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 naar de toegang tot Suwinet voor niet-Suwipartijen bij het Uitvoeringsinstituut Werknemersverzekeringen (UWV), organisatieonderdeel Bureau Keteninformatisering Werk en Inkomen (BKWI)

z2013-00560
Openbare versie

Rapport van bevindingen

November 2014

DATUM 4 november 2014

INHOUDSOPGAVE

Samenvatting **3**

1 Inleiding **4**
1.1 Achtergrond en aanleiding onderzoek 4
1.2 Doel, reikwijdte en uitvoering onderzoek 4
1.3 Wettelijk kader 5

2 Organisatie UWV/ BKWI **6**
2.1 Verantwoordelijke 6

3 Bevindingen onderzoek **6**
3.1 Overeenkomsten inzake toegang Suwinet door niet-Suwipartijen 6
3.1.1 Norm 6
3.1.2 Bevindingen 7
3.1.3 Beoordeling 7
3.2 Toekenning van autorisaties 8
3.2.1 Norm 8
3.2.2 Bevindingen 8
3.2.3 Beoordeling 9
3.3 Geselecteerde beveiligingsaspecten van Suwinet 9
3.3.1 Norm beveiligingsplan, controle gebruik Suwinet en beveiligingsincidenten 9
3.3.2 Bevindingen 10
3.3.3 Beoordeling 11
3.4 Bevindingen onderzoek Department of Social Protection, Ierland 12
3.4.1 Norm 12
3.4.2 Bevindingen 12
3.4.3 Beoordeling 13

4 Conclusies **14**

Bijlage I: Reactie CBP op zienswijze UWV **16**
1. De verschillende verantwoordelijkheden met betrekking tot het aansluitprotocol Suwinet 16
2. Reactie UWV op voorlopige bevindingen 17
2.1 Overeenkomsten met nationale niet- Suwipartijen 18
2.2 De toekenning van autorisaties 20
2.3 Geselecteerde beveiligingsaspecten van Suwinet 20
2.4 De overeenkomst met het Department of Social Protection van Ierland 21
3. Aanpassingen ten opzichte van de voorlopige bevindingen 23

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 (SUWI). Dit vindt plaats door middel van de Gezamenlijke elektronische Voorzieningen SUWI (GeVS/Suwinet)[1]. 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).

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: het BKWI.

Uit het onderzoek blijkt dat het UWV de Wbp overtreedt.

- Ten aanzien van het aansluiten van niet-Suwipartijen op Suwinet werkt het UWV op meerdere punten (uitwerking Wbp-vereisten, rollen en autorisaties, ondertekening overeenkomst beheerder GeVS) niet volgens het aansluitprotocol uit bijlage III van de Regeling SUWI. Dit betekent dat op deze punten artikel 6 Wbp wordt overtreden.

- Voorts voldoet het UWV op verschillende punten (toekennen en controle autorisaties, beveiligingsplan, incidentenbeheer, controle gebruik) niet aan de vereisten uit bijlage I van de Regeling SUWI en het in de Verantwoordingsrichtlijn opgenomen Normenkader GeVS, waardoor artikel 13 Wbp wordt overtreden.

- Tot slot overtreedt het UWV artikel 6 Wbp bij het verlenen van toegang voor het *Department of Social Protection* van Ierland, door het ontbreken van een geldige overeenkomst als bedoeld in artikel 5.23 Regeling SUWI. Ten aanzien van de beveiliging gebruik Suwinet (toegang zonder filters, controle gebruik) door het *Department of Social Protection* van Ierland overtreedt het UWV artikel 13 Wbp.

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

1 INLEIDING

1.1 Achtergrond en aanleiding onderzoek

Sinds 2002 wisselen diverse overheidsorganisaties (persoons)gegevens van burgers uit in het domein Werk en Inkomen op basis van de Wet SUWI. Dit vindt plaats door middel van Suwinet. Suwinet is een besloten netwerk dat wordt ondersteund, beheerd en verder (technisch) ontwikkeld door het BKWI, formeel onderdeel van het UWV. Suwinet beschikt over diverse applicaties (bijvoorbeeld Suwinet Inkijk en Suwinet-Inlezen) die toegang geven tot (persoons)gegevens van burgers via Suwinet. 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 het BKWI. Zoals in artikel 60 lid 2 Wbp is bepaald, is het UWV (als Wbp verantwoordelijke) in de gelegenheid gesteld zijn zienswijze te geven op de voorlopige bevindingen. Het CBP heeft de reactie van het UWV bij brief van 2 september 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 bij het BKWI. Het onderzoek is gericht op het controleren van de naleving van de door de Wbp en SUWI wet- en regelgeving gestelde vereisten.

Hierbij zijn de volgende onderzoeksvragen leidend geweest:

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

1. Hebben de door het CBP geselecteerde niet-Suwipartijen die gegevens verwerken afkomstig van Suwinet daarvoor een overeenkomst als bedoeld in artikel 5.23, eerste lid, van het Besluit SUWI ondertekend?
2. Welke concrete afspraken zijn gemaakt met betrekking tot de naleving van de Wbp?
3. Worden vereisten met betrekking tot toegang tot en beveiliging van Suwinet (bijvoorbeeld toekenning en beheer van autorisaties tot Suwinet, beveiligingsplan Suwinet, logging gebruik Suwinet en beveiligingsincidenten) door deze partijen nageleefd?

Bij brief van 5 juli 2013 heeft het CBP bij het BKWI het onderzoek aangekondigd en de relevante schriftelijke stukken opgevraagd (o.a. modelovereenkomst), alsmede een lijst van niet-Suwipartijen die in de periode tussen 1 januari 2011 en 1 mei 2013 toegang tot Suwinet hebben gekregen. Het CBP heeft bij brief van 10 oktober 2013 een aantal overeenkomsten van geselecteerde niet-Suwipartijen opgevraagd, en heeft deze op 28 oktober 2013 bij brief van het BKWI ontvangen.
Op 25 februari 2014 heeft een onderzoek ter plaatse bij het BKWI te Utrecht plaatsgevonden, waarbij het CBP interviews heeft gehouden met diverse medewerkers van het BKWI en kennis heeft genomen van de werking van Suwinet. Daarnaast heeft het CBP ter plaatse de relevante documentatie (o.a. selectie logbestanden en *print screens* Suwinet) van het BKWI opgevraagd. Een groot deel van deze documentatie heeft het BKWI later, te weten op 28 februari 2014 en 3, 4 en 6 maart 2014 per e-mailbericht aan het CBP opgestuurd. Een ander deel van deze documentatie is door een BKWI medewerker op 3 maart 2014 ten kantore van het CBP overgelegd.

Het CBP heeft op 15 juli 2014 het Rapport voorlopige bevindingen vastgesteld.
Het CBP heeft het UWV 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 het UWV vertrouwelijke (bedrijfs)gegevens bevatten. Het UWV heeft bij brief van 14 augustus 2014 verzocht om uitstel van de termijn voor het geven van een zienswijze tot en met 2 september 2014. Het CBP heeft per brief van 19 augustus 2014 uitstel verleend tot en met 2 september 2014. Het UWV heeft zijn zienswijze, alsmede een reactie op de (bedrijfs) vertrouwelijkheidstoets, op 2 september 2014 schriftelijk ingebracht.

1.3 Wettelijk kader

De bevindingen van dit onderzoek zijn getoetst aan het volgende wettelijk kader:
- Artikel 6 Wbp
- Artikel 13 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)
- De Verantwoordingsrichtlijn GeVS en het daarin opgenomen Normenkader GeVS

2 ORGANISATIE UWV/ BKWI

Op grond van de wet SUWI heeft het UWV een wettelijke taak om werknemersverzekeringen landelijk uit te voeren, en te zorgen voor re-integratie van uitkeringsgerechtigden richting arbeidsmarkt. Het UWV verwerkt persoonsgegevens als houder van de polisadministratie, waarin informatie over loon, uitkeringen en arbeidscontracten van alle verzekerde werknemers in Nederland zijn opgenomen. Hieronder vallen de gegevens over arbeidscontracten tussen werknemers en werkgevers, maar ook lijfrentes en pensioenen. In deze context van Suwinet is het UWV bronhouder.

Het verlenen van toegang tot Suwinet wordt gerealiseerd door een zelfstandig en herkenbaar organisatieonderdeel van het UWV[3]: het BKWI. Het BKWI is verantwoordelijk voor het technisch en functioneel beheer van Suwinet. Het BKWI heeft de wettelijke taak om de beheerstaken uit te voeren ten aanzien van de inrichting van een centrale elektronische voorziening (Suwinet); de inrichting van een gemeenschappelijke faciliteit voor de toegangsbeveiliging; de ondersteuning van de gebruikers bij het beheer en gebruik van de centrale elektronische voorzieningen[4]. Het BKWI ontwikkelt samen met de Suwipartijen de standaarden voor het gegevensverkeer. Dit zijn afspraken tussen de Suwipartijen over de kwaliteit van Suwinet, het beveiligingsniveau, het ontwerp van Suwinet en de gegevensdefinities.

Indien Suwipartijen persoonsgegevens willen leveren aan niet-Suwipartijen dient het aansluitprotocol GeVS te worden gevolgd. In het aansluitprotocol GeVS wordt aangegeven dat indien een niet-Suwipartij van Suwinet gebruik wil maken, een formeel verzoek daartoe moet worden ingediend door de niet-Suwipartij bij het BKWI. Een dergelijk verzoek kan ook afkomstig zijn van een of meerdere Suwipartijen, die wensen dat een niet-Suwipartij aansluit als afnemer. Hierop wordt de technische invulling en de gegevensvulling van de beoogde aansluiting c.q. ontsluiting gebaseerd. Tot slot wordt op basis hiervan de inhoud van de te sluiten overeenkomst bepaald.

2.1 Verantwoordelijke

Omdat het BKWI onderdeel is van het UWV is het UWV de verantwoordelijke in de zin van artikel 1, onder d, Wbp voor gegevensverwerkingen door het BKWI als beheerder van Suwinet. Het UWV is tevens als bronhouder verantwoordelijke in de zin van artikel 1, onder d, Wbp voor gegevensverwerkingen die het BKWI uitvoert.

3 BEVINDINGEN ONDERZOEK

3.1 Overeenkomsten inzake toegang Suwinet door niet-Suwipartijen

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

[3] Artikel 5.21 Besluit SUWI.

[4] Idem.

opgenomen protocol – het zogenaamde aansluitprotocol– bevat nadere regels ten aanzien van de overeenkomst. De overeenkomst wordt gesloten tussen de contractpartijen, zijnde de betrokken verantwoordelijken (bronhouders) en de aanvrager (niet-Suwipartij), alsook de beheerder van de GeVS (het BKWI) . Volgens het 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.

3.1.2 Bevindingen

Het CBP heeft een overzicht van alle niet-Suwipartijen bij het BKWI opgevraagd die in de periode tussen 1 januari 2011 en 1 juni 2013 toegang tot persoonsgegevens via Suwinet hebben gekregen en na 1 juni 2013 nog steeds op Suwinet waren aangesloten. In het vervolg heeft het CBP een steekproef van tien niet-Suwipartijen geselecteerd en de overeenkomsten, als bedoeld in bijlage III Regeling SUWI, tussen niet-Suwipartijen en het UWV, van deze partijen opgevraagd. Bij de geselecteerde niet-Suwipartijen bevond zich één buitenlandse partij: *Department of Social Protection* van Ierland.

De in deze paragraaf beschreven bevindingen hebben betrekking op de overeenkomsten die gesloten zijn met de nationale niet-Suwipartijen. De bevindingen met betrekking tot *Department of Social Protection* van Ierland zijn apart weergegeven (zie paragraaf 3.4).

De door het CBP ontvangen overeenkomsten zijn ondertekend door twee partijen: het UWV (als bronhouder) en de desbetreffende niet-Suwipartij (aanvrager). Het BKWI heeft als beheerder van Suwinet geen van de tien gecontroleerde overeenkomsten ondertekend.
In de overeenkomsten staat niet vermeld op welke wijze de Wbp-vereisten met betrekking tot bewaartermijnen (artikel 10 Wbp), 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.
Tijdens het onderzoek ter plaatse, hebben de geïnterviewde BKWI medewerkers toegelicht dat rollen en autorisaties, vooraf en buiten de overeenkomst om, met het BKWI worden afgestemd en besproken. De afspraken over rollen en autorisaties worden niet in een document vastgelegd.

3.1.3 Beoordeling

In de vermelde overeenkomsten wordt niet aangegeven op welke wijze de vereisten uit de artikelen 10, 11 en 34 Wbp worden nageleefd en de overeenkomsten zijn niet ondertekend door de beheerder van de GeVS (het BKWI). De benodigde rollen en autorisaties worden evenmin in de overeenkomst als bedoeld in artikel 5.23, eerste lid, van het Besluit SUWI geregeld. Voormelde is niet conform het aansluitprotocol, zoals opgenomen in bijlage III van de Regeling SUWI, hetgeen betekent dat de verwerkingen van persoonsgegevens, die op basis van deze overeenkomsten plaatsvinden, in strijd zijn met artikel 6 Wbp.

3.2 Toekenning van autorisaties

3.2.1 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.
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.

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. De verantwoordingsrichtlijn 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.

3.2.2 Bevindingen

De werkwijze zoals hieronder beschreven is ontleend aan de informatie die de BKWI medewerkers mondeling tijdens het onderzoek ter plaatse hebben verstrekt.

Het BKWI autoriseert een niet-Suwipartij op verzoek van de leverende Suwipartij. De leverende Suwipartij geeft de opdracht tot de autorisatie. Het BKWI maakt ook afspraken met de aan te sluiten niet-Suwipartijen over autorisaties. De benodigde rollen en autorisaties worden buiten de overeenkomst als bedoeld in bijlage III van de Regeling SUWI om geregeld.

Per afnemende niet-Suwipartij ontwikkelt het BKWI verschillende autorisatierollen, afhankelijk van het type van organisatie. Het BKWI en de aangesloten niet-Suwipartij zijn verantwoordelijk voor de feitelijke toekenning (daadwerkelijke uitvoering) en het operationeel beheer van de autorisaties tot Suwinet. Nadat de hoofdgebruiker (administrator) door het BKWI is geautoriseerd, worden alle individuele accounts op medewerker niveau bij en door de niet-Suwipartij zelf verdeeld. De administrator autoriseert andere medewerkers in de eigen organisatie en bepaalt de rollen op basis van hun functie. Het BKWI maakt de toegang tot het systeem technisch mogelijk.

Het BKWI heeft geen formeel vastgestelde en gedocumenteerde procedure met betrekking tot de werkwijze toekenning autorisaties aan Suwinet gebruikers aan het

CBP overgelegd. Het BKWI heeft op een later moment (een aantal dagen na het CBP onderzoek ter plaatse) een werknotitie getiteld 'Nieuwe gebruikersbeheerder Suwinet-Inkijk autoriseren' aan het CBP gemaild. Deze notitie is geschreven in een conceptvorm, en bevat geen datum en geen auteur.

3.2.3 Beoordeling

Het BKWI heeft geen formeel vastgestelde en gedocumenteerde procedure met betrekking tot het toekennen van autorisaties. Om deze reden voldoet de handelwijze van het BKWI op dit punt niet aan norm 13.1 uit het Normenkader GeVS. Omdat het Normenkader GeVS kan worden beschouwd als een wettelijke uitwerking van het beveiligingsvoorschrift uit artikel 13 Wbp, betekent dit een overtreding van artikel 13 Wbp door het UWV.

3.3 Geselecteerde beveiligingsaspecten van Suwinet

3.3.1 Norm beveiligingsplan, controle gebruik Suwinet en beveiligingsincidenten

Artikel 13 Wbp schetst het algemeen beveiligingsvoorschrift. Op grond van het onder paragraaf 3.2.1 geschetste normenkader kunnen Bijlage I van de Regeling SUWI en het in de Verantwoordingsrichtlijn opgenomen Normenkader GeVS worden beschouwd als uitwerkingen van artikel 13 Wbp.

De volgende normen zijn thans van belang:

A. Beveiligingsplan

Volgens het Normenkader GeVS dient voor de Suwi omgeving een Suwinet beveiligingsplan te zijn 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 worden jaarlijks geëvalueerd en indien nodig geactualiseerd (norm 1.5).

B. Incidentenbeheer

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. 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 Suwipartij 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).

C. Controle gebruik Suwinet: logging en gebruikersrapportages

Het realiseren van logische toegangsbeveiliging geschiedt volgens bijlage I van de Regeling SUWI mede door middel van logging. Het BKWI faciliteert het invoeren van autorisaties voor afgesproken rollen en houdt een logging bij van de geautoriseerde inkijk op gegevens van de diverse bestandseigenaren bij diverse ontvangende partijen (wie raadpleegt wanneer welke gegevenssoorten). Log-informatie wordt door beheerder van de centrale voorziening maandelijks geanonimiseerd beschikbaar gesteld aan de leverende en ontvangende partijen die het betreft. Partijen kunnen zo detecteren of er sprake is van oneigenlijk gebruik. Als dat zo blijkt te zijn kan meer specifieke en niet anonieme informatie worden verstrekt door de beheerder van de

centrale voorziening. De beheerder van de centrale voorziening neemt passende maatregelen bij geconstateerde beveiligingsinbreuken of misbruik van de GeVS.

3.3.2 Bevindingen

A. Beveiligingsplan

Er bestaat geen integraal beveiligingsplan met betrekking tot Suwinet en de SUWI-keten. Elke aan Suwinet deelnemende partij is zelf verantwoordelijk voor een eigen beveiligingsplan.
Het BKWI beschikt over een eigen beveiligingsplan. Deze heeft echter geen betrekking op Suwinet maar op de eigen interne werkprocessen. Processen die invulling geven aan de wettelijke taken die het BKWI uitvoert ten behoeve van de Suwiketen vallen hier buiten. Het toegezonden meest recente document getiteld 'Baseline beveiliging' van 2012, betreft een conceptversie. De laatste vastgestelde definitieve versie van het 'Beveiligingsbeleid BKWI' is van september 2011. In de genoemde documenten wordt verwezen naar de Code voor Informatiebeveiliging uit 2005. Het beveiligingsplan is voor het laatst in 2011 geëvalueerd. Daarna is er geen aantoonbare evaluatie meer geweest.

B. Beveiligingsincidenten

Het BKWI hanteert een generieke definitie van beveiligingsincidenten. Tijdens het onderzoek ter plaatse wordt desgevraagd mondeling een definitie gegeven: een vermoeden van inbreuk op privacy of beveiliging. Wat er precies als een beveiligingsincident in de context van Suwinet wordt gezien, is niet duidelijk omschreven.

Het BKWI beschikt over een ICT incidentenprocedure. Er is geen afzonderlijk systeem specifiek gericht op de registratie van beveiligingsincidenten. Beveiligingsincidenten staan samen met andere typen ICT incidenten geregistreerd in het ticketsysteem, waarin aan elk incident een eigen registratienummer (ticket) wordt toegekend.
Het label 'beveiligingsincident' wordt 'handmatig' toegekend op basis van de specifieke kenmerken van de zaak. Over beveiligingsincidenten wordt slechts verder gecommuniceerd wanneer deze incidenten relevant zijn voor de hele keten.

Op verzoek van het CBP heeft het BKWI een lijst uitgedraaid van alle beveiligingsincidenten die in 2013 in het ticketsysteem zijn geregistreerd. Periodieke overzichten van beveiligingsincidenten worden niet gemaakt. Er wordt niet gecategoriseerd naar het type beveiligingsprobleem dat plaats heeft gevonden. Het BKWI kan niet globaal noemen welke (hoofd)typen beveiligingsincidenten met betrekking tot Suwinet zich in het verleden hebben voorgedaan. Het BKWI meldt dat elk incident anders is en dat er individueel naar de oplossing wordt gezocht.

C. Controle gebruik Suwinet: logging en gebruikersrapportages

Niet –Suwipartijen kunnen gebruik maken van verschillende applicaties om persoonsgegevens via Suwinet te raadplegen. In dit onderzoek zijn twee applicaties van belang: Suwinet-Inkijk en Suwinet-Inlezen.

Bij Suwinet-Inkijk wordt de gegevensset in de centrale applicatie getoond. De applicatie Suwinet-Inkijk biedt overheidsorganisaties de mogelijkheid om persoonsgegevens te raadplegen in één centrale web applicatie, waardoor de raadplegingen ook door het BKWI gelogd kunnen worden. Bij raadplegingen door

middel van Suwinet-Inkijk wordt elke invoering/opvraging gelogd. Hierbij wordt onder meer accountnaam, naam gebruiker, URL (pagina) en zoeksleutel (BSN, kenteken, etc.) gelogd. Het BKWI rapporteert alleen over gebruik of de raadplegingen. Het BKWI maakt van deze gelogde gegevens gebruiksrapportages. Er zijn enerzijds generieke rapportages, die maandelijks worden opgesteld en toegestuurd aan de afnemende partij, anderzijds specifieke rapportages die op aanvraag worden opgesteld. Doel van de rapportages is volgens het BKWI het signaleren van afwijkend gedrag. Het BKWI heeft aangegeven dat het niet op eigen initiatief specifieke rapportages over bepaalde organisaties mag opstellen. Het BKWI kan slechts tips dan wel advies over het gebruik geven. Naar aanleiding van bepaalde signalen dient de afnemende partij zelf actie te ondernemen.

Partijen die gebruik maken van Suwinet-Inlezen, lezen de gegevens direct in de eigen bedrijfsapplicatie, waardoor de persoonsgegevens ook direct ingevuld kunnen worden op elektronische aanvraagformulieren. Hierdoor kunnen de persoonsgegevens ook lokaal in het eigen systeem worden bewaard of opgeslagen[5].

Er is met betrekking tot het loggen van het gebruik van Suwinet een verschil tussen Suwinet-Inkijk en Suwinet-Inlezen. Raadplegingen door middel van Suwinet-Inlezen worden niet centraal door het BKWI gelogd. Het BKWI heeft alleen zicht op het berichtenverkeer, niet op de inhoud. Suwinet-Inlezen wordt derhalve niet gelogd door het BKWI (slechts het aantal verstuurde berichten wordt geregistreerd, alleen het BSN is zichtbaar in de titel, inhoud van de berichten is niet zichtbaar voor het BKWI) en over het gebruik worden geen rapportages opgesteld.

3.3.3 Beoordeling

A. Beveiligingsplan

Het BKWI heeft geen beveiligingsplan dat specifiek voor de uitvoering van wettelijke taken is opgesteld. Hiermee handelt het BKWI in strijd met 1.2 uit het Normenkader GeVS. Doordat het BKWI het beveiligingsbeleid niet jaarlijks heeft geëvalueerd en geactualiseerd, handelt het tevens in strijd met norm 1.5 uit het Normenkader GeVS. Het niet naleven van de normen 1.2 en 1.5 van het Normenkader GeVS maakt dat tevens artikel 13 Wbp wordt overtreden.

B. Beveiligingsincidenten

Het Normenkader GeVS vereist dat incidenten centraal vastgelegd, gerapporteerd, geanalyseerd, gekwantificeerd en afgewikkeld worden 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). Partijen dienen een procedure te hanteren voor het analyseren en het trekken van lering uit incidenten en zorgen ervoor dat het beleid en maatregelen overeenkomstig wordt aangepast (norm 9.1). Van al het vorenstaande is bij het BKWI geen sprake.
Het BKWI handelt hiermee in strijd met voormelde normen. Dit betekent tevens een overtreding van artikel 13 Wbp.

C. Controle gebruik Suwinet: logging en gebruikersrapportages

[5] Veilig gebruik Suwinet 2013, *Een onderzoek naar de beveiliging van gegevens die worden uitgewisseld binnen het Suwinet door gemeenten*, Inspectie SZW, Ministerie van Sociale Zaken en Werkgelegenheid, 26 augustus 2013, pagina 10.

Bij raadplegingen door middel van Suwinet-Inkijk wordt elke invoering/opvraging gelogd. Het BKWI rapporteert over de raadplegingen. Het BKWI maakt van deze gelogde gegevens gebruiksrapportages. Op dit punt wordt derhalve conform bijlage I van de Regeling SUWI gehandeld.

Het is voor het BKWI niet mogelijk om de raadplegingen via de applicatie Suwinet-Inlezen adequaat te loggen, waardoor ook geen gebruiksrapportages kunnen worden opgesteld. Doordat raadplegingen via Suwinet-Inlezen niet (goed) worden gelogd en hiervan geen gebruiksrapportages kunnen worden opgesteld, vindt de (logische) toegangsbeveiliging niet conform bijlage I van de Regeling SUWI plaats. Dit betekent dat op dit punt artikel 13 Wbp wordt overtreden.

3.4 Bevindingen onderzoek *Department of Social Protection*, Ierland

Het *Department of Social Protection* van Ierland is een buitenlandse niet-Suwipartij die sinds maart 2013 toegang heeft tot persoonsgegevens via Suwinet via Suwinet-International die qua werking met Suwinet-Inkijk vergelijkbaar is.

In het kader van het onderzoek heeft het CBP de overeenkomst gecontroleerd die het UWV, met het *Department of Social Protection* van Ierland heeft gesloten. Het UWV is hierbij als bronhouder verantwoordelijk voor de verwerking van persoonsgegevens. Tijdens het onderzoek ter plaatse bij het BKWI heeft het CBP (aanvullende) vragen gesteld met betrekking tot de genoemde overeenkomst, de toegang tot Suwinet, de verleende autorisaties en de controle van het Suwinet gebruik. Daarnaast heeft het BKWI laten zien hoe Suwinet-International werkt en welk type gegevens het *Department of Social Protection* van Ierland via Suwinet kan raadplegen.

3.4.1 Norm

Artikel 6 Wbp bepaalt dat persoonsgegevens in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt moeten worden. Bij de beoordeling of persoonsgegevens conform de wet worden verwerkt, is het in bijlage III van de Regeling SUWI opgenomen aansluitprotocol van belang. Bij de aansluiting van zogenaamde niet-Suwipartijen dient dit protocol te worden gevolgd. 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 is besproken in paragraaf 3.2.1 van dit rapport. Voor de beoordeling van de controle van het gebruik van persoonsgegevens door middel van Suwinet is bijlage I van de Regeling SUWI van toepassing (zie paragraaf 3.3.1, onder C).

3.4.2 Bevindingen

A. Overeenkomst

Het *Department of Social Protection* van Ierland heeft sinds 20 maart 2013 (feitelijk) toegang tot Suwinet. De aan het CBP toegestuurde overeenkomst heeft betrekking op de periode van 1 september 2012 – 1 maart 2013. De overeenkomst is opgesteld in het Engels en is qua opzet en inhoud vergelijkbaar met de overeenkomsten die het UWV met nationale niet-Suwipartijen sluit. In de overeenkomst wordt niet aangegeven op welke wijze de Wbp vereisten met betrekking tot bewaartermijnen (artikel 10 Wbp),

bovenmatigheid (artikel 11Wbp) en informatieplicht (artikel 34 Wbp) worden ingevuld. De overeenkomst bevat geen passage over de benodigde rollen en de wijze waarop de toegekende autorisaties worden toegekend en beheerd.

Een recente versie van deze overeenkomst, met geldigheid vanaf 20 maart 2013 is niet aanwezig. Het BKWI heeft aan het CBP per e-mailbericht (3 maart 2014) laten weten dat het UWV er 'in overleg met Ierland' voor heeft gekozen om het contract stilzwijgend te verlengen. Het betreft een pilot, maar de pilotperiode is niet nader omschreven (het einde van de pilot staat niet vast).

B. Toegang tot persoonsgegevens via Suwinet
Via Suwinet kan het *Department of Social Protection* van Ierland nagaan of een persoon een uitkerings- of arbeidsrelatie heeft (gehad) met Nederland[6].
Binnen het *Department of Social Protection* van Ierland zijn drie medewerkers geautoriseerd tot Suwinet. Het autorisatieproces is op dezelfde wijze ingericht als bij de nationale niet-Suwipartijen: het BKWI heeft een hoofdgebruiker (administrator) geautoriseerd, en deze heeft vervolgens op lokaal niveau autorisaties verleend.

Door het aanbrengen van de selectiecriteria (filters) kan de toegankelijke dataset worden begrensd, zodat bepaalde categorieën van persoonsgegevens worden weggelaten, bijvoorbeeld door alleen persoonsgegevens in een bepaalde regio toegankelijk te maken of slechts persoonsgegevens beschikbaar te stellen van een bepaalde leeftijdsgroep of nationaliteit. Het toepassen van selectiecriteria zorgt er voor dat alleen de relevante informatie wordt aangeboden.
Het *Department of Social Protection* van Ierland heeft toegang tot de gegevens van alle personen die bij het UWV in de polisadministratie geregistreerd staan. Uit Suwinet-International – het systeem waar Ierland gebruik van maakt – bleken ten tijde van het onderzoek ter plaatse (ook) de persoonsgegevens van niet-Ierse onderdanen opvraagbaar.
Het BKWI heeft desgevraagd aangegeven dat er geen filters worden toegepast, hoewel dat technisch mogelijk is. Die wens is aan het BKWI door de bronhouder niet voorgelegd.

C. Beveiliging: controle gebruik Suwinet
Het BKWI logt het gebruik van Suwinet door het *Department of Social Protection* van Ierland. Er zijn echter geen generieke en specifieke rapportages over het gebruik van Suwinet door de Ierse partij beschikbaar.

3.4.3 Beoordeling
A. Overeenkomst
Gelet op het feit dat het *Department of Social Protection* van Ierland pas toegang heeft gekregen na het verstrijken van de looptijd van de overeenkomst, concludeert het CBP dat de verstrekking niet heeft plaatsgevonden op basis van een geldige overeenkomst als bedoeld in bijlage III van de Regeling SUWI. Het UWV en het *Department of Social Protection* van Ierland handelen hiermee in strijd met bijlage III van de Regeling SUWI. Hiermee overtreedt het UWV ook artikel 6 Wbp.

[6] http://www.bkwi.nl/nieuws/item/eerste-mijlpaal-onderlinge-gegevensuitwisseling-europese-uitkeringsinstanties-bereikt/

B. Beveiliging: toegang gegevens alle personen Suwinet
Niet is aangetoond dat het ter beschikking stellen van persoonsgegevens van alle geregistreerde personen noodzakelijk is, gelet op het doeleinde van de gegevensverwerking (de bepaling en vaststelling van uitkeringen bij werkloosheid). Het aantal uitkeringsaanvragen waarbij persoonsgegevens afkomstig van het UWV moeten worden geverifieerd voor deze doeleinden, rechtvaardigt niet dat de persoonsgegevens van alle personen die in de polisadministratie geregistreerd zijn, beschikbaar worden gesteld voor het *Department of Social Protection* van Ierland.

Verwacht mag worden dat de toegang beperkt is tot personen die aanspraak kunnen maken op bepaalde voorzieningen (uitkeringen) die worden uitgevoerd door de Ierse overheid ofwel die bepaalde verplichtingen (premies) moeten nakomen jegens de Ierse overheid.

Het niet toepassen van selectiecriteria (filters) heeft tot gevolg dat de Ierse overheid in beginsel toegang heeft tot (veel) meer persoonsgegevens dan noodzakelijk is voor de uitvoering van haar wettelijke taak. Een systeem mag niet meer informatie geven dan strikt noodzakelijk is voor het doel. Het UWV heeft geen dan wel onvoldoende maatregelen getroffen om onnodige verzameling van persoonsgegevens als bedoeld in artikel 13 Wbp te voorkomen. Derhalve is niet voldaan aan de in dat artikel gestelde vereisten.

C. Beveiliging: logging en gebruiksrapportages
De raadplegingen door het *Departement of Social Protection* van Ierland worden gelogd, maar er worden geen gebruiksrapportages opgesteld door het BKWI. Het UWV handelt hiermee in strijd met bijlage I van de Regeling SUWI en daarmee ook met artikel 13 Wbp.

4 CONCLUSIES

Uit het onderzoek blijkt dat het UWV de Wbp overtreedt.

- Ten aanzien van het aansluiten van niet-Suwipartijen op Suwinet werkt het UWV op meerdere punten (uitwerking Wbp-vereisten, rollen en autorisaties, ondertekening overeenkomst beheerder GeVS) niet volgens het aansluitprotocol uit bijlage III van de Regeling SUWI. Dit betekent dat op deze punten artikel 6 Wbp wordt overtreden.

- Voorts voldoet het UWV op verschillende punten (toekennen en controle autorisaties, beveiligingsplan, incidentenbeheer, controle gebruik) niet aan de vereisten uit bijlage I van de Regeling SUWI en het in de Verantwoordingsrichtlijn opgenomen Normenkader GeVS, waardoor artikel 13 Wbp wordt overtreden.

- Tot slot overtreedt het UWV artikel 6 Wbp bij het verlenen van toegang voor het *Department of Social Protection* van Ierland, door het ontbreken van een geldige overeenkomst als bedoeld in artikel 5.23 Regeling SUWI. Ten aanzien van de beveiliging gebruik Suwinet (toegang zonder filters, controle gebruik) door het *Department of Social Protection* van Ierland overtreedt het UWV 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 UWV

De zienswijze van het UWV bestaat uit twee delen. Het eerste deel van de zienswijze bevat een beschrijving van de wijze waarop het UWV met het BKWI invulling geeft aan het Aansluitprotocol, de verantwoordelijkheid als bronhouder en de verantwoordelijkheid van de beheerder van Suwinet inzake de aansluiting op Suwinet. Het tweede deel bevat de reactie op de voorlopige bevindingen van het CBP-onderzoek. Deze bijlage bevat de onderdelen van de zienswijze die volgens het CBP relevant zijn voor het onderzoek.

1. De verschillende verantwoordelijkheden met betrekking tot het aansluitprotocol Suwinet

Het UWV maakt in zijn zienswijze ten aanzien van de verantwoordelijkheid onderscheid tussen drie verschillende partijen: de bronhouder, de beheerder van Suwinet en de afnemer van gegevens via Suwinet.

- Verantwoordelijkheid bronhouder

De Suwipartij als bronhouder en de niet-Suwipartij als afnemer zijn verantwoordelijk voor de totstandkoming van de overeenkomst bedoeld in het Besluit SUWI. De bronhouder toetst het verzoek op de aanwezigheid van een wettelijke grondslag voor de gegevenslevering. Zonder wettelijke grondslag voor de gevraagde levering van gegevens sluiten bronhouder en afnemer geen overeenkomst en levert de bronhouder geen gegevens.
Bij aanwezigheid van een wettelijke grondslag toetst het UWV als bronhouder de gevraagde gegevens op doelbinding, proportionaliteit en subsidiariteit. UWV stelt als bronhouder de set van gegevens vast en legt die vast in een bijlage van de overeenkomst.

- Verantwoordelijkheid beheerder Suwinet

In geval de niet-Suwipartij voor de levering van gegevens gebruik wil maken van Suwinet, dan dient hij daartoe een verzoek in bij UWV als beheerder van Suwinet. In opdracht van UWV als bronhouder en in opdracht van UWV als beheerder levert BKWI vervolgens ondersteuning aan de niet- Suwipartij bij het vaststellen van de rollen en de benodigde autorisaties en start BKWI met de voorbereiding van de technische aansluiting op Suwinet. De afspraken hierover worden vastgelegd in een SLA (Service Level Agreement, toevoeging CBP) tussen UWV, BKWI enerzijds en de afnemer anderzijds.
Nadat de regeling met de wettelijke grondslag in werking is getreden en de overeenkomst is ondertekend, zorgt BKWI, in opdracht van de bronhouder voor de daadwerkelijke aansluiting (de autorisatie) van de gebruikersbeheerder van de afnemer. BKWI is, in opdracht van de bronhouder, verwerker van de gegevens van de bronhouder en transporteert de gegevens naar de afnemer.

- Verantwoordelijkheid afnemer

Door de autorisatie (de aansluiting, toevoeging CBP) krijgt (de gebruikersbeheerder van) de afnemer toegang tot Suwinet en daarmee tot de overeengekomen en vastgelegde gegevens van UWV als bronhouder. De afnemer is verantwoordelijk en draagt zorg voor het toekennen van de autorisaties binnen zijn organisatie, het beheer van de autorisaties en de controle daarop. De gebruikersbeheerder van de afnemer

autoriseert -op instructie en onder verantwoordelijkheid van de afnemer- de individuele medewerkers en verschaft hun feitelijk toegang tot de gegevens op basis van de voor hun functie vastgestelde rol. De gebruikersbeheerder is derhalve degene die namens de afnemer de autorisaties voor Suwinet beheert (laatste zin toegevoegd door het CBP).
Voor het bepalen van de verantwoordelijkheid in de zin van de Wbp is volgens het UWV het onderscheid van de bronhouder voor de levering van gegevens, de verantwoordelijkheid van de beheerder van Suwinet inzake de aansluiting op Suwinet en de verantwoordelijkheid van de niet-Suwipartijen als afnemer en gebruiker van de gegevens van de bronhouder, van belang.
Het UWV deelt de opvatting van het CBP, dat het UWV verantwoordelijke is in de zin van de Wbp voor de gegevensverwerkingen die het UWV in het kader van zijn wettelijke taken uitvoert als bronhouder.

Naast verantwoordelijke voor de gegevensverwerkingen als bronhouder is het UWV ingevolge het Besluit SUWI verantwoordelijk voor de inrichting en het beheer van Suwinet. Het feitelijk beheer van Suwinet ligt bij BKWI, een apart organisatieonderdeel van het UWV. BKWI zorgt in opdracht van de bronhouder voor de technische aansluiting van afnemers op de voorziening Suwinet en voor het beheer van het systeem. Suwinet wordt gebruikt voor het transport van meerdere bronhouders naar meerdere afnemers. Het UWV stelt dat het BKWI gegevens verwerkt (transporteert) onder verantwoordelijkheid van de afzonderlijke bronhouders die daartoe een uitdrukkelijke opdracht geven aan het BKWI. Het is volgens het UWV de afzonderlijke bronhouder, die in de zin van de Wbp verantwoordelijke is en blijft voor de gegevensverwerkingen via Suwinet. Het UWV gaat graag met het CBP in gesprek over de opmerking in het rapport dat het UWV de verantwoordelijke is in de zin van artikel 1, onder d, Wbp, voor alle gegevensverwerkingen door het BKWI.

Reactie CBP

Het CBP-onderzoek is primair gericht op het beheer van Suwinet. De beheerder van Suwinet, zijnde het BKWI, is vanuit zijn rol verantwoordelijk voor het technisch en functioneel beheer van Suwinet, waaronder de gemeenschappelijke faciliteit voor toegangsbeveiliging van Suwinet[7]. Nu het BKWI onderdeel is van het UWV, wordt het UWV in dit verband conform artikel 1, onder d, Wbp aangemerkt als verantwoordelijke voor gegevensverwerkingen door het BKWI als beheerder van Suwinet. Aan de passage in de bevindingen met betrekking tot de verantwoordelijke is toegevoegd dat het UWV wordt aangemerkt als verantwoordelijke voor gegevensverwerkingen door het BKWI als beheerder van Suwinet.

2. Reactie UWV op voorlopige bevindingen

De reactie van het UWV gaat in op de volgende punten:

- De overeenkomsten met nationale niet- Suwipartijen
- De toekenning van autorisaties
- De door het CBP geselecteerde beveiligingsaspecten van Suwinet en
- De overeenkomst met de Department of Social Protection Ierland

Deze punten van de reactie van het UWV zullen hieronder afzonderlijk worden weergegeven.

[7] Artikel 5.21., Besluit Suwi (inrichting en beheer).

2.1 Overeenkomsten met nationale niet- Suwipartijen

Het UWV geeft in zijn zienswijze aan dat het CBP in zijn rapport van voorlopige bevindingen de overeenkomsten, die door het UWV als bronhouder zijn ondertekend, toetst aan de eisen van de Wbp en aan de voorschriften in het aansluitprotocol ter zake van de overeenkomst. Voorts constateert het CBP dat de overeenkomsten op de in het rapport genoemde punten niet voldoen aan de voorschriften van het aansluitprotocol, hetgeen in strijd is met artikel 6 Wbp. Naar aanleiding van deze punten heeft het UWV op een andere wijze invulling gegeven aan de van toepassing zijnde voorschriften, namelijk[8]:

- Ondertekening van de overeenkomst

De overeenkomst is niet, zoals volgens het UWV in het rapport is aangegeven, ondertekend door het BKWI als beheerder van Suwinet. Het UWV sluit als bronhouder een overeenkomst met de afnemer over de levering van gegevens. Het BKWI zorgt in opdracht van het UWV als bronhouder voor de technische realisatie van de gegevenslevering met inbegrip van de technische aansluiting op Suwinet. De afspraken tussen het UWV als bronhouder, BKWI als opdrachtnemer en de niet-Suwipartij als afnemer, over de technische realisatie van de levering (de uitvoering van de overeenkomst) worden en zijn vastgelegd in een aparte SLA.
Artikel 5 van de overeenkomst verwijst naar de toepasselijkheid van de Keten SLA, waarin de bepalingen staan omtrent de feitelijke levering. In de Keten SLA staat hoe bronhouder, afnemer en BKWI zich op operationeel niveau tot elkaar verhouden. De Keten SLA wordt jaarlijks ondertekend door de directeur van het BKWI.

- Bewaartermijnen

In de overeenkomst zelf wordt, zoals volgens het UWV in het rapport is aangegeven, geen invulling gegeven aan de bewaartermijnen. Afnemers van gegevens zijn wettelijk gehouden de voor afnemer geldende wettelijke bewaartermijnen te hanteren in geval de afnemer –na inkijk in de gegevens van de bronhouder- gegevens in de eigen administratie overneemt. Om die reden heeft het UWV in de Algemene Voorwaarden (bijlage bij de overeenkomst in artikel 16, derde lid) de verplichting voor afnemers opgenomen de gegevens slechts te bewaren voor zover dit noodzakelijk is voor het doel waarvoor de gegevens verkregen zijn.

- Bovenmatigheid

Voorafgaande aan elke toegang tot gegevens aan een niet- Suwipartij toetst het UWV in zijn verantwoordelijkheid van bronhouder de aanwezigheid van een wettelijke grondslag voor de gevraagde levering. Bij aanwezigheid van een wettelijke grondslag toetst het UWV vervolgens de gevraagde gegevens op doelbinding, subsidiariteit en proportionaliteit. De uitkomst van deze toetsing is een concrete set van gegevens, die als bijlage bij de overeenkomst is gevoegd en dus onderdeel uitmaakt van de overeenkomst. In geval een leveringsverzoek bovenmatig is, valt de juridische toets door het UWV negatief uit en komst –zonder aanpassing van het leveringsverzoek- geen overeenkomst tot stand.

[8] Het UWV geeft in de zienswijze aan dat het UWV graag met het CBP in gesprek gaat over de vraag of deze wijze van invulling past binnen de geldende voorschriften dan wel op onderdelen aanpassing behoeft.

- Informatieplicht

In de overeenkomst wordt, zoals volgens het UWV in het rapport is aangegeven, geen invulling gegeven aan de informatieplicht. De informatieplicht geldt volgens het UWV op grond van het vijfde lid van artikel 34 Wbp niet, in geval de gegevensuitwisseling zijn grondslag vindt in een wettelijke bepaling. Aangezien alle gegevensuitwisselingen via Suwinet plaatsvinden op basis van een wettelijke bepaling is in de overeenkomst geen bepaling opgenomen over informatieplicht.

- Benodigde rollen en wijze van toekenning, beheer en controle van autorisaties

De overeenkomst zelf bevat, zoals volgens het UWV in het rapport wordt aangegeven geen passage over de benodigde rollen en de wijze van toekenning, beheer en controle van autorisaties. Het auditreglement UVW Gegevensdiensten, dat onderdeel uitmaakt van de overeenkomst schrijft in punt IIB-2 aan de afnemer voor dat autorisaties tot applicaties dienen te worden toegekend aan geïdentificeerde en geautoriseerde gebruikers conform de autorisatieprofielen en autorisatieproces binnen de applicatie te kunnen garanderen.

Reactie CBP

Ter zake van de ondertekening van de overeenkomst staat in de Regeling SUWI aangegeven dat de overeenkomst wordt gesloten tussen de contractpartijen, zijnde de betrokken verantwoordelijken (bronhouders) en de aanvrager (niet-Suwipartij), alsook de beheerder van de GeVS (het BKWI). Het BKWI geeft als beheerder uitvoering aan de overeenkomst en is mede bepalend voor de wijze waarop de overeenkomst wordt uitgevoerd. Dit betekent dat ook de beheerder van Suwinet de overeenkomst dient te ondertekenen. Het CBP ziet geen aanleiding om de bevindingen op dit punt aan te passen.

Inzake de bewaartermijnen bepaalt artikel 10, eerste lid, Wbp dat persoonsgegevens niet langer mogen worden bewaard in een vorm die het mogelijk maakt de betrokkene te identificeren, dan noodzakelijk is voor de verwerkelijking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt. Het aansluitprotocol vereist dat in de overeenkomst wordt aangegeven op welke wijze dit vereiste wordt nageleefd. Met het opnemen van de verplichting voor afnemers de gegevens slechts te bewaren voor zover dit noodzakelijk is voor het doel waarvoor de gegevens verkregen zijn, wordt niet duidelijk op welke wijze artikel 10, eerste lid, Wbp wordt nageleefd. Dit betreft slechts een verkorte weergave van voornoemde bepaling. Indien wettelijke bewaartermijnen van toepassing zijn, dan dienen deze te worden opgenomen in de overeenkomst. Het CBP ziet op dit punt eveneens geen aanleiding de bevindingen te wijzigen.

Met betrekking tot de bovenmatigheid stelt het UWV dat het vooraf een toets uitvoert op doelbinding, subsidiariteit en proportionaliteit, waarmee eveneens een toets op bovenmatigheid plaatsvindt. Als een verzoek om gegevenslevering bovenmatig is, dan kan er geen overeenkomst tot stand komen. In de overeenkomst wordt echter niet aangegeven hoe wordt voldaan aan de vereiste uit artikel 11, eerste lid, Wbp. De hoeveelheid en het soort gegevens dat door het UWV wordt verstrekt moeten ter zake dienend zijn in relatie tot het doel waarvoor de gegevens worden verzameld. Ook mogen ze niet bovenmatig zijn. Partijen dienen in de overeenkomst op te nemen hoe zij aan deze verplichting voldoen. Op dit punt zullen de bevindingen niet worden aangepast.

Verder bepaalt artikel 34, vijfde lid, Wbp dat deze niet van toepassing is indien de vastlegging of de verstrekking bij of krachtens de wet is voorgeschreven. De gegevensverstrekking wordt echter niet wettelijk voorgeschreven als bedoeld in artikel 34, vijfde lid, Wbp. In dat geval zou er een wettelijke verplichting zijn om gegevens te verstrekken, en daar is geen sprake van. De bevindingen worden op dit punt dan ook niet aangepast.

Ter zake van de benodigde rollen en wijze van toekenning, beheer en controle van autorisaties is het CBP van oordeel dat voormeld punt IIB-2 onvoldoende helder is. In de overeenkomst of in één van de bijlagen van de overeenkomst dient nader geconcretiseerd te worden welke rollen en autorisaties benodigd zijn. Dit wordt voorgeschreven in het aansluitprotocol, zoals opgenomen in bijlage III van de Regeling SUWI. Het UWV dient hier nadere afspraken over te maken met de desbetreffende niet- Suwipartij. De bevindingen worden op dit punt evenmin aangepast.

2.2 De toekenning van autorisaties

Het UWV geeft in zijn zienswijze aan dat het CBP bijlage I van de regeling SUWI als de wettelijke uitwerking van artikel 13 Wbp ziet. Deze bijlage verwijst onder andere naar de gezamenlijke vaststelling van een Verantwoordingsrichtlijn en bijbehorend normenkader. Conform het bepaalde in norm 13.1 van het normenkader dient de Suwipartij de gebruikers van Suwinet te autoriseren en registreren op basis van een formele procedure. Zoals volgens het UWV in het rapport is aangegeven, beschikt BKWI niet over een vastgestelde en gedocumenteerde procedure met betrekking tot het toekennen van autorisaties.
Het UWV zal samen met het BKWI zorg dragen voor de vaststelling van een gedocumenteerde procedurebeschrijving met betrekking tot de autorisatie van de gebruikersbeheerder van de afnemer. De afnemer is volgens het UWV verantwoordelijk voor het toekennen en formeel vastleggen van autorisaties binnen zijn organisatie.

Reactie CBP

Het UWV erkent dat het BKWI niet over een vastgestelde en gedocumenteerde procedure met betrekking tot het toekennen van autorisaties beschikt. Het rapport zal op dit punt dan ook niet worden aangepast.

2.3 Geselecteerde beveiligingsaspecten van Suwinet

De reactie van het UWV ter zake van de beveiligingsaspecten is als volgt:

- Beveiligingsplan

Zoals volgens het UWV in het rapport is aangegeven, is het beveiligingsplan van het BKWI (als beheerder van Suwinet) niet actueel en voor het laatst in 2011 geëvalueerd. Het UWV zal samen met het BKWI zorgen voor een evaluatie en hernieuwde vaststelling in 2014. Het beveiligingsplan zal worden aangevuld ten aanzien van het gebruik van Suwinet door het BKWI voor de uitvoering van beheeractiviteiten en voor de ondersteunende activiteiten ten dienste van de afnemer.

- Beveiligingsincidenten

Het BKWI beschikt niet, zoals volgens het UWV in het rapport is aangegeven, over een adequate procedure inzake beveiligingsincidenten.
Elke partij dient, aldus het UWV, te beschikken over een procedure voor het analyseren en trekken van lering uit incidenten, en zorgt ervoor dat het beleid en maatregelen overeenkomstig worden aangepast. In de keten SLA is een incidentenprocedure opgenomen, die ziet op partij-overstijgende incidenten en de rol van de beheerder daarin. De door het BKWI daartoe gehanteerde incidentenprocedure voldoet niet aan de eisen die aan de dergelijke procedure moeten worden gesteld.
Het UWV geeft aan samen met het BKWI te gaan zorgen voor een vaststelling van een adequate procedure inzake beveiligingsincidenten.

- Controle gebruik Suwinet logging en gebruiksrapportages

Het BKWI kan, zoals volgens het UWV in het rapport is aangegeven, raadplegingen via Suwinet-Inlezen niet loggen en kan ook geen gebruiksrapportages opstellen. Het UWV geeft aan dat het CBP terecht onderscheid maakt tussen Suwinet-Inkijk en Suwinet-Inlezen. De logging en de gebruiksrapportages met betrekking tot Suwinet-Inkijk voldoen, aldus het UWV, aan de voorschriften uit Bijlage I van de regeling SUWI.

In hun gezamenlijke reactie op de PIA rapportage hebben het UWV, de Vereniging Nederlandse Gemeenten (VNG) en de Sociale Verzekeringsbank (SVB) de minister van Sociale Zaken en Werkgelegenheid (SZW) de toezegging gedaan aansluitvoorwaarden de gebruiksvoorwaarden Suwinet-Inlezen te ontwikkelen. Logging en gebruiksrapportages maken daar onderdeel van uit. De toezegging wordt als maatregel opgenomen in het programmaplan Beveiliging en Privacy Suwinet, dat de Suwipartijen voor oktober 2014 aan SZW aanbieden.
Het UWV zal samen met de VNG en SVB aansluitvoorwaarden en gebruiksvoorwaarden Suwinet-Inlezen ontwikkelen en vaststellen.

Reactie CBP

Ter zake van het beveiligingsplan van het BKWI (als beheerder van Suwinet) erkent het UWV dat dit niet actueel is en voor het laatst in 2011 geëvalueerd. De bevindingen worden op dit punt derhalve niet aangepast.

Verder erkent het UWV dat hij op het punt van beveiligingsincidenten niet beschikt over een adequate procedure. De bevindingen worden op dit punt evenmin aangepast.

Inzake Suwinet-Inlezen erkent het UWV dat het BKWI raadplegingen via Suwinet-Inlezen niet kan loggen en ook geen gebruiksrapportages kan opstellen.
Nu het BKWI niet kan voldoen aan zijn wettelijke opdracht om raadplegingen van Suwinet-Inlezen te loggen, zijn gegevensverwerkingen via Suwinet-Inlezen inherent strijdig met bijlage I van de Regeling SUWI. De bevindingen worden op dit punt dan ook niet aangepast.

2.4 De overeenkomst met het *Department of Social Protection* Ierland

Het UWV is op grond van internationaal en nationaal recht verplicht tot gegevensverstrekking aan buitenlandse bestuursorganen. Het UWV geeft hier uitvoering aan door – op verzoek van het bevoegde buitenlandse bestuursorgaan - de

gevraagde informatie te verstrekken door middel van het invullen en verzenden van in EU verband vastgestelde en voorgeschreven (papieren) formulieren.
Onder verantwoordelijkheid en in opdracht van het UWV als bronhouder heeft het UWV samen met het BKWI een pilot gestart met het bevoegde buitenlandse bestuursorgaan van Ierland. Inde pilot wordt beproefd of –ter vervanging van het papieren berichtenverkeer- het berichtenverkeer op elektronische wijze kan plaatsvinden met gebruik van Suwinet. De pilot is vastgelegd in een door het UWV als bronhouder met het *Department of Social Protection* Ierland gesloten overeenkomst als bedoeld in het Besluit en de Regeling SUWI.

Het CBP heeft de overeenkomst met het *Department of Social Protection* van Ierland getoetst aan de Bijlagen I en III van de Regeling SUWI. De bevindingen van het CBP in dat kader geven het UWV aanleiding tot de volgende reactie:

- De overeenkomst met het *Department of Social Protection* Ierland

Het UWV beschikt niet, zoals het rapport aangeeft, over een geldige overeenkomst met het *Department of Social Protection* Ierland. Door dat het *Department of Social Protection* Ierland pas feitelijk toegang heeft gekregen na het verstrijken van de looptijd van de overeenkomst, is sprake van levering van gegevens op basis van een niet- geldige overeenkomst. Het UWV heeft verzuimd de overeenkomst tijdig te verlengen. Het UWV heeft de levering naar aanleiding van het rapport stopgezet.

- De beveiliging toegang gegevens alle personen Suwinet

De bevinding in het rapport, dat meer informatie wordt gegeven dan strikt noodzakelijk is voor het doel, geeft aanleiding tot nader onderzoek over de voorwaarden tot het verlenen van toegang tot Suwinet.
In de pilot hebben een beperkt aantal daartoe geautoriseerde medewerkers van het *Department of Social Protection* Ierland toegang tot de gegevens van alle in de polisadministratie opgenomen werknemers. Het CBP verwacht, aldus het UWV, dat de toegang beperkt is tot personen die aanspraak kunnen maken op bepaalde voorzieningen die worden uitgevoerd door de Ierse overheid, ofwel die bepaalde verplichtingen moeten nakomen jegens de Ierse overheid. Het BKWI heeft geen dan wel onvoldoende maatregelen genomen om onnodige verzameling van persoonsgegevens als bedoeld in artikel 13 Wbp te voorkomen.
Het UWV merkt hierbij op dat het BKWI in opdracht van het UWV als bronhouder samen met het UWV uitvoering geeft aan de pilot. Het BKWI draagt geen eigenstandige verantwoordelijkheid. Het ligt op de weg van het UWV als bronhouder nader te onderzoeken onder welke voorwaarden en op welke wijze toegang voor Ierland kan worden gerealiseerd tot de gegevens van die personen die aanspraak kunnen maken op een voorziening of een verplichting jegens de Ierse overheid moeten nakomen.
UWV verricht nader onderzoek over de voorwaarden tot het verlenen van toegang tot Suwinet.

- Beveiliging op de onderdelen logging en gebruiksrapportages

De raadplegingen door het *Department of Social Protection* Ierland worden door BKWI gelogd. Het CBP heeft een overzicht van alle raadplegingen van april 2013. Laatstgenoemd overzicht is gebaseerd op de logging.

Reactie CBP

Ter zake van de overeenkomst erkent het UWV dat het niet over een geldige overeenkomst voor gegevensleveringen met het *Department of Social Protection* Ierland beschikt. De bevindingen worden op dit punt niet aangepast.

De bevinding in het rapport, dat meer informatie wordt gegeven dan strikt noodzakelijk is voor het doel, geeft volgens het UWV aanleiding tot nader onderzoek over de voorwaarden tot het verlenen van toegang tot Suwinet. Het CBP maakt uit de reactie van het UWV op dat het de bevindingen op dit punt niet bestrijdt. De bevindingen worden op dit punt evenmin aangepast.

De raadplegingen door het *Department of Social Protection* Ierland worden door het BKWI gelogd. Het CBP heeft een overzicht van alle raadplegingen van april 2013. Laatstgenoemd overzicht is gebaseerd op de logging. De voorlopige bevinding dat de raadplegingen door het *Department of Social Protection* Ierland niet worden gelogd door het BKWI, is verwijderd.

3. Aanpassingen ten opzichte van de voorlopige bevindingen

Naar aanleiding van de zienswijze van het UWV worden de bevindingen op het volgende punt aangepast:

De raadplegingen door het *Department of Social Protection* Ierland worden door het BKWI gelogd. Het CBP heeft een overzicht van alle raadplegingen van april 2013. Laatstgenoemd overzicht is gebaseerd op de logging. De gevolgtrekking in het rapport van voorlopige bevindingen dat de raadplegingen door het *Department of Social Protection* Ierland niet door het BKWI worden gelogd, zal worden verwijderd.