffende medewerkers te controleren op onrechtmatig gebruik van de persoonsgegevens omdat de toegekende autorisaties niet zijn toegekend op basis van de taken en verantwoordelijkheden van de betreffende medewerkers.

De omstandigheid dat de genoemde medewerkers enige tijd geen toegang hebben gezocht tot Suwinet, waardoor hun account is geblokkeerd, doet niet af aan deze vaststelling. De mededeling dat voor deze bijzondere situatie vooraf met het BKWI is afgesproken dat de rol WMO-consulent wordt gebruikt ontneemt de gemeente 's-Hertogenbosch niet de verantwoordelijkheid voor deze autorisatie, aangezien de afnemer van persoonsgegevens (de gemeente 's-Hertogenbosch) via Suwinet zelfstandig verantwoordelijk en aanspreekbaar is voor toepassing en naleving van de wettelijke regels ten aanzien van de verwerking en beveiliging van persoonsgegevens.[6]

Op basis van het bovenstaande concludeert het CBP dat de gemeente 's-Hertogenbosch onvoldoende maatregelen heeft getroffen om onbevoegde kennisneming van persoonsgegevens via Suwinet tegen te gaan. Hierdoor wordt artikel 13 van de Wbp overtreden.

3.3 Beveiligingsaspecten Suwinet

3.3.1 Norm beveiligingsplan, audit, beveiligingsincidenten en beveiliging inloggegevens

Artikel 13 Wbp schetst 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. Voorts kunnen op grond van het onder paragraaf 3.1.1 geschetste normenkader Bijlage I van de Regeling SUWI en het in de Verantwoordingsrichtlijn opgenomen Normenkader GeVS worden beschouwd als uitwerkingen van artikel 13 Wbp.

A. Beveiligingsplan

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

[6] Bijlage I. , bedoeld in artikel 6.3 van de Regeling SUWI, Stelselontwerp & Beveiliging Kaders en uitgangspunten aangaande de Gezamenlijke elektronische Voorzieningen Suwi (GeVS).

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

Artikel 6.4. eerste lid, Regeling SUWI stelt onder meer dat de op Suwinet aangesloten niet-Suwipartijen 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 over de voor het stelsel van maatregelen en procedures te hanteren normen wordt bepaald in bijlage I ('Stelselontwerp & Beveiliging Gezamenlijke elektronische Voorzieningen SUWI'). Artikel 6.4, tweede lid, Regeling Suwi bepaalt onder meer dat aangesloten niet-Suwipartijen in een beveiligingsplan aan dienen te geven op welke wijze zij invulling geven aan het eerste lid.

B. Audit
Op basis van artikel 6.4, derde lid, Regeling SUWI dienen niet-Suwipartijen een jaarlijkse audit uit te voeren op het gebruik en de inrichting van Suwinet.

C. Beveiligingsincidenten
Onder 'Incident- en probleembeheer' (norm 7 van het Normenkader GeVS) wordt het registreren, profiteren en (doen) verhelpen van gebeurtenissen die een onderbreking of vermindering van de kwaliteit van de dienstverlening aangaande de informatiehuishouding veroorzaken en van de achterliggende oorzaken daarvan verstaan. De incidenten worden centraal vastgelegd, gerapporteerd, geanalyseerd, gekwantificeerd en afgewikkeld in relatie tot het betrouwbaarheidsniveau en de ernst van de storing voor de bedrijfsvoering van Suwinet conform de afspraken in de Suwiketen (norm 8.2). De afnemer beschikt over een procedure voor het analyseren en het trekken van lering uit incidenten en zorgt ervoor dat het beleid en maatregelen overeenkomstig wordt aangepast (norm 9.1).

D. Beveiliging inloggegevens
De Code voor informatiebeveiliging[7] is een algemeen geaccepteerde technologie-neutrale beveiligingsstandaard binnen de praktijk van de informatiebeveiliging, die breed wordt toegepast bij het formuleren en implementeren van beveiligingsmaatregelen en kan worden beschouwd als een algemene en gezaghebbende uitwerking van het beveiligingsvoorschrift uit artikel 13 Wbp.
De Code voor informatiebeveiliging vereist onder meer dat wachtwoorden in beschermde vorm moeten worden opgeslagen en dat gebruikers geen geheime authenticatie-informatie dienen te registreren tenzij deze informatie veilig kan worden opgeslagen en de opslagmethode is goedgekeurd.[8]
Vertrouwelijke authenticatie-informatie dient geheim te worden houden en er mag aan geen enkele andere partij bekend gemaakt te worden.

3.3.2 Bevindingen

A. Beveiligingsplan
De gemeente 's-Hertogenbosch heeft een beleid Informatiebeveiliging en een beveiligingsplan overgelegd. In het beleid Informatiebeveiliging staat aangegeven dat toepassingen waarin gegevens over personen worden verwerkt, moeten voldoen aan

[7] NEN-ISO/IEC 27002:2013
[8] NEN-ISO/IEC 27002:2013, 9.3.4 i) en 9.3.1 b).

de Wbp, de Wet Gemeentelijke Basis Administratie en de Regeling SUWI. Voorts wordt aangegeven dat, in het kader van Regeling SUWI, het Suwinet-Normenkader leidend is voor de te nemen beveiligingsmaatregelen. Het beveiligingsplan betreft een concept dat uitsluitend beveiligingsmaatregelen voor Bureau Automatisering bevat. Voor beveiligingsmaatregelen met betrekking tot specifieke informatiesystemen binnen de gebruikersorganisatie zijn volgens dit beveiligingsplan afzonderlijke (generieke) beveiligingsplannen opgesteld. De gemeente 's-Hertogenbosch heeft geen beveiligingsplan specifiek gericht op Suwinet.

B. Audit

Over 2013 heeft de gemeente 's-Hertogenbosch geen audit laten uitvoeren op het gebruik en de inrichting van Suwinet door niet-Suwipartijen. De gemeente 's-Hertogenbosch heeft tijdens het onderzoek ter plaatse aangegeven dat hierover contact is opgenomen met het BKWI waarbij is gevraagd naar de noodzaak van een audit voor 2013. Over 2013 is in overleg met het BKWI geen audit gedaan, hetgeen met het BKWI telefonisch is afgesproken. Financiële redenen speelden een belangrijke rol bij de beslissing om geen audit uit te voeren.

C. *Beveiligingsincidenten*

Er is, in concept, een generieke procedure voor de omgang met beveiligingsincidenten (Procedure Informatiebeveiligingsissues, versie 0.2, 6 december 2013), deze is niet specifiek gericht op Suwinet. In deze procedure wordt een beveiligingsincident ('informatiebeveiligingsissue') omschreven als een gebeurtenis die de beschikbaarheid, integriteit en/of de vertrouwelijkheid van de ICT dienstverlening binnen de Gemeente 's-Hertogenbosch in gevaar brengt. Beveiligingsincidenten worden niet gecategoriseerd. Er wordt wel een algemeen logboek bijgehouden van ICT-beveiligingsincidenten.

Beveiligingsincidenten met betrekking tot Suwinet worden noch aan het BKWI noch aan de voorzitter van de domeingroep Privacy & Beveiliging van de Suwiketen gerapporteerd. Deze groep is bij de gemeente 's-Hertogenbosch niet bekend.

D. Beveiliging inloggegevens Suwinet RMC

Tijdens het onderzoek ter plaatse heeft het CBP verzocht om een korte demonstratie van de werking van Suwinet. Een RMC-medewerker is gevraagd om in Suwinet in te loggen. De benodigde inloggegevens (gebruikersnaam en wachtwoord) voor Suwinet werden opgehaald vanuit een (onversleuteld) Word-document opgeslagen op het netwerkschijf G in een map 'wachtwoorden'. Het Word-document bevatte tevens de inloggegevens voor andere applicaties, waarvoor de desbetreffende medewerker is geautoriseerd.

De gemeente 's-Hertogenbosch stelt in haar zienswijze op de voorlopige bevindingen dat het niet versleuteld vastleggen van inloggegevens in strijd is met haar beveiligingsbeleid. De gemeente heeft in haar zienswijze tevens aangegeven dat de inloggegevens waren verouderd en daardoor niet meer bruikbaar zijn.

Het informatiebeveiligingsbeleid van de gemeente 's-Hertogenbosch bevat geen passage die betrekking heeft op het opslaan van wachtwoorden. Het beveiligingsplan Automatisering 2013-2017 stelt onder paragraaf 7.2.1. dat wachtwoorden 'niet vast gelegd mogen worden tenzij deze registratie veilig kan worden opgeslagen en de

methode van opslag is goedgekeurd'. Het beveiligingsplan Automatisering 2013-2917 is echter in conceptvorm, en dus in niet vastgestelde vorm, door het CBP ontvangen.

3.3.3 Beoordeling

A. Beveiligingsplan

De gemeente 's-Hertogenbosch heeft geen beveiligingsplan dat specifiek is opgesteld voor Suwinet, waarin wordt aangegeven hoe de gegevensuitwisselingen die plaatsvinden in het kader van de gezamenlijke elektronische voorzieningen SUWI, worden beveiligd tegen inbreuk op de beschikbaarheid, integriteit en vertrouwelijkheid. De gemeente 's-Hertogenbosch handelt hiermee in strijd met artikel 6.4 Regeling SUWI en daarmee artikel 13 Wbp.

B. Audit

De gemeente heeft met de betrekking tot de verwerking van persoonsgegevens via Suwinet in het kader van de RMC-taak geen audit over 2013 uitgevoerd, hetgeen een overtreding van artikel 6.4 Regeling SUWI en daarmee tevens een overtreding van artikel 13 Wbp inhoudt.

C. Beveiligingsincidenten

Er is geen formeel vastgestelde procedure aanwezig voor de omgang met beveiligingsincidenten. Beveiligingsincidenten met betrekking tot Suwinet worden niet centraal gerapporteerd, geanalyseerd, gekwantificeerd en afgewikkeld in relatie tot het betrouwbaarheidsniveau en de ernst van de storing voor de bedrijfsvoering van Suwinet conform de afspraken in de Suwiketen. Dit is niet in overeenstemming met de normen uit het Normenkader GeVS (norm 7, norm 8.2) en strijdig met artikel 13 Wbp.

D. Beveiliging inloggegevens

Het niet versleuteld opslaan van inloggegevens (gebruikersnaam en wachtwoord) in een Word document staat op gespannen voet met de Code voor informatiebeveiliging die voorschrijft dat wachtwoorden in beschermde vorm moeten worden opgeslagen en dat gebruikers geen geheime authenticatie-informatie dienen te registreren tenzij deze informatie veilig kan worden opgeslagen en de opslagmethode is goedgekeurd.[9] Het gegeven dat de inloggegevens waren verouderd en daardoor niet meer bruikbaar doet niet af aan het feit dat inloggegevens onversleuteld waren opgeslagen.

Het gegeven dat een medewerker inloggegevens onversleuteld heeft opgeslagen betekent echter (nog) niet dat de gemeente ten aanzien van het opslaan van wachtwoorden geen of onvoldoende beveiligingsmaatregelen, als bedoeld in artikel 13 Wbp, heeft genomen. Maatregelen ten aanzien van (het opslaan van) wachtwoorden moeten zijn beschreven in het beveiligingsbeleid of het beveiligingsplan.

Echter, het informatiebeveiligingsbeleid van de gemeente 's-Hertogenbosch bevat geen passage die betrekking heeft op de omgang met wachtwoorden. Het beveiligingsplan Automatisering 2013-2017 stelt onder paragraaf 7.2.1. dat weliswaar dat wachtwoorden 'niet vast gelegd mogen worden tenzij deze registratie veilig kan

[9] NEN-ISO/IEC 27002:2013, 9.4.3 i) en 9.3.1 b).

worden opgeslagen en de methode van opslag is goedgekeurd' maar is slechts in conceptvorm, en dus in niet vastgestelde vorm door het CBP ontvangen.

Het CBP concludeert op basis van bovenstaande dat de gemeente 's-Hertogenbosch onvoldoende maatregelen heeft getroffen met betrekking tot (het vastleggen van) wachtwoorden. Dit is niet conform de Code voor informatiebeveiliging (NEN-ISO/IEC 27002:2013) en daarmee in strijd met artikel 13 Wbp.

3.4 Naleving informatieplicht

3.4.1 Norm

Artikel 34 Wbp bepaalt dat indien buiten de betrokkene om persoonsgegevens worden verkregen, de verantwoordelijke de betrokkene zijn identiteit en de doeleinden van de verwerking mededeelt, alsmede nadere informatie geeft voor zover dat gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen. Deze informatieverstrekking dient plaats te vinden op het moment van vastlegging van de hem betreffende gegevens, of wanneer de gegevens bestemd zijn om te worden verstrekt aan een derde, uiterlijk op het moment van de eerste verstrekking.

3.4.2 Bevindingen

De gemeente 's-Hertogenbosch informeert een betrokkene niet over de verwerking van diens persoonsgegevens in het kader van de RMC-taak.

3.4.3 Beoordeling

Door betrokkenen niet te informeren over de verwerkingen van persoonsgegevens in het kader van de RMC-taak handelt de gemeente 's-Hertogenbosch in strijd met artikel 34 Wbp.

4 Conclusie

Uit het onderzoek volgt dat de Wbp wordt overtreden.

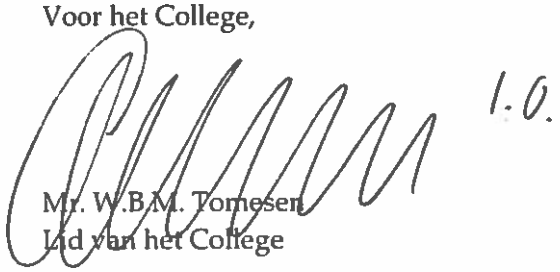
- Ten aanzien van het aansluiten van niet-Suwipartijen op Suwinet wordt door de gemeente 's-Hertogenbosch op meerdere punten (uitwerking Wbp-vereisten, rollen en autorisaties) niet gewerkt volgens het aansluitprotocol uit bijlage III van de Regeling SUWI. Dit betekent dat op deze punten artikel 6 Wbp wordt overtreden.

- Medewerkers van de gemeente 's-Hertogenbosch hebben in hoedanigheid van WMO-consulent toegang tot Suwinet. De gemeente 's-Hertogenbosch handelt hiermee in strijd met artikel 13 Wbp.

- Voorts voldoet de gemeente 's-Hertogenbosch op verschillende punten (toekennen en controle autorisaties, beveiligingsplan, audit, beveiligingsincidenten, beveiliging inloggegevens RMC-taak) niet aan de vereisten uit bijlage I van de Regeling SUWI, het in de Verantwoordingsrichtlijn opgenomen Normenkader GeVS en de Code voor Informatiebeveiliging waardoor de gemeente 's-Hertogenbosch artikel 13 Wbp overtreedt.

- Tot slot wordt de wettelijke informatieplicht conform artikel 34 Wbp niet nageleefd door de gemeente 's-Hertogenbosch.

Het College bescherming persoonsgegevens,
Voor het College,



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

BIJLAGE I: REACTIE CBP OP ZIENSWIJZE GEMEENTE 'S-HERTOGENBOSCH

De gemeente 's-Hertogenbosch (hierna ook: de gemeente) gaat in haar zienswijze puntsgewijs in op de bevindingen van het CBP. Deze bevindingen betreffen:

1. De overeenkomsten inzake toegang tot Suwinet door niet-Suwipartijen;
2. De toekenning en controle van autorisaties Suwinet;
3. Toegang tot Suwinet door consulenten in het kader van de Wet Maatschappelijke Ondersteuning (WMO);
4. Een specifiek beveiligingsplan voor Suwinet;
5. Het uitvoeren van een audit over 2013 door het Bureau Keteninformatisering Werk en Inkomen (BKWI);
6. Het melden van beveiligingsincidenten;
7. De beveiliging van inloggegevens;
8. De naleving van de informatieplicht.

De punten van de zienswijze van de gemeente 's-Hertogenbosch zullen hieronder - deels samengevat - afzonderlijk worden weergegeven.

1. **De overeenkomsten inzake Suwinet door niet-Suwipartijen**

De gemeente 's-Hertogenbosch stelt vast dat deze overeenkomst een standaardovereenkomst is die door het Uitvoeringsinstituut Werknemersverzekeringen (UWV) en het BKWI worden voorgelegd. Zij heeft zowel voor- als achteraf geen invloed kunnen uitoefenen op de inhoud van de overeenkomst. De bevinding valt volgens de gemeente buiten de *scope* van het onderzoek, nu andere partijen hier aan zet en verantwoordelijk zijn.

Reactie CBP

Het CBP constateert dat de gemeente een overeenkomst heeft getekend voor de gegevenslevering door het UWV. De gemeente is één van de contractuele partijen. Het feit dat het een standaardovereenkomst betreft, betekent niet dat de uiteindelijke inhoud van de overeenkomst bij voorbaat al vaststaat. Van een standaardovereenkomst kan desgewenst worden afgeweken. Met de ondertekening van deze overeenkomst is de gemeente 's-Hertogenbosch akkoord gegaan met de uiteindelijke inhoud van de overeenkomst. De bevindingen zijn op dit punt derhalve niet aangepast.

2. **Toekenning en controle van autorisaties Suwinet**

De gemeente 's-Hertogenbosch stelt vast dat de bedoelde procedures (formele procedures ten aanzien van het toekennen en de controle van autorisaties Suwinet) aanwezig zijn en door het betreffende Management Team zijn vastgesteld. De gemeente verwijst hierbij naar bijlage 1 bij de zienswijze, protocol gebruik gegevens Suwinet. De gemeente 's-Hertogenbosch verwijst daarnaast naar bijlage 2, verslag vaststelling protocol door het Management Team.

Reactie CBP

Het CBP heeft opnieuw naar het protocol en het verslag gekeken. Het protocol met betrekking tot het gebruik van gegevens van Suwinet bevat weliswaar regels ten aanzien toekenning en controle van autorisaties, maar het protocol bevat geen datum

en historie, en is nog nooit geëvalueerd. Daarbij is het slechts van toepassing op de afdeling Arbeidsmarkt en Sociale Zaken (AmSZ), terwijl medewerkers van verschillende afdelingen gebruik maken van gegevens via Suwinet. In het kader van de RMC-taak zijn medewerkers van meerdere gemeenten geautoriseerd om gebruik te maken van gegevens via Suwinet. Het genoemde protocol bevat noch bepalingen ten aanzien van medewerkers van andere afdelingen van de gemeente 's-Hertogenbosch, noch bepalingen ten aanzien van RMC-medewerkers van andere gemeenten. Het CBP constateert dat de wettelijke regels met betrekking tot toekenning en controle autorisaties Suwinet niet worden nageleefd. De bevindingen zullen ten aanzien van het protocol met betrekking tot het gebruik van gegevens van Suwinet worden genuanceerd, maar dit gedeelte van de beoordeling van de bevindingen blijft ongewijzigd.

Het CBP heeft de bevindingen en de daarop gebaseerde conclusie met betrekking tot norm 13.5 (controle op verleende toegangsrechten) van het Normenkader GeVS uit het rapport van bevindingen verwijderd.

3. **Toegang tot Suwinet in het kader van de WMO**

De gemeente 's-Hertogenbosch stelt het volgende vast. In de toelichting van norm 13.1 van het Suwinet normenkader staat het volgende: "Er is geen toegang verstrekt buiten de sociale dienst, de gemeentelijke belastingdeurwaarders, burgerzaken en de regionale meld- en coördinatiefunctie bij voortijdig schoolverlaten. Voor het gebruik door gemeentelijke belastingdeurwaarders, burgerzaken en de regionale meld en coördinatiefunctie bij voortijdig schoolverlaten is een apart contract afgesloten.

Het beleid van de gemeente 's-Hertogenbosch is erop gericht om deze norm te handhaven. Buiten de genoemde afdelingen zijn er geen autorisaties verstrekt. Wel geldt het volgende. Een aantal medewerkers van de gemeente 's-Hertogenbosch behandelt zowel WMO als bijzondere bijstand aanvragen (WWB). Voor de taakuitoefening van bijzondere bijstand vallen zij, aldus de gemeente 's-Hertogenbosch, onder de Wet SUWI. Voor deze bijzondere situatie is vooraf met het BKWI afgesproken dat de rol WMO-consulent gebruikt wordt. Het doel hiervan is volgens de gemeente 's-Hertogenbosch juist transparantie én gerichte controle bij audits.

De behoefte voor het gebruik van Suwinet door de betreffende consulenten is overigens minimaal. Aan het CBP is in het kader van het onderzoek een overzicht verstrekt waaruit blijkt dat alle accounts met de rol van WMO-consulent op het tijdstip van de audit waren geblokkeerd, nu deze accounts al langere tijd inactief waren. Uit het aan het CBP aangeleverde overzicht van 4 april 2014, opgenomen als bijlage 3, blijkt ook dat er op 6 september 2013 voor het laatst een consulent met die rol heeft ingelogd. Pas bij een actief account die onder een WMO-rol hangt zou er sprake kunnen zijn van een overtreding.

Reactie CBP

Artikel 13 Wbp vereist onder meer dat maatregelen ten uitvoer worden gelegd om onrechtmatige verwerking en onbevoegde kennisneming van persoonsgegevens tegen te gaan. 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. Voorts schrijft norm 2.2 van het Normenkader GeVS voor dat 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 zijn beschreven en duidelijk gescheiden zijn belegd. De code voor informatiebeveiliging stelt voorts dat gebruikers verantwoordelijk gesteld moeten kunnen worden voor hun handelingen[10].

WMO-consulenten mogen, gelet op het gesloten verstrekkingenregime van de SUWI wet- en regelgeving en gezien de aard van hun werkzaamheden, geen toegang krijgen tot Suwinet. Dit betekent dat de gemeente 's-Hertogenbosch ervoor moet zorgen dat er voor bepaalde functies, zoals de functie van WMO-consulent, geen autorisaties worden gecreëerd voor Suwinet.

Het CBP heeft tijdens het onderzoek vastgesteld dat WMO consulenten geautoriseerd zijn voor toegang tot Suwinet. Uit de toelichting van de gemeente 's-Hertogenbosch blijkt dat deze medewerkers een dubbele uitvoerende taak hebben. Naast WMO aanvragen behandelen zij ook aanvragen op het gebied van het bijzondere bijstand (WWB). Gezien het gesloten verstrekkingenregime mag het Suwinet niet worden ontsloten voor WMO doeleinden. Autorisaties voor gebruik van Suwinet mogen slechts verleend worden voor de uitvoering van de bijzondere bijstand taak.

In haar zienswijze op de voorlopige bevindingen heeft de gemeente 's-Hertogenbosch naar voren gebracht dat WMO-consulenten juist geautoriseerd zijn voor het doel van transparantie en gerichte controle bij audits. Hierover merkt het CBP het volgende op.

WMO-consulenten mogen in de rol van WMO-consulent toegang krijgen tot de informatiesystemen en diensten die ze voor de uitvoering van hun taken nodig hebben. Hiertoe behoort, gelet op het gesloten verstrekkingenregime van de SUWI wet en regelgeving, niet het Suwinet. Op het moment dat deze medewerkers in het kader van bepaalde WWB taken worden geautoriseerd voor toegang tot Suwinet dient dit, mede met het oog op transparantie en controleerbaarheid, op heldere wijze te worden weergegeven in een autorisatieoverzicht. Dit houdt in dat de rol op basis waarvan deze medewerkers toegang mogen krijgen tot Suwinet gebaseerd dient te zijn op de feitelijke taken die zij uitvoeren als medewerker bijzondere bijstand WWB. Dit sluit aan op norm 13.1 van het Normenkader GeVS, die stelt dat het verlenen van toegang tot de benodigde gegevens op basis van de uit te voeren functie en taken dient plaats te vinden.

Voorts dient te worden aangegeven dat in dit geval sprake is van twee uitvoerende taken die op gespannen voet met elkaar staan (conflicterende taken) omdat de gegevens via Suwinet slechts mogen worden ontsloten voor de WWB taak en niet voor de WMO taak. Hierbij dient tevens te worden aangegeven welke beheersmaatregelen zijn genomen. Op deze wijze is sprake van autorisaties die transparant zijn belegd en die controleerbaar zijn. In dit geval dient de gemeente in ieder geval te controleren of de persoonsgegevens via Suwinet niet zijn geraadpleegd voor het uitvoeren van WMO taken.

[10] NEN-ISO/IEC 27002:2013, 9.2.1. a)

Gelet op het feit dat diverse medewerkers van de gemeente 's-Hertogenbosch op grond van hun rol als WMO consulent geautoriseerd zijn om gegevens via Suwinet te raadplegen ten behoeve van taken ten aanzien van bijzondere bijstandsaanvragen, concludeert het CBP dat de gemeente 's-Hertogenbosch onvoldoende in staat is om de handelingen van de betreffende medewerkers te controleren op onrechtmatig gebruik van de persoonsgegevens omdat de toegekende autorisaties niet zijn toegekend op basis van de taken en verantwoordelijkheden van de betreffende medewerkers.

De omstandigheid dat de genoemde medewerkers enige tijd geen toegang hebben gezocht tot Suwinet, waardoor hun account is geblokkeerd, doet niet af aan deze vaststelling. De mededeling dat voor deze bijzondere situatie vooraf met het BKWI is afgesproken dat de rol WMO-consulent wordt gebruikt ontneemt de gemeente 's-Hertogenbosch niet de verantwoordelijkheid voor deze autorisatie, aangezien de afnemer van persoonsgegevens (de gemeente 's-Hertogenbosch) via Suwinet zelfstandig verantwoordelijk en aanspreekbaar is voor toepassing en naleving van de wettelijke regels ten aanzien van de verwerking en beveiliging van persoonsgegevens.

Op basis van het bovenstaande concludeert het CBP dat de gemeente 's-Hertogenbosch onvoldoende maatregelen heeft getroffen om onbevoegde kennisneming van persoonsgegevens via Suwinet tegen te gaan. Hierdoor wordt artikel 13 van de Wbp overtreden.

De bevindingen zijn op basis van het bovenstaande aangepast.

4. Een specifiek beveiligingsplan voor Suwinet

De gemeente 's-Hertogenbosch stelt in haar zienswijze dat, conform het normenkader Suwinet, het door het Algemeen Management Team en College vastgestelde beleid een specifieke passage over Suwinet bevat en daarmee voldoet aan het normenkader. Alle generieke normen van het Suwinet normenkader worden aantoonbaar afgedekt door het beveiligingsplan Automatisering, de Suwinet specifieke normen door het protocol Suwinet. In dit verband wordt verwezen naar bijlagen 4a (Beleid informatieveiligheid 2014-2018) en 4b (beveiligingsplan 2013-2017).

Reactie CBP

Het normenkader GeVS stelt dat de Suwipartij voor de Suwi-omgeving een Suwinet beveiligingsplan dient te hebben opgesteld dat gebaseerd is op het informatiebeveiligingsbeleid van de organisatie en afspraken in de Suwiketen (norm 1.2). Dit beveiligingsplan dient derhalve een uitwerking te bevatten van de relevante normen uit het informatiebeveiligingsbeleid en de afspraken in de Suwiketen. Hierbij hoort volgens norm 1.2 onder meer aandacht te worden besteed aan de meer jaren activiteiten voor Suwinet en de afspraken gebaseerd op de Keten SLA.

De gemeente 's-Hertogenbosch heeft een passage in het Beleid informatieveiligheid opgenomen waarin wordt verwezen naar de Regeling Suwi en het Suwinet-normenkader. Deze passage luidt als volgt:

'Toepassingen waarin gegevens over personen worden verwerkt, dienen te voldoen aan de Wet Bescherming Persoonsgegevens, de Wet Gemeentelijke Basis Administratie en de Regeling SUWI. In het kader van Regeling SUWI is het Suwinet-Normenkader leidend voor de te nemen beveiligingsmaatregelen.'

In deze passage wordt in zijn algemeenheid verwezen naar wet- en regelgeving en bevat derhalve geen uitwerking van het normenkader GeVS en de meer jaren activiteiten voor Suwinet. Evenmin bevat deze passage een uitwerking van de afspraken gebaseerd op de Keten SLA GeVS voor de gemeente 's-Hertogenbosch.

Zoals aangegeven onder punt 2, bevat het protocol met betrekking tot het gebruik van gegevens van Suwinet bevat geen datum en historie, en is nog nooit geëvalueerd. Daarbij is het slechts van toepassing op de afdeling Arbeidsmarkt en Sociale Zaken (AmSZ), terwijl medewerkers van verschillende afdelingen gebruik maken van gegevens via Suwinet. Bovendien bevat dit protocol geen uitwerking van alle normen uit het normenkader GeVS.

Het beveiligingsplan is in conceptvorm en bevat geen verwijzingen naar de beveiligingsmaatregelen die specifiek ten aanzien van Suwinet ten uitvoer worden gelegd.

De hierboven genoemde passage in het informatiebeveiligingsbeleid, het beveiligingsplan Automatisering 2013-2017 en het protocol met betrekking tot het gebruik van gegevens van Suwinet, voldoen, zowel afzonderlijk als gecombineerd, niet aan norm 1.2 uit het normenkader GeVS. De bevindingen zijn op dit punt derhalve niet aangepast.

5. Het houden van een audit over 2013

De gemeente 's-Hertogenbosch geeft aan de audit over 2013 op een alternatieve wijze te hebben uitgevoerd. Gezien de recente ontwikkelingen met betrekking tot de vaststelling van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en de Suwinet zelftest van de Vereniging Nederlandse Gemeenten (VNG), heeft de gemeente ervoor gekozen daar de focus op te leggen. Juist omdat bij de BIG en de Suwinet zelftest de gehele organisatie in *scope* is, waarbij het bij de zelftest het grootste deel van de Suwinet gebruikers betreft (de medewerkers van de sociale dienst). Een audit toetst slechts een klein gedeelte van de organisatie (RMC en belastingen).

Het BKWI heeft, op verzoek van de gemeente, hierover in een telefonisch consult aangegeven het niet vreemd te vinden als zij de audit zouden laten vervallen en de prioriteit bij de implementatie van de BIG (Baseline Informatiebeveiliging Gemeenten, toevoeging CBP) zouden leggen. Voor het jaar 2013 heeft het BKWI geen bericht verstuurd over de verplichting van de audit, hiervan is uitsluitend melding gemaakt op hun website.
Gelet op de reactie van het BKWI, is ervoor gekozen om over het jaar 2013 geen audit door een accountant te laten uitvoeren en prioriteit te geven aan de implementatie van de BIG en het uitvoeren van de Suwinet zelftest van de VNG. Door de uitvoering van de BIG en de zelftest, is een accurate rapportage over het gebruik van Suwinet 2013 aanwezig.

Reactie CBP

Op basis van artikel 6.4, derde lid, Regeling SUWI dienen niet-Suwipartijen een jaarlijkse audit uit te voeren op het gebruik en de inrichting van Suwinet. De rapportage wordt vergezeld van een oordeel van een tot de Nederlandse Orde van

Register EDP-Auditors toegelaten persoon of van een verklaring van getrouwheid van een dergelijke persoon.

Het houden van een zelftest en de ontwikkeling van een BIG moeten worden beschouwd als maatregelen die naast de bestaande wettelijke verplichtingen kunnen worden genomen. Zij kunnen niet worden beschouwd als alternatieven voor wettelijke verplichtingen.

De zelftest die de VNG heeft ontwikkeld is een globale inschatting van de beveiliging van het gebruik van gegevens via Suwinet, terwijl de rapportage als bedoeld in artikel 6.4, derde lid, Regeling SUWI een gedetailleerder beeld geeft van de beveiligingsmaatregelen ten aanzien van het gebruik van Suwinet door niet-Suwi afdelingen binnen de gemeente. Bovendien is de zelftest een eigen evaluatie van de beveiliging van Suwinet, die niet wordt vergezeld van een oordeel van een tot de Nederlandse Orde van Register EDP-Auditors toegelaten persoon of van een verklaring van getrouwheid van een dergelijke persoon.

De BIG is bedoeld om gemeenten op een vergelijkbare manier efficiënt te laten werken met informatiebeveiliging. De BIG is ook een zelfevaluatie-instrument waarmee gemeenten in staat zijn om te meten of de organisatie zijn informatiebeveiliging op orde heeft. De BIG is gebaseerd op de Code voor informatiebeveiliging en bevat derhalve normen waaraan gemeenten volgens de VNG moeten voldoen. De BIG is derhalve geen audit, maar kan dienen als toetsingskader voor gemeenten die willen weten of de informatiehuishouding binnen de eigen organisatie op orde is. Op deze wijze zou de BIG er toe kunnen leiden dat de auditlast voor gemeenten op termijn verminderd.

Tot slot heeft het BKWI geen formele zeggenschap over het voornemen van een gemeente om een wettelijke vereiste audit niet uit te voeren.

De bevindingen zijn op dit punt niet aangepast.

6. Het melden van beveiligingsincidenten

De gemeente 's-Hertogenbosch stelt vast dat er aantoonbaar een vastgestelde procedure is voor het melden van incidenten. Incidenten worden volgens de gemeente centraal vastgelegd. Onrechtmatige verwerkingen van persoonsgegevens worden gezien als een incident. De procedure voor de afhandeling hiervan staat in het aan het CBP overlegde protocol Suwinet (zie bijlage 1, onder 5). Ook phishingmails zijn incidenten die regelmatig worden gemeld en vastgelegd. Specifiek met betrekking tot Suwinet of persoonsgegevens zijn er, tot op heden, geen phishingmails gemeld. Er zijn de afgelopen jaren geen incidenten met betrekking tot Suwinet geweest. Vanwege het ontbreken hiervan, zijn meldingen gericht aan het BKWI niet aan de orde geweest. Voorts stelt de gemeente dat de domeingroep Privacy en Beveiliging niet bij hen bekend is. De verplichting voor gemeenten om incidenten te melden aan de domeingroep Privacy en Beveiliging heeft de gemeente niet in wetgeving, het normenkader dan wel contracten kunnen terugvinden.

Reactie CBP

In het door de gemeente overgelegde protocol met betrekking tot het gebruik van gegevens van Suwinet (bijlage 1, onder 5) wordt aangegeven dat onrechtmatig

gebruik van Suwinet door medewerkers wordt geëscaleerd en dat daar mogelijk disciplinaire maatregelen aan worden verbonden.

Beveiligingsincidenten omvatten echter meer dan onrechtmatig gebruik door medewerkers of ander tijdelijk personeel: bijvoorbeeld inbraakpogingen door hackers of andere onbevoegden van buiten de gemeentelijke organisatie, maar ook foutieve inlogpogingen of het onbeveiligd opslaan van wachtwoorden dienen te worden gecategoriseerd als beveiligingsincidenten. Evenmin wordt door de gemeente 's-Hertogenbosch aangegeven dat onrechtmatig gebruik van Suwinet door medewerkers gecategoriseerd wordt als beveiligingsincident, waardoor er ook geen nadere analyse plaatsvindt en vervolgacties kunnen worden gedefinieerd.

Het CBP heeft in de door de gemeente 's-Hertogenbosch overgelegde stukken geen vastgestelde procedure voor het melden van incidenten kunnen vinden. In het beveiligingsbeleid wordt op pagina 11 aangegeven dat beveiligingsincidenten zo snel mogelijk via de juiste kanalen dienen te worden gerapporteerd. Het beveiligingsplan 2013-2017, dat in conceptvorm is opgestuurd naar het CBP, wordt verwezen naar een bijlage 13, hetgeen de procedure met betrekking tot beveiligingsincidenten zou bevatten. Het beveiligingsplan bevat echter geen bijlage 13 noch een incidentenprocedure. Op 27 maart 2014 is een conceptprocedure met betrekking tot de omgang met beveiligingsincidenten opgestuurd. Deze procedure is eveneens in conceptvorm en bevat daarbij geen passage die specifiek betrekking heeft op de Suwi-omgeving, zoals de verplichting om incidenten te melden aan de – door het BKWI voorgezeten – domeingroep Privacy en Beveiliging.

De passages met betrekking tot phishingmails en onrechtmatig gebruik door medewerkers worden naar aanleiding van de zienswijze uit het rapport van bevindingen verwijderd. Verder zijn de bevindingen op dit punt niet aangepast.

7 Beveiliging van inloggegevens

De gemeente 's-Hertogenbosch stelt dat het onversleuteld vastleggen van inloggegevens in strijd is met haar beveiligingsbeleid. Het niet naleven hiervan is onbewust onbekwaam gedrag van de desbetreffende medewerker. De gemeente onderkent het belang van bewustwording op het gebied van informatieveiligheid. Dit is een speerpunt in het Beleid informatieveiligheid voor de komende jaren. In 2014 is daarom een Bewustwordingsprogramma Informatieveiligheid gestart om de informatieveiligheid ook op dit punt binnen de gemeente naar een hoger plan te tillen.

Tijdens het CBP-onderzoek haalde de desbetreffende medewerker inderdaad als eerste handeling de benodigde inloggegevens (gebruikersnaam en wachtwoord) uit een niet versleuteld Word document vanaf een persoonlijke schijf die niet kan worden benaderd door anderen. De gegevens waren echter verouderd en daarmee onbruikbaar. Een tweede poging verliep vervolgens wel geheel conform de te stellen eisen van beveiliging inloggegevens.
Deze constatering tijdens het CBP-onderzoek is volgens de gemeente 's-Hertogenbosch feitelijk bijvangst, maar valt niet binnen het bereik van het onderzoek. De feitelijke en beveiligde inlogmethodiek is immers correct toegepast. De beoordeling door het CBP is gebaseerd op een beperkt deel van de onderzoeksinformatie en is bovendien niet volledig weergegeven.

Reactie CBP

Het niet versleuteld opslaan van inloggegevens (gebruikersnaam en wachtwoord) in een Word document staat op gespannen voet met de Code voor informatiebeveiliging die voorschrijft dat wachtwoorden in beschermde vorm moeten worden opgeslagen en dat gebruikers geen geheime authenticatie-informatie dienen te registreren tenzij deze informatie veilig kan worden opgeslagen en de opslagmethode is goedgekeurd.[11] Het gegeven dat de inloggegevens waren verouderd en daardoor niet meer bruikbaar doet niet af aan het feit dat inloggegevens onversleuteld waren opgeslagen. De gemeente 's-Hertogenbosch onderschrijft bovengenoemde norm door te stellen dat het niet versleuteld vastleggen van inloggegevens in strijd is met haar beveiligingsbeleid. Desalniettemin beschouwt het CBP het als een goede stap dat de gemeente 's-Hertogenbosch een bewustwordingsprogramma is gestart om de informatieveiligheid ook op dit punt binnen de gemeente naar een hoger plan te tillen.

Het gegeven dat een medewerker inloggegevens onversleuteld heeft opgeslagen betekent echter (nog) niet dat de gemeente ten aanzien van wachtwoorden geen of onvoldoende beveiligingsmaatregelen, als bedoeld in artikel 13 Wbp, heeft genomen. Maatregelen ten aanzien van (het opslaan van) wachtwoorden moeten zijn beschreven in het beveiligingsbeleid of het beveiligingsplan.

Echter, het informatiebeveiligingsbeleid van de gemeente 's-Hertogenbosch bevat geen passage die betrekking heeft op de omgang met wachtwoorden. Het beveiligingsplan Automatisering 2013-2017 stelt onder paragraaf 7.2.1. dat weliswaar dat wachtwoorden 'niet vast gelegd mogen worden tenzij deze registratie veilig kan worden opgeslagen en de methode van opslag is goedgekeurd' maar is slechts in conceptvorm, en dus in niet vastgestelde vorm door het CBP ontvangen.

Het CBP concludeert op basis van bovenstaande dat de gemeente 's-Hertogenbosch onvoldoende maatregelen heeft getroffen met betrekking tot (het vastleggen van) wachtwoorden. Dit is niet conform de Code voor informatiebeveiliging (NEN-ISO/IEC 27002:2013) en daarmee in strijd met artikel 13 Wbp. De bevindingen zijn ten aanzien van de beveiliging van inloggegevens op basis van het bovenstaande aangepast.

De gemeente 's-Hertogenbosch geeft aan dat deze bevinding niet tot de oorspronkelijke reikwijdte van het onderzoek behoort. Het CBP-onderzoek richt zich onder meer op de vereisten met betrekking tot toegang en beveiliging van Suwinet. Deze bevinding behoort derhalve tot de oorspronkelijke reikwijdte van het onderzoek.

8. Naleving informatieplicht

De gemeente 's-Hertogenbosch betoogt dat artikel 34 Wbp vragen oproept met betrekking tot de in het artikel benoemde omstandigheden waaronder de informatieplicht aan de orde is. Een eenduidig toets criterium ontbreekt. De gemeente heeft ter zake van de informatieplicht maatregelen getroffen. Bij de invoering van de Wbp zijn alle verwerkingen van de gemeente in kaart gebracht en is door juridische medewerkers bepaald of er voor de betreffende verwerkingen een meldingsplicht en/of informatieplicht was. Uitgangspunt hierbij is dat de gemeente de wet naleeft en, indien wettelijk vereist, aan de informatieplicht voldoet. De gemeente geeft aan met de mensen die de gemeente raadpleegt te communiceren.

[11] NEN-ISO/IEC 27002:2013, 9.4.3 i) en 9.3.1 b).

Aanvullende merkt de gemeente het volgende op. De informatieplicht is complex. Er dient primair te worden vastgesteld of er daadwerkelijk een taak is voor de gemeente. Deze vaststelling dient te gebeuren in nauw overleg met het BKWI. In de Service Level Agreement (SLA) voor Suwinet zijn veel bepalingen opgenomen met betrekking tot het omgaan met informatie, maar niets ten aanzien van het informeren van de burger. In het rapport van het CBP wordt op dit punt ook niet verwezen naar Suwi-normen, alleen naar de Wbp.

Reactie CBP

De informatieplicht is in dit geval van toepassing op de onderzochte verwerkingen van persoonsgegevens en geldt derhalve voor de gemeente 's-Hertogenbosch. De verplichting van de verantwoordelijke om de betrokkene op eigen initiatief op de hoogte te stellen van het bestaan van de gegevensverwerking is een belangrijk instrument om het gegevensverkeer transparant te maken. De ratio van de informatieverplichting is dat de verwerkingen van de verantwoordelijke voor de betrokkene transparant zijn en daarmee de verantwoordelijke in rechte aan is te spreken. De betrokkene is hiermee in staat te volgen op welke wijze gegevens over hem worden verwerkt.

De gemeente 's-Hertogenbosch geeft aan dat de informatieplicht af te willen stemmen met het BKWI. De in punt 1 genoemde overeenkomst dient inderdaad een bepaling te bevatten ten aanzien van de informatieplicht en op welke wijze hier vorm aan wordt gegeven. Het CBP heeft echter vastgesteld dat een dergelijke bepaling in de overeenkomst ontbreekt.
De bevindingen zijn op dit punt niet aangepast.

Aanpassingen ten opzichte van de voorlopige bevindingen

Naar aanleiding van de zienswijze van de gemeente 's-Hertogenbosch zijn de bevindingen op het punt van de toegang tot Suwinet in het kader van de WMO worden aangepast. Ook de bevindingen ten aanzien van de beveiliging van inloggegevens is aangepast. Voorts zijn de bevindingen en conclusies ten aanzien van de controle van autorisaties Suwinet (Norm 13.5 van het Normenkader GeVS) en de passage ten aanzien van phishingmails is uit het rapport van bevindingen verwijderd. Tot slot zijn passages met betrekking tot de *security officer* van de gemeente 's-Hertogenbosch aangepast opdat deze passages geen persoonsgegeven meer bevatten.