Privacy Impact Assessment

Toegang persoonsgegevens Suwinet

December 2016

Definitief

Colofon

Datum	1 december 2016
Versie	1.0
Classificatie	Vertrouwelijk
Status	Definitief
Auteurs	Albert Katoen Arnold Roosendaal Luuk Akkermans
Opdrachtgever	Ministerie van Sociale Zaken en Werkgelegenheid

Ministerie van Sociale Zaken en Werkgelegenheid

Disclaimer

Dit onderzoek is uitgevoerd in opdracht van het Ministerie van Sociale Zaken en Werkgelegenheid en is met uiterste zorg samengesteld. 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

Sinds het Programmaplan Borging Veilige Gegevensuitwisseling via Suwinet (BVGS) en de vorige PIA Suwinet zijn er een aantal goede stappen genomen om de privacy rondom het gebruik van Suwinet-Inkijk beter te waarborgen. De onderzoeksvragen die in deze PIA centraal staan, zijn (1) op welke wijze de toegang kan worden beperkt tot personen en (2) op welke wijze de toegang kan worden beperkt via zoeksleutels. De maatregelen uit het programmaplan die hierop aansluiten zijn met name de maatregelen acht en negen: het beperken van de toegang via zoeksleutels respectievelijk het beperken van de toegang tot personen. Deze PIA bouwt daarop voort en onderzoekt of de uitvoering die gegeven is aan deze maatregelen de privacy beter beschermen en of er aanvullende uitvoeringsmaatregelen kunnen worden genomen. De nadruk zal liggen op maatregel negen, omdat daar de meeste winst valt te behalen wat betreft het beschermen van de privacy. Maatregel acht, de toegang via zoeksleutels beperken, is al geïmplementeerd met goede resultaten voor privacybescherming. De toegevoegde waarde is echter beperkt en wordt in dit verband meer behaald met een fijnmaziger structuur van pagina's (maatregel één, die hier buiten scope valt). Het onderzoek dat ten grondslag ligt aan dit rapport liep tot 12 oktober 2016. Het rapport is vastgesteld op 23 november 2016.

Voor de invulling van maatregel negen is gekozen voor een filtermechanisme in de vorm van een whitelist. Alleen personen op een whitelist kunnen door medewerkers worden opgevraagd. Suwi-partijen stellen zelf de whitelist samen. De mate waarin de privacy wordt beschermd is afhankelijk van het 'niveau' waarop een whitelist wordt geïmplementeerd. Bij een whitelist op medewerkersniveau, vanuit privacyperspectief de meest ideale situatie, kunnen medewerkers alleen personen opvragen die relevant zijn voor het uitvoeren van hun wettelijke taak. Als keerzijde heeft dit wel een meer intensieve werklast voor het toekennen en onderhouden van autorisaties tot gevolg en dit kan ingrijpende gevolgen voor processen en ICT-systemen hebben.

Voor gemeenten wordt de whitelist geïmplementeerd op organisatieniveau, waardoor de omvang is beperkt tot de personen waar de gemeente een dienstverleningsrelatie mee heeft. Ook voor SVB wordt de whitelist geïmplementeerd op organisatieniveau. Het aantal personen op de whitelist bij de SVB zal daardoor gereduceerd worden tot circa 400.000 personen. Vergeleken met de situatie voorheen waarin alle Nederlanders konden worden opgevraagd, is dit in beide gevallen een significante reductie van het risicobeeld.

UWV heeft ook gekeken naar de mogelijkheid om een whitelist op organisatieniveau te implementeren. Gezien de zeer brede doelgroep van de materiewetten die UWV uitvoert – namelijk alle verzekerde werknemers in heel Nederland – zou dit betekenen dat de whitelist zou bestaan uit alle personen in de polisadministratie (ca 8 miljoen). Aangezien dit nog steeds te omvangrijk is, onderzoekt UWV de mogelijkheden om whitelists op een lager niveau te implementeren en om op andere wijze de toegang tot personen te beperken. Op dit moment onderzoekt UWV via een impactanalyse welke mogelijkheden er zijn binnen de processen en het architectuurlandschap van UWV. Ultimo december zullen de resultaten van de impactanalyse gereed zijn. Begin 2017 kan dan door middel van een uitvoeringstoets in beeld worden gebracht wat de exacte uitvoeringsconsequenties en doorlooptijden zijn van deze mogelijkheden. Een uitspraak over de behaalde resultaten ten gunste van de bescherming van de privacy van burgers door aanpassingen bij UWV kan op dit moment dus nog niet gedaan worden.

De whitelist is een maatregel aan de voorkant. Ook aan de achterkant kunnen en zijn er goede maatregelen genomen om de privacy rondom Suwinet-Inkijk beter te waarborgen. Daarbij gaat het met name om controle van logging, bewustwording en beleid voor onbedoeld gebruik. Deels is hier al uitvoering aan gegeven. Zo hebben alle Suwi-partijen een bewustwordingscampagne in een

bepaalde vorm opgezet dat ofwel betrekking heeft op Suwinet-Inkijk ofwel meer algemeen van aard is, waar Suwinet-Inkijk dan een onderdeel van is.

In de komende Algemene Verordening Gegevensbescherming (AVG) zal Privacy by Design een meer prominente rol spelen. Het is dan ook belangrijk om hier nu al naar te kijken. Er zijn weliswaar al goede stappen genomen om de privacy beter te beschermen, maar redenerend vanuit het huidig wettelijk kader is dit nog niet voldoende. Dit omdat, ondanks de significante reductie van het risicobeeld dat wordt bereikt met de voorgenomen implementatie van de whitelist, nog steeds personen kunnen worden geraadpleegd die niet relevant zijn voor de werkzaamheden van een medewerker. Ook op grond van de AVG, die op 25 mei 2018 in werking treedt, is vereist dat verdere stappen worden gezet in het beschermen van persoonsgegevens, die tevens toekomstbestendig dienen te zijn. Extra aandacht is dan ook vereist om te zoeken naar mogelijkheden die vanuit het ontwerp (Privacy by Design) de privacy nog beter te kunnen waarborgen. Voor alle Suwi-partijen betekent dit dat de mogelijkheden om op een lager niveau binnen de organisaties de whitelist te implementeren nader onderzocht dienen te worden. De techniek is hierbij niet de beperking; tijdens het onderzoek is naar voren gekomen dat met de huidige stand der techniek verdergaande stappen tot de mogelijkheden horen.

Aanbevelingen

In de aanbevelingen van dit rapport worden enkele aanvullende (ideeën voor) uitvoeringsmaatregelen omschreven om de privacy van burgers nog verder te beschermen. De Suwi-partijen worden voor de keuze gesteld om de whitelist nog verder aan te scherpen (een maatregel aan de voorkant) dan wel, als er goede redenen zijn om daarvan af te wijken, de controle van het gebruik van Suwinet-Inkijk te intensiveren (een maatregel aan de achterkant). Het heeft echter de voorkeur om een maatregel aan de voorkant te nemen. Om een whitelist op een lager niveau toe te passen dienen de Suwi-partijen dan ook niet alleen de bestaande werkprocessen kritisch onder de loep te nemen, maar ook te kijken naar mogelijkheden buiten de bestaande processen.

De real-time werking van de whitelist is ook belangrijk voor het verder beperken van de toegang tot personen. Een meer real-time werking van de whitelist betekent dat personen eerder van de whitelist op- en afgevoerd kunnen worden dan met de huidige techniek mogelijk is. Wijzigingen aan de whitelist zouden dan real-time moeten kunnen worden doorgevoerd in plaats van in een batch 's nachts te worden verwerkt. Een meer real-time werking van de whitelist is gunstig voor de privacy van de burger. Afhankelijk van de inrichting van het proces rondom het beheren van de real-time whitelist, zorgt deze functionaliteit in potentie voor een reductie van de periode waarin gegevens over personen met wie de dienstverleningsrelatie is geëindigd alsnog kunnen worden geraadpleegd. Afhankelijk van de mate van real-time werking die behaald kan worden dient dit samen met de escapefunctionaliteit bezien te worden om vast te stellen of de escapefunctionaliteit volstaat om een korte periode te overbruggen totdat een whitelist is geactualiseerd in de systemen.

Ten slotte dienen er ook doelen te worden gesteld voor 2017 en 2018. De uitvoering die tot nu toe is gegeven aan de maatregelen draagt al significant bij aan het beter beschermen van de privacy van burgers. Zoals eerder aangegeven is daarnaast blijvende aandacht nodig om de privacy beter te beschermen. Met name in het licht van de komende Europese privacyverordening, waarin privacy strenger wordt gereguleerd en ook Privacy by Design een meer centrale rol speelt, is het van belang dat er continu gekeken wordt naar aanvullende privacybeschermende maatregelen. Toegepast op maatregel negen zou dit ook vorm kunnen worden gegeven door een opdeling van de whitelist in kleinere eenheden, zoals divisies of regio's. Een goede balans van maatregelen aan de voorkant en

achterkant is essentieel voor goede privacyborging binnen Suwinet-Inkijk. De aanbevelingen bieden hiertoe handvatten.

1 Inleiding

Het Ministerie van Sociale Zaken en Werkgelegenheid (SZW) heeft Privacy Company aangezocht een Privacy Impact Assessment (PIA) uit te voeren in het kader van enkele voorgestelde maatregelen ten aanzien van 'Suwinet-Inkijk'. In dit rapport zijn de bevindingen van de PIA uiteengezet. Deze PIA richt zich op het beperken van de toegang tot persoonsgegevens in 'Suwinet-Inkijk'. De PIA komt voort uit de motie Ulenbelt-Van Weyenberg en de daaropvolgende brief van de Staatssecretaris van SZW.[1] Deze motie werd opgesteld naar aanleiding van berichten dat medewerkers van sociale diensten gegevens van bekende Nederlanders hebben opgevraagd. Naar aanleiding van de motie is besloten dat de toegang tot Suwinet verder dient te worden beperkt.

Met brieven van 30 juni 2015 (UWV, SVB en gemeenten nemen met het programma "Borging veilige gegevensuitwisseling via Suwinet" een aantal verbetermaatregelen gericht op het beperken van de toegang van medewerkers tot gegevens) en 23 december 2015 (de voortgang daarvan) heeft de Staatssecretaris van SZW de Tweede Kamer geïnformeerd over te hanteren uitgangspunten bij het gebruik van zoeksleutels en de toegang tot personen. De staatssecretaris heeft in de brieven opgemerkt dat UWV, SVB en gemeenten onderzoeken onder welke condities de toegang tot andere personen dan de personen die medewerkers zelf behandelen, wordt verleend en op welke wijze deze toegang wordt vormgegeven. In de brief van 23 december 2015 merkt de staatssecretaris op dat zij daaropvolgend in het voorjaar van 2016 een PIA laat uitvoeren naar de zoekmogelijkheden en de toegang tot andere personen dan de personen die medewerkers zelf behandelen. Dit is de betreffende PIA. Het onderzoek dat ten grondslag ligt aan dit rapport liep tot 12 oktober 2016. Het rapport is vastgesteld op 1 december 2016.

Daarnaast is het gezien het toegenomen gebruik van de applicatie en de ontwikkelingen op de genomen maatregelen om de privacy beter te waarborgen verstandig om (opnieuw) een PIA uit te voeren. Bij belangrijke wijzigingen in systemen is het immers raadzaam om weer het licht te laten schijnen op de stand van de privacy en informatiebeveiliging van een systeem, product, proces of ander initiatief.

1.1 Aanleiding

Deze PIA vormt een aanvulling op de eerdere 'PIA Suwinet' uit april 2014. In de 'PIA Suwinet' werd inzichtelijk gemaakt of en zo ja welke wijzigingen in de Wet Suwi en Suwinet nodig zijn om de gegevensuitwisseling veilig te laten blijven verlopen. Naar aanleiding van de 'PIA Suwinet' en het rapport 'De burger bediend' hebben de Minister en de Staatssecretaris van SZW aan de Suwi-partijen – SVB, UWV en GSD – gevraagd om maatregelen te nemen om o.a. de privacy rondom Suwinet te verbeteren. Eind 2013 is het Opdrachtgeversberaad BKWI opgericht met BKWI als opdrachtnemer. De bestuursleden van het Opdrachtgeversberaad – SVB, UWV en VNG – hebben vervolgens het Programmaplan Borging Veilige Gegevensuitwisseling via Suwinet (BVGS) opgesteld.

In het Programmaplan BVGS worden tien samenhangende maatregelen, uit te voeren door de Suwi-partijen, uiteengezet om persoonsgegevens beter te beschermen. Daarnaast worden vier maatregelen beschreven waarbij de Suwi-partijen hebben gevraagd aan SZW om het initiatief te nemen.

In deze PIA wordt voornamelijk gekeken naar de **maatregelen acht en negen van het Programmaplan BVGS**: of en in welke mate het gebruik van zoeksleutels in Suwinet-Inkijk kan

[1] Motie Ulenbelt-Van Weyenberg, Kamerstukken 26 448, 28 mei 2014.

worden beperkt respectievelijk op welke wijze de toegang kan worden beperkt tot de personen waar de organisatie of de medewerker een dienstverleningsrelatie mee heeft of onlangs heeft gehad.[2]

Zoals vermeld zijn de maatregelen uit BVGS een samenhangend geheel. De maatregelen acht en negen zijn dan ook verbonden met andere maatregelen. In dit geval is er met name samenhang met **maatregel één** – een meer fijnmazige autorisatiestructuur door bijvoorbeeld meer pagina's – en **maatregel twee** – verbetering controle op logging en rapportage.[3] Maatregel één hangt vooral samen met maatregel acht (beperken van zoeksleutels), aangezien de zoeksleutels verbonden zijn aan bepaalde pagina's. Anderzijds kunnen pagina's, mits een medewerker daartoe is geautoriseerd, worden benaderd op basis van zoeksleutels. De maatregelen die zijn genomen of nog worden genomen aan de achterkant, zoals logging en rapportage, zijn oppervlakkig meegenomen (maatregel twee). De reden hiervan is dat een vorm van controle aan de achterkant cruciaal is om de effectiviteit van de maatregelen aan de voorkant te meten en/of als compenserende maatregel kan dienen als maatregelen aan de voorkant minder effectief zijn.[4]

De betrokken partijen hebben inmiddels gezamenlijk en afzonderlijk stappen genomen om deze maatregelen uit te voeren. In de derde voortgangsrapportage van het Programmaplan BVGS is de stand van zaken geschetst in de periode 1 oktober 2015 tot en met 31 maart 2016. Belangrijke korte termijn maatregelen zijn gerealiseerd, zoals andere pagina's voor gemeenten waardoor minder gegevens worden getoond en een filtermechanisme in de vorm van een whitelist. Ook heeft er een pilot plaatsgevonden bij enkele gemeenten met betrekking tot deze whitelist en met betrekking tot de andere pagina's. Deze PIA volgt op deze ontwikkelingen.

Het doel van de PIA is het beoordelen van de effectiviteit van deze maatregelen en het analyseren of aanvullende maatregelen dienen te worden genomen om de privacy van de personen wiens persoonsgegevens worden getoond via Suwinet-Inkijk zoveel mogelijk te waarborgen.

Opgemerkt dient te worden dat waar in dit rapport wordt gesproken over Suwinet het gaat om de Gezamenlijke elektronische Voorzieningen Suwi (GeVS), waar Suwinet een onderdeel van is. Het Suwinet valt onder het centrale deel van de GeVS dat in beheer is bij het BKWI. De GeVS bestaat ook uit decentrale delen. In de volksmond wordt echter vooral (ten onrechte) gesproken over Suwinet.

1.2 Vraagstelling

In deze PIA staan de volgende twee onderzoeksvragen centraal. Beide onderzoeksvragen zijn gebaseerd op een maatregel uit het Programmaplan BVGS en hebben als doel de privacy van de burger beter te beschermen. Zoals in de vorige paragraaf aan de orde is gekomen dient in het achterhoofd te worden gehouden dat deze twee maatregelen niet op zichzelf staan.

1. Op welke wijze kan de toegang tot personen worden beperkt? (maatregel negen)
2. Op welke wijze kan de toegang via zoeksleutels worden beperkt? (maatregel acht)

De eerste onderzoeksvraag beoogt de toegang via Suwinet-Inkijk zoveel mogelijk te beperken tot personen die relevant zijn voor de werkzaamheden van de medewerker. De Suwi-partijen hebben deels al uitvoering gegeven aan deze maatregelen. In het Programmaplan BVGS is opgemerkt dat

[2] Programmaplan BVGS, p. 18 e.v.
[3] Een meer fijnmazige autorisatiestructuur wil zeggen dat medewerkers niet onnodig allerlei gegevens krijgen te zien.
[4] In het Programmaplan BVGS worden maatregel één (meer fijnmazige autorisatiestructuur) en maatregel twee (verbeteren van logging en gebruiksrapportages) ook beschreven als 'randvoorwaardelijk' voor de realisering van de maatregelen acht en negen.

het niet mogelijk is de toegang tot alle niet-relevante personen af te sluiten, omdat voorafgaand aan een dienstverleningsrelatie niet kan worden vastgesteld welke personen wel en niet relevant zijn. Wel is het van belang, en dat is ook aangegeven in het programmaplan, dat partijen zich maximaal inzetten om de toegang tot niet-relevante personen te beperken.[5] In deze PIA worden de genomen maatregelen onder de loep genomen en wordt gekeken naar eventuele aanvullende beschermende maatregelen die in dit opzicht kunnen worden genomen.

De tweede onderzoeksvraag gaat over het beperken van de toegang via zoeksleutels. Het is belangrijk dat er niet onnodig op andere zoeksleutels dan BSN wordt gezocht, omdat andere zoeksleutels het makkelijker maken om gegevens op te vragen die niet relevant zijn voor de taken van de medewerker. Hierbij dient rekening te worden gehouden met het feit dat voor de uitvoering van opgedragen wettelijke taken niet altijd kan worden volstaan met alleen zoeken op BSN.[6] De Suwi-partijen hebben hier al deels uitvoering aan gegeven, bijvoorbeeld door alle beschikbare zoeksleutels te documenteren. Ook deze maatregel staat centraal in deze PIA en er wordt gekeken naar eventuele aanvullende maatregelen die kunnen worden genomen om de privacy nog beter te waarborgen.

1.3 Scoping/afbakening

Deze PIA is beperkt tot een beoordeling van hoe de toegang tot persoonsgegevens via Suwinet-Inkijk kan worden beperkt, zoals besproken in de vorige paragraaf. Verder zijn de volgende afbakeningen van toepassing:

- Een beschrijving van de bestaande (IST) situatie komt slechts gedeeltelijk aan de orde. De hoofdmoot ligt op het schetsen van de gewenste (SOLL) situatie.
- Deze PIA heeft alleen betrekking op de Suwi-partijen (UWV, SVB en gemeenten) en niet op de niet-Suwi-partijen.

1.4 Leeswijzer

In hoofdstuk 2 staat de aanpak van deze PIA centraal. In de praktijk bestaan verschillende PIA standaarden die als basis hebben gediend. Om in te spelen op de specifieke aard van deze PIA, waar ook enkele informatiebeveiligingselementen in terugkomen, is gekomen tot een op maat gemaakte PIA die dus niet direct te herleiden is tot een bestaand PIA model. Hierdoor worden de onderzoeksvragen optimaler beantwoord dan wanneer vastgehouden wordt aan een vastomlijnde structuur waar niet of nauwelijks van mag worden afgeweken. Er is een gefaseerde aanpak gehanteerd die ook in dit hoofdstuk aan de orde komt, gevolgd door de juridische kaders en kaders van informatiebeveiliging.

In hoofdstuk 3 worden de uitgangspunten van het onderzoek uiteen gezet, te beginnen bij een korte algemene omschrijving van Suwinet en van Suwinet-Inkijk. Tevens wordt besproken wie de Suwi-partijen zijn en welke maatregelen uit het Programmaplan BVGS centraal staan. Een belangrijk onderscheid daarbij, dat ook in de rest van het rapport wordt gehanteerd, is enerzijds de maatregelen die betrekking hebben op de onderzoeksvragen en anderzijds maatregelen die niet betrekking hebben op de onderzoeksvragen, maar wel indirect effect erop uitoefenen. In het Programmaplan BVGS wordt erover gesproken dat ze 'randvoorwaardelijk' zijn voor de andere maatregelen.

Hoofdstuk 4 bevat de resultaten van de inventarisaties. Het belang hiervan is om te achterhalen welke uitvoering de Suwi-partijen reeds hebben gegeven of van plan zijn te geven aan de

[5] Programmaplan BVGS, p. 20.
[6] Derde voortgangsrapportage, p. 14.

maatregelen. Deze 'gezichtspunten' van de Suwi-partijen zijn van belang voor het verder uitwerken van ideeën voor het beperken van de toegang tot personen en het beperken via zoeksleutels.

De informatie die is vergaard uit documenten en gesprekken met de Suwi-partijen, waarbij het o.a. ging over in hoeverre al uitvoering is gegeven of zal worden gegeven aan de onderzoeksvragen, dient te worden getoetst aan relevante beginselen in het privacyrecht en normen uit de informatiebeveiliging om te beoordelen in hoeverre de privacy wordt gewaarborgd.

Welke beginselen en normen dit zijn, wordt uiteengezet in hoofdstuk 5. In hoofdstuk 6 wordt het resultaat van deze toetsing besproken in de vorm van enkele conclusies. Ten slotte volgen in hoofdstuk 7 enkele aanbevelingen die bij kunnen dragen aan een betere borging van de privacy dan alleen met de huidige en voorziene implementaties van de maatregelen. Uitgangspunt daarbij is dat de mate waarin de privacy wordt beschermd in ieder geval dient te voldoen aan de privacywetgeving en aan relevante normen uit de informatiebeveiliging.

2 Aanpak

In dit hoofdstuk wordt de aanpak van de onderzoeksvragen uiteengezet. Allereerst worden PIA's in het algemeen besproken, welke PIA standaarden in de praktijk bestaan en in hoeverre deze relevant zijn voor deze PIA. De aanpak is verdeeld in drie fasen. De uitwerking hiervan komt aan de orde. Ten slotte worden de relevante juridische kaders en kaders van informatiebeveiliging besproken.

2.1 Privacy Impact Assessment

Een privacy impact assessment (hierna: PIA[7]) heeft tot doel het in kaart brengen van de gegevensverwerkingen binnen een organisatie en het bieden van handvatten om gesignaleerde risico's zoveel mogelijk weg te nemen. Een PIA kan betrekking hebben op producten, processen, diensten en projecten waarbij privacy een rol speelt, zoals wetgeving of beleid. Sinds de motie Franken, en daarna de motie Segers/Oosenbrug, is het voor overheden verplicht om een PIA uit te voeren op nieuwe wetgeving die invloed heeft op de privacy.[8]

Een PIA kan worden uitgevoerd op verschillende momenten. Het is echter raadzaam om een PIA zo vroeg mogelijk uit te voeren, bij voorkeur voor de start van een traject, om zo onnodige kosten te voorkomen. In dit opzicht kan een PIA worden gezien als een maatregel die Privacy by Design ondersteunt. Privacy by Design wordt in de nieuwe Europese privacyverordening een verplicht onderdeel om rekening mee te houden bij privacygevoelige verwerkingen van persoonsgegevens.[9] Ook in latere stadia, met name bij (ingrijpende) wijzigingen in bijvoorbeeld een systeem of proces, kan het verstandig zijn een PIA (opnieuw) uit te voeren om de gevolgen voor de privacy in kaart te brengen. Dit is ook de insteek voor deze PIA over de onderzoeksvragen.

Er bestaan op dit moment een aantal standaarden of templates die richtlijnen geven voor het uitvoeren van een PIA. In Nederland zijn dat met name de NOREA PIA en het Toetsmodel PIA van de Rijksdienst.[10] NOREA is de beroepsgroep voor IT-auditors. De NOREA PIA is onlangs aangepast aan de meldplicht datalekken en kan worden gebruikt voor alle typen organisaties. Het Toetsmodel PIA van de Rijksdienst wordt toegepast op nieuwe wetgeving en beleid waarmee de privacy mogelijk in het geding is. Buiten Nederland is er een standaard ontwikkeld in het kader van het PIAF Project voor Europa. [11] Al deze standaarden worden verder aangepast en verfijnd aan de hand van voortschrijdende inzichten en ervaringen in de praktijk.

In deze PIA zijn de belangrijkste elementen van de standaarden meegenomen in de analyse. Met betrekking tot de NOREA PIA is dat bijvoorbeeld onderdeel 5 over het gebruik van gegevens (is het gebruik van de gegevens verenigbaar met het doel?). Wel is uit onderzoek gebleken dat de NOREA PIA niet alle juridische eisen uit de Nederlandse privacywetgeving, de Wet bescherming persoonsgegevens, meeneemt en geen stappenplan biedt om privacyrisico's in maatregelen te

---

[7] In het jargon van de Algemene Verordening Gegevensbescherming ook wel een 'gegevensbeschermingseffectbeoordeling' genoemd, of in het Engels een 'data protection impact assessment'.

[8] Motie Franken c.s. (https://zoek.officielebekendmakingen.nl/kst-31051-D.html) en motie Segers en Oosenbrug (https://zoek.officielebekendmakingen.nl/kst-34000-VII-21.html). Zie ook https://zoek.officielebekendmakingen.nl/kst-26643-335.html.

[9] Zie art. 25 van de Algemene Verordening Gegevensbescherming (AVG). De AVG is vanaf 25 mei 2018 van toepassing. Volgens art. 35 van de AVG moet een 'gegevensbeschermingseffectbeoordeling', oftewel een PIA, worden uitgevoerd door bedrijven en overheden op (voorgenomen) privacygevoelige verwerkingen van persoonsgegevens.

[10] Zie voor de NOREA PIA: http://www.norea.nl/Norea/Actueel/Recente+publicaties/default.aspx. Zie voor het Toetsmodel PIA van de Rijksdienst: https://zoek.officielebekendmakingen.nl/blg-233721.pdf.

[11] Zie http://piafproject.eu/.

vertalen.[12] Daarom is ook gekeken naar andere PIA standaarden, zoals uit het Europese PIAF Project. Hierdoor is een PIA ontstaan die beter toegespitst is op de onderliggende materie en daardoor de onderzoeksvragen optimaler beantwoord.

2.2 Gefaseerde aanpak

De aanpak is verdeeld in drie fasen:

1. Verkennend onderzoek
2. Inventarisatie bij Suwi-partijen
3. Risico-analyse en aanbevelingen

De eerste fase had tot doel zicht te krijgen op de huidige staat van Suwinet-Inkijk. Daarbij ging het bijvoorbeeld om in hoeverre er reeds uitvoering is gegeven aan de maatregelen die centraal staan in deze PIA (paragraaf 1.2) en het in kaart brengen van relevante wetgeving, kaders voor informatiebeveiliging en welke plannen er op de agenda staan om de privacy nog beter te waarborgen.

In de tweede fase zijn er inventarisaties verricht bij de Suwi-partijen. Deze inventarisaties hadden tot doel inzichtelijk te krijgen voor welke processen in de organisatie van de Suwi-partijen Suwinet-Inkijk wordt geraadpleegd, bij welke functies en op basis van welke wettelijke grondslag. Ook is er geïnformeerd naar tot op welk niveau de toegang in Suwinet-Inkijk is te beperken tot een beperkt aantal personen en, voor zover het mogelijk is, wanneer en hoe het zal worden ingericht in de organisatie, zoals op organisatie-, functie- of medewerkersniveau.

In de derde fase is er op grond van de bevindingen van de eerste twee fasen en de ondertussen gevoerde gesprekken en ontvangen documenten een privacy- en risico-analyse verricht naar de (uitvoering van de) maatregelen en in hoeverre ze daadwerkelijk bijdragen aan het verder waarborgen van de privacy. Op basis van deze analyses zijn er vervolgens aanbevelingen gedaan om de gegevensuitwisseling nog verder te beveiligen.

In de derde en afsluitende fase is ook het concept eindrapport opgeleverd. Vervolgens heeft er wederom een afstemmingsmoment plaatsgevonden met de Begeleidingscommissie waarbij het concept eindrapport is gepresenteerd. De feedback hierop is verwerkt in dit eindrapport.

Aan het einde van iedere fase was er een afstemmingsmoment met alle Suwi-partijen tijdens de begeleidingscommissie. Ook zijn er met alle partijen één of meerdere gesprekken gevoerd. Van elk gesprek is een verslag gemaakt en afgestemd met betrokkenen. Een overzicht van de gevoerde gesprekken is te vinden in hoofdstuk 4.3.

2.3 Kaders voor beoordeling

Er zijn verschillende kaders van toepassing op deze PIA: het juridisch kader en het informatiebeveiligingskader. Hieronder staat een overzicht met alle concrete kaders.

Juridisch kader	IB-kader
•Wbp •WEU •Wet SUWI, Besluit SUWI en Regeling SUWI	•ISO 27001 •**BIR /** BIG •Suwi-normenkader

[12] Over het NOREA Privacy Impact Assessment, 10 maart 2015, Joep Kockelkorn.

Juridisch kader

Het juridische kader wordt gevormd door de Wet bescherming persoonsgegevens (Wbp), de Wet Eenmalige Gegevensuitvraag Werk en Inkomen (WEU) en de Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (Wet SUWI). Uitwerkingen van de Wet SUWI, het Besluit SUWI en de Regeling SUWI, vallen ook onder het relevante juridische kader.

- De Wbp, in werking getreden op 1 september 2001, is een uitwerking van de Europese privacyrichtlijn 95/46/EG. De wet reguleert met name de informationele privacy, en stelt vereisten zoals een wettelijke grondslag en doelbinding. De wet is van toepassing als er persoonsgegevens worden verwerkt. Een persoonsgegeven is elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijk persoon. Een verwerking is iedere mogelijke handeling met betrekking tot een persoonsgegeven, zoals opvragen, opslaan, verstrekken en verwijderen.
- De WEU regelt dat burgers die beroep doen op een van de Suwi-partijen in het domein werk en inkomen, bijvoorbeeld door zich in te schrijven voor werk of voor het aanvragen van een uitkering, maar éénmaal hun gegevens hoeven af te geven. De Suwi-partijen moeten ervoor zorgen dat de gegevens vervolgens binnen de keten beschikbaar zijn. Als een klant bij bijvoorbeeld het UWV zijn werkgegevens heeft afgegeven, kunnen deze gegevens worden hergebruikt door andere Suwi-partijen in het domein werk en inkomen.
- In de Wet SUWI worden de diverse taken en verantwoordelijkheden van verschillende partijen die werkzaam zijn op het terrein van werk en inkomen beschreven. Ook bepaalt de wet hoe verschillende uitvoeringsorganen onderling gegevens uitwisselen. De Suwi-partijen, gemeenten, UWV en SVB, wisselen voor de uitkeringsverstrekking en handhaving persoonsgegevens uit via GeVS.
- Wet SUWI en Besluit SUWI regelen op hoofdlijnen de uitvoeringsstructuur voor het domein werk en inkomen. Zo bepaalt artikel 62 lid 1 Wet SUWI dat de Suwi-partijen gegevens met elkaar uitwisselen. Lid 2 bepaalt dat deze Suwi-partijen gezamenlijk zorg dragen voor de instandhouding van de elektronische voorzieningen (ofwel Suwinet) voor de uitwisseling van gegevens. Het Besluit SUWI gaat o.a. in op wat onder de elektronische voorziening moet worden verstaan en waar de verantwoordelijkheden liggen (bijlage 1). De Regeling SUWI is een uitwerking van de Wet SUWI en het Besluit SUWI en bevat bijvoorbeeld ook de planning- en controlecyclus.

Bij de gegevensuitwisseling binnen GeVS is sprake van een gesloten systeem, inhoudende dat een gegevensverstrekking door één van de SUWI-partijen alleen mag plaatsvinden als er een expliciete wettelijke grondslag is of als betrokkene voor een specifieke eenmalige gegevensverstrekking toestemming heeft gegeven.

Verder mogen persoonsgegevens alleen worden geraadpleegd voor een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel. Dit volgt uit het doelbindingsbeginsel, één van de pijlers van de bescherming van persoonsgegevens. Dit beginsel is terug te vinden in artikel 7 van de Wbp.

Ten slotte is van belang op te merken dat de Algemene Verordening Gegevensbescherming (AVG) de Wbp (en de Europese privacyrichtlijn) zal vervangen. De AVG is al in werking getreden en is van toepassing vanaf 25 mei 2018. Vanaf die datum zullen de strengere privacyregels van de AVG gelden. Zo zal Privacy by Design meer op de voorgrond komen en kunnen er veel hogere boetes worden opgelegd indien de wet wordt overtreden.[13] Dat de AVG een verordening is betekent dat

[13] Zie artikel 25 van de AVG.

deze rechtstreeks toepasselijk is in alle Europese lidstaten. De regels hoeven dus niet eerst te worden omgezet in nationale wetgeving. Het is belangrijk om zo vroeg mogelijk rekening te houden met de regels van de AVG, zodat organisaties over twee jaar zoveel mogelijk compliant zijn.

Informatiebeveiligingskader

Het kader van informatiebeveiliging bestaat uit de ISO 27001 norm, de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG), de Baseline Informatiebeveiliging Rijksdienst (BIR) en het normenkader Gezamenlijke elektronische Voorzieningen SUWI (GeVS).

- ISO 27001 – De ISO 27001 norm is de internationale standaard op het gebied van informatiebeveiliging. De norm vereist het opzetten, onderhouden en verbeteren van een management systeem (Plan, Do, Check, Act cyclus) om zodoende de informatiebeveiligings-maatregelen gestructureerd binnen de organisatie te beleggen. Voor dit onderzoek is gebruik gemaakt van de 2013 versie [14] van de norm (inclusief de updates in september 2014 en december 2015).
- BIR – De BIR (2012)[15] is het gestandaardiseerde normenkader voor de beveiliging van informatie binnen de Rijksoverheid en is verplicht door middel van het "comply or explain" principe. De BIR bestaat uit een tactisch normenkader en een operationele handreiking die zijn gebaseerd op ISO 27001 (2005) en ISO 27002 (2007), aangevuld met specifieke normen voor de Rijksoverheid. Voor dit onderzoek is gebruik gemaakt van het tactisch normenkader.
- BIG – De BIG[16] is de basis voor informatiebeveiliging voor de gemeentelijke markt en is gebaseerd op de BIR en VIR (Voorschrift Informatiebeveiliging Rijksoverheid).De BIG is in 2013 opgesteld door de IBD (Informatiebeveiligingsdienst voor gemeenten), een gezamenlijk initiatief van KING (KwaliteitsInstituut Nederlandse Gemeenten) en VNG. De BIG bestaat uit twee varianten, de strategische- en tactische- baseline, aangevuld met operationele producten ter ondersteuning van de implementatie. Voor dit onderzoek is gebruik gemaakt van de tactische baseline.
- Normenkader GeVS – Als onderdeel van de verantwoordingsrichtlijn Privacy & Beveiliging GeVS (opgesteld in 2011) is in het normenkader GeVS voor afnemers, die herijkt is naar aanleiding van maatregel zes van het Programmaplan BVGS, een set van eisen uitgewerkt ter beheersing van de risico's bij het gebruik van Suwinet.[17] Door de inspectie SZW is uit dit normenkader een set van 7 essentiële normen vastgesteld die door de inspectie als toetsingskader is gebruikt.[18] Voor dit onderzoek is gebruik gemaakt van de set van 7 essentiële normen.

Bovenstaande normenkaders vormen een uitgebreide set aan normen waarvan een groot deel niet direct van toepassing is op de gestelde onderzoeksvragen. Voor het onderzoek is dan ook een selectie gemaakt van de van toepassing zijnde normen (uit de ISO, BIR en BIG) die op de 7 essentiële normen zijn geplot. Zie de risicoanalyse in paragraaf 5.2 voor een gedetailleerde uitwerking hiervan.

[14] Nederlandstalige versie van de ISO 27001 norm wordt beheerd door de NEN. Meer informatie over de norm: https://www.nen.nl/NEN-Shop/Norm/NENISOIEC-27001C112014C12014C22015-nl.htm.
[15] Baseline Informatiebeveiliging Rijksdienst – Tactisch normenkader (versie 1.0 definitief, 1 december 2012).
[16] Baseline Informatiebeveiliging Nederlandse Gemeenten – Tactische baseline (versie 1.02, juni 2016).
[17] Normenkader GeVS (onderdeel van de verantwoordingsrichtlijn GeVS) – versie 2011 (juni 2011).
[18] Zie Inspectierapport: Suwinet 2015, Vervolgonderzoek 'veilig omgaan met elkaars gegevens', p. 12.

3 Uitgangspositie

3.1 Suwinet

Via de Gezamenlijke Elektronische Voorzieningen Suwi (GeVS) vindt digitale dienstverlening plaats op het gebied van werk en inkomen. Het in 2002 opgerichte systeem wordt gebruikt door overheidsorganisaties om gegevens met elkaar uit te wisselen. Suwinet is voortgekomen uit de Wet structuur uitvoeringsorganisatie werk en inkomen (Wet Suwi), die zijn oorsprong vind in het Regeerakkoord van 1998. De uitvoeringsstructuur van de sociale zekerheid en arbeidsvoorziening is door Suwi ingrijpend gewijzigd.

Sinds 2005 is de ontwikkeling van Suwinet in een versnelling gekomen, doordat de overheid de opdracht gaf om Suwinet te ontwikkelen tot een Digitaal Klant Dossier (DKD) Werk en Inkomen, zowel voor overheidsorganisaties als voor de burger. Het aantal en soort gegevensuitwisselingen via GeVS is enkele jaren gelden fors toegenomen door o.a. toenemende digitalisering en nieuwe organisaties die hun gegevens aanbieden via (o.a.) Suwinet-Inkijk. Maandelijks maken ongeveer 24.500 professionals gebruik van Suwinet-Inkijk en worden gegevens van ca. 680.000 Nederlanders opgevraagd.[19]

3.2 De Suwi-partijen en hun rol

Het Uitvoeringsinstituut Werknemersverzekeringen (UWV), de Sociale Verzekeringsbank (SVB) en gemeentelijke sociale diensten (GSD) zijn de zogenoemde Suwi-partijen en wisselen onderling gegevens uit via Suwinet. Het Bureau Keteninformatisering Werk & Inkomen (BKWI) is de beheerder van Suwinet en valt onder het UWV. Aangezien Suwinet op het domein van werk en inkomen opereert is het vanzelfsprekend dat deze partijen de opdrachtgevers van BKWI zijn. De Suwi-partijen bepalen gezamenlijk het programma van Suwinet via het Opdrachtgeversberaad (OGB).

De SVB is verantwoordelijk voor de uitvoering van de socialeverzekeringswetten in opdracht van het Ministerie van SZW en niet-socialeverzekeringswetten in opdracht van andere overheden. Ook gemeenten doen steeds vaker een beroep op de SVB, zoals bij het uitvoeren van persoonsgebonden financiële regelingen. Gemeenten zijn ook wettelijk verplicht om in bepaalde gevallen met SVB samen te werken.

Het UWV zorgt voor de landelijke uitvoering van werknemersverzekeringen en voor arbeidsmarkt- en gegevensdienstverlening. Net als de SVB doen ze dat als ZBO in opdracht van het Ministerie van SZW. Het UWV heeft een viertal kerntaken: mensen stimuleren om aan het werk te blijven of nieuw werk te vinden, het beoordelen van ziekte en arbeidsongeschiktheid, het verstrekken van uitkeringen als werken niet (direct) mogelijk is en ervoor zorgen dat mensen slechts één keer werkgegevens aan de overheid hoeven te verstrekken.

De gemeentelijke sociale diensten (GSD's) zijn uitvoeringsorganisaties van de gemeenten die zich o.a. bezig houden met het beoordelen van aanvragen om een uitkering. De GSD's gebruiken Suwinet voor verschillende doeleinden. Zie daarvoor de factsheet 'Suwinet voor gemeenten' van de VNG.[20]

Van belang is onderscheid te maken tussen enerzijds de ZBO's UWV en SVB en anderzijds gemeenten. De eerste partijen zijn centraal geleide organisaties die verantwoording afleggen aan de minister van SZW. Voor gemeenten ligt dit anders. Daar wordt verantwoording afgelegd door het college aan de gemeenteraad. De VNG heeft inmiddels voorgesteld om de

[19] Zie de Factsheet Suwinet-Inkijk van BKWI, http://www.bkwi.nl/fileadmin/downloads/Suwinet/Factsheets/BKWI_factsheet_Suwinet-Inkijk.pdf.
[20] Zie https://vng.nl/files/vng/20160530-factsheet-suwinet.pdf.

verantwoordingsplicht van gemeenten wettelijk te verankeren, om de positie van gemeenteraden te versterken.

In de Wet Suwi worden in hoofdstuk 5 de taken van het UWV vastgesteld. Zo heeft het UWV taken in verband met o.a. uitkeringsverstrekking, re-integratie van personen, arbeidsbemiddeling en registratie van werkzoekenden en vacatures. De taken van de SVB worden vastgesteld in hoofdstuk 6. Het gaat onder andere om uitvoering geven aan het AOW-pensioen, de nabestaandenuitkering ANW, kinderbijslag en enkele andere regelingen. De taken van de gemeente staan opgesomd in verschillende relevante wetten, op basis waarvan duidelijke overzichten zijn gemaakt zoals de factsheet Suwinet voor gemeenten. Met name gaat het daarbij om de uitvoering van wettelijke taken die vallen onder de P-wet, IOAW en IOAZ.[21]

3.3 Suwinet-inkijk

Deze PIA heeft alleen betrekking op Suwinet-Inkijk, één van de belangrijkste applicaties van Suwinet. Suwinet-Inkijk "biedt overheidsorganisaties de mogelijkheid om gegevens van burgers, die bij andere overheidsorganisaties of basisregistraties zijn opgeslagen, te raadplegen in één webtoepassing."[22] De gegevensbronnen en de gebruikers van Suwinet-Inkijk worden ingedeeld in Suwi-partijen (UWV, SVB en GSD) en niet-Suwi-partijen (o.a. RDW, DUO, KvK, Kadaster, Belastingdienst). De Suwi-partijen wisselen onderling gegevens met elkaar uit en kunnen gegevens ontsluiten van niet-Suwi-partijen. De niet-Suwi-partijen kunnen alleen gegevens opvragen van Suwi-partijen.[23] Zoals in paragraaf 1.3 aangegeven beperkt deze PIA zich tot gegevensuitwisselingen tussen de Suwi-partijen.

3.4 Maatregelen uit BVGS

De eerste onderzoeksvraag gaat over het beperken van de toegang tot personen (**maatregel negen**). Dat wil zeggen dat er geen gegevens kunnen worden ingezien van personen die niet relevant zijn voor de werkzaamheden van de medewerker. Om de toegang te beperken is er een filtermechanisme gebouwd voor Suwinet-Inkijk. Een filtermechanisme is 'een voorziening die de condities regelt c.q. toetst waaronder gevraagde gegevens mogen worden getoond'.[24] Deze voorziening is in dit geval een whitelist en een blacklist. Een whitelist is een lijst van BSN's van personen wiens gegevens mogen worden opgevraagd. Alleen de BSN's van personen waar de organisatie een dienstverleningsrelatie mee heeft mogen op de lijst worden geplaatst. Bij een blacklist gaat het om het omgekeerde: gegevens van personen kunnen niet worden geraadpleegd in Suwinet-Inkijk, als hun BSN op de lijst staat.

De tweede onderzoeksvraag gaat over het beperken van de toegang tot personen via zoeksleutels (**maatregel acht**). Deze maatregel beperkt de zoekmogelijkheden in Suwinet-Inkijk door niet meer onnodig de bevoegdheid te verlenen om andere zoeksleutels dan BSN te gebruiken. Hierdoor wordt voorkomen dat onnodig of onrechtmatig op andere zoeksleutels dan BSN wordt gezocht.

Deze maatregel hangt nauw samen met het beperken van de gegevens die kunnen worden getoond op een pagina. Via een fijnmazigere autorisatiestructuur (**maatregel één**) is het mogelijk om de gegevensverstrekking strikter te reguleren. Om aan geautoriseerde medewerkers minder gegevens te tonen is het verschil tussen overzichtspagina's en bronpagina's van belang. Een overzichtspagina

[21] Zie https://vng.nl/files/vng/20160530-factsheet-suwinet.pdf.
[22] Beschrijving van BKWI, < http://www.bkwi.nl/producten/suwinet-services/>.
[23] Zie ook het schema 'bronnen en gebruikers' van BKWI, < http://www.bkwi.nl/fileadmin/downloads/Suwinet/Suwinet-Inkijk/Bronnen_en_gebruikers_toelichting_2015.pdf>.
[24] Handreiking whitelist en escapefunctie, p. 3.

bundelt gegevens van verschillende bronnen in één pagina, terwijl een bronpagina slechts gegevens van één bron bevat. Het streven is overzichtspagina's zoveel mogelijk te beperken of te vervangen door bronpagina's. Andere toekomstige ideeën, zoals het werken met gegevensblokken of het tonen van informatie in plaats van gegevens, worden later in deze PIA besproken.

Er wordt beoordeeld in hoeverre de uitvoering die al is gegeven aan het beperken van de toegang tot personen en het beperken van de toegang via zoeksleutels bijdragen aan het verbeteren van de bescherming van de privacy van mensen die kunnen worden geraadpleegd via Suwinet-Inkijk. Ook wordt gekeken of er aanvullende of compenserende maatregelen kunnen worden genomen en, zo ja, welke dit zijn.

Ten slotte is van belang dat de impact van de uitvoering van het beperken van de toegang tot personen en het beperken van de toegang via zoeksleutels per Suwipartij (aanzienlijk) kan verschillen. De oorzaak hiervan ligt in de verschillen tussen de organisaties, de inrichting van de werkprocessen, hun taken en de aansturing.

4 Inventarisatie

Het doel van de inventarisatie is inzichtelijk te maken welke processen en functies binnen de organisatie gebruik maken van Suwinet-Inkijk. Aansluitend op de twee onderzoeksvragen, hebben we bij de inventarisatie ook geïnformeerd naar (1) tot op welk niveau de toegang in Suwinet-Inkijk is te beperken tot BSN's en wanneer en hoe het zal worden ingericht in de organisatie, zoals organisatieniveau, functieniveau, medewerkersniveau, en (2) welke zoeksleutels er in gebruik zijn.

4.1 Gezichtspunten van Suwi-partijen

Hieronder staat beknopt de uitkomsten van de gesprekken met de Suwi-partijen en met de programmamanager BVGS. Veel van de technische (on)mogelijkheden zijn afhankelijk van BKWI. Daarom zullen ook de uitkomsten van de gesprekken met deze partij aan de orde komen. De gesprekken concentreerden zich telkens op de twee onderzoeksvragen, in het bijzonder op de vragen op welke wijze uitvoering is gegeven of gaat worden gegeven aan de maatregelen acht en negen (beperken van het gebruik van zoeksleutels resp. beperken van de toegang tot personen). Waar nodig zal ook kort worden ingegaan op de wijze waarop uitvoering is gegeven of gaat worden gegeven aan maatregel één (fijnmazige autorisatiestructuur) en twee (logging en controle).

Bijeenkomsten met BKWI

Aangezien BKWI beheerder is van Suwinet gingen de gesprekken over de technische werking van Suwinet-Inkijk en welke ideeën en functionaliteiten er op de agenda staan om de privacy nog beter te waarborgen. Doordat ervoor gekozen is veel technische voorzieningen centraal in te regelen speelt BKWI een belangrijke rol. Zo verzorgt BKWI aan de voorkant het aanmaken van nieuwe pagina's en rollen en aan de achterkant logging en rapportage. Wijzigingen of aanvullende functionaliteiten kunnen worden besteld door Suwi-partijen, waarna de bestelling door een 'impact analyse straat' gaat.

Binnen Suwinet-Inkijk wordt nagenoeg alles gelogd. Deze loggegevens staan in rapportages, die bestaan uit generieke en specifieke rapportages. Generieke rapportages tonen geaggregeerde gegevens en specifieke rapportages, die apart opgevraagd dienen te worden als daartoe aanleiding bestaat op basis van een generieke rapportage, tonen gebruiksgegevens van individuele medewerkers. De rapportages worden verzonden met Suwinet-Mail. Het voornemen bestaat om binnenkort een rapportagetool aan te bieden, waarmee rapportages zelf real-time online zijn te genereren en op te vragen.

Bijeenkomst met de programmamanager BVGS

Tijdens de bijeenkomst met de programmamanager BVGS - ingesteld bij de VNG - is Suwinet besproken op een algemeen niveau: de aanleiding voor deze PIA, de categorieën van maatregelen (aanpassingen in GeVS zelf, beleid en awareness), de maatregelen van de werkgroepen die relevant zijn voor de PIA (beperken van het tonen van gegevens op pagina's en fijnmazige autorisatiestructuur, het beperken van het gebruik van zoeksleutels en het beperken van de toegang tot personen) en de sporen die zijn ingezet sinds mei 2015 (korte en lange termijn maatregelen en de module voorwaardelijke levering).

Bijeenkomsten met SVB

Op het moment van schrijven is bekend dat de whitelist zal worden ingericht op organisatieniveau, waardoor het aantal personen dat opvraagbaar zal zijn wordt beperkt tot circa 400.000 (zie paragraaf 5.3 voor een uitwerking van dit getal). Verder is een informatie analyse hieromtrent nog onderhanden. De IT implicaties zijn ook nog onbekend. Zaken als de voorwaarden voor plaatsing op de whitelist, wanneer de whitelist wordt ververst en welke controles er gaan plaatsvinden worden ook nog uitgewerkt.

Verder is, met betrekking tot het beperken van de toegang via zoeksleutels en de randvoorwaardelijke maatregel één, uit uitvoerig onderzoek door SVB gebleken dat er weinig tot geen verandering plaats zal vinden in de huidige pagina's en de zoeksleutels die beschikbaar zijn.

Bijeenkomsten bij UWV
In de bijeenkomsten met UWV is naast maatregel acht en negen ook besproken wat UWV aan de achterkant regelt (maatregel één en twee). Doordat UWV landelijk opereert is whitelisting op regionaal niveau niet praktisch uitvoerbaar en is zwaarder ingezet op de 'achterkant' (logging, rapportages).

In de gesprekken met UWV heeft de focus in eerste instantie gelegen op de mogelijkheid van een whitelist op organisatieniveau en is in deze context uitgegaan van de optelsom van alle klantenbases van alle organisatieonderdelen en het uitgangspunt om de impact op de huidige werkprocessen en ICT systemen zo laag mogelijk te houden. Dit zou betekenen dat de whitelist zou bestaan uit alle personen in de polisadministratie (ca 8 miljoen). Bij de inventariserende vragen (paragraaf 4.2) wordt nader ingegaan op welke maatregelen UWV van plan is te nemen om dit (te grote) aantal te beperken.

Het UWV is tevens een omvangrijk traject gestart om nieuwe pagina's aan te vragen. De uitvoering hiervan gebeurt in twee fasen en zal in 2017 breed worden uitgerold. Daardoor ontstaat de mogelijkheid om per pagina minder gegevens te tonen. De zoekmogelijkheden buiten BSN zijn zeer beperkt en worden bij UWV nog verder teruggedrongen.

Bijeenkomsten met VNG/KING
Ten slotte zijn er meerdere bijeenkomsten geweest met en bij VNG/KING. Ten behoeve van het bevorderen van de implementatie van de maatregelen van het programma werden er in september regiobijeenkomsten georganiseerd in heel Nederland met behulp van accountmanagers, waarna vervolgens de whitelist functionaliteit per gemeente wordt uitgerold. Dit is een behoorlijke stap in de juiste richting, omdat de toegang tot personen wordt beperkt tot slechts de personen waar de gemeente een dienstverleningsrelatie mee heeft (organisatieniveau).

Voor gemeenten zijn er al zes nieuwe bronpagina's gemaakt, ter vervanging van twee overzichtspagina's. De zoekmogelijkheden buiten BSN zijn zeer beperkt. Het gaat om ca. 4,6% aan 'andere' zoeksleutels, waarvan ongeveer 2,2% zoeken via het bedrijvenregister is (waar geen BSN kan worden gebruikt). Deze cijfers schommelen een beetje van maand tot maand, maar het gaat om zeer geringe aantallen.

4.2 Inventariserende vragen

In het kader van de onderzoeksvragen is het belangrijk in kaart te brengen welke wettelijke grondslagen er zijn om Suwinet-Inkijk te raadplegen en welke processen daarvan gebruik maken (vraag a), tot op welk niveau de whitelist kan worden geïmplementeerd (vraag b) en hoe bepaald wordt wie op de whitelist wordt geplaatst (vraag c). Al deze vragen dragen bij aan het onderzoeken of de toegang tot personen in Suwinet-Inkijk (nog) verder kan worden beperkt. Aangezien er al overzichten bestaan met alle zoeksleutels en zoeksleutels anders dan BSN is het niet nodig vragen te stellen met betrekking tot de tweede onderzoeksvraag.

Deels is de gevraagde informatie al beschikbaar in eerder opgestelde documenten, zoals wettelijke grondslagen en bepaalde processen die gebruik maken van Suwinet-Inkijk. Een verwijzing naar het betreffende document volstaat dan ook. Na elke vraag worden de reacties per Suwi-partij kort weergegeven:

(a) Inventarisaties van wettelijke grondslagen van Suwinet taken en de bijbehorende functies en rollen, de gegevens die nodig zijn om deze taken uit te voeren en de processen waarbinnen deze taken plaatsvinden.

Gemeenten: Door VNG is een overzicht van de wettelijke grondslagen al opgesteld en gepubliceerd in de factsheet 'Suwinet voor gemeenten'. Wettelijke taken worden toebedeeld aan functionarissen, die zijn onder te verdelen in specialisten (die (sub)taken uitvoeren) en generalisten (die meerdere taken uitvoeren). Doordat iedere gemeente de functies op haar eigen manier invult, kan de ene medewerker in de ene gemeente andere taken uitvoeren dan in een andere gemeente. Deze diversiteit komt ook terug bij de werkprocessen. Er zijn dan ook geen generieke werkprocessen bij gemeenten. Het proces ter uitvoering van een wettelijke taak kan bij de ene gemeente anders zijn ingevuld dan bij de andere gemeente. Indien de processen van alle gemeenten zouden moeten worden opgeleverd en geanalyseerd zou dit een onwerkbare situatie worden om te verwerken in dit rapport.

SVB: Vanuit SVB is een overzicht hiervan reeds opgesteld in een Excel document in combinatie met de doelbindingsverklaring. Het Excel document bevat o.a. de wettelijke grondslagen voor het raadplegen van Suwinet-Inkijk, het doel van een raadpleging en welke processen gebruik maken van Suwinet-Inkijk. Gezien het feit dat zowel op dit moment (IST) als wanneer de whitelist functionaliteit is geïmplementeerd (SOLL) de situatie niet veel anders is, is de inventarisatie een weergave van beide situaties.

UWV: UWV heeft de 'Notitie inrichting Suwinet-Inkijk BVGS UWV' opgesteld waarin per bedrijfsonderdeel of afdeling wordt ingegaan op de wijze waarop uitvoering is of kan worden gegeven aan de maatregelen acht en één. Het document bevat zowel de IST situatie als de SOLL situatie. De SOLL situatie sluit één op één aan op het UWV autorisatiesysteem, waarin de toegangsrechten per functie/rol zijn vastgelegd. Zo komt het bij bijna alle afdelingen voor dat er na de analyse minder gegevensvelden beschikbaar zijn.

(b) Onderbouwde analyse naar tot op welk niveau de toegang is te beperken tot BSN's in Suwinet-Inkijk en wanneer en hoe het zal worden ingericht in de organisatie: organisatieniveau, functieniveau, medewerkersniveau of, indien mogelijk, combinaties van deze filteringen, zoals alleen op bepaalde bedrijfsonderdelen medewerkersniveau.

Gemeenten: Het samenstellen van de whitelist is een gemeentelijke verantwoordelijkheid. In de regel zullen er tussen gemeenten veel overeenkomsten zijn bij het samenstellen van die whitelist op organisatieniveau, omdat de werkvoorraad wordt bepaald door de wettelijke taken die zij hebben uit te voeren. Wel zijn er (o.a.) verschillen in de duur waarvoor iemand nog als ex-klant van de gemeente wordt aangeduid, waardoor de termijn waarvoor iemand op een whitelist staat per gemeente kan verschillen.

SVB: Binnen de SVB wordt vanuit verschillende wetten en regelingen door medewerkers gebruik gemaakt van Suwinet-Inkijk. Voor de uitvoering van deze wetten en regelingen worden meerdere informatiesystemen gebruikt. In deze informatiesystemen wordt het onderhanden werk geadministreerd middels zogenoemde 'gevalsbehandelingen'. Een gevalsbehandeling heeft altijd betrekking op een klant die veelal ook een BSN heeft. De groep van actieve gevalsbehandelingen is continue in beweging doordat dagelijks nieuwe gevalsbehandelingen worden aangemaakt (aanvragen en mutaties) en uiteraard ook dagelijks gevalsbehandelingen worden afgesloten (afgehandelde aanvragen en mutaties).

Voor de gehele SVB-organisatie geldt dat er continue circa 150.000 actieve gevalsbehandelingen zijn. De whitelist-oplossing voor de SVB komt erop neer dat alle actieve gevalsbehandelingen uit alle relevante informatiesystemen (periodiek: wordt waarschijnlijk dagelijks) worden verzameld en als batch worden aangeleverd aan BKWI ter opname in de SVB-whitelist. Naast de direct bij de gevalsbehandeling betrokken klant/burger, zullen ook andere personen die relevant zijn voor de betreffende gevalsbehandeling (partners, medebewoners, etc.) op de SVB-whitelist komen.

Ook nadat een gevalsbehandeling is afgesloten zal een gevalsbehandeling nog een aantal weken aangeleverd blijven worden voor de SVB-whitelist in verband met de bezwaarperiode en eventuele vragen van klanten over de afgesloten gevalsbehandeling. Dit alles in beschouwing genomen zal de SVB-whitelist continue circa 400.000 personen bevatten, die qua samenstelling continue is afgestemd op de actualiteit van de onderhanden/afgehandelde gevalsbehandelingen. De SVB-whitelist zal dus zorgen voor een teruggang van toegang tot circa 18 miljoen personen naar toegang tot circa 400.000 personen voor de gehele SVB-organisatie.

UWV: In de 'Notitie inrichting Suwinet-Inkijk BVGS UWV' wordt per afdeling een globale indicatie gegeven of het mogelijk is een whitelist te implementeren. Met de huidige, beschikbare functionaliteiten is dit slechts in beperkte mate mogelijk. Gegeven dat de whitelist ingericht wordt op organisatieniveau, schat UWV het rendement en de mate waarin deze oplossing het risico beperkt te laag in. Dit zou namelijk betekenen dat de toegang tot BSN's van circa 17 mln. BSN's terugloopt naar circa 8 mln. BSN's.

UWV heeft hierop besloten een impactanalyse uit te voeren waarmee de mogelijkheden om whitelists op een lager niveau te implementeren, in beeld worden gebracht. Tevens wordt hierbij gekeken naar andere mogelijkheden om de toegang tot personen te beperken. Een whitelist op organisatieniveau zou nog steeds leiden tot een grote groep raadpleegbare personen (8 miljoen personen in de polisadministratie). UWV onderzoekt maatregelen die ertoe bijdragen dat medewerkers alleen gegevens van personen raadplegen waarvoor zij wettelijke taken uitvoeren.

De impactanalyse zal ultimo december 2016 duidelijkheid geven over welke mogelijkheden UWV ziet om whitelists binnen de processen van UWV te implementeren en welke andere mogelijkheden er zijn om de toegang tot personen te beperken. Vervolgens zal UWV begin 2017 door middel van een uitvoeringstoets in beeld brengen wat de exacte uitvoeringsconsequenties en doorlooptijden zijn van deze mogelijkheden. Voorlopig wordt gewerkt met controlerende maatregelen zoals scherpere en snellere controles op het raadplegen van BSN via Suwinet-inkijk, aanscherping van de sanctiemogelijkheden wanneer een medewerker oneigenlijk gebruik maakt van Suwinet-inkijk en een bijbehorende bewustwordingscampagne. Ook van deze maatregelen gaat een preventieve werking uit.

Het zal voor UWV en BKWI een omvangrijk traject zijn, waar vrijwel alle onderdelen van UWV mee te maken krijgen en dat ook raakt aan veel UWV materie (ICT) systemen.

(c) De criteria waaraan moet zijn voldaan om te kunnen spreken van een dienstverleningsrelatie/behandelrelatie (waardoor iemand op de whitelist terecht komt). Onder een behandelrelatie vallen ook medewerkers die belast zijn met opsporings- en/of handhavingstaken, zoals sociale rechercheurs. Daarnaast is het zo dat ook mensen opgevraagd worden die niet onder een dienstverleningsrelatie vallen, zoals ex-partners of huisgenoten. Hiervoor dient de escape functie te worden gebruikt.
Als sprake is van integrale dienstverlening ligt het niet voor de hand mensen te whitelisten op medewerkersniveau. Waar mogelijk dienen dan de integrale criteria, die bepalen of iemand op de whitelist terecht komt, te worden geïnventariseerd.

Gemeenten: Zoals eerder opgemerkt is het samenstellen van de whitelist een gemeentelijke verantwoordelijkheid. Iedere gemeente bepaalt dan ook welke criteria er gelden om opgenomen te worden op de whitelist. Dit zal in de regel neerkomen op het uitvoeren van een wettelijke taak.

SVB: De voorwaarden voor wanneer sprake is van een dienstverleningsrelatie met een klant is dat er een actuele gevalsbehandeling is en een wettelijke grondslag voor het uitvoeren van een taak.

UWV: UWV onderzoekt op dit moment de mogelijkheden voor whitelists via een impactanalyse.

4.3 Overzicht gesprekken

In het onderstaande tabel staat in chronologische volgorde aangegeven wanneer met welke Suwi-partij werd gesproken en wanneer bijeenkomsten met de begeleidingscommissie hadden plaatsgevonden.

21 april	Startbijeenkomst bij SZW
11 mei	BKWI
13 mei	Programmamanager BVGS
19 mei	SVB
25 mei	UWV
30 mei	Begeleidingscommissie
03 juni	VNG/KING
16 juni	BKWI
23 juni	SVB
27 juni	Begeleidingscommissie
06 juli	UWV
07 juli	Inspectie SZW
11 juli	VNG/KING
19 juli	BKWI (demo)
24 augustus	UWV
29 augustus	Begeleidingscommissie
26 september	Begeleidingscommissie

5 Analyse van de informatie

De informatie die is ontvangen uit documenten, uit de inventariserende vragen en uit gesprekken met Suwi-partijen dient te worden getoetst aan relevante privacybeginselen en principes uit de informatiebeveiliging om te kunnen beoordelen in hoeverre de maatregelen bijdragen aan een betere bescherming van de privacy. Welke privacybeginselen en welke principes uit de informatiebeveiliging dit zijn, komt aan de orde in dit hoofdstuk. Dit hoofdstuk wordt afgesloten met een overzicht op hoofdlijnen van de bevindingen. De bevindingen zijn alleen gebaseerd op de vergaarde informatie uit documenten en gesprekken met de Suwi-partijen en bevatten geen conclusie (toetsing van de informatie) of aanbeveling (onze visie op het resultaat van de toetsing).

In het volgende hoofdstuk vindt de toetsing van de informatie plaats aan de hand van de beginselen en normen uit dit hoofdstuk en wordt het resultaat daarvan weergegeven in een aantal conclusies. Er wordt met andere woorden gekeken of de uitvoering die is of gaat worden gegeven aan het beperken van de toegang tot personen en het beperken via zoeksleutels in voldoende mate overeenstemmen met de eisen uit het privacyrecht en de normen uit de informatiebeveiliging. Tot slot volgen in de aanbevelingen aanvullende voorstellen voor uitvoeringsmaatregelen die zoveel mogelijk dienen te worden opgevolgd om de waarborging van de privacy rondom Suwinet-Inkijk verder aan te scherpen.

5.1 Privacy Analyse

In de eerdere PIA is met name vanuit juridisch perspectief gekeken naar de vereisten voor de verwerking van persoonsgegevens binnen Suwinet. De legitieme grondslagen voor de verwerking zijn onderzocht en er is gekeken in hoeverre er mitigerende maatregelen vereist zijn. In dit onderzoek is hierop voortgebouwd, met name op de aanbeveling dat doelbinding dient te worden verbetert door meer filtering functionaliteit en actieve monitoring.[25] Het begrip doelbinding wordt hieronder besproken. Bij doelbinding gaat het overigens niet om het hebben van een wettelijke grondslag voor het raadplegen van Suwinet-Inkijk (dat is altijd vereist), maar om te beoordelen of het doel van de raadpleging nog in overeenstemming is met de uitvoering van een wettelijke taak (paragraaf 3.2).

De wijze waarop uitvoering is gegeven aan maatregel één van het Programmaplan BVGS speelt overigens ook een beperkte rol in deze PIA. In het programmaplan werd immers duidelijk gemaakt dat maatregel één randvoorwaardelijk is voor een effectieve uitvoering van de maatregelen acht en negen. Om een duidelijk onderscheid te maken met de onderzoeksvragen, wordt maatregel één, net zoals bij de conclusies en aanbevelingen, apart besproken onder 'overige bevindingen' (paragraaf 5.4).

Er wordt in deze PIA gekeken naar de winst die behaald kan worden met betrekking tot de bescherming van privacy door het beperken van de toegang tot personen en het beperken van de zoekmogelijkheden (maatregelen acht en negen, zie paragraaf 3.4). De vraag die centraal staat is of de uitvoering die al is gegeven aan deze maatregelen toereikend is en of er eventuele andere uitvoeringsmaatregelen kunnen worden genomen om de privacy nog beter te waarborgen. Niet alleen de juridische grondslagen zijn dan van belang, maar ook de technische implementatie (-mogelijkheden) versus organisatorische mogelijkheden om waarborgen te creëren.

Met de technische implementatie kunnen immers een aantal privacyvereisten nader ingevuld worden en tot op zekere hoogte technisch afgedwongen. Dat leidt in de praktijk tot een Privacy by Design benadering, waarbij technische en organisatorische maatregelen elkaar in evenwicht

[25] PIA Suwinet van PMP, p. 78.

houden. Waar technisch bepaalde zaken moeilijk afgedwongen kunnen worden, omdat daarmee de dagelijkse werkbaarheid voor de betrokken organisaties in het gedrang zou komen, zijn organisatorische maatregelen (zoals controles achteraf) de aangewezen manier om toch voldoende waarborgen in te bouwen. Belangrijk daarbij is dat als het bouwen en implementeren van de techniek of aanpassen van de processen een behoorlijke investering vergt, dat niet wil zeggen dat het om die reden niet mogelijk is. Naarmate de privacy beter beschermd kan worden door deze wijze van uitvoering van de maatregelen is het eerder aannemelijk dat wél een dergelijk (intensief) traject dient te worden gevolgd.[26]

Met de uitvoering van de maatregelen wordt gedoeld op het beperken van toegang tot gegevens (whitelisting) door de beschikbare sets te beperken (fijnmazigere pagina's), maar ook door de wijze van raadplegen te beperken (zoeksleutels). In aanvulling daarop wordt gekeken op welke wijze het aantal gegevens dat verwerkt wordt, beperkt kan worden wanneer op basis van een zoeksleutel of whitelist toegang wordt verkregen.

Aan de hand van de volgende privacybeginselen kan worden getoetst of de technische en organisatorische uitvoering die reeds is gegeven aan de maatregelen leiden tot een betere borging van de privacy:

- **Dataminimalisatie**: dit houdt in dat persoonsgegevens ter zake dienend en niet bovenmatig zijn (art. 11 Wbp). In feite betekent het dat er een voortdurende verplichting wordt gelegd op de verantwoordelijke om, wanneer persoonsgegevens worden verwerkt, te toetsen of deze gegevens ter zake dienend en niet bovenmatig zijn. Het hangt van het doel van de verwerking af of voldaan is aan de eisen van dataminimalisatie.
- **Doelbinding**: naast het vereiste van een wettelijke grondslag voor een verwerking van persoonsgegevens moet er ook een duidelijk doel zijn waarvoor de gegevens worden verwerkt. De persoonsgegevens mogen niet verder worden verwerkt voor een doel dat onverenigbaar is met het oorspronkelijke doel waarvoor ze zijn verzameld (art. 9 Wbp). Ze mogen dus wel worden verwerkt voor een ander doel, als dat doel maar verenigbaar is met het oorspronkelijke doel.
- **Verwerkingsduur**: persoonsgegevens mogen niet langer worden verwerkt dan noodzakelijk (art. 10 Wbp). In de context van deze PIA gaat het niet om de daadwerkelijke opslag van persoonsgegevens, maar om de termijn waarop iemand staat geregistreerd op een whitelist. Gedurende die termijn zijn persoonsgegevens immers opvraagbaar door geautoriseerde medewerkers. De duur van de termijn wordt (bij voorkeur) bepaald door het begin en het einde van de dienstverleningsrelatie. Een dienstverleningsrelatie duurt net zolang voort totdat de wettelijke taak, waarvoor Suwinet-Inkijk mag worden gebruikt, is uitgevoerd en afgerond. Een dienstverleningsrelatie kan soms wat langer doorlopen in verband met bezwaartermijnen en/of eventuele vragen van de klant.

Duidelijk dient te worden gemaakt hoe deze beginselen zich verhouden tot de onderzoeksvragen, in het bijzonder tot de wijze waarop uitvoering is of gaat worden gegeven aan de maatregelen acht en negen. Dataminimalisatie houdt voornamelijk verband met de whitelist en de, in dit rapport niet centraal staande, overzichts- en bronpagina's. De whitelist zorgt ervoor dat geen overbodige persoonsgegevens kunnen worden opgevraagd van personen met wie geen dienstverleningsrelatie bestaat. De pagina's dienen alleen de noodzakelijke gegevens te tonen. Als persoonsgegevens van

[26] Zie in dit verband bijvoorbeeld ook de brief die de Autoriteit Persoonsgegevens naar de minister van BZK stuurde over de toepassing van Privacy by Design in het eID stelsel: https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-onvoldoende-aandacht-voor-privacy-bij-eid .

personen worden getoond die niet verband houden met het uitvoeren van een wettelijke taak, kan worden gesteld dat deze gegevens niet ter zake dienend en bovenmatig zijn. Er vindt dan immers een verwerking plaats in de vorm van raadpleging.

Doelbinding heeft betrekking op de uitvoering van beide maatregelen. Zo is een zoeksleutel aangemaakt voor een bepaald doel, namelijk ten behoeve van het kunnen uitvoeren van een wettelijke taak. Als een zoeksleutel voor een ander doel wordt ingezet dan is sprake van strijd met het doelbindingsbeginsel. Datzelfde geldt voor de whitelist. Personen op de whitelist kunnen alleen worden geraadpleegd voor een bepaald doel, namelijk voor het uitvoeren van een bepaalde wettelijke taak. Als personen worden geraadpleegd voor een ander doel dan is er ook in deze situatie in strijd gehandeld met het doelbindingsbeginsel.

Ten slotte heeft de verwerkingsduur betrekking op de whitelist. Personen met wie geen dienstverleningsrelatie is of waarvan de dienstrelatie is beëindigd (en de bezwaartermijnen zijn verlopen en er zijn geen vragen meer van de klant) dienen niet meer op de whitelist te staan. Met behulp van whitelisting kan dit technisch ingebed worden, waarmee Privacy by Design wordt toegepast in de uitvoering.

5.2 Risicoanalyse

Zoals in de inleiding gesteld, worden hier de principes uit de informatiebeveiliging besproken die relevant zijn voor de onderzoeksvragen.

5.2.1 Normen

Bij het uitvoeren van een risicoanalyse vanuit informatiebeveiligingsperspectief wordt gekeken naar risico's die de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie nadelig kunnen beïnvloeden. In het kader van de PIA en uitgaande van het feit dat het onderzoek zich richt op Suwinet-inkijk, is bij het uitvoeren van de risicoanalyse alleen gekeken naar risico's die impact hebben op de vertrouwelijkheid van de informatie in Suwinet. De beschikbaarheid en integriteit vallen buiten de scope van de PIA, omdat de onderzoeksvragen geen betrekking hebben op de beschikbaarheid van de dienst op afgesproken momenten respectievelijk de mate waarin gegevens actueel en correct zijn.

Om de risicoanalyse zo specifiek mogelijk uit te voeren binnen het onderzoek is ervoor gekozen om geen gebruik te maken van een bestaande methodiek, maar is op basis van de van toepassing zijnde normen (zie hoofdstuk 2.3 voor een overzicht van de normenkaders) bepaald welke gerelateerde risico's van toepassing zijn op de onderzoeksvragen. Hierbij zijn de zeven essentiële normen die worden gehanteerd door de Inspectie SZW als basis gebruikt (kolommen 'GeVS' en 'Norm') en zijn normen uit de andere normenkaders hierop geplot (kolom 'ISO / BIR / BIG ref'). Vervolgens wordt in de laatste kolom beoordeeld of de norm van toepassing is op één of beide onderzoeksvragen.

Nr.	# GeVS	Norm	ISO / BIR / BIG ref	Opmerking
1.	1.3	Het informatiebeveiligingsbeleid en het beveiligingsplan van het Suwinet zijn goedgekeurd door het management van de Suwipartij.	ISO – A.5.1.1 BIR/BIG – 5.1.1	Niet direct van toepassing op het onderzoek.
2.	1.4	Het informatiebeveiligingsbeleid en het beveiligingsplan van het Suwinet worden uitgedragen in de organisatie.	ISO – A.5.1.1 BIR/BIG – 5.1.1	Niet direct van toepassing op het onderzoek.

Nr.	# GeVS	Norm	ISO / BIR / BIG ref	Opmerking
3.	1.5	Het informatiebeveiligingsbeleid en het beveiligingsplan van het Suwinet worden jaarlijks geëvalueerd en indien nodig geactualiseerd.	ISO – A.5.1.2 BIR/BIG – 5.2.1	Niet direct van toepassing op het onderzoek.
4.	2.2	De taken, verantwoordelijkheden en bevoegdheden ten aanzien van het gebruik, de inrichting, het beheer en de beveiliging van Suwinet gegevens, applicaties, processen en infrastructuur moeten zijn beschreven en duidelijk en afhankelijk van de schaalomvang van de organisatie gescheiden zijn belegd.	ISO – A.6.1.1, A.6.1.2, A.9.1.1, A.9.4.1 BIR/BIG – 8.1.1, 8.2.1, 10.1.3, 11.2.1, 11.2.2, 11.6.1	Van toepassing op beide onderzoeksvragen.
5.	2.3	De Security Officer beheert en beheerst beveiligingsprocedures en maatregelen in het kader van Suwinet, zodanig dat de beveiliging van Suwinet overeenkomstig wettelijke eisen is geïmplementeerd.	ISO – A.6.1.2, A.18.1.4 BIR/BIG – 6.1.2, 15.2	Niet direct van toepassing op het onderzoek.
6.	13.1	De Suwipartij autoriseert en registreert de gebruikers die toegang hebben tot de Suwinet applicaties op basis van een formele procedure.	ISO – A.9.2 BIR/BIG – 11.2, 11.5.2	Van toepassing op beide onderzoeksvragen.
7.	13.5	De controle op verleende toegangsrechten en gebruik vindt meerdere keren per jaar plaats.	ISO – A.9.2 BIR/BIG – 11.1.1, 11.2.4	Van toepassing op beide onderzoeksvragen.

5.2.2 Geïdentificeerde risico's

Op basis van de analyse van de normenkaders is gekozen om de risicoanalyse toe te spitsen op de volgende essentiële normen:

Nr. 4. De taken, verantwoordelijkheden en bevoegdheden ten aanzien van het gebruik, de inrichting, het beheer en de beveiliging van Suwinet gegevens, applicaties, processen en infrastructuur moeten zijn beschreven en duidelijk en afhankelijk van de schaalomvang van de organisatie gescheiden zijn belegd (norm 2.2 GeVS).

Nr. 6. De Suwipartij autoriseert en registreert de gebruikers die toegang hebben tot de Suwinet applicaties op basis van een formele procedure (norm 13.1 GeVS).

Nr. 7. De controle op verleende toegangsrechten en gebruik vindt meerdere keren per jaar plaats (norm 13.5 GeVS).

Aan de hand van bovengenoemde normen is een aantal risico's vastgesteld (kolom 'Risico') die direct te relateren zijn aan de onderzoeksvragen (kolom 'Onderzoeksvraag'). In de laatste kolom is vervolgens voor elk van de risico's op basis van de aangeleverde informatie en de gevoerde gesprekken met de Suwi-partijen bepaald welke mitigerende maatregelen uit het programmaplan zijn of worden geïmplementeerd die de impact en kans van het risico verlagen of verminderen. De blauwgedrukte onderzoeksvragen en essentiële normen houden in dat het risico zich met name kan voordoen in het kader van die onderzoeksvraag en die essentiële norm. De blauwgedrukte

mitigerende maatregel betekent dat het risico voornamelijk (deels) wordt gedekt door deze maatregel.

#	Risico	Onderzoeksvraag	Essentiele norm	Mitigerende maatregelen uit het programmaplan (al geïmplementeerd / implementatie gestart)
1.	Gebruikers bekijken persoonsgegevens van een voor de taak niet relevante persoon (zonder doelbinding)	1,2	4,6,7	- Maatregel 2 (logging en monitoring) - Maatregel 5 (beleid onbedoeld gebruik) - Maatregel 8 (beperken zoeksleutels) **- Maatregel 9 (whitelist)**
2.	Gebruikers maken misbruik van het systeem, zoals voor persoonlijk gewin.	1,2	4,6,7	- Maatregel 2 (logging en monitoring) - Maatregel 5 (beleid onbedoeld gebruik) **- Maatregel 8 (beperken zoeksleutels)** **- Maatregel 9 (whitelist)**
3.	Gebruikers hebben toegang tot persoonsgegevens van reeds afgehandelde dossiers.	1	7	- Maatregel 2 (logging en monitoring) **- Maatregel 9 (whitelist)**
4.	Gebruikers hebben de beschikking over niet-doelmatige zoeksleutels.	2	4,6,7	- Maatregel 2 (logging en monitoring) **- Maatregel 8 (beperken zoeksleutels)**
5.	Gebruikers hebben een te grote set aan autorisaties, waaronder ook te veel zware rollen vallen (zie paragraaf 6.2.2. voor een definitie van zware rollen).	1,2	4,6,7	**- Maatregel 1 (fijnmazige autorisatiestructuur)** - Maatregel 2 (logging en monitoring) **- Maatregel 8 (beperken zoeksleutels)** - Maatregel 9 (whitelist)

Als de beschreven maatregelen vanuit het Programmaplan BVGS op de vastgestelde risico's worden gelegd, biedt dit (de daadwerkelijke implementatie per organisatie daargelaten) voor elk van de risico's een zekere dekking. Met name maatregel negen (whitelist) kan voor een significante reductie zorgen van het risicobeeld. Niet alleen bij de implementatie van deze maatregel op medewerkersniveau, maar in sommige gevallen ook op een hoger niveau. In het Programmaplan BVGS is echter al opgemerkt dat het met de huidige processen en techniek slechts in beperkte mate mogelijk is om een whitelist in te zetten op medewerkersniveau.[27] Daarnaast dient rekening te worden gehouden met het feit dat een whitelist op een lager niveau kan leiden tot een verzwaring van de controletaken, afhankelijk van de technische implementatie. Het niveau van implementatie van de whitelist is dan ook afhankelijk van dergelijke en andere (organisatiespecifieke) factoren.

Tijdens dit onderzoek is gebleken dat de Suwi-partijen al veel zeer belangrijke stappen hebben genomen om uitvoering te geven aan de maatregelen in het Programmaplan BVGS. De uitvoering van sommige voorgenomen maatregelen – waarvan slechts maatregelen acht, negen en in beperkte mate één relevant zijn voor dit rapport – is echter (nog) niet geheel voltooid, waardoor de benoemde risico's nog niet afdoende worden gemitigeerd. Ondanks dat dit voorgenomen

[27] Programmaplan BVGS, p. 20 e.v.

maatregelen zijn (die al wel in werking zijn getreden bij de pilotgemeenten), resulteert dit op dit moment wel in restrisico's die in de conclusies in het volgende hoofdstuk zijn verwerkt.

5.3 Bevindingen

Op basis van de inventarisatie en de uitgevoerde analyse is een aantal bevindingen vastgesteld. De bevindingen beschrijven slechts de constatering op basis van de beschikbare informatie; in hoofdstuk 6 worden de conclusies en aanbevelingen op basis van deze bevindingen beschreven.

Voor het onderzoek was het van belang dat de belanghebbende partijen (inclusief BKWI) volledige medewerking verlenen om zodoende het volledige spectrum van het gebruik van Suwinet-Inkijk in relatie tot de onderzoeksvragen in kaart te kunnen brengen. Belanghebbende partijen hebben dan ook volledige medewerking gegeven aan het onderzoek en hebben alle relevante informatie op korte termijn beschikbaar gesteld.

De belanghebbende partijen hebben elk een duidelijk afgebakend taakgebied en hebben elk een geheel eigen organisatie inrichting en structuur. Dit impliceert dat de wijze waarop de partijen Suwinet-Inkijk gebruiken in de dagelijkse bedrijfsprocessen significant van elkaar verschilt.

Het Programmaplan BVGS beschrijft de wijze waarop het beperken van het gebruik van zoeksleutels (maatregel acht) en het beperken van toegang tot relevante personen (maatregel negen) moet worden vormgegeven. Het implementeren van deze maatregelen bij elk van de partijen zorgt voor een significante reductie van het risicobeeld.

Implementatie van maatregel negen (en de andere maatregelen) is aangevangen bij de gemeenten, met ondersteuning vanuit VNG/KING. De andere Suwi-partijen, SVB en UWV, zijn in de voorbereidende fase om de wijze van implementatie verder vorm te geven aan de hand van de bedrijfsprocessen. Geen van de partijen heeft ervoor gekozen om de implementatie van deze maatregel op medewerkersniveau uit te voeren (caseload per medewerker). Implementatie vindt bij voorkeur op een hogere laag ("organisatieniveau") in de organisatie plaats. De achterliggende redenen hiervan en de gekozen oplossingsrichting van elk van de Suwi-partijen staat hieronder aangegeven.

- **Gemeenten**: Bij gemeenten wordt vaak door meerdere mensen aan een zaak gewerkt. Beperking tot medewerkersniveau kan daardoor problematisch zijn en de voortgang van een dienstverlening hinderen en de uitvoeringslasten onevenredig doen oplopen. Medewerkersniveau dient dan ook niet uitgelegd te worden als op het niveau van een individuele medewerker, maar op het niveau van een rol, functie of team. Ook vervanging bij afwezigheid wordt hiermee afgevangen.

- **SVB**: Er worden alleen personen op de whitelist geplaatst waarmee een actuele behandelrelatie bestaat, zoals personen die een Anw-aanvraag hebben ingediend of personen die tijdelijk in het buitenland gaan werken wat mogelijk consequenties heeft voor de AOW-opbouw. De actuele dienstverlening is verbonden aan een bericht met begin- en einddatum. De looptijd van een bericht, en dus van het bestaan van een BSN op de whitelist, is afhankelijk van deze looptijd. De SVB verwacht een teruggang tot circa 400.000 personen voor de gehele organisatie. De whitelist binnen de SVB zal dus continue in beweging zijn door toevoeging van nieuwe actuele behandelrelaties en het verwijderen van oudere behandelrelaties.

- **UWV**: UWV heeft aangegeven dat een whitelist op organisatieniveau nog steeds zou leiden tot een grote groep personen. UWV onderzoekt daarom ook de mogelijkheden om whitelists op een lager niveau te implementeren en om op andere wijze de toegang tot personen te

beperken. De verwachting is wel dat dit forse aanpassingen van processen en ICT-systemen met zich mee zal brengen. Op dit moment onderzoekt UWV via een impactanalyse welke mogelijkheden er zijn binnen de processen en het architectuurlandschap van UWV. De resultaten van deze analyse zullen meer helderheid moeten bieden over de vraag of de voorgenomen stappen toereikend zijn.

Daarnaast investeert UWV sterk in de controle aan de achterkant met specifiekere rapportages, sneller rapportages inzien en de interne processen hierop te verbeteren zodat onjuist gedrag direct wordt gesignaleerd en gesanctioneerd. Dit heeft ook een preventieve werking aan de voorkant.

Het gebruik van zoeksleutels anders dan het BSN (maatregel acht) is bij elk van de organisaties beperkt te noemen. In minder dan 3% van het totaal aantal bevragingen (zoekacties in het bedrijvenregister daargelaten vanwege het ontbreken van BSN) wordt gebruik gemaakt van een andere zoeksleutel.

5.4 Overige bevindingen

Tijdens het onderzoek is veel informatie over de overige maatregelen uit het programmaplan gedeeld en besproken gezien de onderlinge relaties van de maatregelen. Hier zijn ook een aantal bevindingen uit voortgekomen welke hieronder apart zijn benoemd.

- De zes nieuwe pagina's die voor gemeenten ter beschikking zijn gesteld zijn vooral ontwikkeld met de gedachte dat werk en inkomen vandaag de dag strikt gescheiden zijn. Daarvoor is één grote overzichtspagina in tweeën geknipt die de taken voor werk en inkomen ondersteunen en zijn er daarnaast enkele bronpagina's bij gekomen om disproportionaliteit (onnodig veel gegevens tonen) tegen te gaan.
- Techniek voor het beschikbaar stellen, configureren en gebruiken van partij-specifieke (overzicht) pagina's is beschikbaar en wordt gebruikt (maatregel 1).
- Generieke en specifieke rapportages zijn via BKWI beschikbaar voor alle partijen. Generieke rapportages worden regelmatig aan iedere Suwi-partij verstrekt en bevat geaggregeerde statistieken over het gebruik van Suwinet-Inkijk door medewerkers van de organisatie. Specifieke rapportages, die het gebruik inzichtelijk maken van individuele medewerkers, worden op aanvraag van een Suwi-partij gedeeld door BKWI. Dit gebeurt doorgaans wanneer de generieke rapportage aanleiding geeft tot nader onderzoek naar de handelingen van één of meerdere medewerkers. Gebleken is dat specifieke rapportages slechts beperkt worden opgevraagd door de partijen. Belangrijk is dat maatregel twee van het Programmaplan BVGS enkele significante verbeteringen voorstelt, waaraan deels al uitvoering is gegeven, ten aanzien van het controleproces (via rapportages) achteraf door de Suwi-partijen.

6 Conclusies

In het vorige hoofdstuk zijn de privacybeginselen en principes uit de informatiebeveiliging besproken die worden gebruikt als toetssteen om te beoordelen in hoeverre de reeds gedane uitvoering die is gegeven aan het beperken van de toegang tot personen en het beperken via zoeksleutels voldoen aan de eisen die volgen uit deze beginselen en principes. Het hoofdstuk is afgesloten met een overzicht van de bevindingen (zie inleiding van hoofdstuk 5 voor een omschrijving van wat bevindingen in deze PIA zijn). Dit hoofdstuk bevat het resultaat van deze toetsing, vormgegeven in conclusies.

6.1 Conclusies met betrekking tot de onderzoeksvragen

De onderstaande conclusies hebben direct betrekking op de twee onderzoeksvragen, in het bijzonder maatregel acht (beperken van zoeksleutels) en maatregel negen (filtermechanisme in de vorm van een whitelist). Conclusies die niet direct te maken hebben met de onderzoeksvragen komen aan de orde in paragraaf 6.2.

6.1.1 Eenduidige aanpak

Een overkoepelende conclusie is dat er geen eenduidige aanpak op het gebied van het verbeteren van de privacy is die op alle Suwi-partijen past. De oorzaak hiervan ligt in de verschillende wijze waarop de organisaties van de Suwi-partijen zijn gestructureerd en de diversiteit van processen die gebruik maken van Suwinet-Inkijk. Er is dus geen *one size fits all* benadering mogelijk.

Ook in het Programmaplan BVGS kwam deze kwestie (deels) terug. In het programmaplan werd de verwachting geopperd dat de maatregelen verschillend zouden uitpakken vanwege een andere vorm van organisatie en aansturing bij enerzijds UWV en SVB en anderzijds de gemeenten.[28]

6.1.2 Dataminimalisatie

Zoals beschreven in paragraaf 5.1 houdt dataminimalisatie vooral verband met het filtermechanisme in de vorm van een whitelist. Strikt genomen gaat dataminimalisatie over het verwerken van minder gegevens, maar dat kan ook worden bereikt door minder personen opvraagbaar te maken, en daardoor minder gegevens van die personen, door te werken met een kleinere whitelist.

Met behulp van (een verregaande vorm van) whitelisting kan grote winst behaald worden op het gebied van dataminimalisatie. Suwi-partijen kunnen allereerst zelf bepalen wie op de whitelist terecht komt. Door alleen personen met wie een actuele dienstverleningsrelatie bestaat op de whitelist te zetten wordt voorkomen dat personen die niet relevant zijn voor het uitvoeren van wettelijke taken op de whitelist terecht komen. Daardoor zijn veel minder gegevens opvraagbaar voor medewerkers van de Suwi-partij. Dit dient te worden onderscheiden van het implementeren van de whitelist. De implementatie geschiedt op een bepaald niveau binnen de organisatie, bijvoorbeeld organisatie-, functie of medewerkersniveau. De ideale situatie vanuit privacyperspectief is een implementatie op medewerkersniveau. De wijze waarop uitvoering is of gaat worden gegeven aan het implementeren van de whitelist verschilt per Suwi-partij:

- Voor gemeenten betekent een whitelist op organisatieniveau een significante reductie van het risicobeeld, aangezien de hoeveelheid personen die kunnen worden geraadpleegd wordt beperkt tot het aantal personen waarmee de gemeente een dienstverleningsrelatie heeft of (recent) heeft gehad. Als voorbeeld de gemeente Best: 28.954 inwoners, waarvan bijna 1.100 personen met een dienstverleningsrelatie. Dit is 3,8% van het aantal inwoners van de gemeente of 0,006% van het inwonersaantal van Nederland. Een whitelist op medewerkersniveau is

[28] Programmaplan BVGS, p. 8.

moeilijk haalbaar, omdat vaak meerdere medewerkers betrokken zijn bij een dienstverleningsrelatie.
- Bij de SVB zal de whitelist op organisatieniveau worden geïmplementeerd. Een whitelist op medewerkersniveau is op dit moment moeilijk haalbaar, omdat vaak meerdere medewerkers betrokken zijn bij de gevalsbehandeling. De SVB verwacht dat de implementatie van de whitelist resulteert in een teruggang tot circa 400.000 personen voor de gehele organisatie (zie de bevindingen in paragraaf 5.3 voor een uitleg van dit getal). Net als bij gemeenten is dit ook een significante reductie van het risicobeeld.
- Tijdens het onderzoek heeft de focus bij UWV gelegen op een whitelist op organisatieniveau. Gelet op het uitgangspunt dat de impact op de huidige werkprocessen en ICT systemen zo laag mogelijk dient te worden gehouden, is uitgekomen op een omvang van 8 miljoen personen. Dit aantal is het totaal van alle klantenbases van alle organisatieonderdelen. Dat is een minder significante 'winst' ten opzichte van de huidige situatie. Aangezien de eerste resultaten van de uitvoeringstoets pas in december in beeld komen kan hier nu nog geen uitspraak over worden gedaan.

6.1.3 Doelbinding

In het verlengde van dataminimalisatie ligt de doelbinding. Indien er meer gegevens worden geraadpleegd of getoond dan noodzakelijk is dit in strijd met het doelbindingsvereiste. De whitelist en het aanpassen van de pagina's kunnen hier helpen door alleen personen opvraagbaar te maken die relevant zijn voor het uitvoeren van de wettelijke taak resp. niet meer gegevens te tonen dan noodzakelijk voor het doel. Dit tweede aspect – het aanpassen van pagina's zodat alleen gegevens worden getoond die nodig zijn voor het doel van de raadpleging – valt eigenlijk onder de overige conclusies in de volgende paragraaf, omdat dit niet direct te maken heeft met de onderzoeksvragen. De focus ligt echter op whitelisting, omdat deze functie borgt dat alleen gegevens van personen met wie een dienstverleningsrelatie bestaat kunnen worden geraadpleegd. Dit hangt direct samen met de tweede onderzoeksvraag.

Bij beide bovengenoemde vereisten wordt in de uitwerking gerefereerd aan een (dienstverlenings-)relatie. De whitelists dienen dan ook gebaseerd te zijn op het bestaan van een dergelijke relatie. Een persoon wiens gegevens worden geraadpleegd dient te behoren tot de caseload van een medewerker van een Suwipartij. De whitelist functionaliteit (zie voor een andere uitleg hierover paragraaf 6.1.2) waarborgt dat alleen personen kunnen worden geraadpleegd die relevant zijn voor het uitvoeren van de wettelijke taak van een medewerker. In zoverre kan dan ook worden geconcludeerd dat de techniek achter de whitelist voldoet aan het doelbindingsprincipe.

6.1.4 Verwerkingsduur

Verder kan winst behaald worden op het gebied van de verwerkingsduur. Wanneer een persoon niet meer tot de caseload van een Suwipartij of medewerker daarvan behoort verdwijnt deze van de whitelist. Deze beperking zit dus al in de dienstverleningsrelatie. Dat wil zeggen dat als de dienstverleningsrelatie voorbij is, dit impliciet betekent dat de whitelist moet worden aangepast. Hieraan kan worden voldaan door bijvoorbeeld een autorisatiemanager die zeer regelmatig de whitelist update en/of een automatisch mechanisme dat ervoor zorgt dat BSN's worden verwijderd wanneer ze niet meer tot de caseload behoren. De partijen geven op verschillende wijzen vorm aan de uitvoering:

- Doordat bij gemeenten een whitelist op organisatieniveau wordt geïmplementeerd zullen personen van de lijst worden gehaald op het moment dat zij niet meer een dienstverleningsrelatie hebben met de gemeente. In de regel zullen gemeenten de lijst wekelijks verversen.

- De actuele dienstverlening bij SVB is verbonden aan de begin- en einddatum van een bericht. Een bericht vormt de dienstverlening die door SVB wordt geboden aan een individuele klant. Bij het bereiken van de einddatum wordt het BSN verwijderd. Er is wel enige uitloop na het einde van de gevalsbehandeling in verband met bezwaartermijnen en eventuele vragen van de klant.
- Voor UWV draagt de whitelist op organisatieniveau onvoldoende bij aan een substantiële reductie van het aantal personen op de whitelist. Daarom is UWV voornemens de mogelijkheden te onderzoeken om whitelists op lager niveau in te richten. De resultaten van dit onderzoek zullen (ook) moeten uitwijzen of de frequentie waarop de whitelist wordt ververst toereikend is.

Voor gemeenten en SVB kan worden geconcludeerd dat de whitelist zodanig werkt dat personen die niet meer relevant zijn niet onnodig lang op de whitelist blijven staan. Of dit bij UWV ook het geval is moet nog blijken uit de resultaten van de onderzoeken die ze aan het uitvoeren zijn.

6.1.5 Balans tussen technische en organisatorische maatregelen

Zoals eerder besproken in het kader van Privacy by Design kunnen technische en organisatorische maatregelen elkaar in evenwicht houden. Technische maatregelen zijn in dit geval maatregelen aan de voorkant, zoals het filtermechanisme. Organisatorische maatregelen zijn maatregelen aan de achterkant, zoals het monitoren en loggen van het gebruik van Suwinet-Inkijk. Het evenwicht kan vorm worden gegeven door bijvoorbeeld lichte organisatorische maatregelen aan de achterkant te compenseren door zware technische maatregelen aan de voorkant. Als bijvoorbeeld een whitelist op een lager niveau wordt geïmplementeerd is daardoor minder intensieve controle achteraf nodig. Wel resulteert dit in een hoger gebruik van de escapefunctie en daardoor een hogere controlelast.

Anderzijds is meer intensieve controle, monitoring en bewustwording vereist in het geval de whitelist op een hoger niveau wordt geïmplementeerd. De maatregelen aan de achterkant vallen buiten de scope van de onderzoeksvragen, maar zijn wel randvoorwaardelijk voor een effectieve werking van de uitvoering van maatregelen acht en negen. Zie ook de opmerkingen die zijn gemaakt over de whitelist in paragraaf 5.2.2.

Uit dit onderzoek kunnen we concluderen dat de balans tussen maatregelen aan de voorkant en aan de achterkant kan worden verbeterd. Vaak is er sprake van een whitelist op een hoger niveau (organisatieniveau) gecombineerd met controles, logging en bewustwording aan de achterkant. Er zijn wel diverse initiatieven genomen en (deels) uitgevoerd om de controle achteraf te verbeteren.

6.2 Overige conclusies

De hieronder staande conclusies hebben niet direct betrekking op de twee onderzoeksvragen, maar zijn er wel sterk aan verwant. Dit is ook teruggekomen in het Programmaplan BVGS waarin de maatregelen één en twee als randvoorwaardelijk worden omschreven voor een effectieve uitvoering van de maatregelen acht en negen.

6.2.1 Aanpassen van pagina's

Uitgaande van de situatie waarin slechts personen via Suwinet-Inkijk worden geraadpleegd waar een behandelrelatie mee is, kan ook mogelijke winst behaald met het aanpassen van pagina's. De hoeveelheid gegevens die op een pagina getoond wordt kan hiermee beperkt worden, zodat geen gegevens worden verwerkt zonder dat dat noodzakelijk is voor het doel van de verwerking (de raadpleging van Suwinet-Inkijk). De Suwi-partijen hebben al deels uitvoering gegeven aan

- Voor gemeenten zijn zes additionele bronpagina's gemaakt ter vervanging van twee overzichtspagina's.

- SVB heeft op maat gemaakte schermen (zie het doelbindingsdocument). Rollen en werkzaamheden wijzingen nauwelijks of niet. Hierdoor krijgen SVB medewerkers toegang tot een zo klein mogelijk aantal gegevens. Ook wordt regelmatig bekeken of de set van gegevens aanpassing behoeft. Zo wordt momenteel in samenwerking met BKWI gewerkt aan het verkleinen van de set aan RDW-gegevens voor een specifieke doelgroep binnen de SVB.
- UWV heeft een analyse traject doorlopen waarbij een meer fijnmazigere gegevensset per rol per organisatieonderdeel is gedefinieerd. Er loopt nog een laatste WTA (Wet Technisch Adviseurs) toets om te bekijken welke gegevens nodig zijn per functierol en of de opzet past in het wettelijke kader. Inmiddels is een omvangrijk traject opgestart om op basis van deze gegevenssets de pagina's in Suwinet-Inkijk aan te passen.

Bovenstaande maatregelen dragen bij aan het reduceren van het risico dat er bovenmatige verwerking van gegevens plaatsvindt en zorgt voor een verlaging van het risicobeeld. Gezien het feit dat de inhoud van werkzaamheden en functies continu in beweging zijn, is het belangrijk dat de Suwi-partijen regelmatig de aanwezige pagina's evalueren om te kijken of de gegevens op de pagina's nog noodzakelijk zijn voor het uitvoeren van de wettelijke taak.

6.2.2 Beperken van de hoeveelheid zware rollen

Ten slotte is ook winst te behalen bij het beperken van de hoeveelheid accounts met zware rollen die als autorisaties gecreëerd (kunnen) worden. Deze conclusie valt buiten de scope van de PIA, omdat het niet direct betrekking heeft op de onderzoeksvragen. Wel valt het onder maatregel één, die randvoorwaardelijk is voor de maatregelen acht en negen.

Zware rollen zijn rollen met één of meerdere zoeksleutels anders dan BSN. De beschikbaarheid van deze rollen verhoogt het risico op onrechtmatig gebruik, omdat het eenvoudiger is om op naam te zoeken in plaats van het minder publieke BSN. Uit overzichten die door BKWI als technisch beheerder van Suwinet zijn aangeleverd is per gemeente af leiden hoeveel accounts en hoeveel accounts met zware rollen er bestaan.

In totaal zijn er 13.762 accounts en 2987 accounts met zware rollen. Dit komt neer op een gemiddelde van 21,70%. Bij bepaalde gemeenten blijkt dat er een afwijking is ten opzichte van het gemiddelde. Dat wil zeggen dat zij verhoudingsgewijs meer accounts met zware rollen hebben dan het gemiddelde. Wel is het zo dat de omvang van het risico beperkt is, aangezien het gaat om minder dan 3% van alle bevragingen.

Verder zijn deze aantallen in sommige gevallen verklaarbaar vanuit de werkprocessen en de gemeentegrootte. In kleinere gemeenten zijn medewerkers belast met meerdere taken waarvoor ook zware rollen nodig zijn. Het accountteam wijst gemeenten er in het kader van maatregel acht op dat de autorisatiematrix opnieuw tegen het licht gehouden moet worden en de vraag moet worden gesteld of deze nog actueel en adequaat is.

Daarnaast wordt veel sociaal recherchewerk uitgevoerd in een centrumgemeente constructie. Daar concentreren de zware rollen zich. De mate waarin ze zich daar concentreren hangt af van het aantal gemeenten ten opzichte van de centrumgemeente en de omvang van de centrumgemeente ten opzichte van de andere gemeenten. Soms zijn er in dit verband samenwerkingen tussen gemeenten waarbij taken verdeeld zijn. Eén gemeente is dan bijvoorbeeld aangewezen voor handhaving voor meerdere gemeenten en heeft daardoor meer zware rollen.

Concluderend kan worden gesteld dat er in sommige gevallen sprake is van het bestaan van veel zware rollen. Dit kan ook het gevolg zijn van het bestaan van inactieve accounts met zware rollen. In

veel gevallen zijn echter goede verklaringen te geven voor deze zware rollen (zie hierboven). De aandacht ligt dan vooral op die gemeenten waar deze verklaringen niet of minder goed opgaan.

7 Aanbevelingen

In hoofdstuk 5 zijn de privacybeginselen en principes uit de informatiebeveiliging besproken die worden gebruikt om de vergaarde informatie te toetsen. Deze toetsing, die beschreven is in hoofdstuk 6, vind plaats om te bekijken in hoeverre de reeds gedane uitvoering die is gegeven aan het beperken van de toegang tot personen en het beperken van de toegang via zoeksleutels in overeenstemming is met de eisen uit het privacyrecht en met normen uit de informatiebeveiliging. In dit hoofdstuk gaan wij ten slotte in op onze visie op het resultaat van de toetsing en geven we, indien nodig, nadere aanbevelingen om de privacy nog beter te beschermen. Hierbij wordt niet elke conclusie opnieuw behandeld. In plaats daarvan is ervoor gekozen om meer concrete handvatten te bieden aan de Suwi-partijen, waarbij het resultaat van de toetsing verspreid terugkomt over de diverse aanbevelingen.

7.1 Aanbevelingen met betrekking tot de onderzoeksvragen

Net zoals bij de bevindingen en conclusies, wordt ook hier een onderscheid gemaakt naar aanbevelingen die direct betrekking hebben op de onderzoeksvragen en aanbevelingen die weliswaar belangrijk zijn voor het realiseren van een effectieve uitvoering van het beperken van de toegang tot personen en het beperken van de toegang via zoeksleutels, maar niet direct onder de onderzoeksvragen vallen. Hierna volgen de aanbevelingen die onder de scope van de PIA vallen.

7.1.1 Keuze uit principes

De twee onderzoeksvragen richten zich op het beperken van de toegang tot personen (maatregel negen) en het beperken van de toegang via zoeksleutels (maatregel acht). De wijze waarop deze maatregelen zijn en worden uitgevoerd verschilt per Suwi-partij. Zo wordt vermoed dat een whitelist op organisatieniveau een effectievere maatregel is voor de ene Suwi-partij, terwijl een andere Suwi-partij het meer wil hebben van controle aan de achterkant om de privacy beter te waarborgen. Door deze diversiteit in de geschatte effectiviteit van de uitvoering van het beperken van de toegang tot personen en het beperken van de toegang via zoeksleutels ontstaan er dus op maat gemaakte oplossingen om de privacy rondom Suwinet-Inkijk te verbeteren.

De tabel hieronder bouwt hierop voort en bevat een overzicht van op maat gemaakte principes. Het is de bedoeling dat partijen ten minste één keuze maken voor een sterk principe (de groene blokjes), zoals een whitelist op een laag niveau. Belangrijk is dat de maatregelen aan de voorkant eerst moeten worden langsgegaan. Alleen als er goede redenen zijn om de toegang niet aan de voorkant te beperken, kan gekozen worden voor meer intensieve logging, controle en bewustwording aan de achterkant.

De daadwerkelijke invulling van de principes wordt overgelaten aan de Suwi-partij. In de kolom met voorbeelden wordt een mogelijke aanvliegroute gegeven voor de invulling van een principe. Door een reeks aan mogelijke oplossingen aan te bieden, in plaats van verplicht een bepaald principe voor te schotelen, wordt beter ingespeeld op de (technische) mogelijkheden van de Suwi-partijen.

De keuzes die gemaakt worden dienen uitgebreid te worden toegelicht, inclusief toelichting waarom de keuze voor een sterker principe, volgens de Suwi-partij, niet mogelijk is. Met name de rode blokjes vereisen extra toelichting waarom daarvoor gekozen is, omdat deze niet de voorkeur hebben. Let wel dat het niet zo is dat als een keuze gemaakt wordt, het principe dat in de kolom ernaast staat ook van toepassing is. Een Suwi-partij kan dus bijvoorbeeld aan de voorkant kiezen voor een whitelist op laag niveau en aan de achterkant voor meer intensieve controle. De principes zijn in rijen gezet om in het voorbeeld aan te geven op welke wijze de gekozen principes in de praktijk kunnen worden ingevuld.

Voorkant	Achterkant	Voorbeeld
Whitelist op laag niveau	Minder intensieve controle van logging en bewustwording	Zoals een whitelist op medewerkersniveau gecombineerd met maandelijkse controles van de rapportages. Dit kunnen generieke rapportages zijn, waarbij slechts bij opvallend gedrag specifieke rapportages in een online omgeving worden opgevraagd.
Whitelist op midden niveau	Middelmatige logging, controle en bewustwording	Zoals een whitelist op functieniveau gecombineerd met wekelijkse bijeenkomsten met de security officer om de rapportage door te nemen van de afgelopen week. Het proces van rapportage en goedkeuring van raadplegingen dient formeel te worden vastgelegd.
Whitelist op hoog niveau	Meer intensieve logging, controle en bewustwording	Zoals een whitelist op organisatieniveau gecombineerd met het dagelijks doornemen van specifieke rapportages. Signaleringsrapportages zouden een nog betere bijdrage kunnen leveren aan een effectievere controle. Ook dienen de sancties van onrechtmatige raadplegingen, zoals ontslag, duidelijk te worden gecommuniceerd naar alle medewerkers.

Zoals aangegeven in dit rapport verdient vanuit privacyperspectief de implementatie van een whitelisting functionaliteit op zo laag mogelijk niveau de voorkeur. Dat betekent dus dat waar mogelijk op medewerkersniveau of, afhankelijk van de organisatie, of functie- of rolniveau implementatie dient plaats te vinden. Voor de korte termijn is door Suwi-partijen vooral uitgegaan van de huidige functionaliteit en daarmee whitelisting op organisatieniveau. Dit zal in de praktijk nog onvoldoende resultaat opleveren, zeker met het oog op de verplichting om Privacy by Design toe te passen.

Met name in het geval van het UWV zou een lagere implementatie van whitelists nieuwere functionaliteiten en enige technische aanpassingen vergen, maar ook aanpassingen in werkprocessen. De impact hiervan wordt bij UWV door middel van een impactanalyse en uitvoeringstoets bepaald. Wanneer de impact duidelijk is dient bezien te worden of daarmee ook daadwerkelijk het beste resultaat wordt behaald voor de bescherming van de privacy van burgers. Indien immers processen worden aangepast dient zich ook de gelegenheid aan om een zo optimaal mogelijke situatie te realiseren.

Het aanvankelijke idee om het aantal BSN's terug te dringen van 17 miljoen naar 8 miljoen – bestaande uit alle personen in de polisadministratie – is een goede stap vooruit, maar niet het best haalbare resultaat met het oog op Privacy by Design. Omdat UWV nog mogelijkheden onderzoekt kan op dit moment nog geen definitieve uitspraak hierover worden gedaan.

7.1.2 Kritische processen onder de loep nemen

Zoals in de conclusie is teruggekomen wordt de whitelist bij elke partij op organisatieniveau geïmplementeerd of is de verwachting dat het op organisatieniveau gaat worden geïmplementeerd. Veelgehoorde argumenten om het niet op een lager niveau te implementeren, zoals functie- of medewerkersniveau, is dat het niet past binnen de integrale dienstverlening van de organisatie en/of dat het teveel tijd en geld kost.

Met betrekking tot de whitelist dienen partijen echter kritisch de eigen processen onder de loep te nemen, om mogelijkheden van een filtermechanisme maximaal te benutten. Niet alleen dient er te worden gekeken naar mogelijkheden om de whitelist te implementeren in de bestaande processen,

maar ook buiten de bestaande processen. Dat wil zeggen dat (delen van) de organisatiestructuur van een Suwi-partij mogelijk moet worden heringericht om de whitelist effectief op een lager niveau te implementeren.

7.1.3 Real-time werking van de whitelist

Interessant is om de mogelijkheden te bekijken in hoeverre de whitelist real-time kan werken. Hierdoor wordt de privacy van nieuwe klanten en van voormalige klanten optimaler beschermd. Bij nieuwe klanten zorgt een real-time whitelist er namelijk voor dat zij zo snel mogelijk worden toegevoegd aan de whitelist. Als een whitelist op medewerkers- of functieniveau is geïmplementeerd, betekent dit dat de nieuwe klant maar door een beperkte groep medewerkers kan worden geraadpleegd. Ook kan met een real-time werking van de whitelist voorkomen worden dat de escape functie (te veel) moet worden gebruikt. Een belangrijke kanttekening is de vraag in hoeverre een real-time whitelist van grotere omvang technisch haalbaar is voor BKWI en de Suwi-partijen.

Daarnaast is met name winst te behalen bij personen die niet meer in behandeling staan bij een bepaalde organisatie. Bij een real-time whistlist wordt een persoon na het einde van de behandelrelatie immers direct of (o.a.) na het eindigen van de bezwaartermijnen en/of eventuele vragen van de klant verwijderd. De privacy van de klant is in deze situatie optimaler beschermd. BKWI dient te onderzoeken in hoeverre het mogelijk is de whitelist (nog meer) real-time te laten functioneren en de resultaten hiervan te bespreken met de Suwi-partijen. Waar een real-time werking van de whitelist niet mogelijk is of een substantiële investering vergt om te realiseren, dient te worden besproken in hoeverre de escape-functie – een specifieke autorisatie voor een medewerker, die ook apart gelogd wordt, waardoor hij een BSN kan inzien dat niet op de whitelist staat – hier een goede oplossing biedt voor overbrugging.

7.1.4 Targets stellen voor 2017 en 2018

Informatiebeveiliging is een doorlopend proces dat niet eindigt bij het nemen van enkele effectieve maatregelen die de privacy beter beschermen. Het is dan ook de bedoeling dat ná dit onderzoek en het mogelijk doorvoeren van (enkele van) onze aanbevelingen, de Suwi-partijen bewust blijven van mogelijke privacy- en beveiligingsrisico's en daarop acteren.

Het gaat dan bijvoorbeeld om het verder verfijnen van de whitelist of te onderzoeken welke andere filtermogelijkheden bestaan naast de white- en blacklist. Ook meer (technische) maatregelen aan de achterkant dienen te worden overwogen om nog beter de uitgevoerde raadplegingen in Suwinet-Inkijk te controleren. Denk daarbij bijvoorbeeld aan (het eerder in een werkgroep besproken) notificatiesysteem, waarbij op het moment dat een potentieel onrechtmatige raadpleging is gedaan, er direct een notificatie per e-mail binnenkomt bij de leidinggevende van de afdeling of bij de security officer. De security officer zou naar de betreffende werkplek kunnen lopen om erachter te komen waarom deze raadpleging is uitgevoerd. Indien de raadpleging buiten kantoor plaatsvindt, zou de security officer een online bericht kunnen versturen met de vraag waarom deze raadpleging is gedaan of eventueel de lopende sessie van de raadpleging (op afstand) kunnen blokkeren. Andere technische mogelijkheden aan de voor- en achterkant dienen samen met de Suwi-partijen te worden besproken.

Met het oog op Privacy by Design en de aandacht die daaraan wordt besteed in de Algemene Verordening Gegevensbescherming is het belang om hier nu al naar te kijken groot. Wijzigingen worden vanaf nu stapsgewijs doorgevoerd en dienen dan ook toekomstbestendig te zijn. Dit vereist dat scherp gekeken wordt welke mogelijkheden bestaan om by design de privacy nog beter te waarborgen. De maatregelen die technisch genomen kunnen worden dienen in dat geval wel

beoordeeld te worden op proportionaliteit en effectiviteit. Zo ontstaat mogelijk bijvoorbeeld een afweging of whitelisting op een lager niveau niet leidt tot een disproportionele inspanning om de autorisaties bij te houden. Dat hangt echter ook van de technische implementatie af.

7.2 Overige aanbevelingen

Net zoals bij de bevindingen en conclusies, wordt ook hier een onderscheid gemaakt naar aanbevelingen die direct betrekking hebben op de onderzoeksvragen en aanbevelingen die weliswaar belangrijk zijn voor het realiseren van een effectieve uitvoering van het beperken van de toegang tot personen en het beperken van de toegang via zoeksleutels, maar niet direct onder de onderzoeksvragen vallen. Hierna volgen overige aanbevelingen die niet direct van toepassing zijn op de onderzoeksvragen.

7.2.1 Beperken van de hoeveelheid zware rollen

Zoals omschreven bij de overige conclusies in hoofdstuk 6 zijn er voor sommige gevallen goede verklaringen te geven waarom een bepaalde gemeente veel meer zware rollen heeft dan het gemiddelde. Rekening houdend met deze mogelijke verklaringen dient de noodzakelijkheid van het bestaan van zware rollen continu te worden gemonitord (zie ook de verplichting uit de BIG), o.a. ter voorkoming van inactieve accounts met zware rollen.