Beveiligingsplan SUWI-net 2018 BWRI

Auteur: Ronald Kedra
Coauteurs: Edward Beverloo

Datum/versie: 12 december 2017
Versie: 2.0

gemeente
Midden-Groningen

Historie document

Versie	Datum/periode	Opmerkingen
1.1	Dec 2013	Suwinet Informatiebeveiligingsplan, versie 1.1, door Directie HS vastgesteld
1.2 – 1.4	Okt – Dec 2014	Evaluatie en actualisatie Suwinet Informatiebeveiligingsplan (vanuit onder andere een hiertoe gehouden Suwinet IB overleg d.d. 26 november ter aanscherping van het Suwinet gebruik en plan), inclusief het treffen van de diverse (verbeter)maatregelen ter beveiliging van de privacygevoelige gegevens binnen het Suwinet: • Proces gebruik(er)srapportages • Protocol/proces in geval van het 'vermoeden van misbruik/ongeoorloofd gebruik • Evaluatie en actualisatie autorisatie-overzichten van de aanwezige rollen en bevoegdheden voor gebruik en inkijk in Suwinet
1.5	17 Dec 2014	Op basis van het BWKI en de IBD verkregen uitsluitsel welke niet-Suwinet partijen wel en welke niet voor Suwinet inkijk geautoriseerd mogen zijn, zijn de autorisatie-aspecten nog eens grondig en kritisch doorgenomen en daar waar van toepassing op betreffende aspecten aangepast. Definitieve versie, ter vaststelling richting Directie HS.
1.6	Sept/okt 2015	Op basis van het gehouden evaluatieoverleg Suwi IB Plan dd 17 sept 2015, vorige versie (1.5) geactualiseerd
1.7	29 okt 2015	Op basis van het gehouden vervolg evaluatieoverleg Suwi IB Plan d.d. 29 okt, is versie 1.6 op paar punten aangepast (met name benamingen en grammaticacontrole)
1.8	Nov - Dec 2016	Op basis van het gehouden evaluatieoverleg Suwi IB Plan d.d. 1 nov 2016, is vorige versie (1.7) geactualiseerd. De autorisatiematrix, de rollen en verantwoordelijkheden zijn gecontroleerd en geactualiseerd. De implementatie van de maatregelen Programma Borging Veilige Gegevenswisseling Suwinet is beschreven.
1.9	Mei 2017	Aanpassing autorisatiematrix naar aanleiding van de technische maatregelen Programma Borging Veilige Gegevenswisseling Suwinet per 1 juli 2017.
2.0	December 2017	Aanpassing van het Beveiligingsplan Suwinet n.a.v. de gemeentelijke herindeling.

Inhoudsopgave

1 Inleiding

Vanaf 1 januari 2018 vormen de gemeenten Hoogezand-Sappemeer, Menterwolde en Slochteren de nieuwe gemeente Midden-Groningen. De uitvoering van de taken op het gebied van werk en inkomen gebeurt in de gemeente Midden-Groningen door de cluster BWRI (Bedrijf voor Werk, Re-integratie en Inkomen).

De gemeente Midden-Groningen heeft als uitvoerder van diverse wetten en regelingen te maken met veel registraties. Om de efficiency en de effectiviteit te verbeteren worden de laatste jaren steeds meer van die registraties gekoppeld en is samenwerking binnen verschillende ketens noodzakelijk. Een van die ketens is de keten van Werk en Inkomen. Dit is gebaseerd op de Wet Structuur uitvoering werk en inkomen, kortweg Suwi. Ketenpartners zijn het Bureau Keteninformatisering Werk en Inkomen (BKWI), de stichting Inlichtingenbureau Gemeenten (IB), het Uitvoeringsinstituut Werknemersverzekeringen (UWV inclusief het UWV WERKbedrijf en gemeenten). Zij wisselen via een elektronische infrastructuur gegevens met elkaar uit. Dit is het Suwinet.

Met de faciliteit Suwinet-Inkijk worden gegevens op basis van burger servicenummers (BSN) toegankelijk gemaakt voor bevoegde medewerkers. Daarnaast kan de burger zelf sinds begin 2008 zijn/haar binnen de Suwi-keten vastgelegde gegevens inzien via het Digitaal Klant Dossier (DKD). Het gaat daarbij om privacygevoelige gegevens. Denk aan arbeidsverleden, loon, uitkeringen en opleiding van burgers die bekend zijn binnen de Suwi-keten. De genoemde organisaties hebben die gegevens nodig om het recht op een uitkering vast te kunnen stellen en de juiste dienstverlening te kunnen leveren.
Andere organisaties, waaronder de Rijksdienst voor het Wegverkeer (RDW), de Sociale Verzekeringsbank (SVB) de Belastingdienst en de Dienst Uitvoering Onderwijs (DUO) leveren ook hun gegevens aan het Suwinet.

Om de Suwi-keten effectief te laten functioneren moeten partijen er op kunnen vertrouwen dat “hun” gegevens door de partners in de Suwi-keten op een zorgvuldige en controleerbare wijze worden behandeld. De wetgever heeft bij de start van Suwinet in 2002 aangegeven dat gegevensbeveiliging noodzakelijk is. Voor alle ketenpartners is dit met beveiligingsvoorschriften uitgewerkt in artikel 6.4 en bijlage 1 van de Regeling Suwi. Dit betekent dat bevoegde gebruikers van Suwinet over nogal wat privacygevoelige informatie van cliënten kunnen beschikken.
In de Regeling Suwi is als een verplichting opgenomen dat de gemeente moet beschikken over een (actueel) informatiebeveiligingsplan. In de Wet Bescherming Persoonsgegevens (WBP) is uitgebreid geregeld hoe met persoonsgegevens moet worden omgegaan. Voor welke doeleinden ze mogen worden verzameld. Op welke wijze ze mogen worden verwerkt. En welke beveiligingsmaatregelen er moeten worden getroffen. Al met al redenen genoeg om dit Beveiligingsplan Suwinet voor BWRI vast te stellen.

Het Beveiligingsplan Suwinet is geen statisch document. Het is gebaseerd op diverse landelijke en sectorale uitgangspunten en documenten. De organisatie en omgeving van BWRI is voortdurend in ontwikkeling, onder andere door wijzigende of vernieuwende inzichten en wetgeving of aanpassingen in de informatiesystemen. Dit betekent dat dit plan periodiek moet worden beoordeeld op actualiteit en dus mogelijk regelmatig aanpassing behoeft.

2 Beveiligingsplan Suwinet in relatie tot de gemeentelijke infrastructuur en organisatie

2.1 Inleiding

De infrastructuur en internetapplicaties vallen technisch, qua gebruik en beveiligingsaspecten onder verantwoordelijkheid van het team Automatisering van de gemeente Midden-Groningen. Het gebruik van internet en het beveiligingsbeleid valt onder het team Informatievoorziening en Organisatie (I&O). Binnen de gemeente Midden-Groningen is één Adviseur informatiebeveiliging/ CISO functionaris aangesteld. De Suwi-wetgeving kent een aparte rol Security officer SUWI. Deze rol wordt vanuit het team I&O door een Adviseur informatiemanagement vervuld.
De Suwi-wetgeving vereist een afzonderlijk beveiligingsplan en stelt specifieke eisen aan (controle op) het gebruik door de functionele afdeling, in dit geval BWRI. Dit plan beperkt zich dan ook tot het beveiligingsbeleid specifiek in relatie tot Suwinet.

2.2 Beveiligd netwerk

Om de Suwinet-Inkijk applicatie te gebruiken maken de gemeente Midden-Groningen en BWRI gebruik van het beveiligde netwerk voor Nederlandse gemeenten, Gemnet genaamd. Bij BWRI is een zeer beperkte gebruikersgroep voor Suwinet-Inkijk. Hierdoor is dit niet toegankelijk voor onbevoegden van buitenaf. Gemnet zorgt ervoor dat er geen onbevoegden kunnen binnen komen in het netwerk Suwinet. Alleen medewerkers werkzaam voor BWRI hebben toegang tot Suwinet-Inkijk.

Verder heeft de gemeente Midden-Groningen maatregelen getroffen voor een zo hoog mogelijk beveiligingsniveau:

- de dataverbindingen met de buitenwereld voor Suwinet lopen via Gemnet;
- alle internetverkeer wordt beveiligd door een dienst van Gemnet en de gemeente Midden-Groningen;
- alle centrale systemen/servers zijn voorzien van actuele toegangsprogrammatuur en programmatuur ter beveiliging tegen virussen.

2.3 Back-up

Door het team Automatisering worden er dagelijks back-ups van de systemen gemaakt. Voor de systemen waarvan het beheer extern is belegd wordt de back-up door die partij uitgevoerd. Alleen de tapewissel gebeurt door de systeembeheerders van de gemeente in de tape-unit. Van de controle en tapewissel wordt een logboek bij gehouden. De beschreven tapes worden dezelfde dag naar een sub-locatie vervoerd en daar in een brandwerende kluis opgeslagen.
Jaarlijks vindt er een uitwijktest plaats om te controleren, dat alle data, die op de back-up staan ook teruggezet kunnen worden op andere systemen.
Tussentijds vindt het terugzetten van data vanaf de back-up plaats bij ongewenste overschrijvingen van de data of per ongeluk gewiste data.

2.4 Werkplekken en thuiswerken

Er zijn richtlijnen opgesteld voor het gebruiken van de werkplekken en thuiswerken. Deze zijn in ‘Beleid logische toegangsbeveiliging ’, ‘Clear desk en clearscreen beleid’, ‘Telewerkbeleid’ en ‘Wachtwoordbeleid’ beschreven en zijn van toepassing op de BWRI medewerkers. De regels met betrekking van de beveiliging van persoonsgegevens in relatie tot de verkregen Suwi-gegevens zijn in hoofdstuk 6 beschreven.

Hierin staat onder andere dat de thincliënts op de werkplekken zijn beveiligd door middel van wachtwoorden. De werknemer moet zijn wachtwoord invoeren alvorens de thincliënt gebruikt kan worden. De Suwinet-Inkijk applicatie heeft een eigen wachtwoord. Bij het actief gebruik van Suwinet is het niet toegestaan om de werkplek te verlaten. Bij het verlaten van de werkplek moet de applicatie worden afgemeld en afgesloten.

Om thuis te kunnen werken is er vooraf toestemming van de teamleider vereist. Via de eigen internetverbinding thuis en een token of een app kan een medewerker thuis veilig op het netwerk van de gemeente inloggen. Printen op de eigen thuisprinter is standaard niet toegestaan.

2.5 Voorschriften gebruik Suwinet-Inkijk

Het spreekt voor zich dat de medewerkers op verantwoorde wijze omgaan met de persoonsgegevens die zij raadplegen via Suwinet-Inkijk. Het is alleen toegestaan om gegevens van cliënten van de teams BWRI Inkomen en Voorzieningen en BWRI Re-integratie te raadplegen bij controle van de rechtmatigheid en doelmatigheid inzake de wettelijke voorschriften. Gegevens die vanuit Suwinet worden afgedrukt komen beschikbaar op de printer van BWRI. Deze printer is via een druppelsleutel beveiligd, zodat alleen de medewerker zelf de uitdraai kan ophalen. De uitdraaien uit Suwinet worden in het persoonsdossier van de cliënten bewaard. De persoonsdossiers worden bewaard in een archiefkast welke 's avonds wordt afgesloten. Het archief valt onder het team staf BWRI.

Bij het verlaten van de werkplek dient men zich af te melden van de applicatie. Voor uitkeringsgerechtigden die hun gegevens in Suwinet via het recht op inzage wensen in te zien en eventueel te corrigeren is een protocol opgesteld (bijlage 1).

Personeel dat in dienst is bij BWRI valt onder het ambtenarenreglement. Dit betekent dat zij bij benoeming niet apart een verklaring behoeven te ondertekenen dat zij op verantwoorde wijze omgaan met privacygevoelige informatie. In het ambtenarenreglement is dit opgenomen. De desbetreffende medewerker wordt voordat toegang tot de diverse applicaties wordt verleend gewezen op de gebruiksafspraken en de regels omtrent de vertrouwelijkheid. Omdat de gemeente de geheimhouding van vertrouwelijke gegevens en het gebruik van Suwinet-Inkijk heel belangrijk vindt, moet elke medewerker een verklaring ondertekenen voor het gebruik van Suwinet (zie bijlage 2).

Voor extern of ingehuurd personeel dat dient te beschikken over de Suwinet-Inkijk applicatie is in de meeste gevallen via de inleenovereenkomst van de uitzendbureaus of de daaraan gekoppelde algemene voorwaarden de geheimhouding van vertrouwelijke gegevens door het bureau en de medewerker gewaarborgd De desbetreffende medewerker wordt voordat toegang tot de diverse applicaties wordt verleend gewezen op de gebruiksafspraken en de regels omtrent de vertrouwelijkheid. Omdat de gemeente de geheimhouding van vertrouwelijke gegevens en het gebruik van Suwinet-Inkijk heel belangrijk vindt, moet elke in- en externe medewerker een verklaring ondertekenen voor het gebruik van Suwinet (zie bijlage 2).
Voor het gebruik van de applicatie Suwinet-Inkijk zijn de medewerkers van BWRI, geautoriseerd door middel van het toekennen van een of meerdere gebruikersrollen. Binnen Suwinet-Inkijk kunnen afhankelijk van de rol brongegevens worden geraadpleegd. In hoofdstuk 4 volgt een opsomming van de gebruikersrollen binnen Suwinet-Inkijk en de daarvoor geautoriseerde functies.

3 Rollen en taken binnen Suwinet-Inkijk

3.1 Specifieke rollen binnen Suwinet-Inkijk

Binnen Suwinet-Inkijk zijn de volgende specifieke rollen gedefinieerd:

- Applicatiebeheerder SUWI-net;
- Gemandateerde SUWI-net;
- Security Officer SUWI-net.

Deze rollen worden door de volgende functies binnen BWRI / gemeente Midden-Groningen uitgevoerd:

Rol SUWI-net	Functie BWRI / gemeente Midden-Groningen
Applicatiebeheerder SUWI-net	Coördinator uitkeringsadministratie / medewerker uitkeringsadministratie A (BWRI inkomen en voorzieningen)
Gemandateerde SUWI-net	Kwaliteitsmedewerker toetsing / interne controle (BWRI stafbureau)
Security Officer SUWI-net	Adviseur informatiemanagement (team I&O)

Tabel 1: SUWI-net rollen in relatie tot de BWRI / Midden-Groningen functies

3.2 Taken in relatie tot Suwinet-Inkijk

Applicatiebeheerder SUWI-net
De applicatiebeheerder heeft de volgende taken in relatie tot Suwinet-Inkijk:
- Periodieke controle logging-gegevens, met als doel: controleren of het gebruik van de gegevens binnen Suwinet-Inkijk plaatsvindt binnen de wettelijke kaders en overeenkomstig de doelen die de organisatie hiertoe heeft geformuleerd;
- Gebruikers Suwinet-Inkijk in opdracht van de teamleider Inkomen en Voorzieningen autoriseren voor toegang tot de applicatie;
- De autorisaties van medewerkers die uit dienst gaan of een andere functie gaan vervullen in opdracht van de teamleider BWRI Inkomen en Voorzieningen verwijderen respectievelijk aanpassen;
- Het operationeel houden van de applicatie en de gebruikers Suwinet-inkijk autoriseren voor de toegang.

Gemandateerde SUWI-net
De gemandateerde SUWI-net rapporteert jaarlijks over het beveiligingsplan en de bevindingen op dit gebied en heeft de volgende taken:
- Periodieke controle logginggegevens. Doel: controleren of het gebruik van de gegevens binnen Suwinet-inkijk plaatsvindt binnen de wettelijke kaders en in overeenstemming met de doelen die de organisatie hiertoe heeft geformuleerd.
- Elk kwartaal opstellen en beoordelen van een gebruikersrapportage
- Stuurt de bevindingen vanuit de gebruikersrapportage naar het Managementteam (met cc richting de IB-coördinator)
- Vraagt minimaal twee keer per jaar specifieke rapportages aan (of indien nodig, dan vaker).

Security Officer SUWI-net
Security Officer SUWI-net heeft de volgende taken:
- Bevordert en adviseert over de beveiliging van Suwinet, verzorgt zonodig rapportages over de status, controleert dat, met betrekking tot de beveiliging van Suwinet, de maatregelen worden nageleefd, evalueert de uitkomsten en doet voorstellen tot implementatie c.q. aanpassing van plannen op het gebied van de beveiliging van Suwinet.
- Jaarlijkse controle op actualiteit. Het beveiligingsplan controleren op actualiteit en volledigheid.

Teamleider BWRI Inkomen en Voorzieningen
De teamleider BWRI Inkomen en Voorzieningen is eindverantwoordelijk voor het gebruik en de beveiliging van Suwinet-Inkijk binnen BWRI en legt daar verantwoording over af. Betreffende functionaris is verantwoordelijk voor het actueel en volledig zijn en blijven van dit Beveiligingsplan Suwinet.
De teamleider BWRI Inkomen en Voorzieningen geeft aan de applicatiebeheerder aan wie toegang krijgt tot Suwinet-inkijk. De applicatiebeheerder geeft hierna het gebruik voor de medewerker vrij.

Directeur van BKWI
De directeur van BKWI is eindverantwoordelijk voor het gebruik en de beveiliging van Suwinet Inkijk.

Bovengenoemde taken behoren tot de genoemde functies en gaan over op de vervanger van de functionaris bij afwezigheid.

4 Autorisaties en gebruik Suwinet-Inkijk

4.1 Geautoriseerde functies voor Suwinet-Inkijk

Binnen BWRI zijn medewerkers al dan niet geautoriseerd om gebruik te maken van Suwinet-Inkijk. Het gaat hierbij om de volgende functies (in alfabetische volgorde):

Toegang tot SUWI-net

- Casemanager inkomen aanvraag, incl. coördinator inkomen;
- Casemanager inkomen beheer, incl. coördinator inkomen;
- Casemanager inkomen minima;
- Casemanager terugvordering en verhaal;
- Kwaliteitsmedewerker bezwaar en beroep;
- Kwaliteitsmedewerker toetsing / interne controle;
- Medewerker huisvesting en integratie vluchtelingen;
- Medewerker uitkeringsadministratie A/B/C, incl. Coördinator;
- Preventiemedewerker;
- Sociaal rechercheur incl. Coördinator preventie en handhaving;
- Team Incasso / casemanager BBZ aanvraag;
- Werkcoach, incl. coördinator werkcoach.

Geen toegang tot SUWI-net

- Administratief medewerker (BWRI stafbureau);
- Armoederegisseur;
- Beleidsmedewerker participatiebeleid A / B;
- Directie ondersteuner / Managementassistente;
- Financieel adviseur BWRI;
- Management BWRI;
- Medewerker administratieve en secretariële ondersteuning (BWRI stafbureau);
- Medewerker archief;
- Medewerker financiële administratie BWRI I / II;
- Medewerkers van het werkbedrijf;
- Projectmedewerker CAZ;
- Scholingsadviseur;
- Telefonist/receptionist;
- Trainer coach werk;
- Uitvoerend beleidsmedewerker participatiebeleid.

4.2 Autorisaties Suwinet-Inkijk voor ESF en leerplicht / onderwijs

In principe mag Suwinet-Inkijk niet gebruikt worden voor het beoordelen van het Europees Sociaal Fonds (ESF) aanvragen. Gemeenten kunnen vanaf januari 2017 via het Inlichtingenbureau met behulp van het product ESF Subsidietoets bepalen of burgers in aanmerking komen voor medefinanciering vanuit het ESF. Op dit moment wordt de ESF Subsidietoets alleen door de centrumgemeenten uitgevoerd. In geval van BWRI is Groningen de centrumgemeente. Gemeente Groningen maakt op dit moment geen gebruik van de ESF subsidietoets.

Projectmedewerkers ESF (BWRI) krijgen toegang tot Suwinet-Inkijk alleen op incidentele basis. Dit gebeurt in afstemming met BKWI en indien de centrumgemeente Groningen nog geen ESF subsidietoets uitvoert.

Voor de uitvoering van de RMC-functie gebruiken leerplichtambtenaren en casemanagers onderwijs de Suwinet-Inkijk van de RMC-regio Groningen.

4.3 Overzicht geautoriseerde rollen en functies Suwinet-Inkijk

In de onderstaande tabel volgen per rol de functies die rechten hebben met betrekking tot het gebruik van Suwinet-Inkijk.

Nr.	Functies en autorisaties Suwinet-Inkijk	BWRI-functies / rollen SUWI-net															
		Casemanager inkomen aanvraag, incl. coördinator inkomen	Casemanager inkomen beheer, incl. coördinator inkomen	Casemanager inkomen minima	Medewerker huisvesting en integratie vluchtelingen	Casemanager terugvordering, verhaal en debiteuren	Medewerker Incasso, teruvordering en verhaal	Medewerker uitkeringsadministratie A/B/C, incl. Coördinator	Werkcoach, incl. coördinator werkcoach	Preventiemedewerker	Sociaal rechercheur incl. Coördinator preventie en handhaving	Kwaliteitsmedewerker bezwaar en beroep	Kwaliteitsmedewerker toetsing / interne controle	Applicatiebeheerder SUWI	Gemandateerde SUWI-net	Security Officer SUWI-net	Projectmedewerker ESF
R4792	Terugvordering						x										
R3130	Beheer: WW & blokkeren																
GSDADM	Gebruikersbeheerder													x			
R4796	Onderhouden correctieservice													x			
R3846	Onderhouden werkvoorraad (Whitelist)													x			
R347	Opvragen generieke gebruiksrapportage															x	
RAPPORT_SPECIFIEK_GSD	Opvragen specifieke gebruiksrapportages														x		
WE_GSD	Whitelist escape	x		x		x			x	x	x						
R1043	Belastingdienst	x	x	x		x		x	x	x	x	x	x				x
G019	Bijstandsregelingen	x	x	x		x		x	x	x	x	x	x				x
R3724	DUO gegevens	x	x	x		x			x			x	x				x
R1272	Fraude vorderingen										x						
G003	G003 UWVWb	x	x	x		x		x	x	x	x	x	x				x
G004	G004 Fraude scorekaart	x	x	x		x		x	x	x	x	x	x				x
G024	G024 Bedrijvenregister	x	x	x		x		x	x	x	x	x	x				x
G031	G031Correctieservice													x			
G042	G042 Klant algemeen							x									
R4794	GBA Volledig	x	x	x		x		x	x	x	x	x	x				x
R3726	UWV Inkomstenverhoudingen								x								x
R2786	Kostendelerstoets	x	x	x		x		x	x	x	x	x	x				x
R4549	Landelijk Doelgroepregister																
R4797	Onderhouden status wijzigingsverzoeken																
G020	RDW	x	x	x									x				
R1919	RDW+					x				x	x						
R454	RDW peildata	x	x										x				
R3728	Rechtmatigheid +	x	x	x		x		x		x	x	x	x				x
R3725	Re-integratie								x								x
R3722	SVB gegevens																
R4816	Zoek+ in GBA					x				x	x						
R3723	UWV uitkeringen																
R1920	Zoek in RDW+					x				x	x						
R2355	Zoek in RDW																
R4793	EROW	x															
SC102	Raadplegen ISI op BSN																
SC103	Raadplegen ISI op BSN of selectie																
SC105	Muteren ISI																
SC106	Alle bevoegdheden incl signalen																
R3841	SCI07 Raadplegen PV gegeven				x												
R4692	SCI08 Muteren PV gegevens				x												
R4832	Kadaster										x						

Tabel 2: autorisatiematrix Suwinet-Inkijk BWRI

4.4 Gebruik Suwinet-Inkijk

Er zijn meerdere functies binnen BWRI waarbij Suwinet-Inkijk gebruikt wordt voor het raadplegen van cliëntgegevens en/of informatie. In onderstaande tabel volgt per functie in welke gevallen Suwinet-Inkijk gebruikt mag/kan worden. We spreken in die gevallen van geoorloofd gebruik.

Functie	Gebruik Suwinet-Inkijk voor
Adviseur informatiemanagement	Uitvoeren rol security officer SUWI-net
Applicatiebeheerder	Configureren correctieservice Beheren autorisaties Afhandelen maandelijkse IB signalen Onderhouden en aanleveren Whitelist gegevens
Casemanager inkomen aanvraag, incl. coördinator inkomen	Aanvragen levensonderhoud Aanvragen bijzondere bijstand jongeren Fraudesignalen Bijzondere onderzoeken Escape-functie
Casemanager inkomen beheer, incl. coördinator inkomen	Verkorte aanvragen Levensonderhoud Aanvragen bijzondere bijstand van de klanten met een lopende levensonderhoud uitkering Fraudesignalen Bijzondere onderzoeken
Casemanager inkomen minima	Aanvragen bijzondere bijstand en minimabeleid Fraudesignalen Bijzondere onderzoeken Escape-functie
Casemanager terugvordering, verhaal en debiteuren	Aanvragen BBZ Fraudesignalen Bijzondere onderzoeken Terugvordering en verhaalszaken Escape-functie
Medewerker huisvesting en integratie vluchtelingen	Raadplegen en muteren van de gegevens participatieverklaring binnen DUO Portal Inburgering
Medewerker Incasso, terugvordering en verhaal	Terugvordering en verhaalszaken
Medewerker uitkeringsadministratie A/B/C, incl. coördinator	Uitvoeren taken uitkeringsadministratie Uitvoeren rol applicatiebeheerder SUWI-net
Kwaliteitsmedewerker bezwaar en beroep	Uitvoeren bezwaar- en beroepszaken
Kwaliteitsmedewerker toetsing en interne controle	Bij uitvoeren kwaliteitszorgtaken Uitvoeren rol gemandateerde SUWI-net
Preventiemedewerker	Aanvragen levensonderhoud Fraudesignalen Bijzondere onderzoeken Escape-functie
Projectmedewerker ESF	Controles i.h.k.v. de ESF-subsidietoets
Sociaal rechercheur incl. coördinator preventie en handhaving	Aanvragen levensonderhoud Fraudesignalen Bijzondere onderzoeken Escape-functie
Werkcoach, incl. coördinator werkcoach	Re-integratietrajecten incl. NUG-gers en Doelgroepenregister

Tabel 3: gebruik Suwinet-Inkijk in relatie tot de rollen BWRI en processen

Wordt Suwinet om andere redenen gebruikt dan zoals hierboven is verwoord, dan is er in principe sprake van ongeoorloofd gebruik.

5 SUWI-net rapportages

5.1 Logging van het gebruik Suwinet-Inkijk

Het BKWI heeft rapportages ontwikkeld omtrent de logging van het gebruik van Suwinet-Inkijk. Het BKWI is verplicht om gegevens te loggen waarmee het gebruik van Suwinet-Inkijk per medewerker van onder andere de gemeente kan worden nagegaan. In het kader van de beveiliging zullen de gegevens over het gebruik van Suwinet-Inkijk één keer per kwartaal uitgevraagd worden. Het betreft dan de volgende gegevens (gebruikersrapportage):

Controle op	Beoordeling afwijkingen	Gevolg
aantal raadplegingen per maand in Suwi	Plausibele reden gebruiker /Geen Plausibele reden gebruiker	Indien er door de desbetreffende geautoriseerde medewerker geen plausibele reden gegeven wordt volgt een gesprek met de desbetreffende leidinggevende van de Suwinet-gebruiker
percentage raadplegingen op zoeksleutel anders dan burgerservicenummers	“idem”	“idem”
percentage raadplegingen buiten kantoortijd (19.00 – 6.00)	“idem”	“idem”
meest geraadpleegde burgerservicenummers	“idem”	“idem”
hoogst aantal gebruikers dat hetzelfde burgerservicenummer heeft geraadpleegd	“idem”	“idem”
hoogst aantal raadplegingen per gebruiker	“idem”	“idem”
percentage geblokkeerde accounts	“idem”	“idem”
ongebruikte accounts	“idem”	“idem”
Aangemaakte, verwijderde accountants en wijzigingsacties		
verdeling van de rollen	“idem”	“idem”
verdeling van de raadplegingen over pagina’s	“idem”	“idem”
gebruik escapefunctie: hoe vaak de escapefunctie is gebruikt, hoeveel pagina’s daarvoor zijn geraadpleegd en met welke reden	“idem”	“idem”
Verzonden suwimail	“idem”	“idem”
Ontvangen suwimail	“idem”	“idem”

Tabel 4: gegevens gebruikersrapportage

5.2 Analyse en controle gebruikersrapportage

De logginggegevens worden door de gemandateerde SUWI-net uitgedraaid. De gemandateerde SUWI-net controleert per kwartaal op afwijkingen in gebruik van Suwinet. Indien er afwijkingen gesignaleerd worden, beoordeelt de gemandateerde SUWI-net deze afwijkingen. Als er een plausibele reden voor de afwijking is, dan worden er geen nadere acties ondernomen. Wanneer er geen aannemelijke reden is voor de afwijking wordt er een specifieke rapportage opgevraagd bij het BKWI. In de specifieke rapportage worden de volgende gegevens weergeven:

- Inkijkacties;
- Opvraging unieke BSN;
- Geldige ten opzichte van ongeldige rollen;
- Inlogpogingen;
- Administrator accounts;
- Accounts per status;
- Opvraging per pagina;
- Vergelijking rechtmatigheid raadplegingen (BKWI-tool);
- Geregistreerde ten opzichte van actieve accounts.

De volgende gegevens worden gelogd:

- Het tijdstip van iedere log-in en log-out;
- De gebruikersnaam van degene die inlogt/uitlogt;
- Elk BSN (of andere zoeksleutel) waarvan gegevens worden opgevraagd wordt als raadpleging geregistreerd;
- Elke raadpleging, zoals de bekeken kolom- of overzichtspagina´s.

Het doel van deze logging is tweeledig:

- Tegengaan en controleren van onrechtmatige, onregelmatige of doeloverschrijdende verwerking;
- Wetenschappelijke en/of statistische doeleinden.

Wanneer er bijzonderheden worden geconstateerd, wordt de leidinggevende van de medewerker ingelicht en volgt er een gesprek. Mocht blijken dat de medewerker (herhaaldelijk) in overtreding is en er dus een vermoeden van misbruik is volgt een officiële waarschuwing en wordt de directie op de hoogte gesteld. De tweede officiële waarschuwing kan uiteindelijk leiden tot ontslag uitgaande hetgeen ten aanzien van de geheimhouding in de wet is bepaald (art. 272 WvSr) en het feit dat schending van de geheimhoudingsplicht een zogenaamde dringende reden kan betekenen die ontslag (op staande voet) rechtvaardigt (art. 7:678 BW).

De gemandateerde SUWI-net rapporteert de bevindingen vanuit de gebruikersrapportage naar het Managementteam (met cc richting de Security Officer SUWI-net).

De gebruikers van Suwinet-Inkijk moeten weten dat over hen gegevens worden verzameld en vastgelegd. Dit is een belangrijk onderdeel van de privacybescherming ten opzichte van deze medewerkers. Met het oog hierop moet de navolgende informatie worden verstrekt aan de medewerkers die (gaan) werken met Suwinet-Inkijk:

- Het bestaan van de logging-applicatie;
- De (aard van de) gegevens die binnen deze applicatie worden gelogd;
- Doelen van de logging;
- Dat de gelogde gegevens niet voor andere doeleinden worden gebruikt dan waarvoor ze zijn
- vastgelegd;
- De wijze en het moment waarop en door wie een onrechtmatig of doeloverschrijdend gebruik van het Suwinet-Inkijk wordt geconstateerd;
- Dat bij bovenstaande constatering dit door de teamleider Inkomen en Voorzieningen wordt gecommuniceerd met de betreffende medewerker(s).

6 Regels bij beveiliging van persoonsgegevens in relatie tot verkregen Suwi-gegevens

Voor het werken met en de omgang met persoonsgegevens zijn vanuit de overheid een aantal regels opgesteld, die zijn verwoord in verschillende wet- en regelgeving. Deze regels zijn in 'Beleid logische toegangsbeveiliging ', 'Clear desk en clearscreen beleid', 'Telewerkbeleid' en 'Wachtwoordbeleid' van de gemeente Midden-Groningen verwerkt en zijn van toepassing op de BWRI medewerkers. Concreet kunnen deze regels als volgt worden vertaald:

6.1 Beheren van wachtwoorden

Wachtwoorden vormen een belangrijk aspect van de gemeentelijke informatiebeveiliging. De gebruiker moet het door de administrator uitgegeven wachtwoord wijzigen zodra de eerste inlog plaatsvindt. Vervolgens vervalt het wachtwoord voor het netwerk na 1 jaar. Zodra een medewerker de gemeente verlaat, wordt het account verwijderd. Wanneer het account voor het netwerk 1 jaar niet wordt gebruikt, vervalt het account automatisch.
Het wachtwoord voor SUWI-net vervalt na 90 dagen. De gebruiker heeft dus het eigen beheer over het wachtwoord. In geval van het verlopen wachtwoord dient het nieuwe wachtwoord voor SUWI-net bij de applicatiebeheerder SUWI-net aangevraagd te worden.

6.2 Melden van beveiligingsincidenten

Het is belangrijk dat beveiligingsincidenten (en daarmee mogelijke datalekken) worden gemeld bij de applicatiebeheerder en de coördinator Informatiebeveiliging. Hiertoe is er een formulier 'Melding Informatiebeveiligingsincident' binnen Topdesk aanwezig.

Meldt het probleem direct of in ieder geval zo snel mogelijk via het aangegeven formulier.
Nadere informatie over het melden van beveiligingsincidenten (en de wet meldplicht datalekken), is op het Intranet beschikbaar.

6.3 Geheimhoudingsplicht

Binnen BWRI wordt met persoonsgegevens gewerkt. Voor het werken met en de omgang met persoonsgegevens zijn vanuit de overheid een aantal regels opgesteld, die zijn verwoord in de Wet bescherming persoonsgegevens (WBP). In de wet Suwi en in de ondertekende verklaring geheimhouding Suwinet (zie bijlage 2) zijn geheimhoudingsbepalingen opgenomen, waarin wordt aangegeven dat de persoonsgegevens niet verder bekend mogen worden gemaakt dan voor de uitoefening van de functie noodzakelijk is.

6.4 Gedragscode internet- en e-mailgebruik

De gemeente hanteert een protocol voor gebruik van e-mail en internet. In dit protocol is aangegeven hoe de medewerkers behoren om te gaan met e-mail en internet op de werkplek. Tevens bevat dit protocol regels voor de manier waarop het gebruik van externe e-mail en internet wordt geobserveerd. Het protocol is voor alle medewerkers van de gemeente te raadplegen op het gemeentelijke Intranet.

6.5 Kennisnemen van het informatiebeveiligingsbeleid

Binnen BWRI geldende SUWI-informatiebeveiligingsbeleid (inclusief instructies en protocollen), is op elke werknemer van toepassing die gebruik maakt van Suwinet-Inkijk. Alle gebruikers en nieuwe medewerkers worden hierop geattendeerd en worden verwezen naar het op het Intranet gepubliceerde Suwinet IB-plan.
Gebruikers van Suwinet-Inkijk moeten weten dat over hen gegevens worden vastgelegd en verzameld. Dit is een belangrijk onderdeel van de privacybescherming ten opzichte van deze medewerkers. In het beveiligingsplan is hier uitgebreid aandacht aan besteed. Minimaal twee keer per jaar zullen de gebruikers (opnieuw) middels diverse acties op het bestaan van het Suwinet IB-plan geattendeerd worden.

Deze acties gaan via de volgende kanalen plaatsvinden:

- Aandacht via het jaarlijkse functioneringsgesprek (Informatiebeveiliging is al een vast onderwerp van het bijbehorende formulier).
- Werkoverleggen (inclusief vastleggen dat het als onderwerp op de agenda staat en vervolgens ook daadwerkelijk besproken is).
- Bijwonen van de diverse Suwinet (IB-)gerelateerde bijeenkomsten.
- Het Suwinet IB-plan is centraal beschikbaar gesteld op het Intranet (inclusief een bijbehorend nieuwsbericht).

6.6 Gegevensverstrekking aan derden via de telefoon

Het uitgangspunt is dat er terughoudend wordt omgegaan aan verzoeken om telefonische informatie te verstrekken. Het voeren van telefoongesprekken brengt namelijk het risico met zich mee dat de identiteit van de gesprekspartner verkeerd wordt vastgesteld of dat persoonsgegevens worden verstrekt aan personen die geen recht op informatie hebben. In principe wordt er dan ook geen telefonische informatie over klanten verstrekt aan personen of instanties die beweren namens betrokkene te bellen. In die gevallen kan er een schriftelijk verzoek worden ingediend, voorzien van een machtiging. Bij een verzoek om telefonische informatieverstrekking van een ketenpartner wordt de verzoeker teruggebeld via het algemene nummer van de (vestiging van de) ketenpartner met het verzoek te worden doorverbonden. Dit terugbellen kan achterwege blijven wanneer het verzoek afkomstig is van een vaste contactpersoon.

6.7 Clear desk en clear screen policy

De vertrouwelijke omgang met persoonsgegevens houdt onder andere in dat elke werkplek zodanig is ingericht, dat onbevoegden niet de beschikking kunnen krijgen over deze informatie. Vertrouwelijke gegevens mogen niet onbeheerd op het bureau achterblijven. Dossiers worden bewaard in een kast die na werktijd wordt gesloten. Bezoekers dienen zich bij binnenkomst eerst te melden bij de receptie. De kans is derhalve gering dat onbevoegden zonder te worden opgemerkt toegang krijgen tot de werkplek van de medewerkers. Clear screen betekent dat het werkstation moet worden vergrendeld met behulp van schermbeveiliging (met wachtwoord). De screensaver is zodanig ingesteld dat na 15 minuten de schermbeveiliging intreedt.
Voor het thuiswerken geldt dat thuis de papieren werk-informatie goed wordt opgeborgen, c.q. niet zomaar rondslingert; papieren klant-informatie bevindt zich alleen thuis bij een medewerker op de dag dat hij/zij thuis werkt.

6.8 Geen vertrouwelijke gegevens in de prullenbak

De correcte omgang met vertrouwelijke gegevens – waaronder persoonsgegevens – is erg belangrijk binnen BWRI. Ook het vernietigen van deze gegevens moet op een veilige manier plaats vinden. Vertrouwelijke gegevens mogen niet terecht komen in een prullenbak of een bak die voor oud papier bestemd is. Daarom worden deze gegevens afzonderlijk ingezameld en vernietigd.

6.9 Aanspreken van onbekende personen

In het geval dat een medewerker van BWRI een voor hem/haar onbekende persoon in de gang van de afdeling tegenkomt waar officieel geen publiek zonder begeleiding mag komen, dient de medewerker deze persoon aan te spreken, zichzelf voor te stellen en de persoon in kwestie te vragen wat hij/zij hier doet. Personen die niet bevoegd zijn om zich op deze plek te bevinden worden hierdoor op deze overtreding gewezen. Het is de taak van de medewerker om hun beleefd maar duidelijk de weg naar het publieke gedeelte van het gebouw te wijzen en ze daar naar toe te begeleiden.

6.10 De dagelijkse werkzaamheden versus Informatiebeveiliging

Informatiebeveiliging is uitermate belangrijk voor het werk binnen BWRI waar veelvuldig met privacygevoelige informatie wordt gewerkt. Dit hoort dan ook bij de professionele en bekwame uitvoering van het werk. Ook cliënten vertrouwen op een zorgvuldige wijze van verwerken van hun gegevens. Reden waarom middels het werkoverleg geregeld aandacht voor dit onderwerp besteed dient te worden.

7 Programma Borging Veilige Gegevenswisseling Suwinet

Vereniging van Nederlandse Gemeenten (VNG) heeft het programma Borging Veilige Gegevenswisseling Suwinet (BVGS) geïntroduceerd. Daarbij zijn diverse tools ontwikkeld om het gebruik van Suwinet veiliger te maken. De tools zijn erop gericht om dienstverlening met inbegrip van passende privacybescherming verder te verbeteren.

7.1 BVGS maatregelen en producten in vogelvlucht

De tools die in het implementatieprogramma zijn ontwikkeld, zijn onder te brengen in drie categorieën: beheerstechnische tools, tools gericht op bewustwording en training van medewerkers en tools gericht op naleving van normen en verantwoording over het gebruik.

Beheerstechnische tools bestaan uit:
- Fijnmazig autoriseren;
- Andere zoeksleutels dan BSN;
- Whitelist met escapefunctie;
- Logging en rapportages.

Tools gericht op bewustwording en training bestaan uit:
- Bewustwording;
- Training;
- Uniform sanctiebeleid.

Tools gericht op naleving van normen en verantwoording over het gebruik bestaan uit:
- Afstemming tussen het Suwi-normenkader en de Baseline Informatiebeveiliging Gemeenten;
- Herijking van de aansluitvoorwaarden.

In de bijlage 3 worden BVGS maatregelen, tools en de voordelen beknopt beschreven.

7.2 Implementatie BVGS maatregelen

Zowel met de inrichting als de uitvoering van de diverse maatregelen uit voorgaande jaren heeft de herindelende gemeenten Hoogezand-Sappemeer, Menterwolde en Slochteren al de nodige slagen gemaakt. Wij zijn daarmee al op de goede weg en voldoen we aan zeven verplichte beveiligingsnormen van het Ministerie van SZW.
Programma Borging Veilige Gegevenswisseling Suwinet introduceert aanvullende en aangescherpte beveiligingsmaatregelen.

Fijnmazig autoriseren en andere zoeksleutels dan BSN
Als gevolg van de beheerstechnische maatregelen ‘Fijnmazig autoriseren’ en ‘Andere zoeksleutels dan BSN’ zijn per 1 juli 2017 enkele overzichten uit Suwinet-Inkijk verwijderd. Daarbij kwamen er vier nieuwe bronpagina’s bij. De nieuwe pagina’s en de nieuw ingedeelde pagina’s vormden een aanleiding om het autorisatiebeleid van de gemeente te herijken.
De bestaande autorisaties waren opnieuw zorgvuldig bekeken, beoordeeld en aangepast. Per 12 juni 2017 waren de autorisaties binnen Suwinet-Inkijk aangepast.

Whitelist met escapefunctie
In het tweede kwartaal van 2018 wordt deze maatregel doorgevoerd.
Om deze oplossing te implementeren zijn de volgende aandachtspunten van belang:
- Welke burgers komen op de whitelist (criteria en populatie vaststellen);
- Welke medewerkers de upload gaan verzorgen en hoe vaak;

De volgende BWRI-functies worden voor de escaperol geautoriseerd: Casemanager inkomen aanvraag, Casemanager inkomen minima, Casemanager terugvordering, verhaal en debiteuren, Werkcoach, Sociaal rechercheur en Preventiemedewerker.

Bijlage 1. Protocol inzage Suwinet door cliënt en/of gemachtigde

Om de privacy van de cliënt te waarborgen is zorgvuldigheid in de omgang met diens gegevens vereist. In bepaalde, in de hieronder beschreven gevallen, is gegevensinzage door derden mogelijk. De via Suwinet-Inkijk opvraagbare gegevens zijn alleen in elektronische vorm te zien. De gegevens mogen niet lokaal worden opgeslagen (op de harde schijf of op een extern opslagmedium). Hieronder volgt een handleiding voor een aantal situaties waar de Suwi-gebruiker mee te maken kan krijgen.

INZAGE

1. De **cliënt** verzoekt uitsluitend schriftelijk om inzage in diens gegevens
    - Stel de identiteit van de cliënt vast aan de hand van een geldig legitimatiebewijs (rijbewijs, paspoort, etc.);
    - Vraag om het BSN van de cliënt;
    - Stel vast dat het BSN is ontleend aan een officieel document (rijbewijs, paspoort etc.)
    - Maak een uitdraai van de geraadpleegde gegevens of laat de cliënt meekijken op het scherm;
    - Berg (mogelijk tweede) uitdraai onmiddellijk op in het cliëntendossier of vernietig eventueel
      uitgedraaid exemplaar;
    - Beëindig inkijksessie.

Het is mogelijk dat een cliënt telefonisch vraagt om een uitdraai van zijn/haar gegevens. In dat geval dient de cliënt verwezen te worden naar de mogelijkheid om daarvoor schriftelijk een verzoek in te dienen, dat binnen de wettelijk verplichte termijn dient te worden afgehandeld. Indien de cliënt inzage wil in al zijn/haar gegevens die bij een ketenpartner zijn geregistreerd, dient de cliënt te worden verwezen naar de betreffende ketenpartner.

2. **Gemachtigde** verzoekt schriftelijk om inzage in cliëntgegevens
    - Stel vast dat de machtiging schriftelijk is gegeven en nauwkeurig omschreven;
    - Stel de identiteit van de gemachtigde vast aan de hand van een geldig legitimatiebewijs (rijbewijs, paspoort, etc.);
    - Stel de identiteit van de cliënt vast aan de hand van een geldig legitimatiebewijs (rijbewijs, paspoort, etc.);
    - Vraag om het BSN van de cliënt;
    - Stel vast dat het BSN is ontleend aan een officieel document (rijbewijs, paspoort etc.)
    - Maak een uitdraai van de geraadpleegde gegevens of laat de gemachtigde meekijken op het scherm;
    - Berg (mogelijk tweede) de uitdraai onmiddellijk op in het cliëntendossier of vernietig eventueel uitgedraaid exemplaar;
    - Beëindig inkijksessie.

3. Een **derde** verzoekt om inzage, hetzij schriftelijk, hetzij mondeling in cliëntgegevens
    - Dit is niet mogelijk

CORRECTIE

1. De **cliënt** verzoekt om correctie
    - Stel de identiteit van de cliënt vast aan de hand van een geldig legitimatiebewijs (rijbewijs, paspoort, etc.);
    - Vraag om het BSN van de cliënt;
    - Stel vast dat het BSN is ontleend aan een officieel document (rijbewijs, paspoort etc.);
    - Maak twee kopieën van het verzoek;
    - Verstrek een kopie aan de cliënt, archiveer de andere kopie.

2. **Gemachtigde** verzoekt om correctie
    - Stel vast dat de machtiging schriftelijk is gegeven en nauwkeurig omschreven;
    - Stel de identiteit van de gemachtigde vast aan de hand van een geldig legitimatiebewijs (rijbewijs, paspoort, etc.);
    - Stel de identiteit van de cliënt vast aan de hand van een geldig legitimatiebewijs (rijbewijs, paspoort, etc.);
    - Vraag om het BSN van de cliënt;
    - Stel vast dat het BSN is ontleend aan een officieel document (rijbewijs, paspoort etc.)
    - Maak twee kopieën van het verzoek;
    - Verstrek een kopie aan de gemachtigde, archiveer de andere kopie

3. Een **derde** verzoekt om correctie
    - Dit is niet mogelijk

Bijlage 2. Verklaring geheimhouding Suwinet

Verklaring inzake geheimhouding van vertrouwelijke gegevens en het gebruik van Suwinet-Inkijk. Deze verklaring is noodzakelijk voor medewerkers waarbij de geheimhouding niet via het ambtenarenreglement of de inleenovereenkomst is geregeld.
Ondergetekende:
Naam:
Functie:
Organisatieonderdeel:
Plaats:
Datum:
zegt toe dat hij/zij:

- er van op de hoogte is dat de privacywet- en regelgeving een zorgvuldige omgang met persoonsgegevens beoogt te beschermen en dat deze wet- en regelgeving het gebruik van persoonsgegevens in de ruimste zin van het woord verbindt aan regels;

- zorgvuldig zal omgaan met de (persoons)gegevens en de inhoud van de documenten die hij/zij bij de uitvoering van de werkzaamheden in Suwi-verband mag inzien en zich daarbij houdt aan de werkinstructies zoals opgenomen in de functionele beschrijvingen van Suwinet-Inkijk en Suwinet-Mail. Concreet betekent dit onder meer dat hij/zij:

    - niet meer (persoons)gegevens inkijkt dan strikt noodzakelijk is;
    - zorgvuldig archiveert;
    - (persoons)gegevens niet aan onbevoegden verstrekt;
    - het wachtwoord zorgvuldig hanteert;

- kennis heeft genomen van het beveiligingsplan Suwinet en de regels die gelden voor het zorgvuldig omgaan met persoonsgegevens;

- gedurende de duur van zijn/haar inzet voor werkzaamheden in Suwi-verband enkel die (persoons)gegevens gebruikt, die van belang zijn voor het nastreven van het doel van SUWI;

- alle medewerking zal geven aan het naleven van de privacywet- en regelgeving door BWRI waar hij/zij werkzaam is;

- gedurende de duur van zijn/haar inzet voor de werkzaamheden in Suwi-verband en na beëindiging van deze werkzaamheden, tegenover derden geheimhouding zal betrachten met betrekking tot alle (persoons)gegevens waarvan hij/zij bij de uitvoering van de voornoemde werkzaamheden kennis neemt.

Naam medewerker: Handtekening medewerker:

Bijlage 3. Maatregelen Programma Borging Veilige Gegevenswisseling Suwinet

Ad 1. Beheerstechnische tools

- Fijnmaziger autoriseren. Door een nieuwe indeling van gegevens van klanten op de inkijkpagina's van Suwinet kan de gegevenslevering aan medewerkers beter worden afgestemd op de wettelijke taken die zij uitvoeren. Hiervoor is het nodig dat autorisaties opnieuw tegen het licht worden gehouden en opnieuw worden verstrekt. De gegevenslevering wordt daardoor proportioneler. Dat wil zeggen dat medewerkers niet onnodig teveel gegevens onder ogen krijgen. Zij zien alleen de gegevens die zij nodig hebben voor hun werk.
- Heroverweging gebruik zoeksleutels. Het uitgangspunt in Suwinet-Inkijk is dat cliëntgegevens worden geraadpleegd met het BSN als zoeksleutel. Hierop zijn soms uitzonderingen mogelijk zoals zoeken op adres of kenteken. Een handreiking beschrijft hoe een gemeente om kan gaan met deze risicovolle zoekmogelijkheden. Deze beschrijft hoe het autoriseren van medewerkers voor deze zoekschermen zorgvuldig kan worden gedaan.
- Meer en beter gebruik van de gebruikersrapportages. Alle raadplegingen door medewerkers worden gelogd. Gemeenten krijgen periodiek beschikking over gebruikersrapportages op basis van die loggingsgegevens. De rapportages worden nog niet door alle gemeenten (optimaal) gebruikt. In de toekomst zullen rapportages sneller en gemakkelijker ter beschikking worden gesteld via een online tool. Gemeenten kunnen de wijze waarop zij de rapportage inzetten in het controleproces, vereenvoudigen en optimaliseren. Gemeenten waarbij de inspectie non-gebruik constateerde, zullen hierop door het accountteam implementatie worden geattendeerd en worden geholpen bij het inpassen van de rapportages in de controleprocessen.
- Per gemeente kan bij het BKWI (Bureau Keteninformatie Werk en Inkomen, beheerder van Suwinet) een filtermechanisme worden geïnstalleerd waardoor alleen gegevens opgevraagd kunnen worden van burgers waar de gemeente een dienstverleningsrelatie mee heeft of had. Daarmee wordt één van de grootste privacyrisico's van Suwinet-Inkijk – namelijk dat alle inwoners van Nederland geraadpleegd kunnen worden, grotendeels weggenomen. Het filter is vormgegeven als een 'white list', de gemeente stelt de inhoud van deze 'white list' zelf vast en houdt deze zelf actueel.

Ad 2. Tools gericht op bewustwording en training van medewerkers

- Bewustwording. Aan gemeenten wordt een mix van communicatiemiddelen ter beschikking gesteld om de medewerkers voor te lichten. Het is van belang om helder aan gebruikers over te brengen wat wel en niet is toegestaan. Gemeenten kunnen dit vastleggen in een gebruikersverklaring en de medewerker vragen dit te tekenen.
- Training. Na het voorlichten van medewerkers kunnen zij getoetst worden op hun inzichten over veilig gebruik van Suwinet-Inkijk. Hiervoor is een e-learning tool ontwikkeld. De medewerker doorloopt een online vragenlijst. Gemeenten kunnen de e-learning tool inzetten in combinatie met de gebruikersverklaring.
- Uniform sanctiebeleid. Wanneer het toch misgaat en een medewerker maakt misbruik van Suwinet is de vraag hoe te sanctioneren. Voor gemeenten is een stappenplan beschikbaar om sanctiebeleid te implementeren.

Ad 3. Tools gericht op de naleving van normen en de verantwoording over het gebruik

- Het Suwi-normenkader (specifiek voor Werk en Inkomen) en de Baseline Informatiebeveiliging Gemeenten (gemeentebreed) zijn beter op elkaar afgestemd. De kaders zijn ontdubbeld en de overgebleven Suwi-normen zijn gerelateerd aan de normen in de BIG. De Suwi-norm is dan een aanvulling op of een uitwerking van de BIG-norm. Er is extra aandacht besteed aan normen over telewerken, doorleveren van gegevens en risicoklassen. Gemeenten kunnen bij de implementatie van de BIG de aanvullingen vanuit Suwi direct meenemen.
- De aansluitvoorwaarden zullen worden herijkt. Dit traject is nog in uitvoering. Wanneer het

implementatieprogramma is afgerond worden gemeenten gevraagd om aansluitvoorwaarden te tekenen die uitgaan van veilig gebruik van Suwinet op basis van de hierboven beschreven tools.

Ad 4. Voordelen
Voor gemeenten biedt het op meerdere manieren voordelen om deze tools te implementeren:

- Met het daadwerkelijk realiseren van de omslag en de implementatie van de veiligheidstools kan gemeente met het gebruik van Suwinet aansluiten op de generieke gemeentebrede trajecten als implementatie van de BIG en de Digitale Agenda 2020. Door proactief in te spelen op deze initiatieven houdt gemeenten zelf regie. Dit helpt nieuwe inspectieonderzoeken te voorkomen.
- Het gebruik van de tools zal initieel een tijdsinvestering vragen bij lokale implementatie. Hierna zullen werkprocessen rond autoriseren en controle op gebruik beter hanteerbaar zijn en in kwaliteit en efficiency toenemen. Door het gebruik van de tools gericht op bewustwording en training zullen medewerkers bewuster kunnen omgaan met persoonsgegevens. Ook dit maakt de controle beter hanteerbaar.
- Met het gebruik van de tools nemen de risico's zoals disproportioneel gebruik van gegevens, te breed autoriseren, teveel zoeksleutels toekennen af. Gemeente kan dus met de tools de privacybescherming van de burgers verbeteren
- Veel gegevensleveranciers willen privacy voorwaarden gaan verbinden aan de levering van gegevens. Met de implementatie van de tools kan gemeente hierop vooruit lopen. Met name het gebruik van de white list – om uitsluitend klanten van de gemeente zelf te kunnen opvragen – zouden gegevensleveranciers bij voorkeur verplicht stellen voor het voortzetten van gegevenslevering.