Suwinet

Privacy Impact Assessment

April 2014

PRIVACY MANAGEMENT PARTNERS

Colofon

DATUM	7 april 2014
VERSIE	1.0
PROJECTREFERENTIE	PIA Suwinet
ONDERZOEKSPERIODE	Februari – Oktober 2013
TOEGANGSRECHTEN	Vertrouwelijk
STATUS	Eindversie
EDITOR	Dr. Bob Hulsebosch
AUTEURS	Dr. Bob Hulsebosch (Novay)
	Dr. Koen Versmissen (Privacy Management Partners)
OPDRACHTGEVER	Ministerie van Sociale Zaken en Werkgelegenheid

Ministerie van Sociale Zaken en Werkgelegenheid

Synopsis

Dit rapport beschrijft onderzoek naar de privacyrisico's van Suwinet. Het beoordeelt de gevoeligheid van gegevens in Suwinet en brengt de privacyrisico's in kaart. Bestaande en nieuw getroffen beveiligingsmaatregelen en wettelijke kaders worden daarbij in ogenschouw genomen. Aanbevelingen worden gegeven om privacyrisico's te mitigeren.

Disclaimer

Dit onderzoek is uitgevoerd in opdracht van het Ministerie van Sociale Zaken en Werkgelegenheid. De verantwoordelijkheid voor de inhoud van het onderzoek berust bij de auteurs. De inhoud vormt niet per definitie een weergave van het standpunt van de Minister van Sociale Zaken en Werkgelegenheid.

Inhoudsopgave

Managementsamenvatting

ACHTERGROND

Digitale dienstverlening in het domein van Werk en Inkomen is mogelijk gemaakt met invoering van de Wet Suwi in 2002. De uit de Wet Suwi voortgekomen Regeling Suwi legt een samenhangend stelselontwerp vast voor de elektronische voorzieningen, verantwoordelijkheden, afspraken, uitgangspunten en ketenproducten die nodig zijn voor digitale dossiervorming en gegevensuitwisseling in het domein Werk en Inkomen. UWV, SVB en de gemeenten dragen gezamenlijk zorg voor de instandhouding van deze gezamenlijke elektronische voorzieningen Suwi (GeVS), beter bekend als Suwinet.

De afgelopen jaren hebben een aantal ontwikkeling plaatsgevonden waardoor het gebruik van Suwinet sterk is toegenomen. Toenemende digitalisering heeft geleid tot meer gegevensuitwisselingen tussen de Suwipartijen. Ook zijn er gegevensuitwisselingen bijgekomen met niet-Suwipartijen, zoals de Belastingdienst, RDW, DUO en het Kadaster. Hiermee zijn zowel de uitgewisselde datasets, de feitelijk uitgewisselde gegevens als de rijkheid van die gegevens sterk toegenomen. Met het oog op nieuwe ontwikkelingen zoals het breder gebruik van Suwinet, de Europese Privacy Verordening en ontwikkelingen als cloud en software-as-a-service is het verstandig om huidige en toekomstige privacyrobuustheid van Suwinet te evalueren.

DOEL EN OPZET

Bij het opzetten van Suwinet is destijds veel aandacht besteed aan het borgen van informatiebeveiliging en privacybescherming. Het doel van deze privacy impact assessment (PIA) was om inzichtelijk te maken of en zo ja welke wijzigingen in de Wet Suwi en Suwinet op korte en langere termijn noodzakelijk zijn om de gegevensuitwisselingen binnen het domein van Werk en Inkomen veilig te laten blijven verlopen. Daarbij lag de focus op informatiebeveiliging, en is ook rekening gehouden met te voorziene toekomstige ontwikkelingen. In de PIA zijn gedurende de periode februari – oktober 2013 de volgende risicogebieden in kaart gebracht en geanalyseerd:

- de gevoeligheid en beveiliging van de gegevens;
- limitering van het verzamelen en gebruik van gegevens;
- doelbinding;
- gegevenskwaliteit en beschikbaarheid;
- rechten van betrokkenen;
- transparantie en verantwoording;
- governance en toezicht.

KWETSBAARHEDEN

Uit de PIA blijkt dat er de afgelopen jaren een aantal samenhangende kwetsbaarheden zijn ontstaan die elkaar op een negatieve manier beïnvloeden en daarmee tot privacyrisico's leiden. Deze kwetsbaarheden zijn voornamelijk geconcentreerd in de risicogebieden beveiliging, transparantie en verantwoording, en governance en toezicht.

BEVEILIGING

Binnen het risicogebied beveiliging zijn er twee majeure kwetsbaarheden geconstateerd.

1. **Mismatch tussen risicoprofiel en beveiligingsmaatregelen.** Het risicoprofiel van de over Suwinet

uitgewisselde gegevens is fors toegenomen. De beveiliging van de gegevens heeft daar niet op alle punten gelijke tred mee gehouden, met name op de volgende twee onderdelen:

   a. de gehanteerde methoden voor authenticatie en autorisatie van gebruikers komen onvoldoende tegemoet aan de daaraan vanuit het huidige risicoprofiel te stellen eisen;
   b. nieuwe elementen in het risicoprofiel als gevolg van ontwikkelingen als *bring your own device* en het nieuwe werken zijn nog onvoldoende doorvertaald naar passende beveiligingseisen die de partijen die via Suwinet gegevens uitwisselen aan elkaar stellen en waarover zij gezamenlijke afspraken maken.

2. **Onvoldoende informatiebeveiliging bij gemeenten.** Veel gemeenten vormen een (veel te) zwakke schakel binnen de beveiliging in Suwinet.

TRANSPARANTIE EN VERANTWOORDING

Effectieve samenwerking binnen het Suwistelsel vergt dat de Suwi-partijen transparant zijn en verantwoording afleggen over hun aandeel in Suwi, zowel onderling als tegenover SZW als stelselverantwoordelijke. Ook hier zien wij twee majeure kwetsbaarheden.

1. **Ineffectieve verantwoording.** UVW en SVB zijn wettelijk verplicht om openbaar verantwoording af te leggen over de beveiliging van Suwinet aan de minister van SZW. Bij de verantwoording die Colleges van B&W afleggen aan de gemeenteraad zijn geen eisen gesteld aan de verantwoording over de beveiliging van Suwinet. Door het ontbreken van deze verantwoording door de Colleges van B&W ontstaat er een incompleet beeld van de door de verschillende partijen getroffen beveiligingsmaatregelen binnen Suwinet.
2. **Afnemende transparantie over feitelijk gegevensgebruik.** Als gevolg van het toenemende aantal partijen in de keten, technologische ontwikkelingen als Suwinet-Inlezen en de opkomst van commerciële brokers en steeds complexere regelgeving is er steeds minder zicht op de feitelijke gegevensstromen binnen Suwinet en de rechtmatigheid daarvan. Zowel de afnemende als aanleverende partijen hebben belang bij traceerbaarheid van gegevensuitwisseling om zich te kunnen verantwoorden. Betere afspraken over en handvatten voor het keten-breed kunnen traceren van gegevensuitwisseling zijn gewenst. Helder dient te zijn wie verantwoordelijk is voor het creëren van transparantie.

GOVERNANCE

Suwinet lijdt aan een **gebrek aan effectieve, stelselbrede governance.** De formele gezamenlijke WBP-verantwoordelijkheid van UWV, SVB en de gemeenten voor Suwinet is onvoldoende ingevuld of uitgewerkt in het wettelijk kader. Daarnaast belemmert het ontbreken van keten-brede transparantie aangaande de getroffen beveiligingsmaatregelen en de traceerbaarheid van gegevensuitwisselingen een gerichte aansturing van Suwinet op verbetering van de efficiëntie en de betrouwbaarheid van de gegevensuitwisseling via Suwinet. De verantwoordelijkheid voor de gezamenlijke governance van informatiebeveiliging en privacy in Suwinet dient bovendien nadrukkelijker belegd te worden en beter voorzien te worden van stuurinformatie op basis van verantwoording van de afzonderlijke Suwipartijen. Hierdoor kan de keten-brede borging van informatiebeveiliging en privacy van Suwinet aantoonbaar geborgd en geoptimaliseerd worden.

AANBEVELINGEN

Om met name de hierboven geschetste kwetsbaarheden op te heffen, bevelen wij op hoofdlijnen het volgende aan:

- Kom tot een passend, actueel, eenduidig en door alle partijen verplicht gedragen **Verantwoordingsrichtlijn en Normenkader**. Bij het verplichtende karakter hoort een passend sanctiebeleid.

- Verhoog de **beveiligingsbaseline** van Suwinet op een aantal specifieke punten: geavanceerdere authenticatie en autorisatie, monitoring, filtering en ontkoppeld koppelen. Hoe partijen hier een invulling aan geven is hun eigen verantwoordelijkheid; de baseline moet voorschrijven waaraan de beveiliging moet voldoen. Veranker de beveiliging in de architectuur van Suwinet en de Keten-SLA.
- Ga over op **gedifferentieerde dienstverlening**, waarbij toegang van afnemers tot gegevens en diensten mede afhankelijk is van het beveiligingsniveau dat zij kunnen garanderen. De gevoeligheid van de gegevens bepaald het vereiste beveiligingsniveau.
- Verbeter de **tracking en tracing** van gegevensuitwisselingen in Suwinet en de **rapportages** daarover. Borg dat alle partijen binnen redelijke termijn overgaan op de nieuwe bericht definities, waarbij end-to-end vaststaat welke unieke persoon van welke organisatie, welke gegevens en voor welk doel heeft opgevraagd en ter beschikking heeft gekregen.
- Verduidelijk de WBP-verantwoordelijkheden en breng de **verhoudingen** tussen de Suwipartijen en de daarbij behorende governance daarmee in overeenstemming. Stel vast welke waarborgen de governance zou moeten bieden en bepaal daarna in welke vorm dat zou kunnen.
- Reduceer de **complexiteit** van wet- en regelgeving. Maak de gegevensbehoefte per wet concreet, consistent en eenduidig en link deze aan het SGR dat wettelijk is vastgesteld zodat geen misinterpretatie kan plaatsvinden en nieuwe diensten sneller uitgerold kunnen worden.

Aangezien het hele stelsel mede draait op basis van vertrouwen is het essentieel dat deze aanbevelingen met alle betrokken partijen gezamenlijk opgepakt worden zodat ze ook vertrouwen hebben in de te treffen maatregelen. De professional speelt daarbij een belangrijke rol. Door te blijven investeren in bewustwording bij en integriteit van professionals kunnen veel privacyrisico’s voortijdig in de kiem gesmoord worden. Het versterken van de informatiepositie van de burger kan hierbij helpen. Het bieden van transparantie over het gebruik van gegevens aan de burger kan het oneigenlijk gebruik ervan voorkomen.

1 Inleiding

1.1 ACHTERGROND

Dit rapport is het resultaat van een onderzoek dat is uitgevoerd in opdracht van het Ministerie van Sociale Zaken en Werkgelegenheid (SZW).

Digitale dienstverlening in het domein van Werk en Inkomen is mogelijk gemaakt met invoering van de Regeling Suwi in 2002. In de Regeling Suwi is een samenhangend stelselontwerp vastgelegd dat het totaal aan elektronische voorzieningen, verantwoordelijkheden, afspraken, uitgangspunten en ketenproducten omvat die nodig zijn om in het kader van digitale (nominatieve) dossiervorming overheidspartijen op efficiënte wijze gegevens met elkaar uit te laten wisselen binnen het domein van Werk en Inkomen. In de Wet Suwi is opgenomen dat het UWV, de SVB en gemeentelijke sociale diensten gezamenlijk zorg dragen voor de instandhouding van de elektronische voorzieningen voor de verwerking van gegevens (zoals genoemd in artikel 62, lid 1 en 2) ten behoeve van de samenwerking zoals genoemd in artikel 9, lid 1 van de Wet Suwi. Deze gezamenlijke elektronische voorzieningen Suwi (GEVS), ook wel Suwinet genoemd, hebben mede betrekking op de verwerking van gegevens waarvan de verkrijging en verstrekking van gegevens door het UWV, de SVB en Gemeentelijke sociale diensten op grond van enig wettelijk voorstel is toegestaan (artikel 62, lid 2).

Omdat er sprake is van uitwisseling van privacy-gevoelige gegevens is in de wet- en regelgeving relatief veel aandacht besteedt aan de beveiliging ervan.

De afgelopen jaren hebben een aantal ontwikkeling plaatsgevonden waardoor het gebruik van Suwinet sterk is toegenomen. De ontwikkeling van het Digitaal Klant Dossier – mogelijk gemaakt met de Wet Eenmalige Gegevensuitvraag (2008) – en de ontsluiting ervan via Suwinet heeft onder meer geleid tot een verdere digitalisering van het aanvraagproces voor een WWB of WW-uitkering. Burgers hoeven geen gegevens meer aan te leveren die al bekend zijn bij de overheid, mits deze gegevens van voldoende kwaliteit zijn. Dit heeft geleid tot een toename in het aantal gegevensuitwisselingen. Daarnaast zijn er ook gegevensuitwisselingen met niet-Suwipartijen als de Belastingdienst, RDW, DUO en het Kadaster bijgekomen. Mede hierdoor is ook de rijkheid van de gegevensuitwisseling toegenomen. Verder is het door technologische ontwikkelingen mogelijk voor aangesloten partijen om gegevens van burgers rechtstreeks op te vragen vanuit ‘inlezende’ applicaties en e-formulieren. Een dergelijk geautomatiseerde gegevensverwerking is aantrekkelijk omdat het een beter en sneller inzicht geeft in de situatie van de klant om passende dienstverlening te bieden, de doorlooptijd van aanvragen kan verkorten doordat processen efficiënter kunnen worden ingericht, en het administratieve lastenverlichting bewerkstelligt omdat professionals geen gegevens meer hoeven over te typen uit Suwinet-Inkijk maar direct en foutloos inlezen in de applicatie waar het gegeven gebruikt gaat worden.

Dat alles heeft in de afgelopen jaren geleid tot fors meer gegevensuitwisseling via Suwinet. In 2012 werden van 5.457.491 burgers via Suwinet gegevens opgevraagd door 24.491 unieke gebruikers van 304 afnemende

organisaties[1]. Dit resulteerde in 111.735.660 uitgewisselde berichten, zo'n 10 procent meer dan in 2011.

Met een dergelijke toename van niet alleen het aantal uitwisselingen maar ook het aantal verschillende gegevens rijst de vraag of de getroffen waarborgen op het terrein van informatiebeveiliging nog voldoende toereikend zijn om de privacy van burger te garanderen. Dat de overheid hier veel waarde aan hecht blijkt wel uit het feit dat beveiliging hoog op de agenda staat en dat in het regeerakkoord wordt aangegeven dat een Privacy Impact Analyse (PIA) noodzakelijk is voor systemen waarin persoonsgegevens verwerkt worden.

1.2 DOEL

Gezien de toename en de groei van het aantal gegevensuitwisselingen via Suwinet wil het ministerie van Sociale Zaken en Werkgelegenheid een PIA op Suwinet laten uitvoeren. Doel van het laten uitvoeren van de PIA is om inzichtelijk te krijgen welke wijzigingen in de Wet Suwi en Suwinet op korte en langere termijn noodzakelijk zijn om de gegevensuitwisselingen binnen het domein van Werk en Inkomen veilig te laten blijven verlopen.

Om de privacy van de gegevens ook de komende jaren te kunnen garanderen zullen toekomstige ontwikkelingen van Suwinet zoals het breder gebruik ervan ter ondersteuning van de verdere digitalisering van de dienstverlening en het (wettelijk verplicht) hergebruik van gegevens, de opkomst van het nieuwe werken en de aankomende Europese privacy wetgeving meegenomen worden in de uitvoering van de PIA.

1.3 ONDERZOEKSAANPAK

In het onderzoek komen zowel kwalitatieve als kwantitatieve aspecten aan bod, met een sterke focus op kwalitatieve aspecten en kwantitatieve onderbouwing waar mogelijk. Hierbij is gebruik gemaakt van bureau-onderzoek om relevante informatie te verzamelen en te bestuderen. Dergelijke informatie bestond o.a. uit de wettelijke kaders rondom Suwinet, rapporten van de Inspectie SZW en adviesorganisaties, en artikelen in de publieke media.

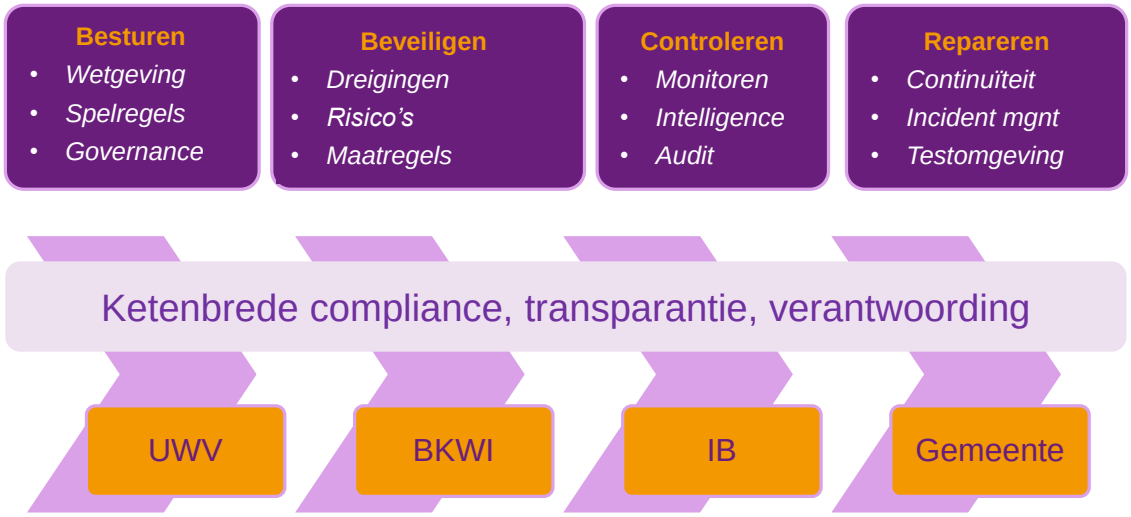
Daarnaast zijn interviews afgenomen met verschillende belanghebbenden om nieuwe inzichten te krijgen en bestaande inzichten te toetsen. De volgende organisaties zijn geconsulteerd tijdens het onderzoek: Inlichtingenbureau, BKWI, KING, VNG, Gemeente Enschede en Rotterdam, UWV en SVB. Om een compleet beeld te krijgen van de privacy uitdagingen zijn vertegenwoordigers van deze organisaties geïnterviewd. Per organisatie is soms gesproken met meerdere vertegenwoordigers. In totaal zijn er negentien personen geïnterviewd waaronder o.a. security officers, juridisch adviseurs, beleidsadviseurs en privacy functionarissen.

Een Privacy Impact Assessment (PIA) biedt inzicht in de risico's van een verwerking van persoonsgegevens. Wanneer die risico's bekend zijn, kunnen maatregelen worden genomen om deze te beheersen. Het inzicht geven in mogelijke mitigerende maatregelen is onderdeel van een goede PIA.

Er bestaat noch op EU-niveau, noch in Nederland een vaststaand model of algemeen aanvaarde methodiek voor het uitvoeren van een PIA. In afgelopen jaren is naar aanleiding van een initiatief van het CBP gebleken dat de gedachten voor het ontwikkelen van een uniforme methodiek voor het uitvoeren van een PIA sterk uiteenlopen. Een

[1] BKWI Jaarverslag 2012, zie http://www.bkwi.nl/uploads/media/BKWI_jaarverslag_1.1.pdf.

bijkomende complexiteit is dat het gegevensuitwisseling betreft tussen meerdere partijen in een keten/netwerk, het Suwinet. De PIA omvat dan een ketenbrede assessment. De PIA dient dan rekening te houden met aspecten als ketenintegratie, ketencompliance en ketentransparantie die stuk voor stuk van invloed kunnen zijn op de privacy van de gegevensuitwisseling. Gebrek aan integratie kan potentieel leiden tot complexe ketens met grote kans op fouten en met gaten in de beveiliging van de gegevens, gebrek aan toezicht resulteert in gebrekkige privacyhandhaving en slap ingrijpen in het geval van een calamiteit, gebrek aan transparantie kan het vertrouwen ondermijnen. Ketenbrede besturing, beveiliging, controle en incident afhandeling completeren het ecosysteem dat nodig is om de privacy van de burger optimaal te borgen. Figuur 1 illustreert dit ecosysteem voor Suwinet.



Figuur 1: Ecosysteem voor ketenbrede borging van privacy.

Voor het uitvoeren van de PIA is de onderstaande aanpak gebruikt. Deze is geïnspireerd door en gebaseerd op de uitkomsten van het Europese PIAF project, waarin recent een basis is gelegd voor een uniforme aanpak van PIA's in de EU[2].

1. Er is een inventarisatie gemaakt van de huidige Suwinet opzet waaronder de genomen technische, organisatorische en juridische privacy waarborgen (beveiligingsmaatregelen, procedures hieromtrent, standaarden, architecturele aanpak, wetgeving en afspraken en verantwoordelijkheden). Hierbij is onder andere ingegaan op de volgende aspecten:
    a. Gegevens in de systemen
        i. Welke gegevens betreffen het?
        ii. Welke bronnen zijn er?
        iii. Welke technologieën worden hiervoor gebruikt?
        iv. Welke identifiers (bv BSN) worden hiervoor gebruikt?
    b. Gebruik van gegevens
        i. Hoe worden de gegevens gebruikt?
        ii. Worden gegevens gecombineerd?
        iii. Worden de gegevens bewerkt en, zo ja, hoe en waarvoor?
        iv. Hoe nauwkeurig (identificerend) zijn de (bewerkte) gegevens?
        v. Hoe lang mogen gegevens bewaard worden?

[2] Zie http://www.piafproject.eu/ref/PIAF_D3_final.pdf.

c. Delen van gegevens
    i. Tussen welke partijen worden gegevens gedeeld?
    ii. Wie is de beheerder van de gegevens en wie is de gebruiker?
    iii. Zijn de uitgewisselde gegevens zichtbaar voor tussenpartijen (b.v. brokers als BKWI of Gemnet operators)?
    iv. Hoe worden de gedeelde gegevens beveiligd (b.v. versleuteling tijdens transport, toegang tot de gegevens, welke processen zijn hiervoor ingericht)?
    v. Is er sprake van privacy awareness onder de gebruikers?
d. Toepasselijke privacyregels
    i. Voor welke doelstellingen worden de gegevens verwerkt?
    ii. Wat is de wettelijke grondslag voor de gegevensverwerking?
    iii. Voor bijzondere gegevens: welke uitzondering op het verwerkingsverbod is van toepassing?
    iv. Welke wettelijke regels (naast de WBP) zijn van toepassing?
e. Toestemming vragen / inzage geven
    i. Worden burgers geïnformeerd over gegevensuitwisseling?
    ii. Hebben burgers de mogelijkheid om gegevensuitwisseling te verbieden of toe te staan?

2. Op basis van de hierboven in kaart gebrachte gegevensuitwisseling zijn de mogelijke kwetsbaarheden en daaraan gerelateerde privacyrisico's afgeleid en zijn deze afgezet tegen de getroffen technische, organisatorische en juridische voorzorgen. Voor het in kaart brengen van de kwetsbaarheden en risico's zijn een aantal risicogebieden gedefinieerd welke gebaseerd zijn op een combinatie van elementen uit het Toetsmodel PIA Rijksdienst[3] en de NOREA handleiding voor PIAs[4]. Deze risicogebieden zijn: gevoeligheid en beveiliging van de gegevens, limitering van het verzamelen en het gebruiken van gegevens, doelbinding, gegevenskwaliteit en beschikbaarheid, rechten van betrokkenen, transparantie en verantwoording. Deze gebieden zijn aangevuld met een aantal ketenspecifieke risicogebieden zijnde governance, verantwoording en toezicht. Op basis hiervan is er een oordeel gevormd over de privacyrisico's en is advies gegeven over vereiste ingrepen om de betrouwbaarheid van de gegevensuitwisseling in Suwinet te borgen.
3. Door toekomstige ontwikkelingen als het breder gebruik van Suwinet en komen Europese privacy wetgeving in ogenschouw te nemen zijn mogelijke nieuwe kwetsbaarheden geïdentificeerd welke hebben bijgedragen om te komen tot toekomstvaste aanbevelingen voor het succesvol borgen van privacy.

Het onderzoek is uitgevoerd in de periode februari – oktober 2013 en heeft betrekking op de privacy situatie in Suwinet op dat moment.

1.4 LEESWIJZER

Dit rapport is als volgt opgebouwd. Hoofdstuk 2 schetst de huidige situatie van Suwinet. Het beschrijft de implementatie ervan en de wettelijke kaders waarbinnen de gegevensuitwisselingen plaats dienen te vinden. Hoofdstuk 3 gaat vervolgens in op de privacyrisico's van Suwinet, daarbij de bestaande maatregelen in ogenschouw nemende. Op basis van een analyse worden risicomitigerende maatregelen voorgesteld. De impact van toekomstige ontwikkelingen wordt in Hoofdstuk 4 beschreven. In Hoofdstuk 5 worden conclusies getrokken en de belangrijkste aanbevelingen benoemd.

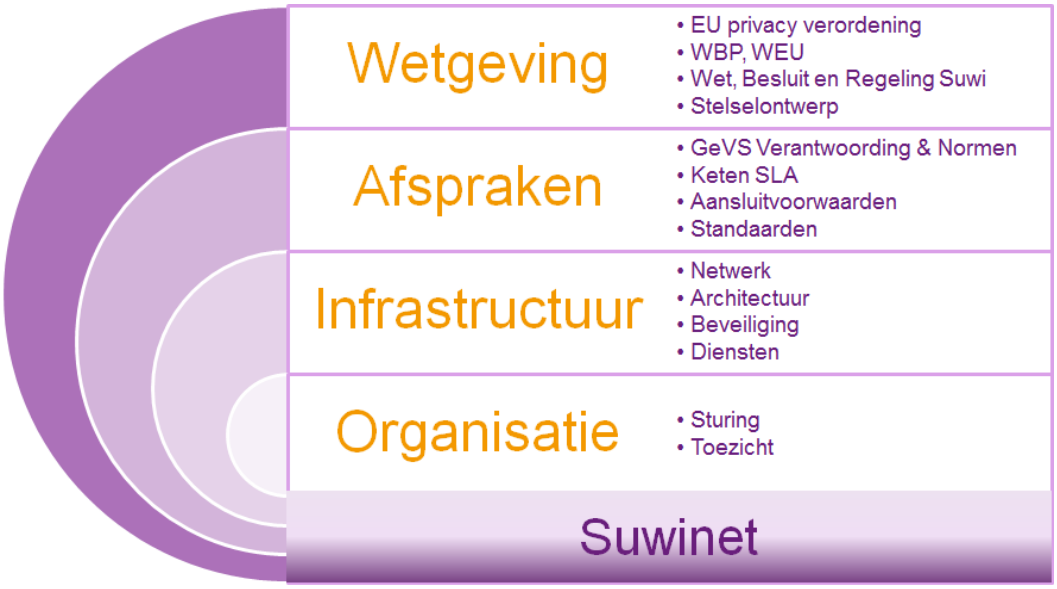
[3] Toetsmodel PIA Rijksdienst, 2013, zie http://www.rijksoverheid.nl/documenten-en-publicaties/publicaties/2013/06/24/toetsmodel-privacy-impact-assessment-pia-rijksdienst.html.
[4] Privacy Impact Assessment (PIA) – introductie, handreiking en vragenlijst, NOREA, 2013, zie http://www.norea.nl/readfile.aspx?ContentID=76469&ObjectID=1101339&Type=1&File=0000040117_NOREA%20A4%20Privacy%20Impact%20Assessment%2003%20WEB.pdf.

2 Beschrijving Suwinet

De eerste stap in de PIA is de huidige situatie van Suwinet in kaart te brengen.

Suwinet is de gezamenlijke infrastructuur voor de ketenpartijen werk en inkomen en voorziet op basis van de wet Suwi in elektronische gegevensuitwisseling tussen deze partijen. Deze partijen – UWV (en BKWI als onderdeel van UWV), SVB, IB en de gemeenten – hebben onderling afspraken gemaakt over hoe ze met elkaar communiceren. De infrastructuur voor gegevensuitwisseling bestaat uit het netwerk zelf en de nodige (technische) maatregelen en processen om adequate beveiliging van uit te wisselen gegevens te garanderen. Bovenop het netwerk draaien een aantal diensten voor het tonen of verwerken van de gegevens.

Figuur 2 schetst de kernelementen die van toepassing zijn op Suwinet.



Figuur 2: Kernelementen Suwinet.

2.1 JURIDISCH – WETTELIJK KADER

Op het terrein van de sociale zekerheid moet voor het gebruik van persoonsgegevens worden voldaan aan de eisen van de Wet Bescherming Persoonsgegevens (WBP), de Wet Eenmalige Gegevensuitvraag werk en inkomen (WEU) en de Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI). Daarnaast zijn er diverse materiewetten waaraan voldaan moet worden. Deze wetten leggen de kaders van het privacy- en beveiligingsbeleid van Suwinet vast.

Bij de informatie-uitwisseling op het gebied van werk en inkomen is sprake van een gesloten systeem. Dit houdt in, dat gegevensverstrekking door UWV, SVB, gemeenten, Minister van SZW en Inspectie SZW slechts plaats mag vinden als er een expliciete wettelijke grondslag voor is of als betrokkene voor een specifieke eenmalige gegevensverstrekking toestemming heeft gegeven. Dit gesloten systeem is in hoofdzaak neergelegd in de Wet SUWI, het Besluit SUWI, de Regeling SUWI en de WWB.

Voor UWV, SVB en gemeenten geldt het beginsel dat gegevens slechts eenmaal door een uitvoeringsinstantie mogen worden uitgevraagd bij de cliënt (of de werkgever) en vervolgens door de overheidsinstanties binnen de SUWI-keten dienen te worden hergebruikt waar dat mogelijk is. Dit beginsel is door de Wet eenmalige gegevensuitvraag werk en inkomen (WEU) vastgelegd in o.a. de Wet SUWI en de WWB.

UWV, SVB en gemeenten dienen zich daarnaast te houden aan de Wet bescherming persoonsgegevens (Wbp). In deze wet is onder andere geregeld dat bij het verstrekken van persoonsgegevens zorgvuldig bekeken dient te worden of deze wel doorgeleverd mogen worden. Er mogen niet meer gegevens verwerkt worden dan strikt noodzakelijk is voor het doel waarvoor men de gegevens nodig heeft (doelbindings- of proportionaliteitsprincipe).

De Wet Suwi en het onderliggende Besluit en Regeling regelen de gegevensuitwisseling, het in stand houden en beheer van een elektronische voorziening daarvoor en de verantwoordlijkheden.

De Wet en het Besluit Suwi regelen op hoofdlijnen de uitvoeringsstructuur voor het domein van werk en inkomen. De Regeling Suwi bevat een nadere uitwerking hiervan. Het gaat daarbij zowel om de organisatorische kant als de meer inhoudelijke kant van de uitvoering van de sociale zekerheid. De diversiteit van onderwerpen die in de Regeling Suwi zijn opgenomen is groot en raakt dan ook alle organisaties die in de Wet Suwi zijn gepositioneerd. De planning- en controlcyclus vormt een belangrijk element in de Regeling Suwi. Dit is onderdeel van de relatie tussen de minister van SZW en de betrokken organisaties. De Regeling bevat onder meer bepalingen met betrekking tot jaarplan, begroting en verantwoording.

In art. 62.1 wet Suwi is vastgelegd dat de UWV, SVB en de colleges van burgemeester en wethouders (de Suwi-partijen) elkaar de gegevens verstrekken die nodig zijn voor de uitvoering van de opgedragen wetten (voor gemeenten de WWB, IOAW, IOAZ). In art. 62.2 is bepaald dat zij gezamenlijk zorg dragen voor de instandhouding van een elektronische voorziening voor de verwerking van die gegevens. In art. 62.3 is bepaald dat UWV en colleges van B&W gezamenlijke verantwoordelijke zijn in de zin van de Wbp voor de gegevensverwerking op de werkpleinen.

De Regeling Suwi bevat een uitwerking van de elektronische voorziening (het stelselontwerp, bijlage I), de beveiliging, de toegang van niet-Suwipartijen (bijlage III, het Aansluitprotocol) en het principe van de eenmalige uitvraag (de Wet Eenmalige Uitvraag).

Het Stelselontwerp beschrijft in algemene termen wat er onder elektronische voorziening moet worden verstaan. Het bepaalt de verantwoordelijkheden van gegevensleveranciers (bronhouders) en gebruikers. De bronhouders zijn verantwoordelijk voor beschikbaarheid, integriteit en vertrouwelijkheid van de gegevens. Verder dienen zij aan de

eisen van privacy en beveiliging te voldoen. De ontvangende partijen zijn verantwoordelijk voor het naleven van de wettelijke regels rond privacy en beveiliging en ze hebben een meldplicht jegens de gegevensleverancier wanneer zij vermoeden dat een gegeven onjuist is.

In het Besluit Suwi art. 5.23 is geregeld dat ook niet-Suwi-partijen van de elektronische voorziening gebruik mogen maken om Suwi-gegevens te gebruiken voor hun wettelijke taken. Voor hun geldt het Aansluitprotocol waarin voorwaarden voor aansluiting en het proces tot aansluiting stap voor stap zijn opgenomen. Bovendien gelden alle afspraken zoals die door de Suwi-partijen zijn gemaakt, waaronder die over privacy en beveiliging, en moeten zij bilaterale overeenkomsten sluiten met de bronhouder.

Art. 5.22 van de Regeling regelt dat UWV, SVB en het Inlichtingenbureau (als sectorloket voor gemeenten) jaarlijks rapporteren over “de opzet en werking van het stelsel van maatregelen en procedures gericht op het waarborgen van een exclusieve, integere en controleerbare gegevensverwerking”. Dit moet vergezeld zijn van een oordeel van een EDP-auditor. De gemeenten (colleges van B&W) zijn hiervan uitgezonderd, althans voor wat betreft hun Suwi-taken. Zij worden geacht op de reguliere wijze verantwoording af te leggen aan de gemeenteraad. Gemeentelijke onderdelen die niet-Suwitaken uitvoeren worden als niet-Suwi-partijen beschouwd. De gemeente is dus Suwipartij wat betreft de Suwitaken en niet-Suwipartij wat betreft niet-Suwitaken. Een dubbelrol die in de praktijk bijna onwerkbaar is, aangezien elke gemeentelijke dienst/afdeling als partij moet worden gezien.

In de Regeling is bepaald dat alle aangesloten partijen (dwz de Suwi-partijen UWV, SVB, colleges van B&W en het IB én de niet-Suwi-partijen) zorgdragen voor de beveiliging van de gegevensuitwisseling en dat zij beschikken over een beveiligingsplan waarin zij aangeven hoe zij dat doen (art. 6.4 Regeling Suwi).

Verder zijn de aangesloten Suwi-partijen gezamenlijk verantwoordelijk voor het maken van afspraken die leiden tot een samenhangend en betrouwbaar samenstel van gezamenlijke voorzieningen. De beheerder (BKWI, als onderdeel van UWV) is operationeel verantwoordelijk voor de coördinatie van de totstandkoming van de gezamenlijke afspraken[5]. Het Stelselontwerp geeft aan waarover die afspraken tenminste moeten gaan:

- de uit te wisselen gegevens, doelbinding, proportionaliteit en eigenaarschap, vast te leggen in het Suwi-Gegevensregister (SGR);
- de wederzijdse resultaatverplichtingen over ICT-beheer, onder andere over beschikbaarheid, integriteit en kwaliteit van de data, toegangsbeveiliging en incidenten-en risicobeleid, die worden vastgelegd in de Keten-SLA;
- het naleven van principes van de elektronische overheid vastgelegd in een ketenarchitectuur.

UWV is verantwoordelijk voor het aansturen van BKWI in zijn beheertaken.

Paragraaf 2 van het Stelselontwerp geeft het kader voor Privacy en Beveiliging dat de Suwi-ketenpartijen gezamenlijk moeten uitwerken in een Verantwoordingsrichtlijn.

[5] Art. 5.21 lid 2 Besluit SUWI zegt dat: “Het UWV belast een afzonderlijk en herkenbaar organisatieonderdeel met de taken, bedoeld in het eerste lid”. BKWI heeft dus een operationele verantwoordelijkheid.

Het UWV, de SVB en het IB rapporteren elk jaar over de opzet en werking van het stelsel van maatregelen en procedures, gericht op het waarborgen van een exclusieve, integere, beschikbare en controleerbare gegevensverwerking. 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.[6]

Op grond van Artikelen 5.22 en 6.4 Regeling SUWI over de opzet, het bestaan en de werking van de beveiliging van Suwinet hebben de Suwipartijen onderling afgesproken dat de security officer van BKWI jaarlijks een totaaloverzicht samenstelt voor SZW en de Inspectie over de wijze waarop de privacy en beveiliging van de elementen van het stelsel is geregeld, welke conclusies daaraan verbonden moeten worden en welke maatregelen nodig zijn ter verbetering. Dit doet hij in de vorm van een Samenvattende Rapportage van de beveiliging van de GeVS, op grond van de onderling afgesproken rapportage cf. de Verantwoordingsrichtlijn. Verder bepaalt het Stelselontwerp dat de beheerder van de centrale voorziening passende maatregelen neemt bij geconstateerde beveiligingsinbreuken of misbruik van de GeVS.

2.2 ORGANISATORISCH – AFSPRAKEN

Artikel 62 lid 2 van de wet SUWI stelt dat de SUWI-partijen gezamenlijk zorg dragen voor de instandhouding van de GeVS. In concreto betekent dit dat de SUWI-partijen onderling en gezamenlijk, met de beheerder van de centrale voorziening, afspraken maken op de verschillende deelgebieden van informatie-uitwisseling binnen de SUWI-keten. De beheerder van de centrale voorziening faciliteert de tot stand koming van de gezamenlijke afspraken, ziet toe op de samenhang en actualiteit van de afspraken en op niet strijdigheid daarvan met gemeenschappelijke, overheidsbrede, afspraken. Indien voldaan is aan de gestelde eisen worden de gemaakte afspraken, namens de SUWI-partijen, door de beheerde van de centrale voorziening voor akkoord voorgelegd aan het ketenoverleg.

Uiteindelijk vinden de afspraken hun weerslag in diverse concrete producten waarvan de belangrijkste voor dit onderzoek de Keten Service Level Agreement[7], het SUWI-Gegevens Register, de SUWI-Ketenarchitectuur en de Verantwoordingsrichtlijn Privacy & Beveiliging GeVS met bijbehorend Normenkader[8], en de aansluitvoorwaarden[9] zijn.

2.2.1 VERANTWOORDINGSRICHTLIJN EN NORMENKADER

Als nadere uitwerking van Bijlage I bij de regeling SUWI is er in 2004 door de gezamenlijke Suwinet-partijen een verantwoordingsrichtlijn en normenkader voor de Suwinet-audit opgesteld. Suwinet-partijen hebben afgesproken deze richtlijn vanaf de verantwoording over 2004 te hanteren. Gebruik van dit normenkader moet leiden tot meer eenduidigheid in de door Suwinet-partijen uitgevoerde audit, en daarmee tot meer inzicht in het beveiligingsniveau van Suwinet als geheel. Het beveiligingsplan dient tegemoet te komen aan deze normen en afspraken. Partijen die geen beveiligingsplan ex artikel 6.4 Regeling SUWI hebben vastgesteld, handelen daarmee niet conform de wet.

[6] Artikel 5.22, eerste lid, Besluit SUWI.
[7] Zie http://www.bkwi.nl/uploads/media/GeVS_Keten_SLA_8.0-def_merged.pdf.
[8] Zie http://www.bkwi.nl/uploads/media/Verantwoordingsrichtlijn_GeVS_2011.pdf.
[9] Zie http://www.bkwi.nl/producten/suwinet-services/suwinet-inlezen/.

De gezamenlijke afspraken voor de rapportage over het beheersen van de risico's aangaande Suwinet zijn vastgelegd in de Verantwoordingsrichtlijn[10]. De Verantwoordingsrichtlijn is een generiek instrument waarmee organisaties transparantie kunnen bieden in hun gehele informatiehuishouding. De Verantwoordingsrichtlijn (privacy en beveiliging van de GeVS) is een gezamenlijk product van de SUWI-partijen en de beheerder van de centrale voorziening welke, op basis van de wettelijke voorschriften rondom privacy en beveiliging, vorm en inhoud is gegeven. Het bevat de normen, criteria en vormvereisten op basis waarvan het oordeel dan wel de verklaring van getrouwheid (ex. art 5.22 regeling SUWI) over de privacy en beveiliging van de GeVS in de Jaarverslagen van de op de GeVS aangesloten ontvangende partijen en de beheerder van de centrale voorziening wordt onderbouwd. In het Jaarverslag wordt daartoe een aparte, als zodanig herkenbare, paragraaf gewijd aan de privacy en beveiliging van de GeVS waarin, waar nodig, verbetermaatregelen worden benoemd.

Onderdeel van de Verantwoordingsrichtlijn is het Normenkader. Het Normenkader definieert een set van eisen ter beheersing van de onderkende risico's aangaande de Suwinet. Het Normenkader biedt concrete aandachtsgebieden variërend van strategische tot operationele controlemaatregelen die gebaseerd zijn op 'best practices' van informatiebeveiliging zoals geboden door o.a. de Code voor Informatiebeveiliging/ISO27002. Een onderdeel van het Normenkader is een jaarlijkse EDP-audit. Voor de EDP-auditor biedt het Normenkader de normen waaraan wordt getoetst of opzet, bestaan, werking en controleerbaarheid van de feitelijke maatregelen voldoen aan de gestelde eisen. De Verantwoordingsrichtlijn biedt een structuur op basis waarvan de partijen rapporteren, transparantie bieden aangaande de naleving van het Normenkader en verantwoording afleggen. De voorgeschreven rapportagevorm biedt tevens de mogelijkheid voor de Security Officer van het BKWI om jaarlijks een beeld samen te stellen voor de risicobeheersing van het hele stelsel.

2.2.2 KETEN-SLA

In de Keten-SLA worden concrete (wederzijdse) prestatie afspraken gemaakt over ICT-beheer. Deze afspraken borgen dat het benodigde samenstel van GeVS-voorzieningen zodanig is ingericht dat deze beschikbaar en integer zijn op het moment dat de diverse SUWI-partijen ze nodig hebben.

2.2.3 GEGEVENSREGISTER

Het Suwi Gegevensregister versie 8.0 bevat de in de Wet Suwi opgenomen verplichte onderdelen: conceptueel gegevensmodel, technische standaarden en een berichtenregister wat weergeeft ten behoeve van welke wettelijke taak (doelbinding), welke gegevenssoorten (proportionaliteit) door wie (verantwoordelijke) aan wie (verwerker) worden uitgewisseld. In het SGR wordt de reikwijdte aangegeven. Dat is het Suwi-domein, dat wil zeggen de uitwisseling tussen UWV, gemeenten en SVB. Voor niet-Suwipartijen gelden bilaterale afspraken tussen bronhouder en gebruiker die in het bilaterale contract (conform het Aansluitprotocol) zijn vastgelegd. De partijen kunnen daarvoor het geldende stramien van de SGR gebruiken.

2.2.4 OVERIGE AFSPRAKEN

Daarnaast zijn er nog de:

[10] Verantwoordingsrichtlijn GeVS 2011, zie http://www.bkwi.nl/uploads/media/Verantwoordingsrichtlijn_GeVS_2011.pdf. Merk op dat sociale diensten niet wettelijk verplicht zijn zich te houden aan deze richtlijn.

- Ketenarchitectuur v2.0 (KarWei) waarin richtinggevende afspraken over diensten, bedrijfsprocessen, ondersteunende informatieprocessen en de infrastructuur die hiervoor nodig is beschreven staan[11].
- SuwiML Transactiestandaard 3.0 dat een taal beschrijft waarmee de gegevens worden uitgewisseld.

2.3 TECHNISCH – INFRASTRUCTUUR EN GEGEVENSUITWISSELING

Suwinet is een besloten netwerk dat organisaties met elkaar verbindt. Via Suwinet kunnen deze organisaties veilig gegevens uitwisselen met elkaar. Daarbij valt onderscheidt te maken in organisaties die gegevens leveren en die gegevens afnemen. Dit kunnen Suwi- of niet-Suwipartijen zijn. Voorbeelden van afnemende partijen zijn de Suwipartijen UWV, SVB, en gemeentelijke sociale diensten, SIOD, Arbeidsinspectie, IND, Interventieteams, College van Zorgverzekeraars, Gemeentelijke belastingdeurwaarders, CAK, en Bureau BIBOB. Voorbeelden van leveranciers zijn de Suwipartijen UWV, SVB en gemeentelijke sociale diensten, GBA-V, Bedrijvenregister, RDW, DUO, Kadaster, Verificatie Informatie Systeem en de Belastingdienst.

Spil in het netwerk is de Suwibroker die de verschillende organisaties koppelt en gegevensuitwisseling mogelijk maakt. Gezien het feit dat de BKWI Suwibroker een belangrijke spin in het web is voor de uitwisseling van gegevens kent BKWI een streng beveiligingsregime. Dit regime is neergeslagen in een passend en doeltreffend beleid waarvan de Bijlagen 1, 2 en 3 van de Wet Suwi, het bijbehorende Stelselontwerp[12], KarWei, de Verantwoordingsrichtlijn en het eigen interne BKWI beveiligingsbeleid de belangrijkste zijn. Dit beleid is geoperationaliseerd middels diverse elektronische voorzieningen (separaat besloten netwerk, autorisatie- en authenticatievoorzieningen, anti-virusscanners, etc.), bijbehorende werkprocessen en een bijbehorende gegevensbeveiligingscultuur binnen BKWI. Het toezicht op het daadwerkelijk gebruik en naleving van het gehanteerde beveiligingsregime binnen het BKWI is geborgd middels periodieke EDP-audits en penetratietests.

Er zijn naast de wettelijke kaders, de gemaakte afspraken en de beslotenheid van het netwerk nog tal van additionele maatregelen getroffen om de privacy van de gegevens te borgen:

- Monitoring / logging en rapportage voorzieningen voor transparantie en verantwoording;
- Awareness campagne “Zorgvuldig gebruik Suwinet” voor het creëren van bewustzijn bij professionals opgezet door het Ministerie van SZW, Divosa, VNG, KING, Inlichtingenbureau en BKWI;
- Suwidesk dashboard voor inzicht en incident response;
- Berichten op maat voor doelbinding;
- Filters voor proportionaliteit;
- Wettelijke toets voor doelbinding;
- Autorisatiematrix voor toegangsbeveiliging;
- Audit (voor niet Suwigebruikers).

Deze maatregelen zullen waar nodig in de risico-analyse in het volgende hoofdstuk benoemd en beschreven worden.

[11] KetenArchitectuur Werk en Inkomen Versie 2.0, 2010, zie http://www.bkwi.nl/uploads/media/KArWeI2.0versie01-11-2010Definitief.pdf.
[12] Het Stelselontwerp & Beveiliging Kaders en uitgangspunten aangaande de Gezamenlijke elektronische Voorzieningen Suwi- (GeVS), zie http://wetten.overheid.nl/BWBR0013280/BijlageI/geldigheidsdatum_30-06-2012.

2.3.1 SUWINET DIENSTEN EN GEGEVENS

Suwinet biedt overheidsorganisaties de mogelijkheid om gegevens van burgers, die bij andere overheidsorganisaties of basisregistraties zijn opgeslagen, te raadplegen in een webtoepassing: Suwinet Inkijk.

Suwinet-Inkijk ontsluit de gegevens die uitvoeringsorganisaties nodig hebben voor de dienstverlening aan de burger. Daarnaast biedt Suwinet-Inkijk een aantal hulpmiddelen aan die de dienstverlening ondersteunen. Suwinet-Inkijk ontsluit een aantal gegevens die bij UWV, GSD en SVB zijn geregistreerd over burgers. Daarnaast kan de gebruiker van Suwinet-Inkijk gegevens over de burger uit enkele andere bronnen vinden, waarvan o.a. GBA-V(oorzieningen) met NAW-gegevens van de klant en gegevens over medebewoners, Verificatie Informatie Systeem (VIS) met de gegevens over gestolen, vermiste en ongeldige ID-bewijzen, het Suwi Bedrijvenregister (SBR) met gegevens over bedrijven vanuit de Kamer van Koophandel en Marktselect, het Kentekenregister van de Rijksdienst Wegverkeer (RDW) met gegevens over voertuigen op naam van de klant, en gegevens over studiefinanciering, opleidingen en diploma's via DUO.

Suwinet-Inlezen is een relatief nieuwe service waarmee gegevens via Suwinet rechtstreeks door overheidsorganisaties kunnen worden opgevraagd in hun eigen lay-out en systeem. Een goed voorbeeld hiervan zijn de zogenaamde e-formulieren die vooringevuld aan de burger ter beschikking worden gesteld. Suwinet-Inlezen biedt organisaties effectiever toegang tot de gegevens die zij nodig hebben voor de uitvoering van hun wettelijke taken. De verwerking van de gegevens vindt plaats met behulp van eigen applicaties of met applicaties van derden. Er is veel belangstelling van overheidsorganisaties voor Suwinet-Inlezen omdat zij hun dienstverlening steeds meer digitaliseren.

Er zijn voorwaarden verbonden aan het inlezen van gegevens. In de voorwaarden is bepaald dat het gebruik is beperkt tot Suwi-taken. Verder zijn alle bepalingen van toepassing zoals die ook regulier voor Suwinet gelden en zijn opgenomen in het Stelselontwerp. Voorwaarden met betrekking tot inlezen zijn vastgelegd in de aansluit- en gebruiksvoorwaarden voor Suwinet Inlezen[13]. De voorwaarden omvatten het hebben van een beveiligingsplan waarin de aan te sluiten partij passende maatregelen heeft genomen om misbruik van ontvangen gegevens te voorkomen, het uitvoeren van een strikt account- en autorisatiebeleid, en het loggen van inlezende activiteiten door de applicatie om misbruik te detecteren. Autorisatie moet op een zelfde manier geregeld zijn als voor de toegang tot Suwinet-Inkijk. Log-gegevens dienen op verzoek van de leverancier verstrekt te kunnen worden. Bij geconstateerd misbruik en/of niet naleving van de voorwaarden heeft de bronhouder het recht de gegevenslevering te beëindigen. De gegevens die worden ingelezen worden gepubliceerd op de site van het BKWI. Er is een aansluitprotocol wat inlezende partijen moeten volgen om gegevens te krijgen. Dit aansluitprotocol (Bijlage Regeling SUWI) geldt alleen voor niet-Suwipartijen die willen gaan inlezen (of inkijken). Partijen die voor Suwi-taken gaan inlezen, ondertekenen de aansluit- en gebruiksvoorwaarden van het IB.

2.3.2 FEITEN EN CIJFERS

In 2012 werden van 5.457.491 burgers via Suwinet gegevens opgevraagd door 24.491 unieke gebruikers van 304

[13] Aansluit- & gebruiksvoorwaarden inlezen en voorinvullen via Gezamenlijke elektronische Voorzieningen SUWI- (GeVS) ten behoeve van SUWI-taken, zie http://www.bkwi.nl/downloads/item/voorwaarden-dkd-inlezen-gemeenten-10/.

afnemende organisaties[14]. Dit resulteerde in 111.735.660 uitgewisselde berichten, zo'n 10 procent meer dan in 2011. Het totaal aantal aangesloten gebruikers bedraagt 39.734. Voor het aantal raadplegingen via Suwinet-Inkijk stopte de teller op 28.411.024. De performance/beschikbaarheid van de centrale componenten is 99,7% en conform de SLA. Het aantal gebruikers is in 2012 verder gedaald met circa 7.100, doordat er ook in 2012 flink geschoond is. Het aantal actieve gebruikers maakt ruim 61% uit van het aantal eindgebruikers.

2.4 ORGANISATIE EN STURING

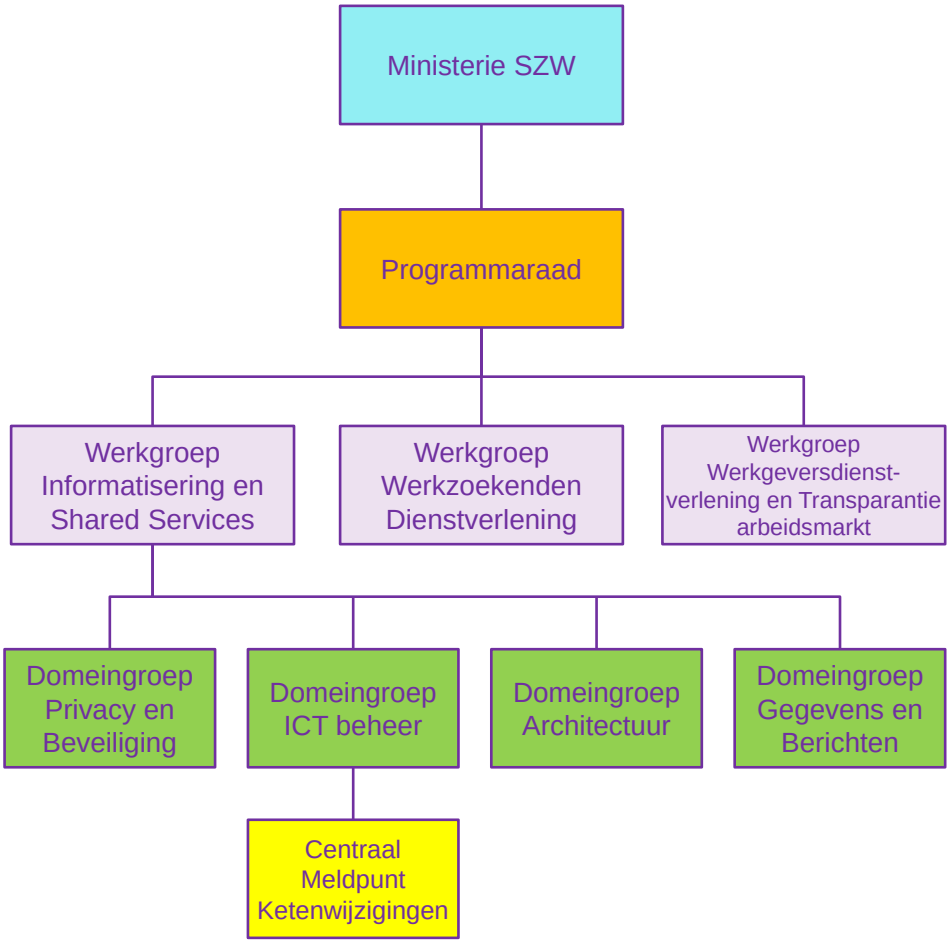
Voor de totstandkoming van de afspraken tussen partijen is een overlegstructuur opgezet met domeingroepen op tactisch en operationeel niveau en met het ketenoverleg voor besluitvorming op strategisch niveau. De structuur is weergegeven in Figuur 3. Het ketenoverleg zoals aangeduid in de Wet Suwi, wordt op dit moment ingevuld door de Programmaraad waarin de Suwipartijen UWV en gemeenten (VNG en Divosa) zijn vertegenwoordigd. De Programmaraad wordt gevoed door een drietal werkgroepen. De Werkgroep Informatisering en Shared Services (WISS) is daarbij voor Suwinet van belang. Hier hangen de vier Domeingroepen onder waarin voor Suwinet relevante onderwerpen besproken en/of uitgewerkt worden.

De taak van de WISS is het vormgeven, monitoren en bijsturen van de voor complementaire dienstverlening (tussen UWV en gemeentelijke sociale diensten) noodzakelijke informatisering. De WISS kan gezien worden als de opdrachtgever voor beide partijen aangaande het verbeteren en bewaken van gegevensuitwisseling via Suwinet. In de praktijk betekent dit dat de WISS inspraak heeft in de programmering van BKWI en het bewaken van de uitvoering ervan via de rapportages uit de verschillende Domeingroepen over bijvoorbeeld het Normenkader, de ketenarchitectuur of de monitoring. Daarnaast hebben BKWI en het Ministerie van SZW regelmatig overleg over Suwinet en fungeert SZW soms als opdrachtgever voor BKWI.

Het Centraal Meldpunt Ketenwijzigingen (CMK) is verantwoordelijk voor coördinatie van het IT-wijzigingsbeleid van Suwinet. Het CMK organiseert het wijzigingsoverleg dat leidt tot afspraken over ICT-wijzigingen. Het wijzigingsoverleg bestaat uit een aantal nieuwe overlegtafels, waaronder het Gezamenlijk Business- en Beleidsoverleg (GBB). De WISS wordt soms ook gevoed vanuit het CMK/GBB.

De Programmaraad rapporteert aan het Ministerie van SZW[15].

[14] BKWI Jaarverslag 2012, zie http://www.bkwi.nl/uploads/media/BKWI_jaarverslag_1.1.pdf.
[15] Per 2014 is het opdrachtgeverberaad ingericht en wordt het ketenoverleg met betrekking tot Suwinet en BKWI niet meer (enkel) door de programmaraad ingevuld.



Figuur 3: Organisatie en sturing van Suwinet.

3 Risicobeoordeling

De volgende stap in de PIA is om op basis van de inventarisatie van het vorige hoofdstuk een inschatting van de privacyrisico's te maken. De risico's worden onderverdeeld in aan aantal risicogebieden. Per risicogebied worden de risico's beschreven.

3.1 RISICOGEBIEDEN

Er zijn een aantal risicogebieden met betrekking tot privacyprincipes en de aandachtspunten daarbinnen die van toepassing zijn op Suwinet en waarvoor passende privacy- en beveiligingsmaatregelen dienen te worden genomen. Zowel het Toetsmodel PIA Rijksdienst als de NOREA handreiking PIA geeft een bruikbaar overzicht hiervan. Deze PIA maakt gebruik van de volgende risicogebieden:

- **Gevoeligheid en beveiliging van de gegevens.** Wat is de gevoeligheid van de gegevens is de beveiliging hiervoor toereikend.
- **Limitering van het verzamelen van gegevens.** Welke maatregelen zijn getroffen om het verzamelen en bewaren van gegevens te beperken? Staat de inbreuk op de belangen van een betrokkene van wie de gegevens worden verwerkt in verhouding tot het door de verwerking te dienen doel?
- **Limitering van gebruik van gegevens.** Welke maatregelen zijn getroffen om hergebruik van gegevens en/of het verwerken van grote hoeveelheden gegevens te voorkomen?
- **Doelbinding.** Worden de gegevens alleen verwerkt op grond van een wettelijke basis en in overeenstemming met het doel waarvoor ze zijn verzameld?
- **Gegevenskwaliteit en beschikbaarheid.** Hoe wordt gewaarborgd dat de gegevens juist, volledig en actueel zijn?
- **Rechten van betrokkenen**. Zijn de betrokkenen voldoende geïnformeerd over de verwerking van de gegevens en hebben zij inzage hierin en zeggenschap hierover?
- **Transparantie.** Is het voldoende transparant welke gegevens door wie en voor welk doel worden gebruikt?
- **Verantwoording.** Hoe wordt verantwoording afgelegd over het op een veilige, behoorlijke en zorgvuldige manier verwerken van gegevens?

Ten aanzien van het laatste risicogebied valt het volgende op te merken. De Wbp maakt duidelijk onderscheid tussen verantwoordelijke en bewerker. Als er meerdere verantwoordelijken zijn, dan zijn er verschillende modellen mogelijk (zie blz. 58 MvT Wbp, maar het denken heeft sindsdien niet stilgestaan, bijv. de SWIFT-zaak en mede naar aanleiding daarvan het Working Paper van de Art. 29 Werkgroep over de begrippen verantwoordelijke en bewerker). Mede daarom moeten de verantwoordelijken hoe dan ook de onderlinge rolverdeling goed met elkaar afspreken of moet die anderszins goed geregeld zijn. Dat is governance; verantwoording en toezicht helpen bij het borgen daarvan. Vooral in de context van ketens zijn naast verantwoording aspecten als **governance**, **verantwoordelijkheden** en **toezicht** belangrijk; deze zullen daarom als aparte risicogebieden meegenomen worden in de PIA.

In de nu volgende secties worden deze risicogebieden nader uitgewerkt. Per risicogebied wordt een vaste uitwerking gehanteerd:

- Een beschrijving van de formele regeling.
- Een overzicht van de getroffen maatregelen
- Een overzicht van de kwetsbaarheden met betrekking tot privacy.
- Een analyse van de risico's en aanbevelingen voor verbeteringen.

3.2 GEVOELIGHEID VAN GEGEVENS EN BEVEILIGING

3.2.1 HOE IS HET FORMEEL GEREGELD?

Tot voor kort werden persoonsgegevens door het CBP geclassificeerd in een viertal risicoklassen variërend van publieke gegevens (klasse 0) tot bijzondere gegevens met een zeer grote privacy gevoeligheid (klasse 3)[16]. Met de komst van de nieuwe richtsnoeren van CBP voor privacy is deze classificatie komen te vervallen. De nieuwe richtsnoeren zijn gebaseerd op een risicogerichte benadering die beter aansluit bij de gangbare praktijk van de informatiebeveiliging en die verantwoordelijken de flexibiliteit biedt om na analyse van de risico's gericht beveiligingsmaatregelen te treffen die in hun situatie en voor de verwerking in kwestie het meest passend zijn. De CBP richtsnoeren hanteren als uitgangspunt een aantal beveiligingsmaatregelen zoals gedefinieerd binnen NEN-ISO/IEC 27002:2007. Er is pas sprake van een passend beveiligingsniveau als er passende maatregelen zijn gekozen en deze onderdeel zijn van de dagelijkse praktijk van de organisatie.

Over beveiliging zegt Art. 76 Wet Suwi dat UWV en SVB hun gegevens adequaat moeten beveiligen. Volgens art. 5.22 lid 1 besluit SUWI moeten UWV, SVB en gemeenten op uniforme wijze zorgdragen voor informatiebeveiliging: "De gebruikers dragen op uniforme wijze zorg voor de beveiliging van de gegevensverwerking door middel van de elektronische voorzieningen tegen inbreuken op de beschikbaarheid, de integriteit en de vertrouwelijkheid."

Dit is nader uitgewerkt in art. 6.4 Regeling Suwi, dat overigens ook geldt voor andere aangesloten partijen dan UWV, SVB en gemeenten: Alle op Suwinet aangesloten partijen moeten de gegevensuitwisselingen over Suwinet beveiligen conform het Stelselontwerp. Hoe ze dat concreet doen, moeten ze aangeven in een beveiligingsplan. En ze moeten jaarlijks rapporteren over de opzet en werking van hun informatiebeveiliging in relatie tot Suwinet, inclusief auditverklaring.

§2.2 Stelselontwerp beschrijft hoe de vertrouwelijkheid van gegevens gegarandeerd wordt. Onder andere: "Beheerder van de centrale voorziening neemt passende maatregelen bij geconstateerde beveiligingsinbreuken of misbruik van de GeVS."

§2.3 Stelselontwerp: Eisen op het gebied van privacy en beveiliging van de gegevensuitwisseling over Suwinet (inclusief de koppelvlakken bij de aangesloten partijen) zijn neergelegd in de Verantwoordingsrichtlijn Privacy & Beveiliging GeVS.

[16] "Beveiliging van persoonsgegevens" (Achtergrondstudies & Verkenningen 23).

3.2.2 WELKE MAATREGELEN ZIJN GETROFFEN?

De beveiligingsmaatregelen die getroffen zijn dienen aan te sluiten bij de gevoeligheid van de gegevens die uitgewisseld worden via Suwinet.

Binnen Suwinet worden meer verschillende gegevens uitgewisseld. Een goed voorbeeld is de implementatie van het recidiveregister via Suwinet. Met dit virtuele register worden fraudevorderingen van gemeenten uitgewisseld om te zien of er sprake is van recidive. Dergelijke gegevens hebben een hoog risicoprofiel en vereisen passende beveiligingsmaatregelen. Het zelfde geldt voor een gegeven als arbeidsongeschiktheid dat geclassificeerd kan worden als een medisch gegeven en al enige tijd via Suwinet uitgewisseld wordt. Ook wordt er gewerkt aan het ontsluiten van zeer gevoelige detentiegegevens vanuit de strafrechtketen. Met het steeds rijker worden van de gegevensset en het toenemen van de aantallen gegevensuitwisselingen via Suwinet neemt de aantrekkelijkheid ervan voor het maken van misbruik of als doelwit voor hackers toe.

Verder stelt het CBP dat het belang van het individu maatgevend is voor het vaststellen van de gevoeligheid van de gegevens. De schade die betrokkenen ondervinden van verlies of onrechtmatige verwerking van hun persoonsgegevens wordt niet bepaald door het aantal anderen van wie de persoonsgegevens eveneens verloren zijn gegaan of onrechtmatig zijn verwerkt. Het maakt voor de gevoeligheid van de gegevens in Suwinet dus niet uit of er nu 400 of 40.000 dossiers van betrokkenen in staan. Wel wordt het Suwinet als geheel een aantrekkelijker doelwit – en dus gevoeliger – als er meer gegevens in uitgewisseld worden.

Een zelfde redenering geldt voor de reikwijdte van de gegevens: het maakt voor de gevoeligheid van de gegevens niet uit of er 400 of 40.000 gebruikers toegang tot hebben. Grote gebruikersgroepen vergroten wel de kans op het schenden van de privacy van de burger door bijvoorbeeld een niet ingetrokken account of een oneigenlijke raadpleging van een dossier.

Behalve de aard van de verwerkte gegevens, kan ook de verwerking zelf risico's met zich meebrengen voor de betrokkenen. Factoren die een rol spelen zijn onder meer:

- Hoeveelheid verwerkte persoonsgegevens per persoon. Naarmate er per persoon meer persoonsgegevens worden verwerkt, kan verlies of onrechtmatige verwerking leiden tot een grotere inbreuk op de persoonlijke levenssfeer. Bijvoorbeeld: het uitlekken van een compleet digitaal klant dossier leidt over het algemeen tot een grotere inbreuk dan het uitlekken van NAW-gegevens. De hoeveelheid gegevens per persoon is de afgelopen jaren toegenomen. Een recent voorbeeld hiervan is het recidiveregister waarvoor een vijftal nieuwe gegevens is toegevoegd aan het GSD bericht. Het Gegevensregister telt inmiddels meer dan 1000 gegevenselementen. Hiermee kan een redelijk goed profiel van een klant opgesteld worden waarmee de zonder passende beveiligingsmaatregelen de privacy flink geschonden kan worden.
- Hoeveelheid verwerkte persoonsgegevens in het algemeen. Naarmate de hoeveelheid uitgewisselde gegevens in zijn algemeenheid toeneemt, heeft het verlies of onrechtmatige verwerking ervan een grote impact op de privacy van heel veel mensen en de reputatie van het verwerkende systeem. Het lekken van gegevens van één burger is minder ingrijpend als dat van alle burgers in Suwinet. Via Suwinet worden per maand ongeveer 10 miljoen berichten uitgewisseld.

- Doel of doelen waarvoor de persoonsgegevens worden verwerkt. Naarmate de beslissingen die op basis van de verwerkte persoonsgegevens worden genomen ingrijpender zijn, is ook de impact van verlies of onrechtmatige verwerking groter. Bijvoorbeeld: als een organisatie medische gegevens gebruikt om iemands uitkering te bepalen zijn de gevolgen ingrijpender dan bij gebruik van dezelfde gegevens voor informatiedoeleinden. De doelen waarvoor de persoonsgegevens gebruikt worden zijn de afgelopen periode toegenomen. Een recent voorbeeld hiervan is het recidiveregister. Dit blijkt ook uit het groeiend aantal partijen dat op Suwinet is aangesloten.
- De complexiteit van de verwerking. Hoe complexer de verwerking, des te groter de kans op fouten is. De verwerking van de gegevens zelf is in Suwinet niet zo heel complex; Suwinet zelf als verwerkend systeem is behoorlijk complex kijkende naar de wettelijke kaders, afsprakenstelsels en voorwaarden die ervoor nodig zijn.

Op basis hiervan kan geconcludeerd worden het risicoprofiel van Suwinet met betrekking tot de gevoeligheid van de gegevens is toegenomen. De vraag is of de beveiliging van de gegevens hieraan tegemoet kan komen.

Er zijn tal van logische en fysieke maatregelen getroffen om Suwinet te beveiligen. Zo maakt Suwinet voor de communicatie van gegevens gebruik van besloten netwerken. Uitwisseling van gegevens met gemeenten loopt via het Gemnet netwerk en met andere organisaties via Suwinet. Het besloten karakter van deze netwerken zorgt ervoor dat niet iedereen zomaar toegang heeft tot het netwerk[17]. Verder wordt er gebruik gemaakt van digitale certificaten om veilige verbindingen op te zetten en gegevens te versleutelen. Alle gebruikers dienen zich te authentiseren en de toegang tot gegevens wordt vervolgens op basis van toegekende autorisaties bepaald. Het gebruik wordt daarbij gelogd wat reactieve ingrepen mogelijk maakt.

De beheerder heeft, op basis van §2.2 van het Stelselontwerp, het mandaat om eventuele gebreken in de beveiliging te signaleren. De beheerder kan niet op grond van de signalen als een “politieagent” sanctionerend optreden. Het is juridisch niet aantoonbaar geregeld dat dit mandaat en de betreffende rol belegd zijn bij de beheerder.

Na aanleiding van het DigiNotar incident zijn er additionele maatregelen getroffen om de veiligheid te verbeteren. Eén van die maatregelen is het kijken naar de IP-adressen om te zien wie de informatie aanvraagt en waar bepaalde informatie vandaan komt. De broker van BKWI is een van de kritische elementen in Suwinet, hierlangs vinden heel veel gegevens hun weg. Deze broker kent een streng beveiligingsregiem dat neergeslagen in een passend en doeltreffend beleid. Dit beleid is geoperationaliseerd middels diverse elektronische voorzieningen (separaat besloten netwerk, autorisatie- en authenticatievoorzieningen, anti-virusscanners, etc.), bijbehorende werkprocessen en een bijbehorende gegevensbeveiligingscultuur binnen BKWI. Het toezicht op het daadwerkelijk gebruik en naleving van het gehanteerde beveiligingsregime binnen het BKWI is geborgd middels periodieke EDP-audits en penetratietests.

Ook zijn er bij de aangesloten partijen diverse organisatorische maatregelen getroffen. Bijvoorbeeld in de werkprocessen rondom het afhandelen van werk en inkomen gerelateerde zaken zijn door gemeenten stappen opgenomen die de kans op privacyschending of belangenverstrengeling verkleinen. Voorbeelden van dergelijke

[17] Hierbij maken we de kanttekening dat het niet bekend is of en in hoeverre Gemnet voldoet aan de vanuit Suwi gestelde eisen.

stappen zijn:

- Verschillende stappen in het werkproces door verschillende personen te laten uitvoeren.
- Geraadpleegde BSNs te vergelijken met BSNs van de eigen medewerkers (mede om stalking te voorkomen).

De kracht van de beveiliging van Suwinet bevindt zich in het stapelen van bovengenoemde maatregelen. Het is echter nog maar de vraag gezien het verhoogde risicoprofiel van de gegevens of dit nog wel voldoende is. Er zijn verschillende redenen waarom dit niet zo is.

3.2.1 WELKE KWETSBAARHEDEN ZIJN ER?

Het niveau van beveiliging in Suwinet laat een wisselend beeld zien. De informatiebeveiliging van de centrale delen van Suwinet en bij leveranciers als UWV en SVB lijkt over het algemeen goed geborgd. Dit blijkt o.a. uit de jaarlijkse audits die UWV en SVB laten uitvoeren voor de rapportage aan de BKWI security officer en de periodieke audits die IB en BKWI laten uitvoeren op hun systemen. In 2012 heeft BKWI ook een penetratietest laten uitvoeren. Er is twijfel over de informatiebeveiliging bij gemeenten. Rapporten van de Inspectie SZW (voorheen Werk en Inkomen) maken melding van ontoereikend beveiligingsbeleid en gebrekkig toezicht op het beheer van accounts en daaraan gerelateerde toegangsrechten voor het inkijken van gegevens[18]. Dit heeft geleid tot verschillende incidenten zo blijkt uit de interviews, rechtszaken[19] en uit een aantal in de pers verschenen berichten[20, 21]. Dergelijke incidenten zijn nooit 100% te voorkomen. Dat door repressieve maatregelen inbreuken gedetecteerd zijn en dat er disciplinaire maatregelen getroffen zijn stemt positief. De vraag blijft natuurlijk hoeveel misstanden ongedetecteerd blijven. Mede daarom heeft de staatssecretaris van Sociale Zaken en Werkgelegenheid onlangs alle gemeenten opnieuw verzocht om nog eens goed naar hun privacy en beveiligingsbeleid te kijken[22]. Gemeenten hebben hier gehoor aangegeven maar geven aan dat de vigerende Suwinet Verantwoordingsrichtlijn en het Normenkader hiervoor niet passend zijn en een te kunstmatig onderscheidt maakt tussen de beveiliging van Suwinet in het algemeen en die van de aangesloten partijen. Bovendien is een meer generiek normenkader wenselijk, in plaats van verschillende sectorale normenkaders en de verantwoording hierover[23].

Om tot een verbetering van de beveiliging bij gemeenten te komen hebben VNG en KING gezamenlijk de Informatiebeveiligingsdienst (IBD) gemeenten in het leven geroepen. Ook de Taskforce Bestuur en Informatieveiligheid Dienstverlening[24] is hierbij betrokken. De IBD gaat aan de slag met een gemeenschappelijk normenkader – de Baseline Informatiebeveiliging Gemeenten (BIG) – en de bijbehorende audit voor gemeenten om

[18] Beveiliging en privacy in de Suwi-keten, rapport Inspectie Werk en Inkomen, 2009, zie http://www.inspectieszw.nl/Images/Beveiliging%20en%20privacy%20in%20de%20SUWI-keten_tcm335-313059.pdf.
[19] Rechterlijke uitspraak misbruik Suwinet, zie http://jure.nl/ecli:nl:rbalk:2011:bq7202.
[20] Ambtenaar gemeente Werkendam ontslagen naar misbruik Suwinet, zie http://www.omroepbrabant.nl/?news/1853981373/Ambtenaar+Werkendam+ontslagen+na+misbruik+computer+met+geheime+gegevens.aspx.
[21] NRC 14 maart 2012: "Gemeenten laks met privégegevens", n.a.v. brief stas De Krom. Meer dan 60% van de gemeenten heeft serieuze problemen met de informatiebeveiliging van (o.a. Suwinet-) gegevens.
[22] Brief van de staatssecretaris van Sociale Zaken en Werkgelegenheid aan de gemeenten met daarin het dringende verzoek om hun privacy en beveiligingsbeleid aan te scherpen, zie http://www.gemeenteloket.minszw.nl/binaries/content/assets/Naleving_x002f_handhaving/2012-06-12-2/brief-informatiebeveiliging-b-en-w.pdf.
[23] Kwaliteitsinstituut Nederlandse Gemeenten (2012). Zorgvuldig gebruik en verbeterpunten, W&I - 31 mei 2012, zie http://www.kinggemeenten.nl/media/502180/04-zorgvuldig-gebruik-en-de-verbeterpunten.pdf.
[24] Taskforce Bestuur en Informatieveiligheid Dienstverlening, zie http://www.taskforcebid.nl.

de huidige auditversnippering weg te nemen. Ondanks deze effort, zal het invoeren van de BIG naar verwachting van de onderzoekers nog wel enkele jaren duren. De praktijk leert dat invoeren van een beveiligingsbeleid op een zodanige manier dat deze is verwerkt in de werkprocessen rondom het verwerken van gegevens tijd kost. Doordat gemeenten met de BIG een eigen baseline voor informatiebeveiliging hebben ontstaat er een situatie waarbij een eenduidige notie van een baseline in Suwinet ontbreekt: gemeenten hebben de BIG en de overige partijen het Normenkader. Hoewel de verschillen klein zullen zijn (beiden zijn gebaseerd op ISO27001) is dit een onwenselijke situatie omdat er geen sprake meer is van één samenhangend en betrouwbaar samenstel van gezamenlijke voorzieningen zoals gepropageerd is in het Stelselontwerp en artikel 5.22 van het Besluit SUWI waarin geregeld is dat partijen op uniforme wijze zorg dienen te dragen voor hun beveiliging. Dit gaat ten koste van de transparantie betreffende de beveiliging in Suwinet en het vertrouwen tussen de partijen onderling.

Ook met betrekking tot het niveau van beveiliging is verbetering wenselijk. Sommige maatregelen zijn meegegroeid met de toenemende gevoeligheid van de gegevensuitwisseling in Suwinet. Zo is bijvoorbeeld de beschikbaarheid van de gegevens verbeterd met de onlangs teruggebrachte response-tijd in de Keten-SLA van 10 naar 6 seconden. Ook geeft de security officer van BKWI in de samenvattende rapportage van 2011 aan dat de schaalvergroting van Suwinet het beveiligingsniveau niet negatief beïnvloed heeft[25]. Een evaluatie van de beveiliging van Suwinet over de gehele breedte van het spectrum (van fysieke en organisatorische tot technische beveiliging zoals bijvoorbeeld gedefinieerd in ISO27002) is nodig om alle afhankelijkheden en kwetsbaarheden in kaart te brengen. Dit valt buiten de scope van dit onderzoek. Desondanks zijn er een aantal kwetsbaarheden met betrekking tot privacy geïdentificeerd.

Kijkende bijvoorbeeld naar de betrouwbaarheid van de authenticatie van de gebruikers is dit op dit moment niet in overeenstemming met de gevoeligheid van de gegevens die kunnen worden ingezien, ingelezen of aangepast. Uit de handreikingen die onlangs door het Forum Standaardisatie[26] en NICTIZ[27] zijn gepubliceerd over het vereiste betrouwbaarheidsniveau van authenticatie in relatie tot de gevoeligheid van de persoonsgegevens die daarmee ontsloten worden blijkt dat het gebruik van de huidige gebruikersnaam en wachtwoord combinaties niet voldoende is. Sterkere authenticatiemiddelen op basis van certificaten of een tweede factor zijn nodig om zeker(der) te zijn van de identiteit van de gebruiker en te voorkomen dat deze kan ontkennen bepaalde handelingen verricht te hebben.

Een andere kwetsbaarheid zijn nieuwe ontwikkelingen als het gebruik van mobiele platformen (“bring-your-own-device”) of thuis-PCs om toegang tot Suwinet te verkrijgen in het kader van flex- of thuiswerken introduceren risico’s. De risico’s die gepaard gaan met het gebruik van dergelijke onveilige platformen en het gebrek aan toezicht daarop zijn aanzienlijk. Mobiele apparaten kunnen verloren worden, thuis-PCs kunnen verborgen key-stroke loggers bevatten, en het thuis of in de trein kunnen meekijken door onbevoegde derden is niet uitgesloten. Zonder additionele beveiligingsmaatregelen dient dergelijke toegang tot Suwinet beperkt te worden. Helderheid dient verschaft te worden over de eisen aangaande de beveiliging in relatie tot 'het nieuwe werken' en 'Bring Your Own

[25] Samenvattende rapportage van de beveiliging van de Gezamenlijke elektronische Voorzieningen Suwi, 24 maart 2011, zie http://www.bkwi.nl/uploads/media/Samenvattende_rapportage_van_de_beveiliging_van_de_GeVS_over_2010.pdf.
[26] Forum Standaardisatie, Betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten, 2012, zie http://www.forumstandaardisatie.nl/fileadmin/os/publicaties/HR_Betrouwbaarheidsniveaus_WEB.pdf.
[27] Nictiz, Handreiking Patiëntauthenticatie, 2013, zie www.nictiz.nl.

Device' om incidenten te voorkomen.

Ook het netwerk zelf is niet waterdicht. Op dit moment wordt de betrouwbaarheid van verbindingen met ketenpartijen niet in alle gevallen gewaarborgd door middel van een beveiligde SSL-verbinding waardoor de confidentialiteit en integriteit van de gegevens op het spel staat. Dit is bekend bij BKWI en IB en hieraan wordt gewerkt. Gezien de beslotenheid van het netwerk vallen de risico's die gepaard gaan met het verlies van confidentialiteit en integriteit mee, maar dat andere partijen op het netwerk kunnen 'meekijken' in de gegevens is onwenselijk.

3.2.2 ANALYSE EN BESCHOUWING

Binnen Suwinet zijn alle partijen verantwoordelijk voor de beveiliging van het eigen deel van Suwinet. UWVis verantwoordelijk voor de beveiliging van het centrale deel van Suwinet. Omdat binnen Suwinet veel privacy-gevoelige informatie uitgewisseld wordt, zijn veel beveiligingsmaatregelen hierop gericht. De toename van via Suwinet uitgewisselde persoonsgegevens, die in sommige gevallen ook een hoger risicoprofiel hebben (bijvoorbeeld gegevens over fraude, arbeidsongeschiktheid en in de toekomst detentie), brengt eisen aan het stelsel met zich mee die het huidige beveiligingsniveau op een aantal vlakken overstijgen.

Het Normenkader voorziet in het beoordelen van de beveiliging voor gegevensverwerking met hoge risicoprofielen. Uit de samenvattende rapportage van de BKWI security officer blijkt dat partijen als BKWI, IB, SVB en UWV over het algemeen voldoen aan het gestelde Normenkader. Vooral BKWI en IB als beheerders van centrale componenten van Suwinet, de brokers, is het belangrijk de beveiliging op orde te hebben. Beide partijen hebben beveiliging dan ook hoog op de agenda staan. BKWI laat naast de jaarlijkse audit ook regelmatig een penetratietest uitvoeren om de beveiliging te testen. Het IB geeft aan dat de organisatorische kant van de beveiliging goed geregeld is en dat het met de toekomstige migratie naar een nieuw platform ook in staat is om technisch een hoog niveau van beveiliging aan te kunnen. Beide partijen geven echter wel aan dat voor het realiseren van een structurele verbetering van het beveiligingsniveau over de gehele breedte van het beveiligingsspectrum zoals bijvoorbeeld in ISO27002 gedefinieerd (dus inclusief aspecten als fysieke en personele beveiliging en continuïteit) nog verbeteringen noodzakelijk zijn die een behoorlijke impact kunnen hebben en kosten met zich meebrengen voor alle partijen in de keten (bijvoorbeeld het verhuizen van een partij naar een ander gebouw waarin de fysieke beveiliging en daarmee de toegang tot en beschikbaarheid van gegevens veel beter geregeld is).

Op een aantal gebieden is echter verbetering wenselijk. Deze gebieden zijn: het verhogen van het baseline beveiligingsniveau en in het bijzonder het authenticatieniveau van professionals, de relatief slechte beveiliging van gemeenten, het ontbreken van een eenduidige baseline voor informatiebeveiliging in Suwinet, het ontbreken van een ketenbreed beleid op basis van gezamenlijke afspraken aangaande het nieuwe werken en het ontbreken van ketenbrede versleuteling van de gegevensuitwisseling.

Bij het verhogen van het authenticatieniveau kan gedacht worden aan het uitrollen van sterkere authenticatiemiddelen aan professionals zoals in de zorgsector gebeurd met de UZI-pas. Ook de financiële sector maakt gebruik van sterke (twee-factor) authenticatiemiddelen en zelfs op het internet is er momenteel een ontwikkeling naar sterkere authenticatie zichtbaar (Google en Facebook maken hier bijvoorbeeld al gebruik van). Het

inzetten van de Rijkspas als sterk authenticatiemiddel valt te overwegen. Binnen eHerkenning en eID Stelsel NL zijn ontwikkelingen gaande waarbij authenticatiemiddelen van verschillende sterkte kunnen worden aangeschaft en hergebruikt over meerdere diensten. Hergebruik van dergelijke authenticatiemiddelen leidt ertoe dat Suwinet zelf geen authenticatiemiddelen hoeft te beheren zoals nu bij Suwinet Inkijk het geval is.

Het is zaak om de hogere authenticatie-eisen vast te leggen in het Normenkader. Eventueel kan hier nog gedifferentieerd worden naar de gevoeligheid van de diensten en de gegevens die gebruikt worden. Het authenticatieniveau kan dan wisselen per dienst of gegevensset. Hoe de partijen de sterke authenticatie regelen is hun eigen verantwoordelijkheid. Daarnaast kan overwogen worden om de beveiliging in de ketenarchitectuur en de Keten-SLA te verankeren. Daarbij kan de uitwisseling van gegevens beter afhankelijk worden gemaakt van het beveiligingsniveau.

De beveiliging binnen een keten is zo sterk of zo zwak als de zwakste schakel. Een punt van zorg is de beveiliging van Suwinet aan de gemeentelijke kant. Die is bij een aantal gemeenten onder de maat, zo blijkt uit onderzoeken van de Inspectie SZW, de rapportage van de BKWI Security Officer en verscheidene andere bronnen. Ondanks dat dit in feite al sinds de ingebruikname van Suwinet speelt, is de aandacht hiervoor recent gelukkig weer flink toegenomen. VNG, KING en de Taskforce BID werken aan het verbeteren van de kwaliteit van de informatiebeveiliging bij gemeenten en het creëren van bewustzijn hiervoor op bestuurlijk niveau. De recent ontwikkelde Baseline Informatiebeveiliging Gemeenten (BIG) kan bijdragen aan niet alleen het verbeteren van de gemeentelijke informatiebeveiliging maar ook aan een uniformering ervan zodat verantwoording richting de keten efficiënter plaats kan vinden.

De verhouding tussen de BIG en de beveiligingseisen vanuit Suwinet behoeft a priori aandacht. Hoe wordt er straks omgegaan met beveiligingseisen vanuit Suwinet die het niveau van de BIG overstijgen? De vraag is echter hoe groot de kans is dat dat probleem zich daadwerkelijk voordoet. Gelet op de taken die gemeenten nu al uitvoeren en de onder handen zijnde decentralisaties lijkt het waarschijnlijker dat gemeenten over een flink deel van hun informatieverwerking een hoog niveau van informatiebeveiliging zullen moeten kunnen garanderen. Des te relevanter is het dat beveiligingseisen vanuit Suwinet worden geïncorporeerd in de BIG. Hiervoor zal een update van het Normenkader nodig zijn om deze beter te laten aansluiten op de vigerende kaders binnen partijen. Tevens biedt dit de mogelijkheid om beleid te definiëren betreffende beveiliging en het nieuwe werken.

Het implementeren van een normenkader als de BIG en het integreren ervan in de organisatie duurt over het algemeen echter enkele jaren. Op korte termijn zullen binnen Suwinet daarom maatregelen moeten worden genomen om – totdat de BIG is ingevoerd én blijkt te werken – de ernstigste risico's als gevolg van inadequate beveiliging aan gemeentekant te mitigeren. Hierbij kan gedacht worden aan het differentiëren van de gegevensuitwisseling op basis van het beveiligingsniveau van de aangesloten partij. Bijvoorbeeld, een gemeente met een laag beveiligingsniveau kan slechts gebruik maken Suwinet-Inkijk en niet Inlezen of heeft geen toegang tot bijzonder gevoelige gegevens als fraudevorderingen of detentiegegevens. Zo kan dus het authenticatieniveau van een professional bepalen welke diensten of gegevens deze mag gebruiken of inzien. Een dergelijke gedifferentieerde aanpak biedt de mogelijkheid om gegevens en diensten te leveren die passen bij het beveiligingsniveau van de

afnemende partij. Zij kunnen daardoor makkelijker aansluiten zonder zich te hoeven conformeren aan een hoog beveiligingsniveau. Voor een gemeente zou dit betekenen dat aan het beveiligingsniveau van een GSD hogere eisen gesteld worden dan aan gemeentelijke deurwaarders. Partijen die gegevens afnemen die wel een hoog niveau van beveiliging vereisen, dienen zich hierover te kunnen verantwoorden door middel van een EDP-audit conform het Normenkader. Een nadeel van een gedifferentieerde aanpak is dat het extra coördinatie en toezicht vereist. Het zal daardoor extra kosten met zich meenemen.

Een alternatieve of aanvullende maatregel is de gebruikers/professionals van Suwinet Inkijk en Inlezen periodiek te laten screenen (bijvoorbeeld door middel van een Verklaring Omtrent Gedrag of een zelf-assessment) zodat duidelijk is/wordt dat inzage in gevoelige gegevens geen sinecure is. Bewustwording van de risico's bij gebruikers is een groot goed. De in 2011 en 2012 gevoerde campagne over "Zorgvuldig gebruik Suwinet" heeft hier mede succesvol aan bijgedragen. Het is verstandig om dergelijke bewustzijnsacties regelmatig te organiseren en op een zodanig variërende manier dat ze blijven aanspreken voor de gebruikers.

Een punt van aandacht bij eenduidige normering van een beveiligingsbaseline in de keten is dat de implementatie ervan vanuit het risicobesef van een specifieke partij, een eigen invulling kan krijgen, terwijl vanuit ketenperspectief toch zwaardere eisen gesteld worden. Dit kan ertoe leiden dat op plaatsen in de keten aanvullende maatregelen getroffen moeten worden om de risico's in de keten het hoofd te bieden. Het bepalen van die ketenrisico's is een taak van de security officer van BKWI. Deze verzamelt jaarlijks op basis van de Verantwoordingsrichtlijn de rapportage van de Suwipartijen en rapporteert hierover. Echter niet alle partijen rapporteren over hun getroffen beveiligingsmaatregelen en incidenten waardoor de samenvattende rapportage een incompleet overzicht biedt (zie sectie 3.8 over Transparantie).

Voor het ontbreken van ketenbrede versleuteling (SSL-encryptie) van gegevensuitwisseling in Suwinet is het belangrijk de 'gaten' in kaart te brengen en deze via digitale certificaten en bijpassende technologie te versleutelen. Dit kan op korte termijn gebeuren om ketenbrede authenticiteit en vertrouwelijkheid van de gegevens te garanderen.

3.2.3 RISICOMITIGERENDE MAATREGELEN

Voor het risicogebied beveiliging stellen we de volgende risicomitigerende maatregelen voor:

- Inventariseer, n.a.v. de toegenomen gevoeligheid van de gegevens in Suwinet, welke beveiligingsonderdelen van het Normenkader versterkt dienen te worden en voer deze in. In ieder geval is het wenselijk om het authenticatieniveau te verhogen indien gewerkt wordt met gevoelige gegevens. Richtlijnen hiervoor kunnen worden vastgelegd in een nieuw, gezamenlijk Normenkader. Overweeg hierbij een gedifferentieerde aanpak waarbij het niveau van beveiliging bepaald welke gegevens en diensten een partij of een gebruiker kan afnemen. Hierdoor kunnen partijen met een laag beveiligingsniveau toch eenvoudig participeren in Suwinet en hoeven partijen die slechts een kleine set van mindergevoelige gegevens afnemen zich niet te conformeren aan een hoog beveiligingsniveau. Daarentegen dienen partijen die zeer privacygevoelige gegevens verwerken en aan stringente beveiligingseisen moeten voldoen verplicht een audit te laten uitvoeren. Bij een gedifferentieerde aanpak is het belangrijk om gezamenlijk afspraken te maken over de differentiaties en de naleving ervan. Een aandachtspunt daarbij is wie verantwoordelijk wordt voor het beoordelen en vaststellen

van een bepaald beveiligingsniveau.

- Zorg voor een eenduidig en door alle partijen gedragen beveiligingsbeleid in Suwinet. Partijen die gegevens leveren via Suwinet, burgers en de verantwoordelijke minister zijn allemaal gebaat bij duidelijkheid over de beveiliging van gegevens door afnemers. Die duidelijkheid kan worden verschaft door het eenduidig vastleggen (en bewaken) van een stelselbreed basisniveau voor informatiebeveiliging met daar bovenop een aantal concrete niveaus om differentiatie mogelijk te maken. Het vereiste beveiligingsniveau dient goed afgestemd te worden op de aansluitvoorwaarden, evenals op de algehele informatiehuishouding en de beveiliging daarvan van de afnemers – echter zonder concessies te doen ten aanzien van het vereiste minimumniveau van beveiliging. Om het basisniveau ook daadwerkelijk geïmplementeerd te krijgen moet gezorgd worden voor draagvlak op zowel uitvoerend als bestuurlijk niveau. Het ligt daarbij voor de hand een meer generiek normenkader te definiëren dat minder Suwinet-specifieke eisen kent waardoor draagvlak voor adoptie sneller te creëren is en er bovendien minder kosten mee gemoeid zullen zijn. Neem deze punten op in een nieuw Normenkader. Zorg dat partijen zich gebonden voelen aan dit Normenkader en er verantwoording over afleggen. Daartoe zal het (wettelijk) afdwingbaar moeten worden, zonodig via een escalatieladder met sancties als boetes, naming en shaming, afsluiten, etc.
- Zet beleid uit over hoe om te gaan met het nieuwe werken (thuis- en flexwerken, gebruik van mobiele platformen) in Suwinet.
- Regel dat alle gegevensuitwisselingen via Suwinet ketenbreed versleuteld zijn.
- Regel processen in om het bewustzijn van de privacyrisico's bij professionals op een continue manier te onderhouden en te verbeteren. De mens blijft een zwakke schakel en vergt vanuit beveiligingsperspectief blijvende aandacht.

3.3 LIMITERING VAN HET VERZAMELEN VAN GEGEVENS

Dit principe gaat over het niet 'zomaar' verzamelen van gegevens. Er moet een grondslag zijn, en dat kan betekenen dat toestemming nodig is van de betrokkene (art. 8 WBP). Los van deze specifieke eisen moet de verwerking sowieso behoorlijk en zorgvuldig zijn (art. 6 WBP).

Suwinet maakt het verzamelen van gegevens een stuk eenvoudiger, doordat het de aangesloten partijen een laagdrempelige mogelijkheid biedt om gegevens van andere aangesloten partijen te raadplegen. Er zijn daarom (ook) op stelselniveau waarborgen nodig om ervoor te zorgen dat uitwisselingen van gegevens een wettelijke grondslag hebben. De Suwipartijen wisselen onderling vrijwel uitsluitend gegevens uit op basis van de verplichting uit de Wet Suwi om dat te doen. Ook structurele uitwisselingen met niet-Suwipartijen zijn altijd gebaseerd op een wettelijke grondslag.

Het vereiste van een behoorlijke en zorgvuldige gegevensverwerking is primair van belang voor de Minister van SZW als stelselverantwoordelijke. Ook al zijn het vooral de Suwipartijen die feitelijk gegevens uitwisselen over het netwerk, de minister heeft los daarvan (uiteraard naast alle andere partijen) een eigen verantwoordelijkheid voor het behoorlijk en zorgvuldig verlopen van gegevensuitwisselingen over Suwinet.

3.3.1 HOE IS HET FORMEEL GEREGELD

Gegevensuitwisseling is via een aantal artikelen in de op Suwinet toepasbare wet- en regelgeving geregeld:

- Art. 62 lid 1 Wet Suwi: De Suwipartijen verstrekken elkaar alle binnen het sociale domein benodigde gegevens.
- Art. 5.19 Besluit Suwi: Suwinet wordt in ieder geval gebruikt voor gegevensuitwisseling tussen de Suwipartijen met het oog op eenmalige gegevensuitvraag en het verstrekken van informatie aan betrokkene.
- Art. 5.20 Besluit Suwi: Er is een Gegevensregister Suwi (SGR). Daarin wordt onder andere opgenomen welke gegevens worden uitgewisseld over Suwinet en wie daarbij de verantwoordelijke is. Het SGR is bijlage XII bij de Regeling Suwi.
- Art. 5.23: De Suwipartijen mogen Suwinet ook gebruiken voor gegevensuitwisseling met andere partijen (vgl. art. 62 lid 2 tweede volzin Wet Suwi). Daar moeten ze dan wel een overeenkomst voor sluiten met een dergelijke partij.
- Art. 6.5 Regeling Suwi: de overeenkomst moet voldoen aan het aansluitprotocol Suwinet (bijlage III).

3.3.2 WELKE MAATREGELEN ZIJN GETROFFEN?

In Suwinet zijn de gegevens gedistribueerd opgeslagen bij de verschillende partijen. De relevante gegevens worden verzameld via de verwijsindex van de IB- of BKWI-broker alvorens ze ontsloten worden via Suwinet. Er worden in Suwinet nergens onnodig gegevens van burgers verzameld of bewaard. Wel worden er gegevens over het gebruik van Suwinet verzameld voor verantwoordingsdoeleinden en rapportages.

3.3.3 WELKE KWETSBAARHEDEN ZIJN ER?

Gemeenten hebben voor het uitvoeren van hun taken gegevens nodig uit alle verschillende leefdomeinen. Meer en meer vindt daar integratie van gegevens plaats om professionals efficiënter hun werk te laten doen en om de klant beter te kunnen helpen.

Een applicatie als MensCentraal voorziet in deze behoefte van veel gemeenten door integrale informatievoorziening aan te bieden. De door MensCentraal ontsloten informatie komt uit verschillende lokale en landelijke bronnen waaronder het DKD van Suwinet.

In 2011 is het CBP in Spijkenisse een onderzoek gestart naar de gemeentelijke applicatie MensCentraal. Het CBP heeft de applicatie niet feitelijk onderzocht, maar heeft op basis van verzamelde informatie wel een aantal algemene constateringen gedaan ten aanzien van de bepalingen uit de Wet bescherming persoonsgegevens (Wbp). Een van de constatering van het CBP betrof het verzamelen van persoonsgegevens. Op basis de informatie die bij CBP bekend was, is geconstateerd dat de doeleinden van verwerking bij MensCentraal zeer ruim worden geformuleerd. De doeleinden zijn volgens het CBP daardoor niet welbepaald en uitdrukkelijk omschreven. De beheerder van MensCentraal heeft hierop aangegeven dat het verzamelen van informatie in MensCentraal gebonden is aan welbepaalde en uitdrukkelijk omschreven doeleinden[28]. Deze doeleinden zijn in MensCentraal vastgelegd in de

[28] Antwoord van MensCentraal op het onderzoek van CBP bij de gemeente Spijkenisse, zie http://www.menscentraal.com/antwoord-op-onderzoek-cbp-bij-gemeente-spijkenisse.

diverse documenten die gemeenten en hun partners kunnen gebruiken bij het inrichten van MensCentraal. Per gegeven c.q. gegevensgroep is vastgelegd voor welk doeleinde de gegevens gebruikt mogen worden. Daarnaast zijn er volgens de beheerder binnen MensCentraal afdoende mogelijkheden (ondersteund met standaard inrichting) ingebouwd om alleen gebruik voor deze doeleinden te faciliteren. Er zijn diverse autorisatieprofielen, ingebouwde beveiligingsmaatregelen, mogelijkheden om taken en signalen automatisch dan wel handmatig te anonimiseren, verwijderen dan wel niet te tonen en het loggen van gebruik om oneigenlijk gebruik te voorkomen. Omdat MensCentraal hierover (zelf of via de gemeenten als verantwoordelijke partij) niet rapporteert aan de security officer van Suwinet, is het vanuit ketenperspectief onduidelijk voor de andere partijen welke autorisatieprofielen dit zijn en hoe deze aansluiten op die van Suwinet en welke ingebouwde beveiligingsmaatregelen getroffen zijn en of deze conform de Verantwoordingsrichtlijn en het Normenkader zijn.

De privacyrisico's aangaande het opslaan van gegevens over het gebruik van Suwinet door professionals zijn beperkt. Wel valt uit handelingen van bepaalde professionals (zoals opsporingsambtenaren) met betrekking tot opvragingen van gegevens over een bepaald persoon af te leiden of deze iets te verbergen heeft. Een soortgelijke situatie speelt ook in de zorgsector: het feit dat een oncoloog het medisch dossier van iemand heeft geraadpleegd is een privacygevoelig gegeven.

3.3.4 ANALYSE EN BESCHOUWING

Binnen Suwinet vindt nauwelijks verzameling van gegevens plaats. Wel is er een groeiende behoefte aan meer integrale informatievoorziening bij de afnemende partijen. Om dit op een betrouwbare manier in te richten is de verantwoordelijkheid van de afnemende partij en niet van het Suwinet stelsel. Dit geldt ook bij het uitbesteden van de integrale informatievoorziening aan derden zoals de dienstenaanbieder van MensCentraal. Belangrijk is echter wel dat transparant blijft richting Suwinet op welke manier de beveiliging en privacy van de gegevens geborgd wordt en dat dit in overeenkomst is met de richtlijnen van Suwinet hiervoor (zie verder ook het privacyrisicogebied Transparantie in sectie 3.8 en Nieuwe ontwikkelingen in sectie 4.1).

Bij integrale informatievoorziening is functiescheiding van essentieel belang om de privacy van de klant te borgen. Daarbij kan gedacht worden aan een regisseur die een hoog niveau overzicht heeft van de situatie van de klant (dat deze heeft gewerkt, dat deze een uitkering heeft, etc.), maar die niet alle details weet. De professional heeft meer informatie nodig, maar alleen voor dat deel van de uitvoering waarvoor zij verantwoordelijk is. Om een dergelijke functiescheiding te realiseren is het zorgvuldig toekennen van de rollen en de daarbij behorende autorisaties aan functies binnen de organisatie erg belangrijk. Bij de grotere partijen met meerdere professionals zal functiescheiding eenvoudiger te realiseren zijn dan bij een kleine organisatie waar vaak één iemand alle rollen en rechten heeft. Suwinet kent een centrale autorisatiestructuur gebaseerd op rollen welke weer gebaseerd zijn op een gegevensset waar de rol toegang toe heeft om de wettelijke taak uit te voeren. Vanuit stelsel wordt echter geen functie-autorisatiestructuur voorgeschreven omdat dit mede de inrichting van de primaire processen en de ondersteunende organisatie daarvan binnen afnemende organisaties bepaald. Dit is de verantwoordelijkheid van de gebruikende organisatie. De vraag is wel of de huidige centrale autorisatiestructuur voldoende fijnmazig is om functiescheiding te faciliteren.

Gegevens over het gebruik van Suwinet worden op een integere manier gebruikt. Hoewel niet iedereen zomaar bij de log-gegevens kan, zijn extra maatregelen vereist om onomstotelijk te kunnen aantonen wie wat en wanneer gedaan heeft. Voor de standaard rapportages op basis van de log-gegevens worden gegevens geanonimiseerd. Specifieke rapportages kunnen alleen door daartoe bevoegde personen worden opgevraagd.

3.3.5 RISICOMITIGERENDE MAATREGELEN

In het kader van integrale informatievoorziening is het raadzaam om gezamenlijk te verkennen welke mogelijkheden er zijn om de autorisaties binnen Suwinet fijnmaziger (bijvoorbeeld meer rollen of het hanteren van een hiërarchie in de rollen) te maken zodat ze beter aansluiten bij de functieprofielen van afnemende partijen en er op basis van need-to-know inzage verstrekt kan worden. Handvatten hiervoor dienen, op basis van gezamenlijke afspraken, vanuit Suwinet aangereikt te worden; de invulling ervan zal door de individuele Suwipartijen zelf vormgegeven moeten worden. Gerelateerd hieraan zijn ook de aanbevelingen in de twee volgende risicogebieden over limitering van het gebruik van gegevens en doelbinding.

Met de toenemende informatiedichtheid in Suwinet dreigt er intransparantie over wie welke gegevens verzamelt en met welk doel dat gebeurt. Maatregelen om transparantie te creëren worden beschreven in sectie 3.8.

Borg dat alle log-records in bestanden op 'write-only' media worden weggeschreven. Daarmee kan BKWI bij eventueel misbruik ook daadwerkelijk onomstotelijk aantonen wie, wanneer, wat heeft gedaan/geraadpleegd.

3.4 LIMITERING VAN HET GEBRUIK VAN GEGEVENS

3.4.1 HOE IS HET FORMEEL GEREGELD?

Het gebruik van gegevens is gebaseerd op een gesloten verstrekkingenregiem. De wettelijke kaders hiervoor zijn zoals al aangegeven in sectie 3.3.1.

3.4.2 WELKE MAATREGELEN ZIJN GETROFFEN?

Een viertal maatregelen zijn genomen om het gebruik van gegevens te beperken: berichten op maat, filtering, autorisaties en aansluitvoorwaarden.

Al enige tijd wordt er binnen Suwinet gewerkt aan het verbeteren van de granulariteit van de gegevensuitwisseling. Deze inspanning heeft vorm gekregen in het maken van afspraken met leveranciers om grote berichten te splitsen in kleinere, meer gespecificeerde berichten. Zo is het UWVRe-intergratie bericht opgesteld en in productie genomen. Daarnaast worden er per afnemer berichten op maat gemaakt. Hierbij levert de BKWI-broker alleen die gegevens door die in het maat-bericht staan. Ook hiervan zijn de eerste berichten in gebruik genomen. Vooral voor inlezende applicaties zijn berichten op maat wenselijk om hergebruik van gegevens voor andere doelen te beperken.

In sommige gevallen worden berichten door BKWI op maat gemaakt. Een voorbeeld is het relatief grote UDP4 bericht dat BKWI ontvangt van UWV. BKWI verwijdert uit het ontvangen UDP4 bericht aan aantal gegevens omdat deze niet

doorgegeven mogen of hoeven worden richting de afnemer. De leverancier bepaald welke gegevens dat betreffen; BKWI zorgt voor de uitvoering ervan. Het nadeel van deze aanpak is dat onnodig teveel bronsystemen van het UWV worden bevraagd wat de performance niet ten goede komt. Bovendien vergroot een dergelijke onnodige uitwisseling van gegevens (tussen BKWI en UWV) het risico op verlies van confidentialiteit en integriteit de gegevens en eventuele reputatieschade.

Om de proportionaliteit te garanderen biedt BKWI een filtermechanisme als dienst aan waarmee de te raadplegen gegevens nader kunnen worden beperkt tot de doelgroep. Dergelijke filters werken op basis van door de inlezende of inkijkende organisatie zelf opgestelde white- of blacklists. Zo zijn er bijvoorbeeld blacklists waarin VIPs, bekende Nederlanders of eigen collega's[29] staan. Whitelists worden vaak gevuld op basis van werkvoorraad door de afnemer zelf.

De toegang tot de gegevens in Suwinet Inkijk wordt bepaald door de rol(len) van de professional. Een rol geeft toegang tot een pagina in Suwinet Inkijk waarin een voor die rol op maat gemaakte set gegevens staat dat nodig is voor het uitvoeren van een wettelijke taak. Rollen zijn gekoppeld aan pagina's en niet aan gegevens binnen pagina's. De rollen worden centraal gedefinieerd en beheerd. Er wordt centraal echter geen functie-autorisatiestructuur voorgeschreven omdat dit mede de inrichting van de primaire processen en de ondersteunende organisatie bepaald.

Voor gegevensuitwisselingen met niet-Suwipartijen geldt het aansluitprotocol. Hierin zijn voorwaarden opgenomen als het hebben van een beveiligingsplan waarin de aan te sluiten partij aantoont passende maatregelen te hebben genomen om misbruik van ontvangen gegevens te voorkomen, voor het uitvoeren van een strikt account- en autorisatiebeleid, en voor het loggen van activiteiten om misbruik te detecteren. Log-gegevens dienen op verzoek van de leverancier verstrekt te kunnen worden, maar hier wordt in de praktijk nauwelijks gebruik van gemaakt. Indien de leverancier van persoonsgegevens misbruik constateert en/of constateert dat de aansluit- en gebruiksvoorwaarden niet worden nageleefd, heeft deze het recht deze vorm van gegevensverstrekking te beëindigen.

3.4.3 WELKE KWETSBAARHEDEN ZIJN ER?

Een aantal kwetsbaarheden is te identificeren ten aanzien van het gebruik van gegevens:

- De reikwijdte van Suwinet-Inkijk is groot. Een groot aantal gebruikers heeft toegang tot relatief veel gegevens van relatief veel klanten. De Klant Algemeen pagina bijvoorbeeld is voor alle GSD medewerkers toegankelijk en bevat o.a. NAW gegevens, geboortedatum, BSN en geslacht. De doelbinding en proportionaliteit staan daardoor onder druk. Het is mogelijk om op basis van BSN of via zoeksleutels zoals postcode, huisnummer en geboortedatum of naam en geboortedatum persoonsgegevens van alle geregistreerde burgers te zien. De toegang van gebruikers tot gegevens die zij voor hun taken niet nodig hebben moet daarom beperkt worden.
- Door de huidige autorisatiestructuur kan het voorkomen dat bij het raadplegen van de persoonsgegevens van medebewoners er teveel onnodige of zelfs ongewenste informatie is getoond.[30]

[29] Om stalking door collega's te voorkomen.
[30] Het jaarverslag 2012 van BKWI maakt melding van een dergelijk incident.

- Teveel stapelen van autorisatierollen waardoor de proportionaliteit van de gegevensverstrekking onder druk komt te staan. Dit blijkt uit de Monitor van Suwinet, verschillende interviews en onderzoek van de inspectie SZW. Verschillende grote gemeenten met in principe voldoende medewerkers om functiescheiding te realiseren zijn hierop aangesproken. Voor kleine gemeenten, waar een handvol medewerkers zich bezig houdt met het uitvoeren van de taken op het terrein van werk en inkomen, is het niet te voorkomen dat in één persoon meerdere rollen worden verenigd. In dat geval zal meer vertrouwd moeten worden op de integriteit van de betreffende medewerker.
- Het toekennen van autorisaties aan gebruikers voor het gebruik van gegevens is niet eenduidig en gaat ten koste van de transparantie richting te leveranciers omdat functies en de toegekende Suwinet autorisatierollen bij afnemende partijen kunnen verschillen. Zelfs bij identieke functies in verschillende organisaties kunnen er verschillende Suwinet autorisaties bestaan. Deze kwetsbaarheid is gerelateerd aan dat van MensCentraal dat ook een eigen autorisatiebeleid heeft voor het ontsluiten van lokale gegevensbronnen (zie sectie 3.3.3).
- Het beëindigen van een gegevensverstrekking in het geval van geconstateerd misbruik of nalatigheid is niet triviaal. Vaak is er spraken van een (wettelijke) leverplicht door de leverancier. Alternatieve vormen voor gegevensverstrekking zijn nauwelijks beschikbaar en zo die er zijn is het onduidelijk in welke mate ze voldoen aan de privacyrandvoorwaarden. Het versturen van de gegevens per post zou bijvoorbeeld een alternatieve vorm kunnen zijn in het geval van een afsluiting van Suwinet. De vraag is of een dergelijke manier van gegevensuitwisseling veel veiliger is. Bovendien neemt dit het risico op toekomstig misbruik of nalatigheid niet weg; daarvoor zal de betreffende organisatie eerst zelf de zaken op orde moeten krijgen.

3.4.4 ANALYSE EN BESCHOUWING

Over het algemeen is het limiteren van het gebruik van gegevens binnen Suwinet goed geregeld. Er zijn hiervoor verschillende maatregelen getroffen. Deze maatregelen dienen verder geoptimaliseerd te worden en kunnen breder ingezet worden ter verdere verbetering van hun effectiviteit.

Betreffende de reikwijdte is het verstandig maatregelen te nemen om deze effectief te beperken. Filters zijn hiervoor een nuttig middel. Op dit moment maakt Suwinet gebruik van relatief eenvoudige filters op basis van black- en whitelists van bijvoorbeeld VIPs, eigen collega’s of werkvoorraadlijsten. Er zijn ook meer intelligente filters die op basis van een leeftijd afgeleid van een geboortedatum snappen dat het geen zin heeft studiefinancieringsgegevens op te vragen, die recidivegegevens pas tonen nadat het filter heeft gezien dat er daadwerkelijk meerdere fraudevorderingen openstaan, die werken op basis van whitelists van 'mensen binnen de eigen gemeente' en mensen waarvoor de leverancier überhaupt gegevens heeft, of die aan de hand van meer business rule-gedreven lists bepalen of iemand tot een bepaalde doelgroep behoort. Bijvoorbeeld iemand met veel vermogen of inkomen hoeft in principe niet door een sociale dienst bekeken te worden.

Het inzetten van dergelijke filters zorgt voor betere proportionaliteit doordat nadere technische invulling wordt gegeven aan het 'need-to-know' principe. Daarnaast kan het flinke efficiëntiewinst opleveren doordat onnodige informatie-uitwisseling wordt voorkomen. Zorgvuldigheid bij het aanbrengen van de filters is zeer belangrijk. Het

genoemde voorbeeld van de vermogende persoon veranderd als deze persoon een ex-partner met alimentatieverplichtingen richting een bijstandsgerechtigde is: dan mag zijn dossier wel door de sociale dienst bekeken worden.

De verantwoordelijkheden voor de filters dienen daarnaast goed belegd te zijn. Op dit moment bepalen vooral de leveranciers de filters. De intelligente filters hebben in veel gevallen minder met de leverancier te maken en meer met de afnemers. Veelal zal de intelligentie in de filters aan de hand van de wettelijke kaders, het doel en de doelgroep van het primaire proces, en gezamenlijke afspraken tussen de stelselpartijen bepaald worden.

Het ‘need-to-know’ principe is een handig middel om autorisatie op te baseren. Hieraan kan invulling gegeven door het principe van ontkoppeld koppelen. Daarmee wordt bedoeld dat de ontvanger niet een hele set aan gegevens ontvangt waaruit hij zelf de informatie moet afleiden die hij nodig heeft. In plaats daarvan wordt eerder in de keten deze informatie automatisch uit de gegevens gehaald. De gebruiker ontvangt dan alleen de afgeleide informatie, en niet de daaraan ten grondslag liggende gegevens.

Voorbeelden van ontkoppeld koppelen zijn het geven van een antwoord op de vraag of iemands loon hoger is dan een bepaalde grenswaarde (in plaats van het verstrekken van alle loongegevens), het bevestigen dat iemand ouder is dan 18 (in plaats van zijn geboortedatum te verstrekken), of het verstrekken van een indicatie dat er sprake is van recidive (in plaats van het beschikbaar maken van alle fraudevorderingen).

Het spreekt voor zich dat op deze algemene werkwijze uitzonderingen mogelijk moeten zijn. Professionals met bijzondere bevoegdheden (bijvoorbeeld handhavers) moeten vaak wel kunnen doorklikken naar specifieke gegevens om verder te kunnen speuren. Ook in geval van een bezwaar of beroep kan dat nodig zijn. Echter, het merendeel van de professionals heeft informatie nodig, geen gegevens.

Grootschalig gebruik van ontkoppeld koppelen heeft grote privacyvoordelen. Het betekent echter ook een behoorlijke paradigmaverschuiving binnen het Suwistelsel. De mogelijkheden en impact ervan verdienen het echter zonder meer om nader verkend te worden.

Betreffende de autorisatiekwetsbaarheden valt het volgende op. De huidige autorisatierollenstructuur van Suwinet lijkt te grofstoffelijk. Zoals al eerder opgemerkt is een fijnmazigere aanpak wenselijk waarbij makkelijker deeloverzichten van de huidige gegevenssets gecreëerd kunnen worden die beter aansluiten bij de eigen rollen en functies van de afnemende partij. Hiermee wordt ook de eenduidigheidskwestie van de rollen ondervangen. Het stapelen van rollen is de verantwoordelijkheid van de afnemende partij. De vraag die hierin ook speelt is of de fijnmazigere autorisatie-aanpak centraal voorgeschreven moet worden of zoals nu decentraal deels vrijgelaten moet worden.

Voor de aansluitvoorwaarden betekent dit het toevoegen van voorwaarden aangaande het melden van incidenten. De huidige aansluitvoorwaarden zijn te karakteriseren als summier en op hoog niveau. Het verzwaren ervan kan bijdrage tot het wegnemen van zorgen die bij de aanleverende partijen over het gebruik van de gegevens door met

name inlezende applicaties weg te nemen. Inspiratie voor het aanscherpen van de aansluitvoorwaarden kan gehaald worden uit die van andere samenwerkingsverbanden waarin beveiliging en vertrouwen essentieel zijn. Voorbeelden van de dergelijke samenwerkingsverbanden zijn eHerkenning[31] voor authenticatie van bedrijven richting de overheid en de SURFfederatie[32] voor herbruikbare identiteiten in het hoger onderwijs. Op basis van de aansluitvoorwaarden van deze samenwerkingsverbanden stellen wij voor de aansluitvoorwaarden van Suwinet-Inlezen de volgende herzieningen en aanscherpingen voor:

- Looptijd van de overeenkomst vaststellen; na afloop kan de overeenkomst geëvalueerd worden en opnieuw worden afgesloten.
- Verplichtingen zoals het inrichten van een helpdesk, specificeren van de gegevens welke gelogd dienen te worden door de inlezende applicatie, doorgeven van log-gegevens aan BKWI op maandelijkse basis, dat het de aansluitende partij vrij staat verplichtingen te delen met derden onder verantwoordelijkheid van de partij. Eventueel de Keten-SLA en het Normenkader waaraan voldoen moet worden expliciet benoemen. Mogelijk ook de verplichtingen van BKWI/IB tegenover de aangesloten partij benoemen.
- Rapportage en concretisering hiervan: de inlezende partij rapporteert maandelijks over het aantal gebruikers van de inlezende partij, hun autorisaties/rollen, en incidenten die hebben plaatsgevonden.
- Privacy: de inlezende partij gebruikt de verstrekte informatie slechts voor het doel waarvoor deze informatie is verstrekt. Aantoonbare maatregelen moeten zijn getroffen om persoonsgegevens adequaat te beschermen.
- Incident melding: er is beschreven wat te doen in het geval van een incident.
- Sancties: opschorting van de inleesdienst door de leverende partij in geval de inlezende partij niet handelt conform de voorwaarden uit de overeenkomst of ingeval Suwinet schade ondervindt van een door aan de inlezende partij verwijtbare situatie. Opzegging van de overeenkomst zal lastiger worden vanwege het wettelijke kader wat gebruik van Suwinet verplicht stelt.
- Eventuele aanvullende bepalingen. Hierbij kan gedacht worden aan het niet kunnen overdragen van rechten of verplichtingen uit de overeenkomst aan een andere partij zonder schriftelijke toestemming van de andere partij. Ook denkbaar is het opleggen van beperkingen voor het gebruik van inlezende applicaties vanaf mobiele platformen of thuis-PCs.

Afstemming met het Normenkader dient hierbij plaats te vinden om te voorkomen dat er dingen dubbel gedaan worden. Verwijzen vanuit de aansluitvoorwaarden naar het Normenkader voor specifieke voorwaarden is daarbij een optie. Echter, omdat niet alle partijen gebonden zijn aan het huidige Normenkader is het verstandig de aansluitvoorwaarden te verzwaren.

3.4.5 TE TREFFEN RISICOMITIGERENDE MAATREGELEN

De volgende maatregelen stellen we voor om de privacyrisico's betreffende het gebruik van gegevens te beperken:

- Optimaliseer het gebruik van gegevens door het toepassen meer en intelligentere filtering.
- Verken de mogelijkheden en impact van meer fijnmazige autorisatierollen of een andere autorisatiestructuur

[31] Gebruiksvoorwaarden eHerkenning, zie http://www.lansigt.nl/sites/default/files/Gebruiksvoorwaarden_eHerkenning.pdf of https://www.zlogin.nl/gfx_content/gebruikersvoorwaarden_zlogin_eherkenning.pdf.
[32] Aansluitovereenkomst SURFfederatie, 12 mei 2010, zie http://www.surfnet.nl/nl/Thema/SURFfederatie/documentatie/template_contract/Pages/Default.aspx.

in Suwinet. Meer fijnmazigheid geeft meer controle over het gebruik van gegevens; wellicht bieden rule-based of hiërarchische rolgebaseerde autorisatiestructuren betere mogelijkheden voor gecontroleerde toegang tot gegevens. Het stapelen van rollen blijft de verantwoordelijkheid van de individuele organisatie. Het opstellen van richtlijnen/best practices voor het gecontroleerd stapelen valt te overwegen om te voorkomen dat organisaties in de fout gaan.

- Verzwaar de aansluitvoorwaarden door extra voorwaarden mee te nemen aangaande het limiteren van het gebruik van gegevens. Het opnemen van sancties is daarvan een onderdeel. Onderzoek hiernaar is nodig aangezien er ook voldaan moet worden aan andere wetgeving zoals de WEU waarop de burger een beroep kan doen. Er moeten dan ook serieuze alternatieven zijn of komen en deze moeten ook voldoende privacy garanties kunnen bieden. Daarnaast is bepalend wie daarin gemandateerd is / wordt om te bepalen of er wordt gesanctioneerd.

3.5 DOELBINDING

3.5.1 HOE IS HET FORMEEL GEREGELD?

Doelbinding houdt in dat gegevens alleen maar mogen worden verwerkt als er een wettelijke basis voor is en is een van de zeven beginselen van de Wbp.

Conform artikel 74 van de wet Suwi dient er altijd een toets plaats voor het bepalen van de wettelijke grondslag en doelbinding van gegevensuitwisseling.

3.5.2 WELKE MAATREGELEN ZIJN GETROFFEN?

Om doelbinding voor Suwinet te garanderen zijn er enerzijds een aantal technische en organisatorische maatregelen getroffen. Daarnaast wordt er een beroep gedaan op het gedrag en de integriteit van de betrokken professional.

Het Suwi Gegevensregister (SGR) is een van die maatregelen. Het SGR legt de structuur van de Suwinet gegevensuitwisseling vast in de vorm van definities, formaten en mogelijke waarden van het betreffende gegeven. In het kader van de Wet Eenmalige Uitvraag van gegevens (WEU) is een overzicht van SGR gegevens ten opzichte van de wettelijke grondslag beschikbaar. Dit met het doel voor zowel de burgers als de professionals, de gegevensuitwisselingen binnen Suwinet zodanig transparant te maken dat inzichtelijk wordt op basis van welke wettelijke grondslag (doelbinding) welke gegevens (proportionaliteit) door wie (verantwoordelijke) aan wie (verwerker) worden geleverd en zodoende partijen aanspreekbaar te maken op naleving van de WBP (Wet Bescherming Persoonsgegevens). Er is een overzicht beschikbaar waarin staat aangegeven welke gegevens een partij (bv GSD) wettelijk mag gebruiken voor inlezen (of voorinvullen)[33].

Daarnaast zijn er, vooral voor inlezende applicaties en afhankelijk van het doel ervan een aantal berichten gedefinieerd die ervoor zorgen dat de juiste gegevens worden gecommuniceerd. Voordat een afnemende niet-Suwipartij toestemming krijgt om bepaalde gegevens te mogen gebruiken vindt er altijd een toets plaats voor het bepalen van de wettelijke grondslag en doelbinding (conform artikel 74 van de wet Suwi).

[33] Matrices voor gebruik van gegevens, zie http://www.bkwi.nl/producten/suwinet/suwinet-inlezen/matrices/.

Vooral betreffende de doelbinding voor het gebruik van gegevens treedt vaak een spanningsveld op met de efficiëntievoordelen, kostenbesparingen en betere dienstverlening die door (rijkere) gegevensuitwisseling te behalen zijn. De focus op doelbinding die per wet is vastgelegd leidt tot vaak starre aanpakken die de efficiëntie en meerwaarde van automatische verwerking van gegevens in de weg staan. Gegevens van bijvoorbeeld de RDW die voor een bijstandsaanvraag geleverd worden, mogen niet hergebruikt worden door de betreffende gemeente voor het verstrekken van een parkeervergunning. Vooral de inlezende partijen ervaren dit als een belemmerende en op onbegrip stuitende factor. Inmiddels heeft dit geleid tot een incident waarbij een afnemer onrechtmatig (her)gebruik van ingelezen gegevens heeft gemaakt [34]. Dit kan, ondanks het feit dat de verantwoordelijkheid voor het juist gebruiken van gegevens bij de afnemende partij ligt, het vertrouwen in het stelsel ondergraven. Toezicht op het gebruik van gegevens is noodzakelijk om dit soort incidenten te voorkomen.

Een dergelijk toezicht vindt deels plaats door middel van het traceren van gegevensuitwisseling door BKWI. Bij Suwinet Inkijk is dit goed te doen door BKWI; bij Suwinet Inlezen is dat wat lastiger. De huidige aanpak bij Inlezen is de berichtuitwisseling te traceren op basis van een applicatie ID, een gemeente ID en een IP-adres, maar dat is niet optimaal om doelbinding aan te kunnen tonen. Gewenst is om te weten welke afdeling (bijvoorbeeld Burgerzaken), van welke gemeente en welke applicatie (bijvoorbeeld applicatie ID) voor welk doel (bijvoorbeeld Parkeervergunning) en wanneer (datum en tijd) gegevens heeft opgevraagd. Gegevensverstrekkers hebben geen behoefte om op persoonsniveau het gebruik te zien (bijvoorbeeld welke gemeenteambtenaar); dat is veel te fijnmazig voor hen. Wat ze wel willen weten is hoeveel personen geautoriseerd zijn om hun gegevens te raadplegen en hoeveel gegevensberichten uitgewisseld zijn om globaal te kunnen bepalen of dit proportioneel is. Maar alleen de inlezend organisatie heeft deze gegevens waardoor het voor BKWI lastiger wordt om hierover te rapporteren naar de aanleverende partijen (zie verder ook sectie 3.8 over transparantie).

De Suwipartijen zijn zelf verantwoordelijk voor het autoriseren en registreren van gebruikers van Suwinet-Inkijk en Suwinet-Inlezen. Echter, uit de Monitor blijkt dat in het accountbeheer vervuiling is opgetreden doordat er meer accounts zijn dan actieve gebruikers. Hierdoor ontstaat het risico dat professionals die uit dienst zijn getreden nog steeds een kunnen account hebben of dat accounts van voormalige medewerkers kunnen worden gebruikt door andere medewerkers. Ook blijkt dat er bij sommige afnemers relatief weinig spreiding is in de verdeling van de autorisaties onder de professionals. Er vindt stapeling van autorisaties plaats waardoor professionals meer gegevens kunnen zien dan nodig is en ten koste gaat van de doelbinding. Het toewijzen en beëindigen van accounts en het toekennen van autorisaties is conform de ketenafspraken de eigen verantwoordelijkheid van elke partij en daarmee geen stelsel issue. Er kan wel overwogen worden om vanuit het stelsel instrumenten aan te bieden die partijen de mogelijkheid bieden zelf meer inzicht in en controle over de autorisaties te hebben (we verwijzen hier verder naar het risicogebied Toezicht en Handhaving waarin dit verder wordt toegelicht in sectie 3.12).

Tot slot is er het instrument van de uitvoeringstoets welke afgenomen dient te worden bij nieuw/gewijzigd beleid dat buiten het reguliere wetgevingstraject valt. De uitvoeringstoets is een korte contra-expertise van voorgenomen beleid.

[34] Het jaarplan 2012 van BKWI maakt melding van een dergelijk incident waarbij onrechtmatig gebruik van gegevens heeft plaatsgevonden.

In de toets wordt vastgesteld of de beleidsuitvoering goed geborgd is en of de beoogde maatschappelijke resultaten haalbaar zijn.

3.5.3 WELKE KWETSBAARHEDEN ZIJN ER?

Op basis van de getroffen maatregelen en wettelijke kaders zijn een aantal kwetsbaarheden te identificeren:

- Er wordt niet regelmatig geëvalueerd of de gegevenshuishouding van Suwinet, de functionaliteiten en in bredere zin het stelsel zelf zich nog verhouden tot doelbinding en proportionaliteit. Vanuit veranderende wet- en regelgeving, beschikbaarheid van gegevens en inzichten over de noodzaak om over bepaalde gegevens te beschikken is dit wenselijk. De organisatie van een dergelijke periodieke toets zal ingeregeld moeten worden. Het instrument uitvoeringstoets kan hierbij gebruikt worden mits het ruimer in te zetten is, ook voor bijvoorbeeld beleidswijzigingen die niet door wetgeving ingegeven worden en voor ketenbrede evaluatiedoeleinden. Een dergelijke evaluatie kan de effectiviteit van de interactie tussen de ketenpartijen ook verbeteren.
- Aanleverende partijen geven aan dat het door de complexiteit van de wet- en regelgeving rondom Suwinet vaak moeilijk is te bepalen of aan doelbinding en proportionaliteit voldaan wordt. Die voorwaarden hiervoor zijn nogal ‘open’ geformuleerd: “is noodzakelijk voor”. De afnemende partij moet kunnen motiveren waarom de gegevens noodzakelijk zijn en de verstrekkende partij moet hier een beslissing over nemen. Hier zijn geen normen voor gedefinieerd die als houvast kunnen dienen in het maken van een beslissing. Illustratief hiervoor is de discussie over de benodigde gegevensset voor het recidiveregister die al enige tijd gevoerd wordt en resulteert in een vertraging van de implementatie en uitrol van het register.

3.5.4 ANALYSE EN BESCHOUWING

Suwinet wordt regelmatig door de Inspectie of onafhankelijke derde partijen (vaak in opdracht van een Suwi-partij) getoetst op het gebied van privacy en beveiliging. Dergelijke toetsen zijn zelden ketenbreed ingestoken en niet van structurele aard.

De open privacynormen leiden overigens tot veel rechtsonzekerheid. Het is vaak lastig om te bepalen c.q. te weten of aan de wet voldaan wordt met betrekking tot gegevensuitwisseling ten behoeve van een bepaald doel. Dit geldt met name voor partijen die niet vallen onder de Wet Suwi, omdat daarvoor meestal niets specifiek geregeld is. Dat wil overigens niet zeggen dat er geen gronden voor verwerking zijn, alleen dat die niet altijd even duidelijk zijn en soms verkeerd geïnterpreteerd worden. Voorbeelden hiervan zijn de ongeoorloofde uitwisseling van BSNs met partijen in het buitenland zoals in een pilot-project gebeurd is en het gebruik van echte BSNs door software ontwikkelaars voor testdoeleinden. Door het identificerend karakter van het BSN is hiermee de privacy van de burger geschaad. Zie hierover meer in sectie 4.1 over het breder gebruik van Suwinet.

Een factor die ook niet bijdraagt aan duidelijkheid over wat wel en niet mag als het gaat om de uitwisseling van gegevens is de complexiteit van Suwinet. Het is een ingewikkeld stelsel, met veel wet- en regelgeving, verschillende sporen (uitwisselingen tussen Suwi-partijen onderling, maar ook verstrekkingen van niet-Suwipartijen aan Suwipartijen en omgekeerd of via derden die bewerkingen uitvoeren), diverse betrokken partijen met verschillende rollen en belangen, en allerlei procedures, overleggremia en dergelijke. Daardoor kan of wil niet altijd iedereen op de

hoogte zijn van alles wat hij wel zou moeten weten.

De in de laatste twee alinea's besproken problematiek is ook elders onderkend.[35] Zij overstijgt het niveau van Suwinet, en betreft in feite de gehele informatiehuishouding van (met name de uitvoerende tak van) de overheid. Vanuit Suwinet, toch een van de belangrijkste onderdelen van deze informatiehuishouding, zou een richtinggevende bijdrage aan dit debat geleverd kunnen worden.

3.5.5 TE TREFFEN RISICOMITIGERENDE MAATREGELEN

De volgende maatregelen stellen we voor om de doelbinding in Suwinet beter te borgen:

- Laat regelmatig de informatiehuishouding van Suwinet toetsen op doelbinding en de effectiviteit van de geboden functionaliteiten. Doe dit voor zowel Suwi als niet-Suwipartijen. Een goed uitgangspunt hierbij is een vraag-gedreven insteek: laat de afnemende partijen aangeven welke gegevens nodig zijn voor het uitvoeren van een wettelijke taak en toets of dit binnen de kaders van relevantie en proportionaliteit valt.
- Verken de mogelijkheden voor vereenvoudiging van het wettelijk kader van Suwinet en voor verduidelijking van doelbinding en proportionaliteit van de gegevensuitwisseling. Voor dit laatste kan gedacht worden aan het bij nieuwe wetsvoorstellen opnemen van een informatieparagraaf in de Memorie van Toelichting, en zonodig ook van bepalingen in de wet zelf. Daarin dient dan te worden geëxpliciteerd welke gegevensverwerkingen en -uitwisselingen noodzakelijk zijn voor het uitvoeren van de voorgestelde wettelijke bepalingen, wat daarvoor het wettelijk kader is en op welke wijze in passende waarborgen wordt voorzien.[36] Het uitvoeren van een Privacy Impact Assessment zal daarvoor doorgaans de opmaat vormen. Indien overwogen wordt om de gegevensset concreet in de wet op te nemen, is het verstandig om daarbij te linken aan het Suwi Gegevens Register (SGR) zodat geen misinterpretatie kan plaatsvinden en nieuwe diensten sneller uitgerold kunnen worden. Het SGR wordt jaarlijks wettelijk vastgesteld.

3.6 GEGEVENSKWALITEIT EN BESCHIKBAARHEID

3.6.1 WAT IS ER FORMEEL GEREGELD

Het Stelselontwerp geeft aan dat de wederzijdse resultaatverplichtingen over ICT-beheer, onder andere over beschikbaarheid, integriteit en kwaliteit van de data, toegangsbeveiliging en incidenten-en risicobeleid, die worden vastgelegd in de Keten-SLA.

3.6.2 WELKE MAATREGELEN ZIJN GETROFFEN

Zowel de burger als de professional moeten er daarom vanuit kunnen gaan dat deze gegevens correct zijn. De kwaliteit van de gegevens in Suwinet is na een ketenbrede inspanning enkele jaren geleden sterk verbeterd. In een professional onjuistheden in de gegevens waarneemt kan deze laten corrigeren door een terugmeldvoorziening. Inmiddels is het terugmelden aan de Gemeentelijke Basis Administratie (GBA) een wettelijke verplichting. Om dit digitaal te ondersteunen kunnen professionals via Suwinet-Inkijk eenvoudig terugmelden aan de terugmeldvoorziening van de GBA. Naast het instrument terugmelding worden ook andere instrumenten ingezet ter

[35] Wetenschappelijke Raad voor het Regeringsbeleid (2011): *iOverheid* (www.ioverheid.nu). iNUP, Programma Stelsel van Basisregistraties, cluster STOUT (2013):, 'Bij twijfel niet gebruiken?' (http://bit.ly/1f7W2fb).
[36] Vergelijk de brief van 29 oktober 2013 van het College Bescherming Persoonsgegevens aan de minister van BZK (http://www.cbpweb.nl/Pages/pb_20131030_privacyrisico-taken-gemeenten.aspx).

verbetering van de kwaliteit, zoals het koppelen van verschillende bestanden.

De Inspectie SZW heeft de kwaliteit van de gegevens onderzocht en concludeert dat deze voldoende is voor het uitvoeren van wettelijke taken[37]. Wel oordeelt de inspectie dat de Suwipartijen meer belang moeten toekennen aan de stelselbrede borging van kwaliteit van gegevens en dat andere partijen deze gegevens ook moeten kunnen gebruiken.

Er geldt voor Suwinet een SLA (Gezamenlijke elektronische Voorzieningen Suwiketen Service Level Agreement) waarin afspraken staan over responsetijden van systemen, beschikbaarheid van systemen, de ondersteuning door de servicedesk en de behandeling van incidenten en storingen[38]. De SLA gaat uit van resultaatverplichtingen. Over het nakomen van de afgesproken resultaatverplichtingen wordt maandelijks door het BKWI gerapporteerd (op basis van logging en monitoring gegevens) zodat gerichte bewaking, sturing en verbetering van de dienstverlening mogelijk zijn. Opvallend is dat niet alle Suwipartijen de SLA ondertekend hebben. Naast het feit dat die partijen niet aangesproken kunnen worden op een eventuele gebrekkige beschikbaarheid, kan dit resulteren in het gebruik van verouderde en daardoor onjuiste gegevens over de klant. Dit kan tot onterechte privacy-issues leiden.

3.6.3 WELKE KWETSBAARHEDEN ZIJN ER?

De SLA bevat geen afspraken over de kwaliteit van gegevens, en dan met name over de actualiteit ervan. Door verschillende manieren van aanlevering van gegevens (via batches of real-time via een web service) kan de actualiteit verschillen maar heeft dit nauwelijks invloed op de uitvoering van de taken door professionals.

Over het algemeen is de beschikbaarheid van de gegevens conform de SLA. Ook is de communicatie over storingen richting de keten de afgelopen tijd sterk verbeterd. Aan de kant van de leveranciers zijn er soms zorgen over de performance van de systemen. Soms moeten er grote berichten gevuld worden vanuit meerdere systemen bij de leverancier waardoor de beschikbaarheid onder druk komt te staan. Vooral in het licht van de recente Denial of Service aanvallen op banken, overheden en uitvoeringsorganisaties is dit een extra risico. Een dergelijke DoS aanval kan resulteren in het onbereikbaar worden van leverancier van gegevens en hiermee de dienstverlening verderop in de keten belemmeren. Daar komt bij dat, als de aanval eenmaal afgeslagen is, het opstarten van dergelijke gedistribueerde systemen enkele dagen kan duren. Met de in Suwinet steeds verder doorgevoerde kleinere berichten op maat worden dergelijke kwetsbaarheden weggenomen. Daar komt bij dat de verschillende Suwipartijen intensief kennis uitwisselen over dergelijke gevaren en hoe ze op te vangen in de context van het Centrum Informatiebeveiliging en Privacybescherming (CIP[39]), een initiatief van UWV, de Belastingdienst, SVB en DUO. Ook partijen als BKWI en KING zijn aangesloten bij CIP.

Opgemerkt dient te worden dat de kwaliteit van de gegevens nog belangrijker wordt bij inlezende applicaties. Er is een risico dat met dergelijke automatische verwerking gegevens de gevolgen van incorrecte gegevens zich sneller zullen verspreiden in allerlei systemen van verschillende partijen waardoor terugdraaien van gemaakte beslissingen

[37] Bredere kijk op kwaliteit persoonsgegevens gewenst in sociale zekerheid, rapport Inspectie SZW, 2013, zie http://www.rijksoverheid.nl/nieuws/2013/04/18/bredere-kijk-op-kwaliteit-persoonsgegevens-gewenst-in-sociale-zekerheid.html.
[38] De GeVS keten-SLA versie 8.0, zie http://www.bkwi.nl/uploads/media/GeVS_Keten_SLA_8.0-def_merged.pdf.
[39] Centrum Informatiebeveiliging en Privacybescherming (CIP), zie www.cip-overheid.nl.

steeds moeilijker wordt.

De consequentie van het feit dat niet alle Suwipartijen de SLA ondertekend hebben is dat minder zekerheid gegeven kan worden over de accuraatheid van de gegevens: zijn ze up-to-date? Het verwerken van verouderde gegevens kan leiden tot vervelende gevolgen voor de burger en kan zelfs privacy risico's met zich meebrengen: iemand kan onterecht als fraudeur in de systemen komen te staan of het dossier van iemand kan op basis van onjuiste gegevens ingezien worden door professionals die dat normalter niet hadden hoeven zien. De partijen die de SLA niet ondertekend hebben kunnen hierop niet worden aangesproken.

Een ander potentieel risico is het ontbreken van bruikbare testgegevens en testomgevingen. In complexe ketens is de beschikbaarheid van goede ketentestomgevingen (verder genoemd KTO) essentieel. Omdat systemen van de ketenpartijen met elkaar verbonden zijn, kunnen testactiviteiten van de ene ketenpartij invloed hebben op andere ketenpartijen en is het nodig hierover afspraken te maken. Dergelijke KTO's zijn niet of nauwelijks ingericht voor de Suwi-keten. Enkele voorbeelden uit de interviews illustreren dit:

- De testomgevingen van BKWI en IB zijn niet gekoppeld waardoor de berichtuitwisseling tussen de brokers van beide partijen wel eens fout gaat.
- Er zijn geen kwalitatief goede testdata voorhanden waardoor ontwikkelaars van applicaties met echte BSNs (van zichzelf of collega's) gaan testen en hiermee niet volgens de regels werken (privacy risico).
- De kwantiteit van de testdata is beperkt waardoor performance testing onmogelijk is.
- Er is geen afstemming tussen de verschillende ketenpartijen over de testdata.
- Er bestaat een volwaardige testomgeving (de 'keten integratie testomgeving', KIT), maar afnemers en aanbieders hebben dit niet altijd. Testen door afnemers gebeurt vaak in de productieomgeving, of met koppeling naar productiegegevens..
- Het 'agile' ontwikkelproces van verschillende softwareleveranciers sluit niet aan bij de testomgevingen van BKWI/IB. Deze omgevingen gaan er vanuit dat een softwareleverancier met een kant en klare applicatie komt om te test. Met agile ontwikkelprocessen is er de behoefte om al vroegtijdig bepaalde deelfunctionaliteiten te kunnen testen.

3.6.4 ANALYSE EN BESCHOUWING

Op basis van de bovenstaande analyse kan geconcludeerd worden dat het met de kwaliteit en beschikbaarheid van de gegevens redelijk goed zit in Suwinet. Zorgen komen voort uit de performance van sommige vaak wat oudere en gedecentraliseerde back-office systemen, de impact van automatische verwerking van incorrecte gegevens en het ontbreken van een ketenbrede testomgeving met bijbehorende testdata. Het adresseren van de eerste zorg is voor de verantwoordelijkheid van de individuele partijen, de andere twee zorgen zijn wel relevant voor Suwinet als stelsel.

Met betrekking tot het snel doorwerken van incorrecte gegevens in de verschillende systemen bij geautomatiseerde verwerking kan overwogen worden processen in te richten die het de partijen in de keten makkelijker maken om fouten te corrigeren. De hoeft niet per definitie op een geautomatiseerde manier te gebeuren, het kan ook

vormgegeven worden door het organiseren van ketenbrede overlegstructuren waarin professionals deelnemen die kunnen inschatten of sprake is van een moedwillig of ongelukkig incident en die het mandaat hebben om binnen hun organisatie de fouten terug te draaien. Een mooi voorbeeld van samenwerking in de keten is te vinden in de voertuigketen. Het overleg in de voertuigketen is naar aanleiding van een werkcongres in 2009 tot stand is gekomen. In deze overleggen worden de casussen van probleemgevallen besproken. De deelnemers aan deze overleggen zijn business managers die ook betrokken zijn bij het ontwerpen van werkprocessen. De overleggen leiden altijd tot een oplossing, uiteraard niet altijd in het voordeel van de indiener. Wat belangrijk is, is dat er bestuurlijke dekking is: de bestuurlijke wil om probleemgevallen op te lossen.

Voor het testen van informatiesystemen met privacygevoelige persoonsgegevens (voorheen klasse 2), zoals het geval is in de Suwinet, mogen uitsluitend gegevens van fictieve personen gebruikt worden. Om bruikbare ketentesten te kunnen doen, is het noodzakelijk dat dergelijke fictieve personen ‘bekend’ zijn bij alle partijen. M.a.w., er zijn fictieve BSNs nodig met daaraan gekoppeld fictieve gegevens bij GBA, fictieve DigiDs bij Logius, en fictieve dossiers bij de bronleveranciers als UWV en RDW. Deze testset van fictieve BSNs en bijbehorende dossiers zou voldoende groot en divers moeten zijn om degelijke performance testen mee te doen. Het GBA heeft fictieve BSNs maar deze worden, mogelijk door onbekendheid, beperkt gebruikt.

3.6.5 MITIGERENDE MAATREGELEN

Twee maatregelen om de risico’s gerelateerd aan de kwaliteit van gegevens (of het ontbreken ervan) zijn:

- Overweeg om processen in te richten die het de partijen in de keten makkelijker maken om fouten te corrigeren. Verken of hiervoor bestuurlijk draagvlak is.
- Steek meer effort in het inrichten van een ketenbrede testomgeving met bijbehorende testdata van voldoende kwaliteit en grootte. Afstemming tussen de verschillende ketenpartijen is daarbij van belang. Ook dient bekeken te worden of en hoe tegemoet gekomen kan worden aan de agile software-ontwikkelmethoden die sommige leveranciers hanteren en die een andere testmethodiek vereisen.

3.7 RECHTEN VAN BETROKKENEN

3.7.1 WAT IS ER FORMEEL GEREGELD?

Het recht van de betrokkene op inzage, correctie, verwijdering, afscherming, verzet, en geheimhouding van gegevens is een van de basisprincipes van de Wbp. Artikel 33 en 34 van de Wbp geven aan dat de betrokkene geïnformeerd moet worden over gegevensverwerkingen.

3.7.2 WELKE MAATREGELEN ZIJN GETROFFEN?

Via het klantbeeld op mijnoverheid.nl kan de de burger zijn gegevens inzien (dit is overigens een beperkte set aangezien bronhouders de burgers liever op hun eigen mijnportaal ontvangen). Het is mogelijk om incorrecte gegevens te laten wijzigen.

3.7.3 WELKE KWETSBAARHEDEN ZIJN ER?

In 2011 meldt de inspectie SZW dat het binnen de sociale zekerheid in de praktijk niet vanzelfsprekend is dat klanten

geïnformeerd worden over de wijze waarop hun gegevens worden verwerkt en over het feit dat hier bepaalde risico´s aan verbonden zijn: “Het proces rondom het verwerken van persoonsgegevens is over het geheel genomen nog onvoldoende transparant voor de burger.”[40]

In het jaarverslag 2012 van BKWI wordt melding gemaakt van een incident waarbij bij het raadplegen van de persoonsgegevens van medebewoners ook gegevens getoond worden die onwenselijk zijn. Het recht op geheimhouding is hierbij geschonden. Deze kwetsbaarheid is ook benoemd in het risicogebied Limitering van het gebruik van gegevens (sectie 3.4.3).

3.7.4 ANALYSE EN BESCHOUWING

Op het gebied van de rechten van de betrokken is verbetering wenselijk en haalbaar. De vraag is of dit centraal door Suwinet geregeld dient te worden of dat dit overgelaten moet worden aan de individuele partijen. De in Suwinet aanwezige brokers bevinden zich als informatiebrokers in een goede positie om de burger vanuit een centraal punt op een efficiënte manier inzicht te geven over welke organisatie op welk moment en met welk doel gegevens heeft geraadpleegd. De burger hoeft dan niet meer bij alle partijen langs met het verzoek tot inzage. Daarnaast profiteren ook de leveranciers van een centrale informatiebroker, zij worden hierdoor beter ondersteund bij de uitvoering van hun wettelijke taak vanuit de WBP om toezicht te houden op de ter beschikking gestelde gegevens.

Technisch dienen er voorzieningen getroffen te worden om de betrokkenheid te ondersteunen, organisatorisch zal er afstemming plaats moeten vinden over welke gegevens via welke kanaal ontsloten worden om zodoende te voldoen aan de Wbp en alvast klaar te zijn voor de komende Europese Privacy Verordening die nog strengere eisen stelt aan betrokkenheid (zie sectie 4.2).

Een toename van de betrokkenheid van de burger bij gegevensuitwisselingen kent nog een tweetal positieve effecten. Het kan een positief effect hebben op de kwaliteit van de gegevens, omdat de burger dan vaker met zijn eigen gegevens geconfronteerd wordt. Daarnaast beperkt het oneigenlijk gebruik van gegevens door transparantie te bieden aan de burger over het gebruik van hun gegevens. Zij kunnen als het ware meekijken over de schouder van de professional die daardoor zal nalaten gegevens voor andere doeleinden te bevragen. Het spreekt voor zich dat bepaalde gegevens niet inzichtelijk gemaakt worden als er een onderzoek loopt.

3.7.1 MITIGERENDE MAATREGELEN

Verken de mogelijkheden om de burger meer transparantie te bieden rondom de verwerking van persoonsgegevens in Suwinet. Bepaald dient te worden of een centrale voorziening hiervoor wenselijk en haalbaar is, welke partij hiervoor het beste in aanmerking komt en wat de rol van het Ministerie van SZW hierin is. Indien het wenselijk geacht wordt om centraal iets in te regelen dient vervolgens gekeken te worden of alle organisaties hiervoor klaar zijn en dient nagedacht te worden over de communicatie richting de burger. Een groeimodel lijkt het meest passend. Daarbij moet zorgvuldig worden afgewogen hoeveel transparantie geboden wordt en op welke manier(en).Gedacht kan worden aan het versturen van een overzicht van bevragingen naar de berichtenbox van de burger (mijnOverheid.nl).

[40] Inspectie Werk en Inkomen. “Transparante verwerking van persoonsgegevens in het SUWI-domein”. Nota van bevindingen, Programma Informatieprocessen. December 2011.

In het overzicht staat welke partij welke gegevens wanneer heeft geraadpleegd. Een dergelijke versterking van de informatiepositie van de burger komt tegemoet aan het rapport i-Overheid van de WRR en aan de wens van de VNG om meer transparantie te bieden richting de burger.[41]

Naast het gebruik van mijnOverheid.nl kunnen ook andere manieren van informatieverstrekking overwogen worden. Een steeds populairder wordend alternatief zijn de 'personal clouds'. Dergelijke cloud oplossingen stellen de burger/gebruiker vaak centraal en hebben als uitgangspunt dat deze een overzicht en controle heeft over zijn/haar gegevens. Een voorbeeld van een personal cloud oplossing is Qiy[42].

3.8 TRANSPARANTIE

3.8.1 WAT IS ER FORMEEL GEREGELD?

Transparantie is een van de basisprincipes van de Wbp.

Met betrekking tot transparantie zijn er twee uitgangspunten gedefinieerd in het Stelselontwerp:

- Transparantie van gegevensleveringen waarvan het SUWI-gegevensregister (SGR) een onderdeel van is.
- Transparantie over de informatiebeveiliging van de gegevens door middel van de Verantwoordingsrichtlijn en Normenkader.

3.8.2 WELKE MAATREGELEN ZIJN GETROFFEN?

Een cruciaal element van privacy control in de keten is de transparantie van de processen waarmee snel helder wordt of de juiste gegevens uit de juiste bronnen uitsluitend naar de juiste afnemers gaan. Door dit transparant te maken is tijdig ingrijpen en bijsturen mogelijk. Een belangrijk element voor het bereiken van transparantie is hierover gezamenlijk een sluitend stel spelregels af te spreken. Deze spelregels zijn vastgelegd in de Verantwoordingsrichtlijn die tot doel heeft te komen tot gelijkwaardige afspraken over het beheersen van de risico's t.a.v. Suwinet en aangeeft hoe de aangesloten organisaties invulling dienen te geven aangaande de transparantie over de beveiliging van de informatiehuishouding. Met deze transparantie bieden de aangesloten organisaties inzicht aan de registratiehouders en aan elkaar in hoeverre de beveiliging van Suwinet voldoet aan de gestelde eisen. Dit wordt in de vorm van een jaarlijkse verantwoordingsrapportage gedaan en draagt bij aan het onderling vertrouwen tussen de ketenpartijen.

Een sterk middel voor het creëren van transparantie in Suwinet is het monitoren door BKWI van alle gegevensuitwisselingen en het gebruik van accounts via Suwinet Inkijk. BKWI kan hierbij onder andere rapporteren over het onderhoud van accounts, toedeling van autorisaties, gebruik, misbruik, optimaal gebruik van Suwinet-Inkijk, en de aanlevering van gegevens[43]. De log-gegevens geven een beter inzicht op naleving en faciliteren een betere sturing ervan. Daartoe worden op basis van de log-gegevens door BKWI rapportages opgesteld voor de afnemende en aanleverende partijen.

[41] Brief VNG en Divosa aan Tweede Kamer der Staten-Generaal Vaste commissie voor SZW, 9 februari 2012, zie http://www.vng.nl/files/vng/vng/Documenten/actueel/brieven/parlement/2012/20120209_Parlement_BAWI-U201200278.pdf.
[42] Qiy, zie www.qiy.nl.
[43] BKWI handreiking bij de monitor "gebruik Suwinet', zie http://www.bkwi.nl/uploads/media/handreiking_bij_monitor_gebruik_Suwinet_01.pdf.

Hoewel minder uitgebreid dan bij Suwinet-Inkijk, zijn dergelijke log-functionaliteiten ook aanwezig voor Suwinet-Inlezen. De broker kan voor Suwinet-Inlezen bijhouden welke applicatie namens welke partij aan het inlezen is. Standaard rapportages over het gebruik van Suwinet-Inlezen voor afnemende partijen zijn er nog niet.

3.8.3 WELKE KWETSBAARHEDEN ZIJN ER?

Ondanks deze maatregelen zijn er een aantal aspecten die zorgen voor minder transparantie of het moeilijker maken om transparantie te creëren en die het vertrouwen in de keten en de wettelijke doelmatigheid van de gegevensverwerking kunnen ondermijnen.

Ten eerste is het is voor de keten onduidelijk welke informatiebeveiligingsmaatregelen door de individuele partijen genomen zijn voor betrouwbare uitwisseling en verwerking van gegevens. Dit komt doordat de Verantwoordingsrichtlijn en het bijbehorende Normenkader niet door alle organisaties in de keten gedragen worden. Het Normenkader zou een te technische insteek hebben met teveel sectorspecifieke eisen waardoor draagvlak bij verschillende organisaties ontbreekt. Daarnaast zijn gemeenten als Suwipartij niet verplicht zich conform de Verantwoordingsrichtlijn te verantwoorden richting Suwinet. In 2012 bleek het onder coördinatie van BKWI voorgestelde nieuwe concept hiervoor geen oplossing te bieden, zodat het nieuwe concept niet is vastgesteld en de oude richtlijn nog vigerend is. Het gevolg is dat er een onvolledig beeld ontstaat van de beveiliging in Suwinet. Dat blijkt onder andere uit de jaarlijkse samenvattende rapportages hierover van de security officer van BKWI. Andere vormen van verantwoording zijn mogelijk (bijvoorbeeld via jaarverslagen) maar gaan ten koste van een eenduidig beeld van de ketenbrede beveiliging.

Een mogelijkheid om dit inzicht wel te verkrijgen op een eenduidige manier is door middel van een audit verklaring. Een EDP-audit is conform de wet Suwi verplicht voor niet-Suwipartijen die willen afnemen van bijvoorbeeld UWV. Zo kan het voorkomen dat de afdeling belastingdienst van een gemeente een audit zal moeten laten uitvoeren terwijl de sociale dienst van dezelfde gemeente dat niet hoeft omdat zij een Suwipartij is. Een dergelijke ‘ongelijke’ behandeling komt eenduidigheid van de beveiliging niet ten goede. De oorzaak hiervan komt voort uit het feit dat een gemeente een Suwipartij wat betreft de Suwitaken en een niet-Suwipartij is wat betreft niet-Suwitaken. Deze dubbelrol is in dit geval praktisch onwerkbaar, aangezien elke gemeentelijke dienst/afdeling als partij moet worden gezien.

Verder blijkt dat er in de praktijk door leveranciers van gegevens nauwelijks iets gedaan wordt met de audit rapportages van niet-Suwipartijen. Uit de samenvattende rapportage van de BKWI Security Officer blijkt overigens wel dat gemeenten op deze manier in staat zijn om transparantie bieden over de beveiliging van de GeVS[44]. Niet-Suwi-afdelingen zoals de gemeentelijke belastingdeurwaarders rapporteren wel over hun beveiliging. Er hangt echter wel een prijs aan deze transparantie: “de kosten van de bijbehorende audit vormen een reële belemmering.”

Daarnaast is het traceren van berichtenstromen door de gehele keten heen lastig. Dit komt door de aanwezigheid van verschillende (commerciële) brokers in de keten die gegevens in sommige gevallen verrijken met gegevens uit

[44] Samenvattende rapportage van de beveiliging van de Gezamenlijke elektronische Voorzieningen Suwi, 24 maart 2011, zie http://www.bkwi.nl/uploads/media/Samenvattende_rapportage_van_de_beveiliging_van_de_GeVS_over_2010.pdf.

andere bronnen en deze verder doorleveren aan afnemende partijen. Voorbeelden van dergelijke brokers zijn Lost Lemon MensCentraal[45], Kluwer Snelbalie[46], T&T CompeT&T[47]. Vooral bij het gebruik van oude berichten waar de originele bron niet is opgenomen is dit een probleem; in de nieuwe berichten is dit wel het geval. Er loopt momenteel een migratietraject om over te gaan op de nieuwe berichten waardoor betere tracing mogelijk wordt.

Een derde aspect is dat bij het gebruik van Suwinet Inlezen de mogelijkheid om te monitoren op bijvoorbeeld ongebruikte accounts aanzienlijk wordt beperkt. Slechts de inlezende partij heeft deze gegevens. Met andere woorden, de monitoring gegevens om end-to-end aantoonbaar te maken wie, wanneer welke gegevens heeft verwerkt vind steeds meer versnipperd plaats. Deze versnippering wordt versterkt door het toenemend aantal afnemende partijen in Suwinet. Aanvullende maatregelen zijn nodig bij de ketenpartijen om ervoor te zorgen dat in het kader van transparantie alle relevante gegevens verzameld kunnen worden.

De rapportages die op basis van de log-gegevens gecreëerd worden zijn niet altijd even bruikbaar voor gericht onderzoek[48]. Bovendien maken niet alle partijen gebruik van de rapportages zo blijkt uit de gesprekken met BKWI.

Tot slot observeert de inspectie SZW naar aanleiding van onderzoek naar gegevensuitwisseling met niet-Suwipartijen dat de privacywetgeving door de uitvoering, al dan niet terecht, als complex ervaren wordt. Hierdoor worden in de praktijk soms directe of indirecte workarounds gebruikt, waarbij de grenzen van de privacywetgeving worden opgerekt en soms ook overschreden om klanten een goede dienstverlening te bieden.[49]

3.8.4 ANALYSE EN BESCHOUWING

De Verantwoordingsrichtlijn en het Normenkader worden niet ketenbreed ondersteund waardoor er een onvolledig beeld van de beveiliging van Suwinet ontstaat. Dit nadelig voor de transparantie van partijen over hun beveiliging en kan ten koste gaan van het vertrouwen tussen de partijen.

Gegevensleveranciers hebben behoefte aan een bepaalde mate van zekerheid over het juiste gebruik van ‘hun’ gegevens door afnemers. Daarvoor willen zij onder meer voldoende inzicht hebben in de berichtenstromen. Gegevens worden echter steeds meer geleverd aan informatiebrokers waardoor het lastiger wordt om de berichtenstromen door de gehele keten heen (end-to-end) goed te traceren en hierover te rapporteren naar de leveranciers. In veel gevallen ‘ziet’ BKWI slechts de broker die informatie opvraagt en niet de achterliggende partij. Bovendien is onduidelijk wat de brokers doen met de ontvangen berichten. Het inzicht op naleving is niet optimaal en belemmert daarmee de sturing op naleving. Hierdoor kan BKWI de leveranciers onvoldoende ondersteunen in hun toezichthoudende rol.

Waar het Suwinet-Inkijk betreft is traceerbaarheid vooral een probleem bij berichten die verouderde specificaties volgen. Daarin is namelijk de originele bron niet opgenomen. In berichten volgens de nieuwste standaarden is dat

[45] Lost Lemon Mens Centraal, zie http://www.lostlemon.nl/menscentraal en www.menscentraal.com.
[46] Kluwer Snelbalie, zie http://www.infofit.nl/snelbalie-algemeen.
[47] T&T CompeT&T, zie www.competent.nl
[48] KING, W&I Zorgvuldig gebruik en verbeterpunten, mei 2012, zie http://www.kinggemeenten.nl/media/502180/04-zorgvuldig-gebruik-en-de-verbeterpunten.pdf.
[49] Rapport Inspectie SZW, Informatie-uitwisseling van de SUWIketen met andere partijen, augustus 2012.

wel het geval. Dit specifieke issue is dus relatief eenvoudig op te lossen door het gebruik van verouderde berichten versneld uit te faseren.

Suwinet-Inlezen is echter een ander verhaal. Met het verschuiven van de controle-elementen naar de afnemende organisaties dienen deze partijen ook zelf te loggen ten behoeve van traceerbaarheid. Om een end-to-end berichttracering mogelijk te maken zullen al deze logs verzameld en gecombineerd moeten worden. Gezien het ontbreken van effectieve ketenbrede verantwoording kan dat in de praktijk moeilijk te realiseren zijn. Verder is onduidelijk voor welk proces het in te lezen bericht gebruikt wordt (er is een applicatie-ID bekend bij BKWI, maar het is niet ondenkbaar dat een inlezende applicatie meerdere processen ondersteunt).

Een belangrijke vraag is wie verantwoordelijk is voor de transparantie van de gegevensuitwisseling. Enerzijds ligt er een belang bij de leverancier om er zeker van te zijn dat de gegevens de juiste partij hebben bereikt zodat deze bijvoorbeeld niet kan ontkennen de gegevens gehad te hebben. Anderzijds is de traceerbaarheid van de gegevens essentieel voor de afnemende partijen om verantwoording te kunnen afleggen over de herkomst en het gebruik van de gegevens zoals vereist door WBP. Het is daarom in het belang van Suwinet om zicht te hebben over welke gegevens allemaal uitgewisseld worden tussen welke partijen. Technisch zijn er voldoende mogelijkheden om invulling te geven aan transparantie. De aanleverende en afnemende partijen zullen duidelijker moeten aangeven welke gegevens zij nodig hebben. Als dat helder is zullen de rapporten die hieruit gegenereerd worden ook bruikbaarder zijn en zal het gebruik ervan toenemen. Hiermee neemt ook de kwaliteit van de controle op het gebruik van gegevens toe (zie ook sectie 3.12 over Toezicht en Handhaving).

3.8.5 MITIGERENDE MAATREGELEN

De volgende maatregelen zijn nodig om transparantie in Suwinet te verbeteren:

- Zorg voor een ketenbreed gedragen Verantwoordingsrichtlijn en bijbehorend Normenkader. De afgelopen jaren is dit niet het geval geweest. De les die hieruit getrokken kan worden is dat een meer verplichtend karakter om te voldoen aan beide kaders noodzakelijk is. Dit maakt het ook mogelijk om partijen die hieraan niet voldoen aan te spreken.
- Creëer betere handvatten voor het kunnen traceren van berichtuitwisseling door de inlezende keten. Inventariseer welke elementen belangrijk zijn bij het traceren van berichtuitwisselingen aan de hand van de door afnemende en aanleverende partijen gewenste gegevens in de rapportages.
- Borg dat alle partijen binnen redelijke termijn overgaan op de nieuwe bericht definities, waarbij end-to-end vaststaat welke unieke persoon van welke organisatie, welke gegevens en voor welk doel heeft opgevraagd en ter beschikking heeft gekregen.
- Maak duidelijk wie verantwoordelijk is voor het creëren van transparantie: de individuele partijen in Suwinet of een centrale partij. Vanuit het perspectief van toezicht en handhaving is een centrale aanpak wenselijk. Ook richting de burger levert een centrale aanpak een effectievere informatievoorziening op.
- Overwogen kan worden de logging van de inlezende applicaties en het gebruik van de log-gegevens op te nemen als onderdeel van de Verantwoordingsrichtlijn en het Normenkader. Dit biedt transparantie aan zowel bronhouder als BKWI en de stelselverantwoordelijke en kan de zorg van aanleverende partijen worden weggenomen. Nu is in de Aansluitvoorwaarden alleen opgenomen dat de aanleverende partij een

verzoek kan doen tot verstrekking van een lograpport. In het verlengde hiervan kan de mogelijkheid overwogen worden om inlezende applicaties te certificeren zodat daadwerkelijk gecontroleerd kan worden of ze voldoen aan alle eisen zoals gesteld in de Verantwoordingsrichtlijn en het Normenkader (bijvoorbeeld met betrekking tot logging).

3.9 (WBP-)VERANTWOORDELIJKHEID

De focus in deze PIA ligt op informatiebeveiliging. Het blijft echter een *privacy* impact assessment, dus moet in ieder geval op hoofdlijnen ook naar de andere privacyprincipes worden gekeken. Daar komt bij dat art. 13 WBP op wetsniveau de basisverplichting is tot het beveiligen van persoonsgegevens. Deze verplichting rust primair op de verantwoordelijke voor de verwerking. Ook een eventuele bewerker moet zich er rekenschap van geven, en de verantwoordelijke die die bewerker inschakelt moet concrete beveiligingsmaatregelen met de bewerker afspraken en ook nagaan of die zich daaraan houdt. De verantwoordelijke is bovendien aan te spreken ('accountable') op governance over de verwerking; die verplichting volgt nu al uit art. 15 Wbp, en zal straks nog veel nadrukkelijker haar plek krijgen in de nieuwe EU-privacyverordening. Reden genoeg dus om in deze en de volgende paragrafen de blik te richten op de thema's (Wbp-)verantwoordelijkheid, governance, verantwoording, toezicht en handhaving.

In complexe samenwerkingsverbanden is het van belang verantwoordelijkheden helder af te bakenen. Voor het verwerken van persoonsgegevens is dit uitgangspunt ook wettelijk verankerd. Iedere verwerking van persoonsgegevens moet een *verantwoordelijke* hebben. Een gegevensverwerking kan meerdere verantwoordelijken hebben, maar dan moeten die onderling goed afspreken wie voor welk deel van de verwerking verantwoordelijk is. Doen ze dat niet, dan zijn alle samenwerkingspartners verantwoordelijk, en dus ook aansprakelijk, voor de gehele verwerking.

3.9.1 HOE IS HET FORMEEL GEREGELD?

De wettelijke basis voor de samenwerking in het kader van Suwinet is gelegd in Hoofdstuk 9 van de Wet Suwi. Art. 62 lid 2 bepaalde oorspronkelijk dat de Suwipartijen "gebruik [maken] van een elektronische infrastructuur die daartoe door hen en Onze Minister wordt ingericht en in stand gehouden." De minister van SZW kreeg de mogelijkheid een organisatie aan te wijzen om het beheer van Suwinet uit te voeren.[50] Verder zijn er een aantal bepalingen te vinden over onder meer verantwoording en het stelselontwerp. Duidelijk is dat de regie lag bij de Minister van SZW.[51]

Met de invoering van de Wet eenmalige gegevensuitvraag (WEU) in 2008 hebben deze verhoudingen een belangrijke wijziging ondergaan. Sindsdien bepaalt art. 62 lid 2 Wet Suwi, kort gezegd, dat de Suwipartijen gezamenlijk Suwinet in de lucht moeten houden. De directe verantwoordelijkheid van de Minister is daarmee komen te vervallen.

[50] Het toenmalige art. 67 lid 1 Wet Suwi.
[51] Zie met name ook de toelichting bij de Regeling Suwi: "Het BKWI heeft geen besluitvormende bevoegdheid omtrent inrichting van voorzieningen en vormgeving van gegevensuitwisselingen. Besluitvorming hieromtrent vindt plaats door de Minister van SZW in overleg met de uitvoeringsorganen (conform artikel 71 van de Wet SUWI). Beleidsmatige en strategische afstemming tussen de partijen vindt plaats in het zogenaamde Ketenoverleg, waarin het ministerie van SZW op ambtelijk niveau met de betrokken organisaties overlegt."

De nieuwe verhoudingen zijn onder meer uitgewerkt in het Besluit Suwi en het Stelselontwerp.
Art. 5.21 Besluit Suwi bepaalt nu dat UWV ten behoeve van de gezamenlijke zorg Suwinet en de bijbehorende autorisatievoorziening beheert. Dat beheer wordt uitgevoerd door 'een herkenbaar en afzonderlijk organisatie-onderdeel' (BKWI). De gebruikers (UWV, SVB, gemeenten) zorgen voor hun eigen elektronische voorziening en de aansluiting daarvan op Suwinet. Een en ander wordt nader uitgewerkt in het Stelselontwerp (Bijlage I bij de Regeling Suwi).

De uitwerking in het Stelselontwerp (§1.2) luidt als volgt: "Op de GeVS aangesloten partijen zijn gezamenlijk verantwoordelijk voor het maken van afspraken die leiden tot één samenhangend en betrouwbaar samenstel van gezamenlijke voorzieningen. De beheerder van de centrale voorziening is operationeel verantwoordelijk voor de coördinatie van het tot stand komen van de gezamenlijke afspraken en de inrichting van een gemeenschappelijke faciliteit voor (logische)toegangsbeveiliging."

Elke Suwipartij verantwoordelijk voor een juist gebruik van via Suwinet afgenomen gegevens. Wanneer twee partijen informatie met elkaar uitwisselen, dan is het primair de verantwoordelijkheid van de ontvangende partij om ervoor te zorgen dat de ontvangen gegevens op rechtmatige wijze verwerkt worden. Vanuit het oogpunt van behoorlijkheid en zorgvuldigheid[52], alsook verenigbaarheid[53] heeft de verstrekker echter óók een verantwoordelijkheid: hij mag niet 'zomaar' gegevens verstrekken. Dit principe is uitgewerkt in art. 74 lid 3 Wet Suwi:: "Degene die op grond van de artikelen 62, 72 of 73 gegevens verstrekt, dient na te gaan of degene aan wie de gegevens worden verstrekt redelijkerwijs bevoegd is te achten om die gegevens te verkrijgen."

Veel gegevensuitwisselingen ten behoeve van gemeenten worden uitgevoerd door het Inlichtingenbureau. Art. 5.24 Besluit Suwi regelt in aanvulling op art. 1 Wet Suwi dat het Inlichtingenbureau daarbij optreedt als bewerker namens de gemeenten.

Van belang is ten slotte nog dat de artikelen 33a en 35 van de Wet Suwi bepalen dat UWV en SVB bij gegevensverkeer met het buitenland optreden als bewerker voor (onder meer) de Minister van SZW.

3.9.2 WELKE MAATREGELEN ZIJN ER GENOMEN?

Voor zover ons bekend is, zijn er geen nadere afspraken gemaakt om de in de vorige paragraaf weergegeven verdeling van verantwoordelijkheden te verduidelijken c.q. nader uit te werken op een enkele uitzondering na. Dit was bijvoorbeeld het geval bij Mens Centraal. Het CBP maakt in 2011 na aanleiding van een onderzoek bij de gemeente Spijkenisse in een brief aan deze gemeente melding van onduidelijkheden over verantwoordelijkheden en bewerkerschap met betrekking tot Mens Centraal[54]. De Nederlandse Vereniging voor Sociale Innovatie (NVSI) heeft als beheerder van Mens Centraal hierop actie ondernomen door met ingang van 2013 bij alle overeenkomsten met

[52] Art. 6 Wbp.
[53] Art. 9 Wbp.
[54] CBP z2011-00366, 2011.

gemeenten ook een overeenkomst toe te voegen tussen NVSI, gemeenten en Lost Lemon[55].

3.9.3 WELKE KWETSBAARHEDEN ZIJN ER?

Er zijn verschillende soorten kwetsbaarheden op het gebied van Wbp-verantwoordelijkheid.

In de eerste plaats zijn er de kwetsbaarheden die samenhangen met de gezamenlijke verantwoordelijkheid van de Suwipartijen voor Suwinet. UWV, SVB en de gemeenten verwerken ieder hun 'eigen ' gegevens en dragen gezamenlijk zorg voor Suwinet. Wat dit betekent voor verantwoordelijkheid (in de zin van de Wbp) voor gegevensuitwisselingen via Suwinet is niet expliciet uitgewerkt. Dat leidt tot juridische en praktische kwetsbaarheden.

De juridische kwetsbaarheden zijn het gevolg van de verplichtingen die de Wbp oplegt aan de verantwoordelijke. Voldoet de verantwoordelijke daar niet aan, dan riskeert hij handhavende actie door het CBP of correctie door de rechter. Bovendien kan hij door betrokkenen aansprakelijk worden gesteld voor geleden (materiële én immateriële) schade. Een onduidelijke verantwoordelijkheidsverdeling betekent dat alle Suwipartijen mogelijk deze risico's lopen, zonder zich ervan bewust te zijn.[56] Indirect betekent dit ook een risico voor de minister van SZW. Weliswaar draagt die geen directe Wbp-verantwoordelijkheid[57], maar hij is wel politiek verantwoordelijk voor het formele kader waarbinnen de Suwipartijen hun verantwoordelijkheid gestalte moeten geven. Gebeurt dat laatste onvoldoende, dan is het aan de minister om partijen tot de orde te roepen of zo nodig de regels aan te scherpen. Naleving van de Wbp als kaderwet moet immers voldoende geborgd zijn.

De praktische kwetsbaarheden komen vooral tot uiting op aanpalende terreinen waarop een heldere verantwoordelijkheidsverdeling een noodzakelijke voorwaarde is voor effectiviteit, zoals governance en verantwoording. Meer daarover in de volgende paragrafen. Hier willen we nog opmerken dat het erop lijkt dat het feit dat er binnen Suwinet veel geregeld is op het gebied van informatiebeveiliging in combinatie met het gebrek aan Wbp-verantwoordelijkheid ook nadelige privacygevolgen heeft: privacy compliance omvat immers veel meer dan alleen informatiebeveiliging, maar geen van de Suwipartijen is of voelt zich er eindverantwoordelijk voor dat Suwinet ook los van informatiebeveiliging voldoet aan alle privacyprincipes.

Tot slot zijn er nog kwetsbaarheden die samenhangen met andere onduidelijkheden op het gebied van Wbp-verantwoordelijkheid:

- De precieze rol van BKWI is onduidelijk. Enerzijds kan betoogd worden dat BKWI verantwoordelijke is: het is immers geen zelfstandig bestuursorgaan, maar een onderdeel van UWV, een van de Suwipartijen, die samen met SVB en gemeenten, verantwoordelijke voor Suwinet is.[58] Ook heeft BKWI de wettelijk opdracht om de nodige maatregelen te nemen bij geconstateerde tekortkomingen in de beveiliging van Suwinet.[59] Anderzijds kan

[55] Antwoord van Mens Centraal op de uitkomsten van het onderzoek van CBP bij de gemeente Spijkenisse, zie http://www.menscentraal.com/antwoord-op-onderzoek-cbp-bij-gemeente-spijkenisse.
[56] In de volgende deelparagraaf zullen we zelfs betogen dat alle Suwipartijen al deze risico's lopen, omdat ze ieder voor zich verantwoordelijk zijn voor heel Suwinet.
[57] Zoals verderop in deze paragraaf zal worden besproken is het overigens nog maar de vraag of dat inderdaad zo is.
[58] Vgl. ook de opmerkingen hieronder over het Inlichtingenbureau.
[59] Stelselontwerp: "Beheerder van de centrale voorziening neemt passende maatregelen bij geconstateerde beveiligingsinbreuken of misbruik van de GeVS."

betoogd worden dat BKWI bewerker is: die rol had het toen de minister nog verantwoordelijk was,[60] en BKWI verricht zijn werkzaamheden nu “ten behoeve van de gezamenlijke zorg” van de Suwipartijen[61]. In de praktijk worden BKWI en UWV veelal ook als twee verschillende organisaties gezien. De waarheid waar het de rol van BKWI betreft ligt waarschijnlijk ergens in het midden – er zijn nog allerlei tussenvormen mogelijk – maar duidelijk is het allerminst.

- Het is de vraag of de wettelijk vastgelegde bewerkersrol van het Inlichtingenbureau juridisch helemaal houdbaar is. In de zgn. SWIFT-zaak hebben de Europese privacytoezichthouders het standpunt ingenomen dat een partij die voor meerdere vergelijkbare organisaties een infrastructurele voorziening verzorgt in sommige gevallen aan te merken is als medeverantwoordelijke in plaats van als bewerker. Of dit zo is, hangt af van de mate waarin deze partij zelfstandig keuzes over vorm en inhoud van de verwerking kan maken.[62]
- Gemeenten maken in toenemende mate gebruik van SaaS-oplossingen, waarbij via Suwinet aangeleverde gegevens via een commerciële broker worden doorgeleverd. Zoals in de vorige deelparagraaf is benoemd, kan het in de praktijk onduidelijk zijn wat de precieze rol van zulke brokers is.
- Het is de vraag of de minister van SZW niet moet worden aangemerkt als medeverantwoordelijke (in de zin van de Wbp) voor Suwinet. Hij gebruikt Suwinet immers voor gegevensuitwisseling met het buitenland (UWV en SVB treden daarbij op als bewerkers).

3.9.4 ANALYSE EN BESCHOUWING

Op basis van het huidige wet- en -regelgevingskader voor Suwinet is duidelijk dat de Suwipartijen gezamenlijke Wbp-verantwoordelijkheid dragen voor Suwinet.[63] Die kan op verschillende manieren ingevuld worden.[64]

De belangrijkste vraag is of er sprake is van één gemeenschappelijke verantwoordelijke. Zoals het nu geregeld is, is daarvan geen sprake. Weliswaar is het beheer van Suwinet belegd bij UWV (concreet: BKWI), maar dat gebeurt expliciet in het kader van de zorgplicht van de gezamenlijke Suwipartijen. De minister van SZW heeft – afgezien van het laatste punt uit de vorige deelparagraaf – geen Wbp-verantwoordelijkheid voor Suwinet.

Vervolgens is de vraag of ieder van de verantwoordelijken aansprakelijk is voor zijn min of meer losse onderdeel van de verwerking, of dat iedere verantwoordelijke voor het geheel aansprakelijk is. Hier lijkt sprake van een combinatie van beide. Enerzijds hebben alle Suwi-partijen duidelijk hun eigen verwerkingen waarvoor zijzelf de verantwoordelijke

[60] Toelichting bij de Regeling Suwi: “Het BKWI heeft geen besluitvormende bevoegdheid omtrent inrichting van voorzieningen en vormgeving van gegevensuitwisselingen. Besluitvorming hieromtrent vindt plaats door de Minister van SZW in overleg met de uitvoeringsorganen.”
[61] Art. 5.21 Besluit Suwi.
[62] Dit standpunt is later nog bevestigd en uitgewerkt in de Working Paper 169 over de begrippen “voor de verwerking verantwoordelijke” en “verwerker”: “In [de SWIFT-zaak] werd duidelijk dat de contractuele aanstelling van een partij als voor de verwerking van gegevens verantwoordelijke of als verwerker weliswaar relevante informatie kan bieden over de wettelijke hoedanigheid van die partij, maar dat een dergelijke contractuele aanstelling toch niet doorslaggevend is voor het vaststellen van de daadwerkelijke hoedanigheid van die partij, die uit concrete omstandigheden moet blijken.”
[63] Vgl. ook nog het hierboven al geciteerde WP169 van de art. 29 Werkgroep, dat een voorbeeld uit de reisbranche geeft: “Het reisbureau, de hotelketen en de luchtvaartmaatschappij besluiten om een gemeenschappelijk online platform te ontwikkelen om beter te kunnen samenwerken bij reserveringen. Zij bereiken overeenstemming over belangrijke aspecten van de te gebruiken middelen, waaronder welke gegevens zullen worden opgeslagen, de wijze waarop reserveringen worden toegewezen en bevestigd en wie toegang tot de opgeslagen informatie heeft. Daarnaast besluiten zij de gegevens van hun klanten te delen om hun marketingactiviteiten te kunnen integreren. In dit geval zijn het reisbureau, de luchtvaartmaatschappij en de hotelketen gezamenlijk verantwoordelijk voor de wijze waarop persoonsgegevens van hun respectieve klanten worden verwerkt en zijn zij daarom gezamenlijk voor de verwerking verantwoordelijk waar het gaat om de verwerkingen voor het gemeenschappelijke online boekingsplatform. Elk van hen zou echter individueel verantwoordelijk blijven voor andere verwerkingen, bijvoorbeeld in verband met hun personeelsbeheer.”
[64] Zie de Memorie van Toelichting bij de Wbp, blz. 55 en verder.

zijn. Waar het de zorg voor Suwinet betreft vallen zij echter in de derde categorie van gezamenlijke verantwoordelijkheid die in de Memorie van Toelichting bij de Wbp wordt onderscheiden: “Verschillende verwerkingen zijn geïntegreerd zonder dat een gemeenschappelijke verantwoordelijke aanwezig is. Er is sprake van gezamenlijke verantwoordelijkheid. Elk van de verantwoordelijken is aansprakelijk voor het geheel van de gegevensverwerkingen.” Dit betekent dat iedere Suwi-partij – UWV, SVB, maar ook iedere individuele gemeente – aan te spreken is op en aansprakelijk is voor alle verwerkingen van persoonsgegevens via Suwinet.

Door een en ander is een hybride situatie ontstaan waarin veel zaken onduidelijk zijn. Formeel is het helder: de Wbp-verantwoordelijkheid berust bij UWV, SVB en de gemeenten gezamenlijk. Deze gezamenlijke verantwoordelijkheid is echter niet nader ingevuld of uitgewerkt. Dat heeft in de praktijk met name gevolgen voor zaken als governance en verantwoording (zie daarvoor de volgende paragrafen). Wil Suwinet de komende tijd een rechtmatige en duidelijke koers varen, dan is verduidelijking van de verantwoordelijkheden daarvoor een *conditio sine qua non*. Gelet op de mate waarin andere aspecten van Suwinet in wet- en -regelgeving zijn uitgewerkt, ligt het voor de hand dat ook met de verantwoordelijkheidsverdeling te doen.

Concluderend kan gesteld worden:

- Op basis van alle feiten en omstandigheden is op hoofdlijnen een redelijk goed beeld te geven van de Wbp-verantwoordelijkheden ten aanzien van Suwinet. Echter, dit beeld is niet heel eenvoudig te construeren, en het is ook nergens expliciet vastgelegd.
- De vraag is bovendien of het gewenst is: de conclusie hierboven luidt dat alle Suwi-partijen, dus ook alle individuele gemeenten, verantwoordelijk en daarmee aansprakelijk zijn voor alle gegevensuitwisselingen over Suwinet.
- Het beeld is bovendien onvolledig: de positie van BKWI is niet helder, er kunnen vraagtekens geplaatst worden bij de bewerkersrol van het Inlichtingenbureau, de minister wordt waarschijnlijk ten onrechte niet als (mede-)verantwoordelijke aangemerkt, en nieuwe ontwikkelingen – in het bijzonder het gebruik van SaaS-software door gemeenten – zijn er niet in verwerkt (zie ook sectie 4.3).
- De onduidelijke verantwoordelijkheidsverdeling leidt tot diverse juridische en praktische privacykwetsbaarheden.
- De verantwoordelijkheidsverdeling moet verduidelijkt worden in de Suwi wet- en -regelgeving.

3.9.5 MITIGERENDE MAATREGELEN

Om de Wbp-verantwoordelijkheid voor Suwinet te verduidelijken, kunnen de volgende maatregelen genomen worden:

- Leg de Wbp-verantwoordelijkheid voor Suwinet op hoofdlijnen vast in de Suwiwet- en -regelgeving.
- Als daarbij gekozen wordt voor een vorm van gezamenlijke verantwoordelijkheid, baken de verantwoordelijkheid van alle betrokken partijen dan helder af, en leg daarbij een solide basis voor effectieve governance.
- Verduidelijk daarbij ook de Wbp-rol van BKWI, Inlichtingenbureau en commerciële brokers.

3.10 GOVERNANCE

3.10.1 HOE IS HET FORMEEL GEREGELD?

Hoe UWV, SVB en gemeenten gezamenlijk de zorg voor Suwinet invullen, is uitgewerkt in het Stelselontwerp.

De inleiding van het Stelselontwerp zegt hierover: “In gezamenlijk overleg zorgen de SUWI-partijen voor de uitwerking van de hoofdlijnen in werkafspraken. De werkafspraken worden namens de SUWI-partijen door de beheerder van de centrale voorziening voor bekrachtiging voorgelegd aan [de Programmaraad]. Na bekrachtiging zijn de werkafspraken bindend.”

Hoe de genoemde werkafspraken tot stand komen, is nader beschreven in §1.3 van het Stelselontwerp:
“[D]e SUWI-partijen [maken] onderling en gezamenlijk, met de beheerder van de centrale voorziening, afspraken op de verschillende deelgebieden van informatie-uitwisseling binnen de SUWI-keten. De beheerder van de centrale voorziening faciliteert de tot stand koming van de gezamenlijke afspraken, ziet toe op de samenhang en actualiteit van de afspraken en op niet strijdigheid daarvan met gemeenschappelijke, overheidsbrede, afspraken. Indien voldaan is aan de gestelde eisen worden de gemaakte afspraken, namens de SUWI-partijen, door de beheerder van de centrale voorziening voor akkoord voorgelegd aan [de Programmaraad]. Uiteindelijk vinden de afspraken hun weerslag in diverse concrete producten, bijvoorbeeld de Keten Service Level Agreement, het SUWI-Gegevens Register, de SUWI-Ketenarchitectuur en de Verantwoordingsrichtlijn Privacy & Beveiliging GeVS.”

Bovenstaand plaatje klinkt redelijk overzichtelijk. In de praktijk ligt het echter wat ingewikkelder. In de Programmaraad zitten vertegenwoordigers van UWV, VNG, Divosa en Cedris (de brancheorganisatie van sociale werkgelegenheids- en reïntegratiebedrijven); SVB is er niet in vertegenwoordigd.
De Programmaraad heeft voor (met name) Suwinet-aangelegenheden een speciale werkgroep ingesteld, die een heel andere samenstelling heeft. Volgens de website van de Programmaraad, samenvoordeklant.nl:
“De werkgroep Informatisering en Shared Services (WISS) is door de Programmaraad ingesteld om zich bezig te houden met [o.a.] Gegevensverkeer/Suwinet [...]. De werkgroep bestaat uit vertegenwoordigers van gemeenten, Divosa, VNG, King Wigo4it, Inlichtingenbureau, UWV WERKbedrijf, UGD, UWV Uitkeren, SVB en BKWI. […]. De WISS is voor BKWI de stem van de opdrachtgever.”

Het is echter niet zo dat de Programmaraad Suwinet-aangelegenheden helemaal aan de werkgroep heeft uitbesteed, getuige het interview met David Jongen (voorzitter van zowel de Programmaraad als de Stuurgroep Ketenservices ICT) in Ketenjournaal #44:
“De Programmaraad keurt de jaarplannen van de stuurgroepen goed en stuurt op de uitvoering daarvan. In de Programmaraad vindt daarnaast vanuit de G4, Divosa, UWV en VNG het bestuurlijk commitment plaats omdat daar de bestuurders in zitten. Wij proberen het bestuurlijk en strategisch af te stemmen en afspraken te maken.”

De aansturing van BKWI blijkt bovendien nog complexer te verlopen dan alleen langs deze lijnen. Uit het Jaarplan 2013 van BKWI: “Ook van UWV, gemeenten en SVB wordt samenwerking verwacht en een integraal aanbod voor zowel werkgevers als werkzoekenden. BKWI is door het Ministerie van SZW in het leven geroepen om deze

samenwerking te ondersteunen en te bevorderen.

- BKWI beheert en ontwikkelt de elektronische gegevensuitwisseling tussen deze organisaties zodat klantgegevens direct beschikbaar zijn en niet iedere keer opnieuw te hoeven worden uitgevraagd. Voor deze activiteiten rapporteert BKWI aan de [WISS];
- BKWI ondersteunt ook de integratie van de dienstverlening zelf op de Werkpleinen. BKWI faciliteert in opdracht van de ketenpartijen de vorming van Werkpleinen. Voor deze activiteiten rapporteert BKWI aan de Stuurgroep Dienstverlening.
- In het verlengde van deze twee kerntaken ondersteunt BKWI ketenpartners met weboplossingen waarin het delen van klantinformatie en kennis centraal staat. Formeel fungeert het Ministerie van SZW als opdrachtgever. De Raad van Bestuur UWV is verantwoordelijk en heeft een aparte organisatorische entiteit (BKWI) belast met de uitvoering; de inhoudelijke aansturing geschiedt door de gezamenlijke ketenpartners, verenigd in de Programmaraad."

3.10.2 WELKE KWETSBAARHEDEN ZIJN ER?

Een aantal kwetsbaarheden zijn uit het onderzoek en de interviews naar voren gekomen met betrekking tot governance:

- De Suwipartijen zijn gezamenlijk verantwoordelijk voor Suwinet. Om te voorkomen dat het adagium "iedereen verantwoordelijk = niemand verantwoordelijk" opgaat, zijn dan heldere afspraken over besturing en besluitvorming. Het is de vraag of dit bij Suwinet voldoende geregeld is.
  Zo is SVB niet vertegenwoordigd in de Programmaraad, en is onduidelijk in hoeverre de gemeentelijk vertegenwoordigers besluiten kunnen nemen die alle individuele gemeenten binden. Daar komt nog bij dat de Programmaraad een sterke focus lijkt te hebben op de samenwerking van UWV en gemeenten ten behoeve van met name de arbeidsmarkt (de Werkpleinen). Ook dat draagt niet bij aan duidelijke besturing over Suwinet.
  In de WISS – waar de Programmaraad een groot deel van zijn verantwoordelijkheid voor Suwinet belegd heeft - is SVB wel vertegenwoordigd, maar die kent nog meer dan de Programmaraad per (type) Suwipartij verschillende typen vertegenwoordigers. Een aantal taken van de WISS zijn bovendien weer belegd bij diverse daaronder ressorterende werkgroepen. Ook dat lijkt geen recept voor heldere en eenduidige besluitvorming.
  Inspectie SZW constateert in zijn Vervolgonderzoek Beveiliging en Privacy uit 2011 dan ook: "Het blijkt geen eenvoudige opgave om de SUWI-partijen, waaronder de 418 gemeenten, op één lijn te krijgen."
  En Zenc/HEC stellen vast[65]: "In de sturing op het stelsel zijn ook verbeteringen nodig. We hebben gezien dat partijen niet altijd weten hoe het hele bouwwerk van overleggroepen etc. in elkaar steekt en wie nu waar over gaat en wat kan verwachten. Stukken die worden voorgelegd aan een hoger echelon komt niet altijd een feed-back, ook is niet duidelijk of dat wel zou moeten."
- Concreet is er – zie elders in dit rapport – een serieus probleem met de informatiebeveiliging bij veel gemeenten. De formele verplichting om het op orde te hebben is er wel, maar die wordt in de praktijk veelal niet nageleefd.[66] Meer hierover in de volgende paragraaf.

[65] Concept eindrapport "Gebruik Suwinet: Een kwestie van vertrouwen", 2012.
[66] Vgl. ook Inspectie SZW in haar vervolgrapport over Privacy en Beveiliging Suwinet uit 2011: "Gezien vanuit het model van de verbetercyclus ('plan-do-check-act'-cyclus) kan worden geconstateerd dat door het ontbreken van een zichtbare verantwoording door de gemeenten de 'check'-fase in de SUWI-keten ten minste gedeeltelijk ongevuld blijft. Daardoor kan er ook geen sprake zijn van een goed bijstellen van de beveiliging van Suwinet als geheel. Er zijn dus gebreken in het verbeterproces rondom Suwinet als geheel."

- Suwinet is sinds de start uitgegroeid tot een groot en complex netwerk. Van verschillende kanten wordt aangegeven dat dat heeft geleid tot problemen met de besturing. In het bijzonder lijken beleid en werkelijkheid steeds meer discrepantie te vertonen.[67] Ook het feit dat BKWI meerdere soorten taken uitvoert en daarvoor op verschillende manieren wordt aangestuurd helpt niet.
- In de vorige paragraaf, over Wbp-verantwoordelijkheid, vermeldden we al dat er te weinig aandacht is voor privacyaspecten in brede zin. Daardoor is niet geborgd dat bijv. de noodzaak van specifieke gegevensuitwisselingen periodiek geëvalueerd wordt, of dat betrokkenen op de juiste wijze geïnformeerd worden. Het heeft ook gevolgen voor de adequaatheid van de informatiebeveiliging. Er is immers niet geborgd dat bij nieuwe uitwisselingen getoetst wordt of die gevolgen moeten hebben voor het vastgestelde beveiligingsniveau.
- In kringen van privacytoezichthouders en -regelgevers wordt steeds meer nadruk gelegd op het belang van goede governance ('accountability' is daarvoor de gangbare term). Dit zal formeel zijn beslag krijgen in de nieuwe EU-privacyverordening, die naar verwachting komend voorjaar wordt vastgesteld. De verordening plaatst stevige boetes op onvoldoende governance.
- In de praktijk blijkt dat het begrip Suwipartij niet eenduidig is en welke rechten en plichten dit met zich meebrengt. Is een partij als Inspectie SZW een Suwipartij? De GSD-afdeling van een gemeente is een Suwipartij; de gemeentelijke gerechtsdeurwaarders niet.

3.10.3 ANALYSE EN BESCHOUWING

Toen Suwinet in het leven werd geroepen, is de minister van SZW aangewezen als (eind)verantwoordelijke. Daarmee is de besturing van een complex geheel als Suwinet natuurlijk niet opgelost, maar het betekent wel dat duidelijk is wie er uiteindelijke aan te spreken (accountable) is, ook op de privacy- en beveiligingsaspecten.

Begin 2008 is dit veranderd. Sindsdien ligt de zorg voor Suwinet bij UWV, SVB en gemeenten. Dat heeft gevolgen voor Wbp-verantwoordelijkheid in de zin van de Wbp, en daarmee voor de governance van privacy en informatiebeveiliging binnen Suwinet.

De governancepraktijk van Suwinet geeft op zijn best een diffuus beeld. In de Programmaraad, waarin formeel de verantwoordelijken verenigd zijn, is SVB niet vertegenwoordigd en zijn de gemeenten indirect vertegenwoordigd (door VNG en Divosa). In de WISS, die in de praktijk verreweg het meeste stuurt, zitten vertegenwoordigers uit verschillende onderdelen van de deelnemende Suwipartijen; ook zijn enkele gemeenten vertegenwoordigd, naast VNG, KING en Divosa. Niet duidelijk is of er heldere regels zijn voor besluitvorming, en in hoeverre met name individuele gemeenten zich daaraan gebonden achten. Effectieve sturing lijkt op deze manier onvoldoende structureel geborgd te zijn. Een en ander onderstreept het belang van een heldere invulling van de stelselverantwoordelijkheid van de minister van SZW.

[67] Inspectie SZW-rapport Informatie-uitwisseling, 2012:
"De inspectie concludeert dat de bescherming van persoonsgegevens nog onvoldoende aandacht krijgt en er veel ruimte is voor verbetering."
"De privacywetgeving wordt door de uitvoering, al dan niet terecht, als complex ervaren. In de praktijk worden soms directe of indirecte workarounds gebruikt, waarbij de grenzen van de privacywetgeving worden opgerekt en soms ook overschreden."

3.10.1 MITIGERENDE MAATREGELEN

Om de governance te verstevigen is allereerst verduidelijking van de Wbp-verantwoordelijkheden nodig. Vervolgens zijn er – grotendeels afhankelijk van de daar gemaakte keuzes – twee oplossingsrichtingen denkbaar:

- Verduidelijk de huidige verhoudingen en de daarbij behorende governance (rollen, taken, bevoegdheden, overleggremia, regels voor besluitvorming enz.). Stel vast welke waarborgen de governance zou moeten bieden en bepaal daarna in welke vorm dat zou kunnen.
- Herzie de huidige verhoudingen, waarbij – onverminderd de zelfstandige verantwoordelijkheid van de ketenpartijen – de ketenverantwoordelijkheid voor Suwinet nadrukkelijker bij één partij wordt gelegd, die onder directe verantwoordelijkheid van de minister van SZW valt.

Vervolgens dienen als onderdeel van de governance ook verantwoording, toezicht en handhaving herzien te worden. Meer daarover in de volgende paragrafen.

3.11 VERANTWOORDING

3.11.1 HOE IS HET FORMEEL GEREGELD?

Art. 5.22 Besluit Suwi bepaalt dat UWV, SVB en het Inlichtingenbureau jaarlijks [aan de minister van SZW en Inspectie SZW] rapporteren over de opzet en werking van hun informatiebeveiliging, inclusief auditverklaring. Art. 6.4 lid 3 Regeling Suwi bepaalt dat deze rapportageverplichting van overeenkomstige toepassing is op het gebruik en de inrichting van Suwinet. Een en ander is conform §2.3 Stelselontwerp nader uitgewerkt in §5.1 en §5.4 Verantwoordingsrichtlijn: van de rapportages door de Suwipartijen worden ook publieke versies gemaakt, en die vormen de input voor een samenvattende rapportage door de Security Officer van BKWI aan de minister van SZW en de Inspectie SZW.

N.B. Niet geheel duidelijk is of art. 5.22 Regeling Suwi wel of niet ook op de gemeenten slaat. De algemene opinie lijkt te zijn dat dat niet zo is, maar klopt dat wel? In §5.1 Stelselontwerp valt het volgende te lezen: "De verantwoording over de beveiliging van Suwinet leidt tot de volgende rapportagevormen: • De jaarlijkse rapportage van de Suwi-partijen en het BKWI aan de Minister van SZW en Inspectie SZW. Deze rapportage moet worden vergezeld van een oordeel en rapport van bevindingen van een register edp-auditor. […]". Met de Suwipartijen worden – eveneens volgens algemeen spraakgebruik, en trouwens ook volgens de inleiding van het Stelselontwerp – UWV, SVB en de gemeenten aangeduid. Dit suggereert dat gemeenten wel degelijk een verantwoordingsverplichting hebben aan de minister van SZW en Inspectie SZW. Ook art. 6.4 lid 3 Regeling Suwi kan *in ieder geval zo gelezen worden dat gemeenten zich ook moeten verantwoorden – dat hangt af van hoe de zinsnede "van overeenkomstige toepassing" wordt geïnterpreteerd. De toelichting in §6.3.1 geeft daarover geen duidelijkheid.*

Bij wijziging wordt de Verantwoordingsrichtlijn voor akkoord voorgelegd aan [de Programmaraad], gehoord de Inspectie Werk en Inkomen.[68]

Er bestaat geen specifieke verantwoordingsverplichting ten aanzien van informatiebeveiliging binnen gemeenten:[69]

[68] §2.3 Stelselontwerp.
[69] Q&A Gemeenteloket SZW n.a.v. brief staatssecretaris De Krom 2012.

"*Is het college van burgemeester en wethouders verplicht zich aan de gemeenteraad te verantwoorden over het veilig gebruik van Suwinet?*

Er bestaat geen wettelijke verplichting voor het college van burgemeester en wethouders om zich in specifieke zin aan de gemeenteraad te verantwoorden over de informatiebeveiliging en bescherming van persoonsgegevens. Wel is in artikel 169 van de Gemeentewet bepaald dat het college in algemene zin verantwoording schuldig is aan de gemeenteraad over het gevoerde bestuur. Gegeven het grote belang van de informatiebeveiliging en bescherming van persoonsgegevens ligt wel voor de hand dat het college zich hierover verantwoord aan de gemeenteraad."

3.11.2 WELKE KWETSBAARHEDEN ZIJN ER?

Een aantal kwetsbaarheden komen naar voren uit de interviews met betrokken partijen en uit de literatuur:

- Er bestaat geen effectieve verantwoordingsverplichting voor gemeenten over hun informatiebeveiliging in verband met Suwinet. Zoals elders in dit rapport is vastgesteld, blijkt het beveiligingsniveau bij gemeenten in de praktijk veelal onder de maat te zijn. Om dat probleem op te lossen, zijn verschillende maatregelen nodig, waarvan het inrichten van effectieve verantwoording door gemeenten er één is.[70] Met dat laatste wordt dan meteen de ongelijke situatie gelijkgetrokken dat "niet-Suwi-onderdelen" van gemeenten (zoals gemeentelijke gerechtsdeurwaarders en schuldhulpverlening) zich wél uitgebreid moeten verantwoorden.
- De samenvattende rapportage door de Security Officer van BKWI geeft een vertekend beeld, doordat er juist geen rapportages verwerkt worden van de partijen waar de meeste problemen zijn (de gemeenten).[71] Mede hierom is de Security Officer gestopt met de samenvattende rapportages, ondanks de wettelijke verplichting hiertoe.
- De Suwipartijen moeten zich over hun eigen gegevensverwerkingen en over het gebruik van Suwinet. Dit leidt tot onnodige administratieve lasten.[72] Gemeenten krijgen daarenboven nog allerlei andere verantwoordingsverplichtingen opgelegd vanuit de Rijksoverheid, wat dit probleem nog verergert.[73]
- De Verantwoordingsrichtlijn is verouderd. Een dienst als Suwinet-Inlezen bestond bijvoorbeeld bij het opstellen van de huidige versie nog niet. Het is partijen in 2012 niet gelukt om het eens te worden over een nieuwe Verantwoordingsrichtlijn.

---

[70] Vgl. het Inspectie SZW Vervolgonderzoek Beveiliging en Privacy 2011: "Tot het moment dat gemeenten zich evenals de andere partijen die gebruik maken van gegevensuitwisseling via Suwinet, gaan verantwoorden, ziet Inspectie SZW risico's voor de beveiliging van persoonsgegevens en ook voor het gebruik en draagvlak van het instrument Suwinet als geheel. Inspectie SZW signaleert in dit verband verder dat nergens de taak is belegd om na te gaan of gemeenten volgens de normen van de Verantwoordingsrichtlijn hun beveiligingsbeleid en hun daaraan gekoppelde beveiligingsplan geregeld evalueren en zo nodig bijstellen."
"Zolang er geen normenkader in wet- en regelgeving is, waaraan alle partijen die gegevens uitwisselen via Suwinet, zich moeten houden, en er voor gemeenten geen verplichting is om zich te verantwoorden over de beveiliging van de gegevensuitwisseling via Suwinet (zoals die wel geldt voor UWV, SVB en IB), kan de sector Werk en Inkomen niet aantoonbaar maken dat er alles aan wordt gedaan om misbruik of oneigenlijk gebruik van persoonsgegevens van burgers te voorkomen."

[71] Samenvattende Rapportage over 2010 (de laatste): "Deze rapportage geeft, voor die organisaties die niet verplicht zijn de relevante informatie voor deze Samenvattende rapportage aan te leveren, geen volledig beeld, maar veeleer een indicatie in van de stand van zaken hun werkveld. De conclusies en aanbevelingen moeten in dit licht worden gezien."

[72] Samenvattende rapportage BKWI over 2010: "In het Normenkader GeVS wordt een kunstmatige onderscheid gemaakt tussen de beveiliging van de gegevensuitwisseling en van de gegevensverwerking en tussen de beveiliging van de GeVS en van de eigen informatiehuishouding. Deze zaken zijn echter verweven en het is dan ook gewenst te komen tot een situatie waarbij aangesloten organisaties transparantie bieden aangaande de beveiliging van de (eigen) informatiehuishouding conform een generieke richtlijn en een generiek normenkader en waarbij elke materiële afwijking, onder vermelding van de hieraan verbonden risico's en getroffen maatregelen, wordt benoemd."

[73] Notitie KING over "Zorgvuldig gebruik en verbeterpunten" (W&I 31 mei 2012): "Op 9 februari 2012 vraagt de VNG in een brief aan de Tweede Kamercommissie om aandacht te vragen voor de wijze waarop gemeenten het gebruik en de verwerking van persoonsgerelateerde informatie moeten verantwoorden. […] Deze aandacht is nodig omdat straks voor elke basisregistratie een audit gaat gelden. Daarbij komt ook nog een beveiligingsassessment voor het gebruik van DigID bij. De VNG blijft zich inzetten voor een eenduidige en centrale verantwoording en wil af van de sectorale verantwoordingen."

- Er is alleen iets geregeld voor verantwoording over informatiebeveiliging, maar niets over privacy compliance in brede zin. Privacy wordt nu impliciet meegenomen als onderdeel van de verantwoording over informatiebeveiliging en impliciet afgedwongen via het Suwi Gegevensregister.

3.11.3 ANALYSE EN BESCHOUWING

De regels voor verantwoording over privacy en informatiebeveiliging door de op Suwinet aangesloten partijen zijn duidelijk. Ze blijken over het algemeen ook effectief, behalve ten aanzien van informatiebeveiliging door gemeenten. Ook daar zijn de regels duidelijk, maar blijkt de verantwoording door B&W aan de gemeenteraad in de praktijk vaak niet te werken, getuige het ondermaatse niveau van informatiebeveiliging bij veel gemeenten.

De oorzaak hiervan is dat er door wetgeving geen level playing field in te richten is voor alle Suwipartijen. Slechts twee van de 410 Suwipartijen hebben een (externe) verantwoordingsplicht.

Op korte termijn is het vooral zaak via toezicht en handhaving de gemeenten te dwingen hun informatiebeveiliging op een acceptabel peil te brengen. Ook dient de huidige ineffectieve wijze van verantwoording door gemeenten herzien te worden. Een effectievere verantwoording is niet alleen noodzakelijk om het vertrouwen in de keten te borgen maar is ook een vereiste in de toekomstige EU Privacyverordening waarin bedrijven en organisaties moeten kunnen aantonen dat zij persoonsgegevens adequaat beschermen (zie verder sectie 4 over nieuwe ontwikkelingen).

Wenselijk is dat de herziende verantwoording aansluit op de binnen Suwinet al geldende verantwoordingsrichtlijnen om de eenduidigheid en uniformiteit ervan te borgen. Nog beter is het om te komen tot een generiekere, minder sectorspecifieke, verantwoordingsrichtlijn en normenkader voor Suwinet. Dit vergemakkelijkt niet alleen de aansluiting van andere partijen, maar levert ook kostenbesparing en lastenverlichting op. Daarnaast verlaagt de betere aansluiting ook de weerstand voor rapporteren ten behoeve van transparantie en sturing. Een alternatieve, of tijdelijke aanpak, is de al eerder genoemde gedifferentieerde aanpak waarbij de eigen baseline voor informatiebeveiliging binnen gemeenten slechts recht geeft op bepaalde gegevens en/of diensten.

3.11.4 MITIGERENDE MAATREGELEN

Aangaande de privacyrisico's met betrekking tot verantwoording zijn de volgende maatregelen te treffen:

- Actualiseer de Verantwoordingsrichtlijn, en voor zover nodig ook de wettelijke kaders waarin die is ingebed.
- Breid de scope uit zodat de Verantwoordingsrichtlijn behalve over informatiebeveiliging ook over privacybescherming gaat.
- Pas de Verantwoordingsrichtlijn op zo'n manier aan dat hij ook de gemeenten dwingt tot het effectief en openbaar afleggen van verantwoording over hun privacybescherming en informatiebeveiliging. De Baseline Informatiebeveiliging Gemeenten (BIG) kan hierbij helpen. Door deze af te stemmen met of als basis te laten dienen voor een nieuw Normenkader wordt het voor gemeenten eenvoudiger zich te verantwoorden over hun beveiliging waarmee een grote drempel weggenomen is. Hierdoor krijgt ook de Samenvattende Rapportage van de Security Officer van BKWI weer nut en dient deze in ere hersteld te worden.
- Zorg ervoor dat Suwipartijen zich niet langer apart hoeven te verantwoorden over hun eigen informatiehuishouding en over hun gebruik van Suwinet.

- Haak zoveel mogelijk aan bij bewegingen om zoveel mogelijk te komen tot één verantwoordingsregime voor gemeenten tegenover Suwinet, DigiD, basisregistraties enz.

3.12 TOEZICHT EN HANDHAVING

3.12.1 HOE IS HET FORMEEL GEREGELD?

Het toezicht op Suwinet is geregeld in art. 37 Wet Suwi. Dat bepaalt dat Inspectie SZW onder gezag van de minister van SZW toezicht houdt op de taakuitoefening door UWV, SVB en Inlichtingenbureau. Inspectie SZW houdt ook toezicht op de rechtmatigheid en doelmatigheid van samenwerking van deze partijen en gemeenten in het sociale domein. Aangezien normen en eisen op het gebied van privacybescherming en informatiebeveiliging voortvloeien uit de WBP en de Suwiwet- en -regelgeving, is het onrechtmatig om die met voeten te treden. Daarmee vallen deze terreinen binnen de toezichtsbevoegdheid van Inspectie SZW.

Naast Inspectie SZW is ook het College Bescherming Persoonsgegevens bevoegd om toezicht te houden op het uitwisselen van gegevens via Suwinet. Dit volgt uit de algemene opdracht aan het CBP om toezicht te houden op de verwerking van persoonsgegevens (art. 51 lid 1 WBP).

Wanneer een partij ernstig in gebreke is met betrekking tot de beveiliging en privacy van gegevens kan de staatssecretaris dit onder de aandacht brengen van het College Bescherming Persoonsgegevens (CBP). Als niet aan de vereisten van de Wet bescherming persoonsgegevens wordt voldaan, kan het CBP deze met dwangsommen handhaven. Als blijkt dat met deze maatregelen de beveiliging van Suwinet onvoldoende verbetert, dan kan de staatssecretaris overwegen om aanvullende maatregelen te nemen.[74]

De Vraag-en-Antwoordpagina van het Gemeenteloket van SZW n.a.v. de brief van staatssecretaris De Krom in juni 2012 aan de Colleges van B&W geeft aan wat in dat uiterste geval de mogelijkheden van de minister van SZW zijn:
"*Welke aanvullende maatregelen kan de Minister van SZW nemen als blijkt dat gemeenten onvoldoende doen om de informatiebeveiliging op orde te brengen?*
In dat geval kan de Minister bijvoorbeeld een zogenaamde aanwijzing geven op grond van artikel 10, derde lid van de Wet SUWI aan gemeenten die ernstig in gebreke blijven. De betreffende gemeente moet dan de informatiebeveiliging en bescherming van persoonsgegevens binnen een te stellen termijn alsnog op orde brengen. Als de gemeente na afloop van die termijn nog niet heeft voldaan aan die aanwijzing, kan de Minister op grond van genoemd wetsartikel "noodzakelijke voorzieningen" treffen. Daarbij kan gedacht worden aan gehele of gedeeltelijke afsluiting van Suwinet (al dan niet tijdelijk) of het inschakelen van een externe partij die op kosten van de gemeente de beveiliging alsnog op orde brengt."

[74] Verzamelbrief special fraudebestrijding maart 2012 (vgl. brief De Krom juni 2012 aan de Colleges van B&W, in afschrift aan de gemeenteraden).

3.12.2 WELKE MAATREGELEN ZIJN GETROFFEN?

Inspectie SZW doet geregeld onderzoeken naar gegevensverwerking, privacybescherming en informatiebeveiliging in het Suwidomein, in het bijzonder via Suwinet.

BKWI stelt ten behoeve van toezicht en handhaving op basis van log-gegevens rapportages op en stuurt deze automatisch door aan UWV, SVB en de gemeenten die zich daarvoor hebben aangemeld. BKWI kan op basis van een verzoek ook gerichte rapportages aanleveren.

3.12.3 WELKE KWETSBAARHEDEN ZIJN ER?

Het is niet duidelijk welke mogelijkheden de staatssecretaris en minister hebben om zonodig in te grijpen, met name richting de gemeenten. De hierboven geciteerde verwijzing naar art. 10 lid 3 Wet Suwi lijkt namelijk geen hout te snijden, aangezien die bepaling alleen ziet op de samenwerking tussen gemeenten en UWV in de Werkpleinen. Ook is de minister formeel niet direct (Wbp-)verantwoordelijk voor Suwinet.

Het CBP kan of wil geen capaciteit vrijmaken voor effectief toezicht en handhaving ten aanzien van Suwinet. Inspectie SZW constateert wel keer op keer misstanden, maar heeft niet de bevoegdheid om in te grijpen[75], terwijl het de staatssecretaris en minister van SZW in de praktijk ontbreekt aan effectieve mogelijkheden daartoe. De onrechtmatigheid als gevolg van de ontoereikende informatiebeveiliging aan gemeentekant die al zeker acht jaar bekend is, is daardoor nog altijd niet doortastend aangepakt.

Gemeenten lijken zich nog onvoldoende bewust van het feit dat zij een ernstig nalevingstekort hebben. Zo hebben lang niet alle gemeenten zich aangemeld voor de toezicht en handhaving ondersteunende rapportages van BKWI. En in haar rapport “De keten volgt klanten” uit 2012 constateert Inspectie SZW (niet expliciet, maar feitelijk wel vooral ten aanzien van gemeenten):
“In de gesprekken met de SUWI-partijen is duidelijk geworden dat het onderwerp bescherming van persoonsgegevens in de praktijk van alle dag minder prioriteit krijgt dan feitelijk gewenst is. Men gaat uit van het integer handelen door de professionals. Bij sommige organisaties moeten professionals een integriteitsverklaring tekenen, maar op schendingen wordt zelden gecontroleerd. Deze worden dus ook niet bestraft bij overtredingen. De sociale controle zou voldoende waarborgen dat de privacy van klanten niet wordt geschonden.”

Om het zorgvuldig gebruik van Suwinet te bevorderen is met succes in 2011-2012 de campagne “Zorgvuldig gebruik Suwinet” gevoerd. De initiatiefnemers voor deze campagne zijn het ministerie van SZW, Divosa, VNG, KING, het Inlichtingenbureau en het BKWI. Het doel van de campagne was het realiseren van een structurele inbedding van een zorgvuldig gebruik van Suwinet om de burger het vertrouwen te geven dat zijn of haar gegevens in veilige handen zijn.

[75] In een van zijn adviezen over Suwi heeft het CBP aangegeven dat zijns inziens toezicht primair binnen de sector geregeld moet worden. Het CBP en Inspectie SZW hebben in die lijn ook afspraken gemaakt over de verdeling van toezichtstaken; daarin wordt echter gezwegen over handhaving, waartoe Inspectie SZW geen en het CBP wel mogelijkheden heeft.

Niet overal zijn security officers aangesteld. Waar die er wel zijn, hebben ze lang niet altijd ook privacy in hun takenpakket, laat staan dat er aparte privacy officers zouden zijn.

Gemeenten die op het terrein van informatiebeveiliging wél hun verantwoordelijkheid nemen, lopen ook tegen problemen aan. In zijn notitie over het “Zorgvuldig gebruik en verbeterpunten” van Suwinet stelt KING voor om de security officers van gemeenten zelf de mogelijkheid te geven om na te gaan welke medewerkers van zijn organisatie persoonsgebonden informatie over een bepaalde burger heeft opgevraagd. Nu kan dat alleen door bij BKWI een gericht verzoek in te dienen. Door een voorziening aan te bieden die alleen gebruikt mag worden door de bij het BKWI geregistreerde security officers kunnen afnemers sneller zelf onderzoeken uitvoeren en hier ook sneller gebruik van worden gemaakt. Deze voorziening is een belangrijke aanvulling op de huidige rapportages. Vanuit organisaties is er kritiek dat de standaard rapportages ondoorzichtig zijn voor gericht onderzoek. Als er specifieke vragen zijn dan kan BWKI hierin voorzien middels specifieke rapportages. Deze specifieke rapportages levert BKWI dan op verzoek van de vragende partij. Het betreft hier dan vragen als:

- Welke gegevens heeft een bepaalde medeweker bevraagd?
- Welke medewerkers hebben bepaalde burgers bevraagd?
- Hebben medewerkers informatie buiten of binnen een bepaald gebied bevraagd?

Niet alle partijen maken gebruik van de rapportages.

3.12.4 ANALYSE EN BESCHOUWING

Het beeld over toezicht en handhaving op het gebied van informatiebeveiliging is helder. Er wordt actief toezicht gehouden namens de minister door Inspectie SZW. Uit dat toezicht blijkt al jarenlang dat er één groot probleem is, namelijk de ontoereikende informatiebeveiliging bij gemeenten. Van effectieve handhaving is echter geen sprake; er wordt nauwelijks gestuurd op verbetering van knelpunten. Dat moet beter. Onder regie van de minister van SZW als stelselverantwoordelijke dienen de betrokken partijen daarom onderling afspraken te maken om te komen tot samenhangend en effectief toezicht en handhaving. Dit dient niet alleen achteraf plaats te vinden via rapportages of onderzoeken van de inspectie, maar ook op een meer proactieve manier om voortijdig in te kunnen grijpen. Bij dit laatste kan bijvoorbeeld gedacht worden aan strenger toezien of de aan te sluiten partijen wel aan de voorwaarden hebben voldoen of dat een bepaalde gedoogsituatie na verloop van tijd opgeheven wordt.

Daarnaast blijft de mens een zwakke schakel. Door onwetendheid of gemakzucht ontstaan soms grote privacyrisico’s. Voorbeelden hiervan zijn ontwikkelaars van applicaties die testen met echte BSNs, het uit nieuwsgierigheid raadplegen van gegevens van bepaalde personen en het doorgeven van gegevens aan derden onder druk of uit financieel gewin. Vaak komen deze zaken achteraf aan het licht (door goede monitorring) maar dan is het kwaad al geschiedt. Investeren in meer bewustwording van de (keten)risico’s bij professionals en in het verbeteren van hun integriteit kan dit soort zaken voorkomen. Dit dient opgepakt te worden door de keten als geheel alsmede de individuele ketenpartijen en zal vormgegeven moeten worden als een continu proces.

3.12.5 MITIGERENDE MAATREGELEN

Ter verbetering van toezicht en handhaving ten aanzien van informatiebeveiliging en privacybescherming kunnen de volgende maatregelen genomen worden:

- Zorg voor heldere en transparante verantwoording en toezicht, zodat volstrekt helder is bij welke partijen er op welke gebieden in welke mate sprake is van een nalevingstekort.
- Zorg dat er één partij is die eindverantwoordelijk is voor toezicht op de naleving van regels en normen op het gebied van privacybescherming en informatiebeveiliging.
- Zorg ervoor dat deze partij ook effectief kan handhaven.
- Zorg ervoor dat deze partij zichzelf ook moet verantwoorden, met name over de genomen actie ten aanzien van vastgestelde nalevingstekorten.
- Investeer continu in bewustwording bij en integriteit van professionals. Hiermee kunnen privacyrisico's voortijdig in de kiem gesmoord worden.

4 Nieuwe ontwikkelingen

Voor het uitvoeren van een PIA is het belangrijk toekomstige ontwikkelingen in ogenschouw te nemen. Deze kunnen van invloed zijn op te treffen juridische, organisatorische en/of technische maatregelen betreffende het borgen van privacy in Suwinet. Dit hoofdstuk schetst enkele nieuwe ontwikkelingen en de impact ervan op privacy in Suwinet.

4.1 BREDER GEBRUIK SUWINET

Er zijn een aantal trends die breder gebruik van Suwinet voor gegevensuitwisseling rechtvaardigen[76]. Ten eerste wordt ICT steeds vaker ingezet om de efficiency van processen bij de overheid te vergroten en om de administratieve lastendruk te verlagen. Steeds meer informatiestromen lopen binnen en tussen verschillende overheden, vaak over de grenzen van beleidsterreinen heen. Ook de grens tussen publieke en private sector wordt vaak overschreden. Op het gebied van werk en inkomen is dit zichtbaar door de flinke groei van bronnen en afnemers die via Suwinet-gegevens met elkaar uitwisselen. Ten tweede is er binnen gemeenten een ontwikkeling zichtbaar om op het beleidsterrein van werk en inkomen steeds meer verbinding met welzijn, inburgering, zorg, maatschappelijke ondersteuning en onderwijs te zoeken. Binnen gemeenten zijn de afdelingen sociale zaken en economische zaken meer gaan samenwerken om bijvoorbeeld werkgevers integrale dienstverlening te kunnen bieden (samen met UWV). De invoering van de Participatiewet maakt het voor gemeenten nog meer noodzakelijk om samen te werken met de aanpalende beleidsterreinen. Alleen zo kan de brede doelgroep van de wet aan werk worden geholpen.

Om dergelijke ontwikkelingen met of via Suwinet te ondersteunen vereist een breder gebruik ervan en is niet zonder risico's. De kaders van Suwinet worden met verbreding van de Suwinet dienstverlening verder opgerekt. Er ontstaan meerdere sporen doordat inlezende en gegevensleverende partijen van buiten het Suwi-domein toetreden met daarbij behorende wettelijke of andere kaders. Dit kan leiden tot rechtsonzekerheid, stroperigheid in de besluitvorming, en toenemende beheerlast bij BKWI. De kans op fouten en non-compliance neemt toe, de doelbinding komt met het koppelen van meerdere bestanden van leverende partijen onder druk te staan[77], mede als gevolg van een afnemende transparantie in de keten, en de ketenperformance kan verminderen en daarmee de beoogde e-efficiency. De afgelopen periode zijn steeds meer partijen aangesloten, zowel leveranciers als afnemers. Met de komst van inlezende applicaties gebeurt het bevragen van gegevens steeds meer automatisch en soms op meerdere BSNs tegelijk. Daarmee zijn veel meer toegangspunten tot meer gegevens ontstaan, waardoor de infrastructuur per definitie onoverzichtelijker en kwetsbaarder is daar er meerdere potentiële zwakke plekken zijn. De infrastructuur is hierdoor zowel technisch als organisatorisch moeilijker te beveiligen. Verder zal door een toename van het gegevensverkeer en waarschijnlijk ook de rijkheid van de gegevensset, de noodzaak voor het verbeteren van het beveiligingsniveau toenemen. Dit zal vooral gelden voor gemeenten als gevolg van de toenemende gegevensdichtheid door de integrale informatievoorziening.

[76] Jaarplan Inspectie SZW 2012.
[77] Een zorg die ook geuit is in het 2012 jaarverslag van het CBP, zie http://www.cbpweb.nl/Pages/jv_2012.aspx.

Vanuit risico-oogpunt is het verstandig te overwegen om meerdere (fysieke of virtuele) instanties van de Suwi-broker te creëren. Dit voorkomt dat de Suwi-broker een te groot single-point-of-failure wordt (minder gevolgen, minder aantrekkelijk target voor aanvallen), maakt de ketens overzichtelijker (minder partijen), en maakt daarmee ook de afspraken die tussen de betrokken partijen gemaakt moeten worden gemakkelijker (minder stroperigheid). Aan de andere kant, is het niet uit te sluiten dat de leveranciers en inlezende partijen in dat geval moeten aansluiten op meerdere brokers wat de beveiliging ook weer niet ten goede komt. Een impactanalyse zou hier meer inzicht in kunnen verstrekken.

Met een verbreding van Suwinet wordt het ook steeds belangrijker om goed te testen alvorens operationeel te gaan met nieuwe diensten of gegevensuitwisselingen met nieuwe partijen. Ketenbrede testomgevingen zijn hiervoor essentieel evenals de beschikbaarheid van testdata die van goede kwaliteit is en van voldoende grootte en door de hele keten heen is afgestemd.

Ook zijn er organisatorische implicaties. Met het toenemende aantal partijen in de keten(s) wordt het moeilijker om afspraken te maken. Wijzigingen in de techniek of processen hebben gevolgen voor steeds meer partijen. Heldere en sluitende wetgeving kan hiervoor een generieke oplossing bieden. Hierbij dient in ogenschouw genomen te worden dat nieuwe voorgenomen wettelijke maatregelen die gericht zijn op de invoering en rechtvaardiging van nieuwe grootschalige verwerkingen van persoonsgegevens nadrukkelijk getoetst moeten worden op effectiviteit[78]. Over de technische en informationele effectiviteit moet op transparante wijze verantwoording worden afgelegd.

UWV, SVB en gemeenten wisselen al gegevens uit met organisaties buiten het SUWI-domein. Dergelijke de uitwisseling van gegevens met organisaties buiten het Suwidomein is noodzakelijk voor zowel handhaving als voor de (overheidsbrede) dienstverlening aan de cliënten. De Inspectie SZW heeft onlangs gerapporteerd over informatie-uitwisseling vanuit Suwinet met partijen buiten het Suwidomein[79]. Uit een aantal observaties van de inspectie volgen risico's met betrekking van de privacy van de cliënt:

- Informatie-uitwisseling op gevalsniveau met partijen buiten het Suwidomein is veel minder gestandaardiseerd en gesystematiseerd en sterk afhankelijk van individuele professionals. Hoewel ook deze gegevensleveringen vanuit Suwinet altijd gebaseerd moeten zijn op wet en regelgeving en de daaraan gerelateerde doelbinding en proportionaliteit is er een grotere kans dat de kwaliteit van de informatie niet geborgd is wat een risico kan vormen voor de privacy van de cliënt.
- Het zodanig inrichten van de informatie-uitwisseling dat deze voldoet aan de WBP en de Wet Suwi, vereist specifieke deskundigheid op het gebied van wetgeving en het uitvoeringsproces. Voor de uitvoering is het vaak moeilijk om de dienstverlening zo in te richten, dat deze voldoet aan de wettelijke kaders, en tegelijkertijd recht doet aan maatwerk en goede dienstverlening aan de cliënt. Er worden vaak, al dan niet terecht, wettelijke belemmeringen ervaren om informatie die nodig is voor goede dienstverlening aan de cliënt, uit te wisselen. Hoewel er een grote mate van privacy bewustzijn is, zijn er aanwijzingen dat de

[78] Bijlage notitie privacybeleid, Ministerie van Veiligheid en Justitie, 29 april 2011, ref. 5688920/11/6.
[79] Informatie-uitwisseling van de SUWIketen met andere partijen, rapport Inspectie SZW, 2012, zie http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2012/10/10/informatie-uitwisseling-van-de-suwi-keten-met-andere-partijen-programmarapportage-informatieprocessen.html.

grenzen van de privacywetgeving soms worden opgerekt of overschreden, om toch die dienstverlening te bieden, die gemeenten nodig achten voor hun cliënten.

Ondanks dat de schaal waarop gegevensuitwisseling vanuit Suwinet met partijen buiten het Suwidomein plaatsvindt nu nog beperkt is (ongeveer 2% van het totale gegevensverkeer), valt niet uit te sluiten dat dit in de toekomst zal toenemen. Hiermee neemt de kans toe dat een van de genoemde privacyrisico's zich zal voordoen.

Ook wordt er geëxperimenteerd met internationale verbreding van Suwinet[80]. Juridisch gezien zijn de leveranciers binnen Suwinet bevoegd om gegevens te delen met buitenlandse uitvoeringsorganen. Artikel 74 lid 2a en artikel 5.6 van de Wet Suwi maken het mogelijk om gegevens te verstrekken aan buitenlandse organen. De geheimhoudingsplicht van artikel 74 wordt ook opzij gezet door supranationale wetgeving waarin de grondslag voor uitvoeringsorganen wordt gelegd om elkaar gegevens te verstrekken die ze nodig hebben voor de uitvoering van hun wettelijke taken. De Verordeningen 1408/71 en 883/2004 zijn voorbeelden van supranationale wetgeving. Langs beide juridische wegen is er dus een basis om gegevens te verstrekken. In principe gaat het hier om gegevens die nodig zijn om de Verordeningen goed te kunnen uitvoeren. Daaronder vallen NAW-gegevens, geboortedatum, BSN, duur van dienstverbanden en inkomensgegevens tijdens die dienstverbanden.

Dat het BSN daar bij zit valt op. Op grond van nationale wetgeving is het gebruik van BSN door buitenlandse organisaties niet toegestaan. De Wet Algemene Bepalingen Burgerservicenummer (Wabb) bepaalt in artikel 1 onder d, dat het gebruik van het BSN alleen is toegestaan voor (nationale) overheidsorganisaties[81] en een ieder ander dan een overheidsorgaan of degene aan wie het BSN is toegekend, voor zover deze werkzaamheden verricht waarbij het gebruik door hem of haar van het BSN bij of krachtens de wet is toegestaan.

De buitenlandse bestuursorganen zoals bedoeld in artikel 5.6 van de Wet Suwi behoren tot de organen waarvoor het aansluitprotocol van toepassing is. Deze organen zullen net als de Nederlandse niet-Suwipartijen moeten voldoen aan de daarin gestelde voorwaarden, inclusief een EDP-audit. Hoe en wie zou moeten controleren of aan de gestelde voorwaarden wordt voldaan door het buitenlandse bestuursorgaan is onduidelijk.

Met het breder gebruik van Suwinet komen de technische, organisatorisch en juridische grenzen ervan snel in zicht waardoor de kans op schenden van de privacy van de burger toeneemt evenals het oplopen van reputatieschade door een van de partijen in Suwinet.

4.2 EU PRIVACY VERORDENING

De Wbp is een implementatie van de Europese privacyrichtlijn. Kortgeleden (25 januari 2012) heeft Europese Commissie de Europese Privacy Verordening voorgesteld die de huidige Europese Privacyrichtlijn moet vervangen. De nieuwe verordening heeft, anders dan een richtlijn, directe werking in alle lidstaten. Zodra de verordening van kracht wordt, zal ook de huidige Wbp daarmee vervangen of daarop aangepast moeten worden. Kenmerkend voor

[80] Zie bijvoorbeeld: http://www.uwv.nl/Zakelijk/gegevensdiensten/klantenservice/nieuwsbrief/2012/oktober-2/start_vooronderzoek_internationale_suwinet-inkijk.aspx.
[81] Als bedoeld in de Algemene wet bestuursrecht, artikel 1:1 onder 1.

de nieuwe verordening is dat het legt veel strengere normen oplegt. Met het oog op de toekomstige ontwikkeling van Suwinet is het belangrijk rekening te houden met deze verordening.

Aandachtspunten voor Suwinet zijn de volgende elementen uit de verordening:

- Versterking rechten betrokkenen. Het voorstel voor de verordening bevat op onderdelen een versterking van de rechten van burgers van wie persoonsgegevens worden verwerkt. Burgers moeten, voordat zij toestemming geven, duidelijk en helder worden geïnformeerd over het gebruik van hun gegevens. Ook moeten zij geïnformeerd worden over en hoe zij hun rechten afdoende moeten kunnen uitoefenen. Uitdrukkelijke toestemming voor het verzamelen en gebruiken van gegevens is in de verordening het uitgangspunt, dat wil zeggen dat betrokkene expliciet zijn wil heeft geuit. De bewijslast ligt bij de verantwoordelijke. De burger krijgt een betere controle over de gegevens en heeft het recht om vergeten te worden.
- Grotere verantwoordelijkheid bedrijven en organisaties. De verordening legt voorts een grotere verantwoordelijkheid bij bedrijven en organisaties die persoonsgegevens verwerken. Hun verantwoordelijkheid gaat dus verder dan actief informeren, Zij moeten betrokkenen dus actie informeren niet alleen duidelijk en begrijpelijk informeren over de gegevensverwerking maar ook informatie geven over de periode van opslag van de gegevens. Zij moeten kunnen aantonen dat zij persoonsgegevens adequaat beschermen. In het geval dat er sprake is van een datalek, moeten bedrijven dit zo spoedig mogelijk melden bij de nationale privacytoezichthouder. Bedrijven met meer dan 250 werknemers worden verplicht een ‘data privacy officer’ aan te stellen.
- Versteviging rol van privacytoezichthouders. In de conceptverordening staan duidelijke criteria voor de onafhankelijkheid van de privacytoezichthouders en hun onderzoeksbevoegdheden. Privacytoezichthouders hebben bijvoorbeeld het recht op informatie van bedrijven en organisaties en moeten toegang kunnen krijgen tot hun panden. Ook krijgen de toezichthouders geharmoniseerde en krachtige handhavingsbevoegdheden, inclusief een boetebevoegdheid. Boetes kunnen oplopen tot 450.000 euro per overtreding en voor bepaalde overtredingen geldt zelfs een boete van 2 procent van de jaarlijkse omzet.

De verordening ligt bij de Europese Raad die erover moet besluiten. De verordening moet 1/2015 van kracht worden.

De nadruk in de nieuwe regelgeving ligt werkelijk op het principe van transparantie en verantwoordelijkheid. De betrokkene moet perfect geïnformeerd zijn over welke gegevens er worden verwerkt, voor welke doeleinden, hoe lang zij worden bewaard en aan wie zij eventueel worden doorgegeven. Zij moeten ook weten tot welke autoriteit zij zich kunnen richten in geval van misbruik en dit alles moet in eenvoudige bewoordingen worden uitgelegd. De betrokkene moet ook de gevolgen kennen indien hij zijn persoonsgegevens niet vrijgeeft, bijvoorbeeld: “Indien u uw persoonsgegevens niet opgeeft, heeft u geen toegang tot onze diensten”.

Suwinet biedt de burger op dit moment nog geen overzicht van welke partij welke gegevens en voor welk doel heeft opgevraagd[82]. De vraag is of het Suwinet stelsel hier ook verantwoordelijk voor is of dat dit de verantwoordelijkheid

[82] Zie ook de nota van bevindingen van de Inspectie SZW over “Transparante verwerking van persoonsgegevens in het SUWI-domein”, 2011, zie http://www.inspectieszw.nl/images/transparante%20verwerking%20persoonsgegevens%20suwi-domein_tcm335-327747.pdf.

van de individuele partijen is. Immers, de verordening stelt ook dat partijen zelf meer verantwoordelijk worden voor het verwerken van persoonsgegevens. In die zin kan de verordening gezien worden als een positief middel voor partijen om hun beveiliging op orde te hebben.

4.3 CLOUD / SAAS

Cloud of Software-as-a-Service (SaaS) oplossingen zijn sterk in opkomst bij veel afnemende partijen (gemeenten). De software is niet geïnstalleerd bij de afnemende partij maar draait op een centrale plek en is daar beschikbaar.De informatie wordt nu niet afgeleverd bij afnemende partij maar bij een tussenstation waar de afnemende partij geen eigenaar van is, de SaaS-leverancier. De SaaS-leverancier is hierdoor een bewerker voor de afnemende partij. Dit betekent ook dat de SaaS-leverancier zich zal moeten conformeren aan vigerende wet- en regelgeving binnen Suwinet. Ook de afspraken zoals gedefinieerd in het Normenkader, de Verantwoordingsrichtlijn en de keten-SLA zullen van toepassing zijn. De vraag is of SaaS-leveranciers hieraan willen en kunnen voldoen. Een minder sectorale en meer generieke aanpak met betrekking tot beveiliging en privacy kan daarbij helpen.

Indien gemeenten gebruik maken dergelijke leveranciers blijven ze verantwoordelijk voor het maken van goede afspraken over de uitvoering van de bewerkersrol. Zoals hiervoor al bleek is de keten SLA geen document waar gemeenten aan gehouden zijn en gelden ook de Verantwoordingsrichtlijn en het Normenkader niet voor gemeenten als Suwipartij. En dus ook niet voor partijen die optreden als bewerker voor gemeenten. Hierdoor wordt het gebrek aan transparantie door verantwoording vergroot met alle risico's van dien.

Een ander potentieel risico dat het gebruik van cloud of SaaS-leveranciers met zich meebrengt is de locatie van de bewerking van de gegevens. Het is onwenselijk dat dit bijvoorbeeld in het buitenland gebeurd waar andere wetten kunnen gelden en men de controle over de gegevens verliest. De Patriot Act is hiervan een goed voorbeeld. Via deze wet kan de Amerikaanse overheid beslag leggen op gegevens op eigen grondgebied of onder beheer van Amerikaanse bedrijven. De Wbp stelt echter eisen aan de doorgifte van persoonsgegevens naar landen buiten de EU. Persoonsgegevens mogen in beginsel slechts naar dergelijke landen worden doorgegeven als deze een 'passend beschermingsniveau' bieden. Handreikingen hiervoor worden beschreven in de nieuwe CBP richtsnoeren voor beveiliging van persoonsgegevens[83]. Er is dus een conflict tussen Europese en Amerikaanse wetgeving. Op basis hiervan heeft KING in 2012 de gemeente Groningen geadviseerd af te zien van cloud dienstverlening[84].

Het College bescherming persoonsgegevens (CBP) heeft in een zienswijze antwoord gegeven op een drietal vragen van SURFmarket over cloud computing in relatie tot de bescherming van persoonsgegevens[85]. In zijn zienswijze benadrukt het CBP dat een belangrijk uitgangspunt is dat Nederlandse bedrijven of organisaties die clouddiensten afnemen bij een Amerikaanse aanbieder eindverantwoordelijk zijn voor de naleving van de Wet bescherming persoonsgegevens (Wbp). Bij het sluiten van een overeenkomst voor clouddienstverlening zal een bedrijf of organisatie zich dan ook moeten vergewissen dat de toepasselijke wettelijke regels zijn afgedekt. Zo nodig moeten zij

[83] CBP richtsnoeren voor beveiliging van persoonsgegevens, 2013, zie http://wetten.overheid.nl/BWBR0033572/geldigheidsdatum_01-08-2013#4.
[84] Advies KING over cloud computing aan de gemeente Groningen, zie http://www.kinggemeenten.nl/data/king-cases/king-informeert-groningen-over-cloud-computing.
[85] Zienswijze CBP over cloud computing, september 2012, zie http://www.cbpweb.nl/Pages/med_20120910-zienswijze-cbp-cloudcomputing.aspx.

aanvullende afspraken in de overeenkomst met de Amerikaanse aanbieder van de clouddiensten opnemen. In ieder geval geldt dat voor de beveiliging van de in de cloud verwerkte persoonsgegevens.

Doorgifte van persoonsgegevens naar de VS is mogelijk als de betreffende Amerikaanse clouddienstverlener zich heeft verplicht tot naleving van de zogeheten Safe Harbor Principles (Veilige Haven Beginselen). De Europese Commissie heeft namelijk bepaald dat in dat geval sprake is van een ‘passend beschermingsniveau’. Het CBP benadrukt in zijn zienswijze dat hierdoor doorgifte weliswaar mogelijk is, maar dat dit echter niet garandeert dat de daadwerkelijke verwerking van persoonsgegevens in de VS ook voldoet aan alle eisen van Europese inclusief Nederlandse privacywetgeving. Voor naleving van de wet blijft de Nederlandse afnemer van clouddiensten verantwoordelijk.

Het gebruik van cloud of SaaS-leveranciers voor gegevensverwerking omvat een complex speelveld van juridische, technische en organisatorische uitdagingen. Vooral als het partijen buiten de EU betreft. Suwipartijen die overwegen gebruik te maken van cloud of SaaS-leveranciers kunnen daarom beter kiezen voor zekerheid en zorgen dat data uitsluitend onder Nederlands of Europees recht valt. Dat biedt meer mogelijkheden voor controle.

5 Samenvatting en conclusies

5.1 PRIVACY: GOED GEREGELD?

Suwinet is destijds neergezet met veel aandacht en waarborgen voor privacybescherming en gegevensbeveiliging. Aansluitend op de WBP is er met de Wet Suwi en de bijbehorende lagere regelgeving een wettelijk kader geschapen met veel aandacht voor de behoorlijke en zorgvuldige omgang met persoonsgegevens. Binnen dit kader zijn er allerlei afspraken gemaakt tussen de betrokken partijen onderling. Die hebben hun beslag gekregen in o.a. het Suwinet Gegevensregister, een keten-SLA en een Verantwoordingsrichtlijn met bijbehorend Normenkader. De centrale infrastructuur zelf voor het uitwisselen van gegevens is besloten en beveiligd op niveau 2.

Mede hierdoor is Suwinet uitgegroeid tot een infrastructuur waarover het gegevensverkeer de afgelopen jaren fors is toegenomen evenals het aantal aangesloten partijen. Op basis hiervan kan Suwinet beschouwd worden als een succesvolle infrastructuur voor gegevensuitwisseling.

Desondanks blijkt uit de PIA dat er bij een aantal risicogebieden kwetsbaarheden in de infrastructuur en kaders voor het gebruik ervan te identificeren zijn. Deze kwetsbaarheden kunnen leiden tot onbevoegd en oneigenlijk gebruik van gegevens waardoor de privacy van klanten in het geding komt en partijen in de keten of Suwinet zelf reputatieschade kunnen oplopen.

5.2 OORZAKEN

Met het toenemende gebruik van Suwinet, in termen van aantallen partijen en hoeveelheden gegevens, zijn er een aantal samenhangende kwetsbaarheden ontstaan die elkaar op een negatieve manier beïnvloeden en daarmee tot privacyrisico's leiden. De kwetsbaarheden zijn vooral gerelateerd aan de in de PIA onderzochte risicogebieden met betrekking tot beveiliging, transparantie en verantwoordelijkheden & governance, en dienen in het licht van de gevoeligheid van de gegevens bezien te worden.

De gevoeligheid van de aard van de via Suwinet uitgewisselde gegevens is toegenomen. Gegevens als arbeidsongeschiktheid, fraudevorderingen, en detentie zijn erg privacygevoelig. Behalve de aard van de verwerkte gegevens brengt ook de verwerking ervan (in termen van o.a. transport, toegang, filtering) risico's met zich mee voor Suwinet als stelsel en voor de betrokkenen partijen daarin. Factoren die hierbij een rol spelen zijn onder meer

- de toename van de hoeveelheid verwerkte persoonsgegevens per persoon in Suwinet,
- de toename van het aantal mensen dat toegang heeft tot de gegevens (inmiddels zijn dat er ongeveer 40.000),
- de toename van de hoeveelheid verwerkte persoonsgegevens in het algemeen (jaarlijks ~120 miljoen berichten van ~5.5 miljoen burgers)
- de toename van het aantal doelen waarvoor de persoonsgegevens worden verwerkt en de impact erop van verlies van privacy of onrechtmatige verwerking.
- de toegenomen complexiteit van de verwerking van gegevens door toegenomen gebruik van Suwinet door een groter aantal partijen en verschillende diensten als Suwinet Inlezen en Inkijk.

Op basis hiervan kan geconcludeerd worden het risicoprofiel van Suwinet met betrekking tot de gevoeligheid van de gegevens is toegenomen. De beveiliging is op veel onderdelen meegegroeid met deze ontwikkelingen maar niet op alle vlakken. Een goed voorbeeld daarvan het niveau van authenticatieniveau dat gebruikt wordt om toegang te krijgen tot gegevens. Deze is te laag waardoor de toegang tot de gegevens onvoldoende kan worden afgeschermd en medewerkers niet kunnen ontkennen dat zij bepaalde handelingen verricht hebben omdat hun identiteit met onvoldoende zekerheid bepaald is. Bovendien sluit het huidige authenticatieniveau niet aan bij de niveaus die gehanteerd worden in de zorg en financiële sector waar twee-factor authenticatie-oplossingen gebruikelijk zijn. Ook het autorisatiebeleid dient naar een hoger niveau getild te worden. Door toenemende integrale informatievoorziening is de huidige autorisatie-aanpak niet geschikt om te voldoen aan de need-to-know en seperation-of-duties principes. Mogelijkheden voor meer fijnmazigere functie- of rule-based autorisatie-oplossingen dienen gezamenlijk verkend te worden. Deze twee voorbeelden illustreren dat de door de Suwipartijen gemaakte gezamenlijke afspraken en vastgestelde normen voor beveiliging in Suwinet toe zijn aan een update.

Beveiliging is een belangrijk element voor het borgen van de privacy van de burger in Suwinet. Hoewel hier onderscheid gemaakt dient te worden tussen een veilig gebruik van door Suwinet verkregen gegevens, wat een verantwoordelijkheid is van de afzonderlijke afnemers, en een veilig stelsel Suwinet, wat de verantwoordelijkheid is van UWV (en BKWI) als beheerder van Suwinet, zijn beide aspecten niet los van elkaar te zien als het gaat om privacyrisico's. Een potentieel falende beveiliging bij een afnemende partij kan een negatieve invloed hebben op het vertrouwen in Suwinet als infrastructuur voor gegevensuitwisseling en zelfs resulteren in reputatieschade. Vice versa, kan een potentieel falend stelsel consequenties hebben voor bijvoorbeeld de integriteit of beschikbaarheid van de gegevens waardoor afnemende partijen onjuiste beslissingen nemen die nadelig kunnen zijn voor de klant. De individuele Suwipartijen zijn zelf verantwoordelijk voor het inrichten van hun eigen beveiliging. De kaders hiervoor worden gezamenlijk vastgesteld.

De kaders voor de beveiliging van de op Suwinet aangesloten partijen staan conform de lagere regelgeving Suwi beschreven in de Verantwoordingsrichtlijn en bijbehorend Normenkader. Deze documenten hebben als doel een gelijkwaardig niveau van beveiliging over alle op Suwinet aangesloten partijen te borgen en afspraken te maken hoe deze partijen hierover verantwoording kunnen afleggen en transparantie kunnen bieden. De voorgeschreven rapportagevorm beoogt een eenduidig inzicht van de situaties van de afzonderlijke partijen te geven op basis waarvan op evenwichtige wijze een totaaloverzicht samengesteld kan worden aangaande de getroffen maatregelen voor het beheersen van de privacyrisico's in Suwinet. Echter, de regelgeving Suwi is niet verplichtend voor de gemeenten. Dit betekent dat zij zich niet hoeven te conformeren aan de Verantwoordingsrichtlijn en het Normenkader waardoor risico's ontstaan. Gemeenten hebben een eigen verantwoordingsregiem en zetten zich in voor een meer algemene verantwoording op basis van een generiek normenkader (in plaats van sectorale verantwoording). Zij werken momenteel aan een eigen baseline voor informatiebeveiliging, de BIG. Hierdoor ontstaat een onvolledig en niet eenduidige beeld van de wijze waarop partijen hun privacy en beveiliging hebben geregeld ten aanzien van via Suwinet afgenomen gegevens waardoor sturing op verbetering lastig is.

Een punt van zorg daarbij is dat in de loop der jaren regelmatig door de Inspectie SZW, het BKWI en achtereenvolgende staatssecretarissen geconstateerd is dat gemeenten een zwakke schakel vormen ten aanzien

van de beveiliging in Suwinet. Recent heeft de staatssecretaris in een brief aan gemeenten nogmaals gewezen op de verplichtingen die voortvloeien uit wet- en regelgeving en ook op de mogelijkheden van het Cbp en de minister om maatregelen te treffen.

Wat er niet toe bijdraagt om deze zorg weg te nemen is het ontbreken van enige **transparantie** of **verantwoording** van de gemeenten over hun beveiliging. Daardoor is er geen inzicht in de door de verschillende partijen getroffen maatregelen. Het (deels) ontbreken van inzicht kan ten koste gaan van het vertrouwen van partijen in het gebruik van Suwinet voor betrouwbare uitwisseling van persoonsgegevens in de toekomst en bij een breder gebruik ervan. Wat ook ontbreekt zijn voorzieningen om meer transparantie richting de burger te verstrekken over de gegevensuitwisselingen in Suwinet. Dit is nodig om straks te kunnen voldoen aan de nieuwe EU Privacy Verordening. Dit is niet zozeer een privacy-risico maar eerder een compliance-risico.

Met het toenemende aantal partijen in de keten en technologische ontwikkelingen zoals Suwinet-Inlezen is de transparantie van het feitelijk gegevensgebruik ten opzichte van dat voor Suwinet-Inkijk verslechterd. Daardoor is er ook minder zicht op bijvoorbeeld de doelbinding en proportionaliteit van het gegevensgebruik, waarmee die onder druk komen te staan. Uit onderzoeken en incidenten blijkt ook dat de genomen maatregelen in ieder geval waar het een aantal gemeenten betreft onvoldoende effectief zijn op deze vlakken en gegevens voor andere doeleinden worden (her)gebruikt. Een ander risico aangaande doelbinding is gerelateerd aan de complexiteit van de wetgeving rondom Suwinet. Het blijkt vaak lastig om de gegevens vast te stellen die nodig zijn voor de uitvoering van een wettelijke taak door een bepaalde groep mensen en onder welke voorwaarden dit moet gebeuren. Een illustratief voorbeeld hiervan is de moeite en tijd die het kost om de gegevensset te bepalen voor het vaststellen van recidive van fraude voor de uitvoering van de Fraudewet.

Omdat partijen zelf verantwoordelijk zijn voor het juist gebruik van afgenomen gegevens moeten zij hier verantwoording over afleggen. Dit betreft de herkomst van de gegevens alsmede de beveiliging ervan. Door de verslechterde transparantie komt deze verantwoording onder druk te staan en wordt gerichte aansturing hierop ter verbetering van de efficiëntie en de betrouwbaarheid van de gegevensuitwisseling via Suwinet belemmerd.

Bovengenoemde punten worden binnen het Suwistelsel onderkend – in ieder geval door sommige partijen. Het ontbreekt echter aan effectieve, stelselbrede **governance**. Daardoor wordt er onvoldoende krachtig werk gemaakt van het verbeteren van beveiliging en transparantie door verantwoording en schiet niet alleen de aansturing van de samenwerking vanuit risicobeheersing tekort maar ook die voor het realiseren van de ketendoelstelling voor betrouwbare uitwisseling van gegevens. Het gebrek aan governance is deels terug te voeren op een tekort aan goede en volledige stuurinformatie, maar vindt zijn oorzaak vooral in de soms onduidelijke, maar vaker eenvoudig niet effectieve manier waarop regievoering en besluitvorming binnen het stelsel zijn vormgegeven. Het gebrek aan governance is voor een belangrijk deel te wijten aan onduidelijkheid over de verdeling van verantwoordelijkheid (in de zin van de WBP) over de verschillende betrokken partijen. Met het zich terugtrekken van de minister van SZW in 2008 is die er bepaald niet helderder op geworden. Een gebrek aan governance is tot op zekere hoogte nog op te vangen door effectief toezicht en handhaving. Ook dat sluitstuk blijkt echter in de praktijk onvoldoende effectief omdat onvoldoende uitgewerkt is welke waarborgen de governance zou moeten bieden.

Gezien de toenemende mate van gegevensuitwisseling en gegevensrijkheid waardoor de privacy-gevoeligheid van Suwinet is toegenomen, de benoemde kwetsbaarheden en toekomstige ontwikkeling als de komst van de nieuwe EU Privacy Verordening, is het urgent om het privacy- en beveiligingsbeleid binnen Suwinet verder te optimaliseren, te verstevigen en te handhaven.

5.3 VERBETERINGEN

In de PIA zijn tal van verbeterpunten naar boven gekomen. De onderstaande secties biedt een overzicht van de verbeterpunten per risicogebied. Om de verbeterpunten verder te ordenen is daarnaast de volgende opdeling gemaakt met betrekking tot het doel van de verbetering:

- Optimalisatie van het gebruik van Suwinet;
- Optimalisatie van de verantwoordelijkheden en governance van Suwinet;
- Optimalisatie van de techniek van Suwinet.

5.3.1 GEVOELIGHEID EN BEVEILIGING VAN DE GEGEVENS

Optimalisatie gebruik Suwinet	
Verbeterpunt	Toelichting
Regel processen in om de bewustwording van privacyrisico's bij professionals te onderhouden en te verbeteren.	De mens blijft een zwakke schakel. Dit vereist vanuit beveiligingsperspectief continu aandacht.
Zet beveiligingsbeleid uit over ontwikkelingen als het nieuwe werken (thuis- en flexwerken, mobiele platformen) en cloud/SaaS.	Om te kunnen omgaan met nieuwe ontwikkeling.
Optimalisatie verantwoordelijkheden en governance van Suwinet	
Zorg voor een eenduidig en verplicht gedragen Normenkader en Verantwoordingsrichtlijn.	Update het Normenkader en zoek afstemming met de BIG om eenduidigheid te borgen. Zorg dat partijen zich gebonden voelen en er verantwoording over afleggen.
Optimalisatie techniek Suwinet	
Inventariseer welke beveiligingsonderdelen van het Normenkader versterkt dienen te worden.	Sterkere authenticatie-oplossingen zijn vereist. Maak hiervoor gebruik van bestaande middelen zoals de Rijkspas of UZI-pas.
Overweeg een gedifferentieerde aanpak waarbij het niveau van beveiliging bepaalt welke gegevens en diensten een partij kan afnemen.	Hierdoor worden niet alle partijen verplicht om te voldoen aan een hoog niveau van beveiliging wat kosten met zich meebrengt. Aansluiten wordt laagdrempeliger en sanctioneren wordt mogelijk indien een partij nalatigheid vertoond.
Realiseren van ketenbrede versleuteling van gegevensverkeer	Inventariseer de gaten en dicht ze.

5.3.2 LIMITERING VAN HET VERZAMELEN VAN GEGEVENS

Optimalisatie gebruik Suwinet	
Verbeterpunt	Toelichting
Verken de mogelijkheden om de autorisaties binnen Suwinet fijnmaziger te maken.	Dit wordt urgenter met de toenemende behoefte aan integrale informatievoorziening.
Optimalisatie verantwoordelijkheden en governance van Suwinet	
Neem maatregelen om, gegeven de toenemende informatiedichtheid, de transparantie in Suwinet te borgen.	Zie ook de sectie Transparantie hieronder.
Optimalisatie techniek Suwinet	
Borg dat alle log-bestanden op een betrouwbare manier opgeslagen/behandeld worden.	Dit om onomstotelijk te kunnen aantonen wie wat gedaan heeft.

5.3.3 LIMITERING VAN GEBRUIK VAN GEGEVENS

Optimalisatie gebruik Suwinet	
Verbeterpunt	Toelichting
Verzwaar de aansluitvoorwaarden.	Inclusief sanctioneren om hergebruik van ingelezen gegevens te voorkomen.
Verken de mogelijkheden en impact van een herijking van de autorisatie-infrastructuur.	Meer fijnmazigheid is gewenst om stapelen van rollen te reduceren.
Optimalisatie verantwoordelijkheden en governance van Suwinet	
-	-
Optimalisatie techniek Suwinet	
Optimaliseer het gebruik van gegevens door meer en intelligentere filtering.	Op basis van de filtering kan ook het gebruik van Suwinet in kaart gebracht worden.

5.3.4 DOELBINDING

Optimalisatie gebruik Suwinet	
Verbeterpunt	Toelichting
Laat regelmatig de informatiehuishouding van Suwinet toetsen op doelbinding en effectiviteit van de gegevensuitwisselingen.	Ketenbreed en structureel. Ook voor niet-Suwipartijen.
Optimalisatie verantwoordelijkheden en governance van Suwinet	

Verken de mogelijkheden voor vereenvoudiging van het wettelijk kader van Suwinet en verduidelijk de relevantie van de uit te wisselen gegevensset.	Indien overwogen wordt om de gegevensset concreet in de wet op te nemen is het verstandig om daarbij te linken aan het SGR zodat geen misinterpretatie kan plaatsvinden en nieuwe diensten sneller uitgerold kunnen worden.
Optimalisatie techniek Suwinet	
-	-

5.3.5 GEGEVENSKWALITEIT EN BESCHIKBAARHEID

Optimalisatie gebruik Suwinet	
Verbeterpunt	Toelichting
Overweeg processen in te richten die het partijen in de keten makkelijker maken om fouten in gegevens te corrigeren.	Verken of hier bestuurlijk draagvlak voor is.
Optimalisatie verantwoordelijkheden en governance van Suwinet	
-	-
Optimalisatie techniek Suwinet	
Steek meer effort in het verbeteren van ketenbrede testomgevingen.	Dit vereist afstemming tussen de ketenpartijen. Er dient tegemoet gekomen te worden aan verschillende ontwikkelmethoden.

5.3.6 RECHTEN BETROKKENEN

Optimalisatie gebruik Suwinet	
Verbeterpunt	Toelichting
Verken de mogelijkheden om de burger meer transparantie te bieden rondom de verwerking van persoonsgegevens in Suwinet.	Is dit centraal te regelen of geniet een decentrale aanpak de voorkeur? Hoeveel transparantie is haalbaar en wat is wenselijk? Via welke kanalen kan transparantie geboden worden (mijnOverheid.nl berichtenbox, peronal clouds als Qiy)?
Optimalisatie verantwoordelijkheden en governance van Suwinet	
-	-
Optimalisatie techniek Suwinet	
-	-

5.3.7 TRANSPARANTIE

Optimalisatie gebruik Suwinet	
Verbeterpunt	Toelichting
Optimalisatie verantwoordelijkheden en governance van Suwinet	
Zorg voor een ketenbreed gedragen Normenkader en bijbehorende Verantwoordingsrichtlijn.	Een verplichtend karakter is noodzakelijk.
Maak duidelijk wie verantwoordelijk is voor het creëren van transparantie.	Vanuit het perspectief van toezicht en handhaving is een centrale aanpak wenselijk. Ook richting de burger levert een centrale aanpak een effectievere informatievoorziening op.
Optimalisatie techniek Suwinet	
Creëer betere handvatten voor het ketenbreed kunnen traceren van gegevensuitwisseling. Borg dat alle partijen overgaan op de nieuwe berichtdefinities.	Inventariseer waar partijen behoefte aan hebben voor rapportages en neem dit mee voor het traceren. Dit vergemakkelijkt de traceerbaarheid.
Overweeg de logging van inlezende applicaties en de rapportage hierover op te nemen in het Normenkader en de Verantwoordingsrichtlijn.	Om ervoor te zorgen dat versnipperde gegevens op een efficiënte en eenduidige manier verzameld kunnen worden. In het verlengde hiervan kan overwogen worden inlezende applicaties te certificeren zodat ze voldoen aan de in het Normenkader en Verantwoordingsrichtlijn gestelde eisen.

5.3.8 WBP VERANTWOORDELIJKHEID

Optimalisatie gebruik Suwinet	
Verbeterpunt	Toelichting
-	-
Optimalisatie verantwoordelijkheden en governance van Suwinet	
Leg de WBP-verantwoordelijkheid voor Suwinet op hoofdlijnen vast in de Suwiwet en –regelgeving.	Hiermee wordt een solide basis voor effectieve governance gelegd.
Baken de verantwoordelijkheid van alle betrokken partijen helder af als gekozen wordt voor een vorm van gezamenlijke verantwoordelijkheid.	Dit draagt ook bij aan een solide basis voor effectieve governance.
Verduidelijk de WBP-rol van BKWI, IB en commerciële brokers.	-

Optimalisatie techniek Suwinet	
-	-

5.3.9 GOVERNANCE

Optimalisatie gebruik Suwinet	
Verbeterpunt	Toelichting
-	-
Optimalisatie verantwoordelijkheden en governance van Suwinet	
Verduidelijk de huidige verhoudingen en de daarbij behorende governance in Suwinet.	Rollen, taken, bevoegdheden, overleggremia, regels voor besluitvorming, etc. Stel vast welke waarborgen de governance zou moeten bieden en bepaal daarna in welke vorm dat zou kunnen.
Herzie de huidige verhoudingen en ketenverantwoordelijkheden.	Is het wenselijk om de ketenverantwoordelijkheid nadrukkelijker bij een partij te beleggen die bijvoorbeeld onder directe verantwoordelijkheid van de minister van SZW valt.
Optimalisatie techniek Suwinet	
-	-

5.3.10 VERANTWOORDING

Optimalisatie gebruik Suwinet	
Verbeterpunt	Toelichting
-	-
Optimalisatie verantwoordelijkheden en governance van Suwinet	
Actualiseer de Verantwoordingsrichtlijn en het Normenkader.	En voor zover nodig ook de wettelijke kaders waarin die zijn ingebed.
Breidt de scope van de Verantwoordingsrichtlijn en het Normenkader uit met privacy-aspecten.	Niet alleen de focus op beveiliging maar ook privacybescherming.
Laat de Verantwoordingsrichtlijn en het Normenkader zoveel mogelijk aansluiten op de BIG en spreek af hoe er met het verschil omgegaan moet worden.	Hierdoor kan de Samenvattende Rapportage weer in ere hersteld worden en krijgt deze weer nut.
Zorg ervoor dat Suwipartijen zich niet langer apart hoeven te verantwoorden over hun eigen informatiehuishouding en het gebruik van Suwinet.	Streef naar zoveel mogelijk generieke verantwoording met een klein meer sectorspecifiek deel.
Haak zoveel mogelijk aan bij bewegingen om zoveel	Om efficiëntie te behalen en kosten te besparen.

mogelijk te komen tot een verantwoordingsregime voor gemeenten tegenover Suwinet, DigiD, basisregistraties, etc.	
Optimalisatie techniek Suwinet	
-	-

5.3.11 TOEZICHT

Optimalisatie gebruik Suwinet	
Verbeterpunt	Toelichting
Zorg voor heldere en transparante verantwoording en toezicht zodat volstrekt helder is bij welke partijen er op welke gebieden en in welke mate sprake is van nalevingstekort.	-
Investeer continu in bewustwording en integriteit van gebruikers/professionals.	Hiermee kunnen privacyrisoco's in de kiem gesmoord worden.
Optimalisatie verantwoordelijkheden en governance van Suwinet	
Zorg dat er één partij is die eindverantwoordelijk is voor toezicht op de naleving van regels en normen op het gebied van privacybescherming en beveiliging.	
Zorg ervoor dat deze partij effectief kan handhaven.	
Zorg ervoor dat deze partij zich ook zelf moet verantwoorden.	Met name over genomen acties.
Optimalisatie techniek Suwinet	
-	-

5.3.12 ONTWIKKELINGEN

Er zijn een aantal ontwikkelingen gaande die van belang zijn voor Suwinet en additionele kwetsbaarheden kunnen introduceren. Deze ontwikkelingen zijn:

- Breder gebruik van Suwinet voor gegevensuitwisselingen (met bijvoorbeeld het buitenland of andere ketens/domeinen);
- EU Privacy Verordening
- Cloud / SaaS

Met het breder gebruik van Suwinet komen de technische, organisatorisch en juridische grenzen ervan snel in zicht waardoor de kans op schenden van de privacy van de burger toeneemt evenals het oplopen van reputatieschade door een van de partijen in Suwinet. Gewaakt dient te worden voor stroperigheid in de besluitvorming met het

toenemend aantal partijen. Onduidelijk is de impact van gegevensuitwisseling met het buitenland voor de governance en toezicht/handhaving.

De EU Privacy Verordening dwingt Suwinet om meer transparantie richting de burger te verschaffen. Hier zal de komende tijd aandacht aan besteed moeten worden. Partijen krijgen een grotere verantwoordelijkheid om de privacy van de burger te beschermen. In het geval ze hieraan niet voldoen zijn privacytoezichthouders meer bevoegd om in te kunnen grijpen (middels boetes). Een dergelijke ingrijp bij een op Suwinet aangesloten partij kan nadelige effecten voor Suwinet zelf hebben als betrouwbare infrastructuur voor gegevensuitwisseling. Hier legt dus een belang voor Suwinet om de privacy goed te regelen.

Het gebruik van cloud of SaaS-leveranciers voor gegevensverwerking omvat een complex speelveld van juridische, technische en organisatorische uitdagingen. Vooral als het partijen buiten de EU betreft. Suwipartijen die overwegen gebruik te maken van cloud of SaaS-leveranciers kunnen daarom beter kiezen voor zekerheid en zorgen dat data uitsluitend onder Nederlands of Europees recht valt. Dat biedt meer mogelijkheden voor controle. Bij cloud of Saas is het van belang dat de verantwoording binnen Suwinet goed geregeld is. Het feit dat gemeenten een eigen verantwoordingsregime hebben zorgt ervoor dat de cloud en SaaS leveranciers die zij gebruiken als bewerker dit ook hebben. Ook zij hoeven zich dus niet te verantwoorden richting Suwinet. Vanuit het perspectief van transparantie en toezicht & handhaving is dit onwenselijk.

5.4 PRIORITERING

Kijkende naar de verschillende kwetsbaarheden en hun impact zijn de belangrijkste verbeterpunten op hoofdlijnen de volgende:

- Het realiseren van een generieke en eenduidige Verantwoordingsrichtlijn en Normenkader die door alle partijen verplicht gedragen zijn wat zorgt voor transparantie over de beveiliging in de keten en eenduidigheid in de rapportage hierover. Het generieke karakter maakt het mogelijk om beter aan te sluiten bij het interne beveiligingsbeleid van de aangesloten partijen waardoor de verantwoording efficiënter/goedkoper kan en het de adoptie vergroot. Het verplichtende karakter is noodzakelijk om partijen die niet voldoen aan de afspraken hierop aan te kunnen spreken. Nieuwe ontwikkelingen zoals de baseline informatiebeveiliging gemeenten (BIG), het nieuwe werken en de komende EU Privacy Verordening dienen meegenomen te worden in bijvoorbeeld een update van het Normenkader.
- Het verhogen van de beveiligingsbaseline op elementen en een differentiërende aanpak. Met het toenemen van de privacygevoeligheid van Suwinet door toenemend gegevensverkeer en gegevensrijkheid is het wenselijk om de beveiliging daarop aan te passen. De te verbeteren technische, fysieke en organisatorische beveiligingselementen (waaronder o.a. het verhogen van het authenticatieniveau door (her)gebruik van bestaande oplossingen als de UZI- of Rijkspas en het herijken van het autorisatiebeleid) dienen geïnventariseerd en vastgelegd te worden in de nieuwe baseline (Verantwoordingsrichtlijn en Normenkader welke afgestemd zijn met de BIG). Een nuttige aanpak hiervoor is de gegevens- en dienstverlening te differentiëren naar het beveiligingsniveau van de afnemende partij. Hierdoor ontstaat meer flexibiliteit met betrekking tot het deelnemen van partijen in Suwinet en het borgen van vertrouwen. Partijen met een laag beveiligingsniveau krijgen toegang

tot minder gegevens en/of diensten. Een dergelijke aanpak maakt aansluiten op Suwinet makkelijker waardoor zij ook kunnen profiteren van efficiënte gegevensuitwisseling (zij het op beperkte schaal) en voorkomt dat partijen die slechts een beperkte set van (relatief ongevoelige) gegevens nodig hebben zich moeten conformeren aan buitenproportionele beveiligingseisen. Zo ontstaat er een baseline voor beveiliging met daarboven enkele goed gedefinieerde beveiligingsniveaus die noodzakelijk zijn voor het afnemen van specifieke gegevens en/of diensten. Ook biedt dit mogelijkheden voor sanctioneren. Bij een dergelijke differentiërende aanpak is het noodzakelijk de verschillende gegevens en diensten te classificeren in niveaus en hiervoor de vereiste beveiligingsvereisten te definiëren. Toezicht op de niveaus zal nodig zijn.

- Meer transparantie door betere tracking en tracing van gegevensuitwisseling in Suwinet en rapportages hierover. Een belangrijke eerste stap is dat alle partijen binnen een redelijke termijn overgaan op de nieuwe berichtdefinities, waarbij ketenbreed vaststaat welke unieke persoon, welke organisatie, welk gegevens en voor welk doel heeft opgevraagd en ter beschikking heeft gekregen. Partijen hebben dit nodig om zich te kunnen verantwoorden naar elkaar toe en naar de burger toe zoals in de komende EU Privacy Verordening vereist is. Vanuit het perspectief van toezicht en handhaving is een centrale aanpak wenselijk. Ook richting de burger levert een centrale aanpak een effectievere informatievoorziening op.
- Het faciliteren van het verbeteren van de doelbinding door meer filtering functionaliteit en actieve monitorring daarop aan te bieden zodat adequaat ingegrepen kan worden als bepaalde filters getriggerd worden. De filters zorgen ervoor dat de gebruiker slechts de gegevens ziet die nodig zijn voor een bepaalde taak (need-to-know principe) en zorgen voor actieve monitorring om misbruik te voorkomen. De verantwoordelijkheden van de filters dienen duidelijk belegd te worden. Naast het inzetten van filters is ontkoppeld koppelen een in potentie minstens zo krachtige manier om invulling te geven aan het need-to-know principe. Daarmee wordt bedoeld dat de ontvanger niet een hele set aan gegevens ontvangt waaruit hij zelf de informatie moet afleiden die hij nodig heeft. In plaats daarvan wordt eerder in de keten deze informatie automatisch uit de gegevens gehaald. De gebruiker ontvangt dan alleen de afgeleide informatie, en niet de daaraan ten grondslag liggende gegevens. De mogelijkheden en impact van ontkoppeld koppelen in Suwinet dienen verkent te worden. De gegevens van de filters bieden inzage in het gebruik van Suwinet en zijn op zichzelf privacygevoelig. De gegevens dienen zodanig beveiligd te worden dat ze bij eventueel misbruik ook daadwerkelijk onomstotelijk aantonen wie, wanneer, wat heeft gedaan.
- Het beter beleggen van de verantwoordelijkheden en het effectiever inregelen van de governance door gemeenschappelijke verantwoording en hierop gebaseerde handhaving. Een dergelijke governance ziet niet alleen toe op controle achteraf (op basis van rapportages), maar ziet ook toe dat aan te sluiten partijen op Suwinet voldoen aan de eisen. Een intelligente, relevante invulling geven aan een vorm van ketenbesturing is een uitdaging waar veel ketens zich gesteld zien en zal in samenwerking met de bestuurders van de betrokken ketenpartijen opgepakt moeten worden.
- Reduceer de complexiteit van wet- en regelgeving om de uitvoering ervan gemakkelijker te maken. Maak de gegevensbehoefte per wet concreet, consistent en eenduidig en link deze aan het SGR dat wettelijk is vastgesteld zodat geen misinterpretatie kan plaatsvinden en nieuwe diensten sneller uitgerold kunnen worden.

Aangezien het hele stelsel mede draait op basis van vertrouwen is het essentieel dat deze verbeterpunten met alle betrokken partijen gezamenlijk opgepakt worden zodat ze ook vertrouwen hebben in de maatregelen die worden

ingezet.

Geconsulteerde organisaties

De volgende organisaties zijn geconsulteerd tijdens het onderzoek: Inlichtingenbureau, BKWI, KING, VNG, Gemeente Enschede en Rotterdam, UWV en SVB.