Inspectie SZW
Ministerie van Sociale Zaken en Werkgelegenheid

Suwinet 2015

Vervolgonderzoek 'veilig omgaan met elkaars gegevens'

Inspectie SZW
Ministerie van Sociale Zaken en Werkgelegenheid

Suwinet 2015

Vervolgonderzoek 'veilig omgaan met elkaars gegevens'

Colofon

Rapport	Suwinet 2015 vervolgonderzoek 'veilig omgaan met elkaars gegevens'
Nummer	R16/04
ISSN	1383-8733
ISBN	978-90-5079-282-0
Datum	april 2016

Voorwoord

Suwinet is een geautomatiseerd systeem waarmee gemeenten en andere (semi-overheids)organisaties gegevens uitwisselen die noodzakelijk zijn voor onder meer de uitvoering van de Participatiewet In 2015 was sprake van 10 miljoen berichtuitwisselingen op maandbasis De beveiliging van het systeem tegen oneigenlijk gebruik en misbruik door medewerkers is noodzakelijk om de beveiliging van persoonsgegevens te waarborgen.

De Inspectie SZW voert sinds 2009 onderzoek uit naar de beveiliging van Suwinet tegen schendingen van de vertrouwelijkheid door (medewerkers van) gemeenten. Uit die onderzoeken kwam naar voren dat de beveiliging niet optimaal functioneerde, en dat verbetering slechts langszaam vorderde

De bevindingen van het onderzoek over 2014 waren aanleiding voor de staatssecretaris om in het Algemeen Overleg van 24 juni 2015 een herhalingsonderzoek bij alle gemeenten aan te kondigen. De resultaten daarvan worden in deze rapportage weergegeven.

Uit het onderzoek van de Inspectie, dat betrekking heeft op de periode 1 september 2014 – 1 september 2015, blijkt dat de situatie nog steeds niet optimaal is. Vergeleken met eerdere jaren zijn echter belangrijke stappen gezet Waar in 2014 slechts 17% van de gemeenten aan alle onderzochte normen voldeed, is dat in 2015 gestegen naar 49% De Inspectie heeft gedurende het onderzoek en ook daarna gemeenten op diverse manieren gefaciliteerd Onder andere is een handreiking opgesteld voor de gemeenten die nog verbeteringen dienen door te voeren De verwachting is dat dit alles tot meer effect zal leiden. De nodige gemeenten hebben ons (na de onderzoeksperiode) aangegeven dat inmiddels de nodige verbeteringen zijn gerealiseerd en dat men nu aan de normen voldoet Het percentage zou dan verder gestegen zijn Dit najaar beoordeelt de Inspectie in het kader van het escalatieprotocol opnieuw een aantal gemeenten die nu nog niet voldoen aan alle normen.

Suwinet is ontstaan in een tijd dat er nog geen sprake was van het sociaal domein en integrale dienstverlening Een belangrijk zorgpunt in de bestuurlijke reacties en die we ook van individuele gemeenten hebben vernomen, is dat er taken bijkomen maar dat het passend informatiearrangement (wettelijk kader) daarbij ontbreekt Suwinet mag voor die nieuwe taken niet geraadpleegd worden Dit leidt in de praktijk tot hogere administratieve lasten en het meerdere keren uitvragen van gegevens. Vanuit de gemeenten wordt al geruime tijd gevraagd om verruiming Daar waar gegevensuitwisseling verbreed zou moeten worden tot het gehele sociaal domein, betreft het uiteraard een departementsoverstijgend onderwerp. Het is van belang dat hier op korte termijn duidelijkheid over ontstaat.

De beveiliging van de persoonsgegevens is substantieel verbeterd Tegelijkertijd kan worden vastgesteld dat er door een aantal gemeenten nog de nodige werkzaamheden dient te worden verricht, vóórdat de beveiliging op orde is Informatiebeveiliging vraagt continu aandacht

mr. M.J. Kuipers
Inspecteur-generaal SZW

Inhoud

1 Inleiding

Aanleiding en achtergrond

Suwinet[1] is een geautomatiseerd systeem waarmee gemeenten en andere (semi-overheids)organisaties gegevens uitwisselen die noodzakelijk zijn voor onder meer de uitvoering van de Participatiewet. In 2015 werden via Suwinet gegevens van bijna 700.000 burgers geraadpleegd, door 22 000 actieve gebruikers, van wie 10.000 gemeenteambtenaren. Hierbij was sprake van 10 miljoen berichtuitwisselingen op maandbasis De beveiliging van het systeem tegen oneigenlijk gebruik en misbruik door medewerkers is noodzakelijk om de privacy van burgers te waarborgen.

De Inspectie SZW rapporteerde in mei 2015 in het rapport Suwinet 'veilig omgaan met elkaars gegevens' over de gebrekkige beveiliging van het gebruik van persoonsgegevens door gemeenten in 2014. De bevindingen lagen in lijn met die van eerdere rapportages. het overgrote deel van de gemeenten voldeed niet aan de 7 essentiele normen uit het Normenkader 'Gezamenlijke elektronische Voorzieningen SUWI (GeVS)' [2] die de Inspectie in het onderzoek betrok
De staatssecretaris kondigde in mei 2015 een herhalingsonderzoek aan voor het najaar van 2015. Daarin dienden alle Nederlandse gemeenten te worden betrokken De uitbreiding van het onderzoek van een steekproef naar alle gemeenten in Nederland, staat in verband met een door de staatssecretaris in november 2015 aan de gemeenten verzonden escalatieprotocol In het protocol staat dat gemeenten die niet voldoen aan de 7 onderzochte normen, binnen 6 tot 12 weken de beveiliging op orde moeten brengen. Doen ze dat niet, dan volgt een aanwijzing en kan hun uiteindelijk zelfs de toegang tot Suwinet worden ontzegd

Onderzoekvraag

De bescherming van de privacy van personen van wie de persoonsgegevens worden verwerkt, vereist vooral dat de vertrouwelijkheid voldoende gewaarborgd is Vertrouwelijkheid wil zeggen dat gegevens alleen te benaderen zijn door iemand die daarvoor gemachtigd is en er niet meer gegevens worden geraadpleegd dan noodzakelijk is voor de taakuitoefening

De centrale vraag in het onderzoek is.

In welke mate voldoen gemeenten aan de eisen van vertrouwelijkheid die worden gesteld aan de beveiliging van het gebruik van gegevens die worden uitgewisseld binnen Suwinet?

---

[1] Waar in het rapport wordt gesproken over Suwinet is in het algemeen sprake van uitsluitend Suwinet-Inkijk Het verschil wordt uitgelegd in bijlage 4

[2] Van de totale set van 115 normen zijn 26 normen als essentieel benoemd Aan deze essentiele normen dient in elk geval te worden voldaan Bij de overige normen is volgens de verantwoordingsrichtlijn ruimte voor 'niet-materiele tekortkomingen'

Toetsingskader

Het gehanteerde toetsingskader is gelijk aan dat van vorige onderzoeken. Getoetst wordt aan 7 essentiele normen uit het Normenkader GeVS. Dit normenkader is door de Suwi-partijen zelf vastgesteld. Het toetsingskader is waar nodig door de Inspectie nader geoperationaliseerd. Het wettelijk kader en de operationalisatie zijn opgenomen in bijlagen 2 en 3. Bijlage 4 bevat een inhoudelijke toelichting over wat Suwinet is.

Onderzoeksmethode

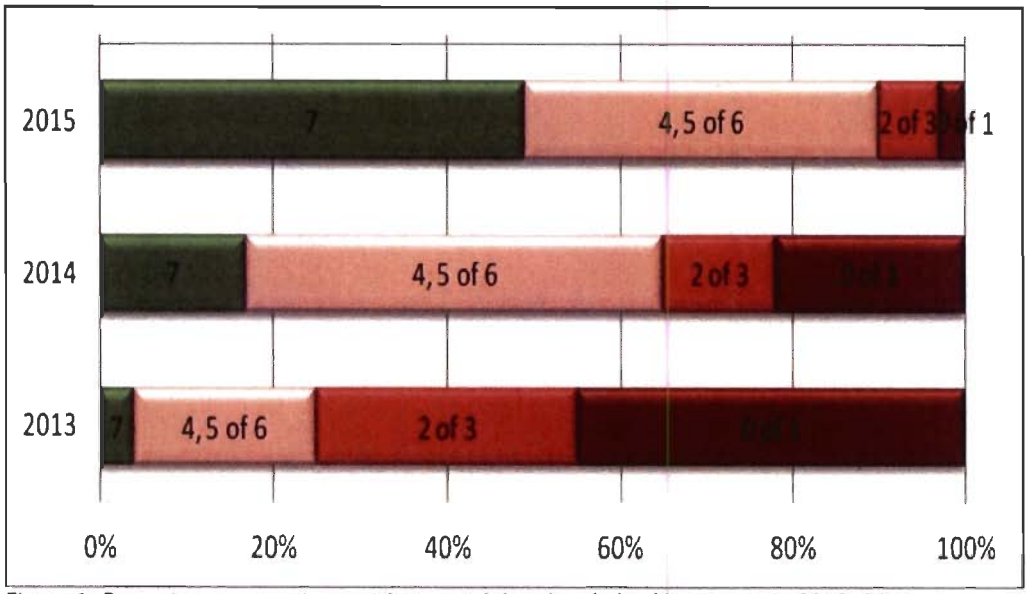
Alle 393 gemeenten van Nederland (stand 1 september 2015) hebben een vragenlijst (zie bijlage 5) ingevuld en documentatie toegestuurd. Deze zijn door de Inspectie getoetst. Ook heeft de Inspectie gebruik gemaakt van loggegevens van BKWI over het gebruik door gemeenten van Suwinet, en over de informatie die de gemeenten over hun gebruik opvragen.
Met de gekozen methode kan de Inspectie met een redelijke mate van zekerheid vaststellen dat de beveiliging van het gebruik van gegevens die via Suwinet worden verkregen, op orde is. De methodologische verantwoording is opgenomen in bijlage 6.

Onderzoeksperiode

Het onderzoek gaat over de periode 1 september 2014 tot 1 september 2015.

2 Bevindingen

2.1 Landelijk beeld



Figuur 1. Percentage gemeenten met het aantal door hen behaalde normen in 2013, 2014 en 2015. Het aantal behaalde normen staat vermeld in de staven. De indeling in vier groepen is conform de indeling van het escalatieprotocol.

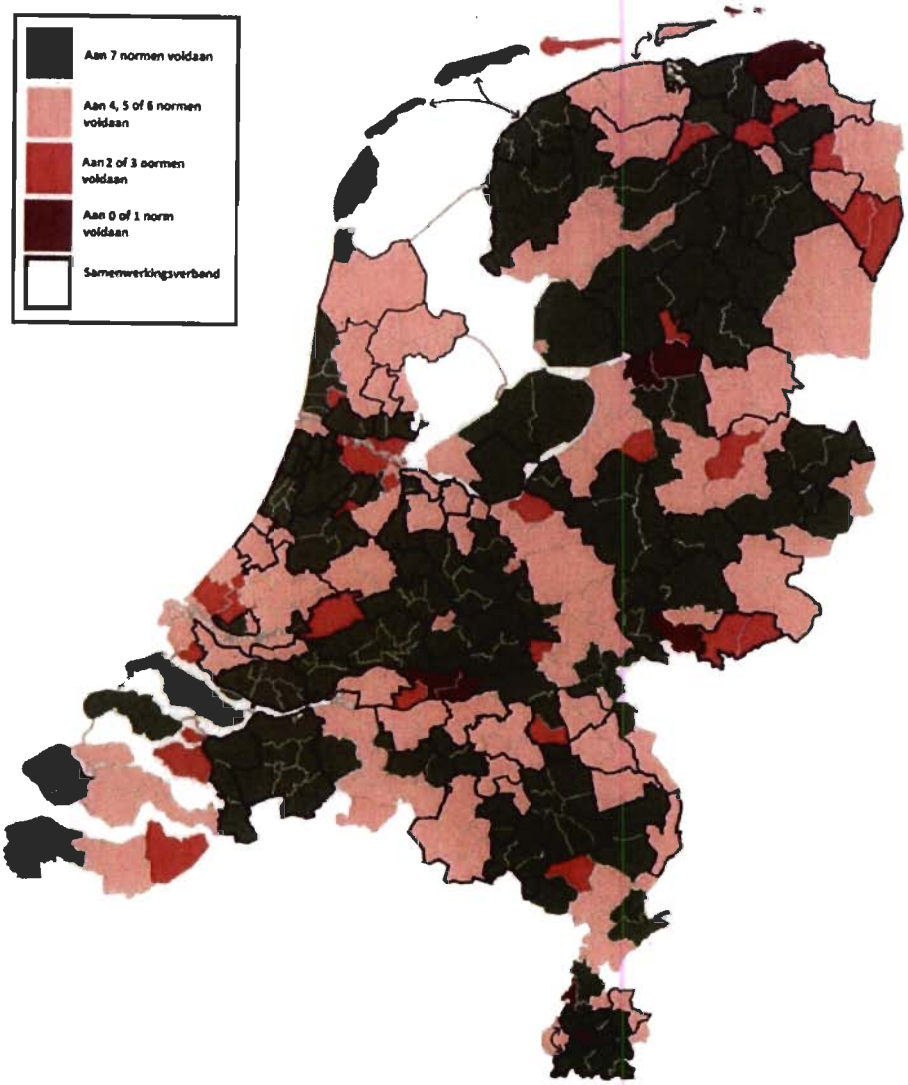
Bijna de helft van de 393 gemeenten (49%) voldoet in 2015 aan de 7 essentiële normen. Dit is een aanzienlijke verbetering ten opzichte van voorgaande jaren (2014: 17%). Maar het betekent ook dat de helft van de gemeenten nog één of meerdere normen niet behaalt. Als aan alle 7 normen is voldaan (zie figuur 1, groene kleur), dan pas is sprake van een beveiliging waarvan met een redelijke mate van zekerheid kan worden gesteld dat deze op orde is.

De omschreven verbeteringen komen ook tot uiting in de gemiddelde score. Deze neemt van 2013 op 2014 toe van 2,4 naar 3,9 correct toegepaste normen, en stijgt in 2015 door naar 5,8.

Hoewel aan alle normen moet worden voldaan, is desondanks natuurlijk positief dat nog maar 10% van de gemeenten in 2015 in de laagste twee groepen van het escalatieprotocol verkeert en er heel weinig gemeenten resteren die geen of slechts één norm behalen. In 2013 werd door bijna de helft van de gemeenten nog aan slechts 0 of 1 norm voldaan.

Een deel van de gemeenten (78) dat niet aan alle normen voldeed, heeft na de uitvoering van het onderzoek de Inspectie gemeld dat het de beveiliging op orde heeft gebracht. Het totaal aantal gemeenten dat aan alle normen voldoet, zou dan uitkomen op circa 70%. Overigens is deze nadere informatie niet verder door de Inspectie onderzocht.

Aangenomen wordt dat het escalatieprotocol, maar ook de diverse acties van organisaties zoals de VNG, BKWI (publicaties, presentaties) en de Inspectie, hebben bijgedragen aan deze verbetering.



Figuur 2. De landkaart geeft de scores per gemeente weer. Ook samenwerkingsverbanden zijn hierin weergegeven.

In bijlage 7 zijn de uitkomsten per individuele gemeente weergegeven. Bijlage 8 geeft een overzicht van de scores over de periode 2013-2015.

2.2 De G4, G32, overige gemeenten en samenwerkingsverbanden nader bezien

G4

Bijna 30% van de gehele populatie van de Participatiewet wordt verzorgd door de G4. Van de vier gemeenten behaalt alleen Utrecht een voldoende op alle normen. Den Haag en Rotterdam halen elk 6 uit 7, maar Amsterdam scoort laag, met slechts 2 behaalde normen.
Den Haag en Rotterdam lopen goedkeuring van een norm mis, omdat ze beide Suwinet inzetten voor andere taken dan de Participatiewet (zie voor de betekenis daarvan verder hieronder). Amsterdam hanteerde een generieke aanpak voor de beveiliging van het gebruik van Suwinet, gebaseerd op haar algemene informatiebeveiliging. Inmiddels heeft Amsterdam een plan van aanpak opgesteld om aan de meer specifieke vereisten uit het normenkader GeVS te voldoen.

G32

De G32 (gemeenten met meer dan 100 000 inwoners) bedienen samen bijna 60% van alle bijstandsgerechtigden. De prestaties van de G32 wijken waar het gaat om het behalen van alle 7 normen, niet af van het gemiddelde beeld in Nederland. Gemiddeld scoort 47% van de G32 de gewenste 7 uit 7 normen, en dat wijkt nauwelijks af van het landelijk gemiddelde van 49%. De gemeenten uit de G32 die aan 4, 5 of 6 normen voldoen, wijken met 44% ook nauwelijks af van het landelijke gemiddelde van 41%. Van de G32 zijn er 10 gemeenten die opereren in een samenwerkingsverband.

Overige gemeenten

Gemeenten die niet tot de G32 behoren en dus minder dan 100.000 inwoners hebben, voldoen globaal genomen vrijwel net zo vaak aan de normen als de G4 en G32. Relatief veel kleinere gemeenten maken deel uit van een samenwerkingsverband. Zo zijn er van de 30 allerkleinste gemeenten nog maar 8 die de uitvoering Participatiewet volledig zelfstandig verzorgen.

Het normenkader houdt (nagenoeg) geen rekening met het verschil in kleine en grote gemeenten. Het normenkader geldt voor Amsterdam met circa 1200 medewerkers met toegang tot Suwinet, maar ook voor Ameland waar het afgelopen jaar niet één raadpleging heeft plaatsgevonden. Hiertegenover staat dat een medewerker van Ameland (nog) net zoveel gegevens kan raadplegen van Nederlandse burgers als een medewerker van Amsterdam. In het kader van het programma *'Borging veilige gegevensuitwisseling via Suwinet'* (zie bijlage 12, onderdeel 3) wordt het door het gebruik van filtering niet meer mogelijk alle gegevens van alle burgers te raadplegen.

Diverse kleine gemeenten hebben er in hun reactie op gewezen dat het gehanteerde normenkader bureaucratie in de hand werkt. Eisen die vanuit GeVS worden gesteld

aan de vastlegging van activiteiten zouden juist kleinere gemeenten op verhoudingsgewijs hoge administratieve kosten jagen Sommige geven aan dat er in kleinere organisaties meer zicht is op wat collega's doen, en dat dergelijke soft controls niet meewegen in de beoordeling van de Inspectie
Concluderend kan worden gesteld dat er geen verschil is waar te nemen tussen het presteren van grotere of kleinere gemeenten Dit is in lijn met het vorige onderzoek

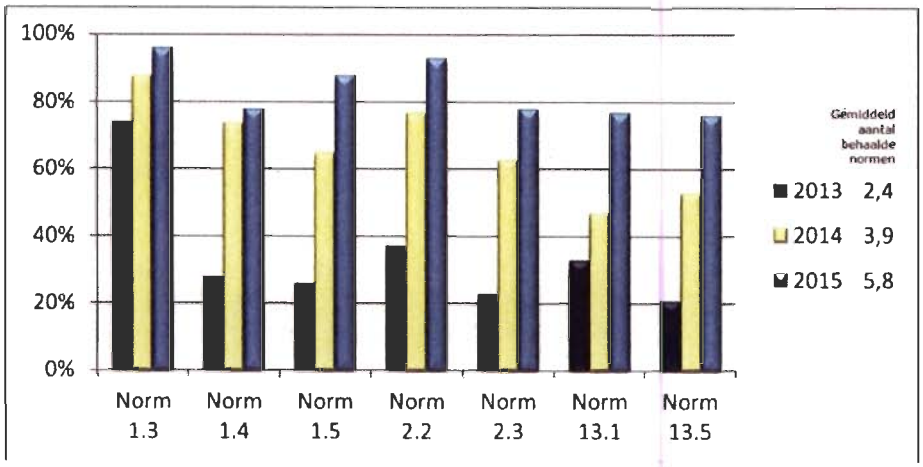
Samenwerkingsverbanden
Van de 393 onderzochte gemeenten werkten er 236 samen in een uitbestedingsconstructie of in een regionale of intergemeentelijke sociale dienst In totaal zijn er 72 van dergelijke verbanden (zie bijlage 9) De overige 157 gemeenten voeren de Participatiewet zelfstandig uit
Van de gemeenten die samenwerken in een verband, voldoet 58% aan de 7 normen Ze scoren aanzienlijk beter dan de gemeenten die zelfstandig opereren Bij deze groep voldoet slechts 34% aan de 7 normen

2 3 Uitkomsten per norm

De ontwikkelingen in de prestaties van de gemeenten per afzonderlijke norm, staan weergegeven in het onderstaande figuur In bijlage 10 zijn de uitkomsten (ook in subnormen) nader uitgewerkt.

De beoordeelde 7 normen zijn hier verkort weergegeven. In bijlage 3 zijn de volledige teksten opgenomen De nummering is overgenomen van het normenkader GeVS

- 1 3. Het informatiebeveiligingsbeleid en het beveiligingsplan van het Suwinet zijn goedgekeurd door het management van de Suwi-partij;
- 1 4· Het informatiebeveiligingsbeleid en het beveiligingsplan van het Suwinet worden uitgedragen in de organisatie,
- 1.5 Het informatiebeveiligingsbeleid en/of het beveiligingsplan van het Suwinet wordt jaarlijks geevalueerd en indien nodig geactualiseerd;
- 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,
- 2 3. -De security officer beheert en beheerst beveiligingsprocedures en beveiligingsmaatregelen in het kader van Suwinet;
  -De security officer bevordert en adviseert over de beveiliging van Suwinet, verzorgt rapportages over de status aan het hoogste management, controleert dat met betrekking tot de beveiliging van Suwinet de maatregelen worden nageleefd,
- 13.1 De Suwi-partij autoriseert en registreert de gebruikers die toegang hebben tot de Suwinet applicaties op basis van een formele procedure;
- 13 5 De controle op verleende toegangsrechten en gebruik vindt meerdere keren per jaar plaats



Figuur 3. Het percentage gemeenten dat voldoet aan de afzonderlijke 7 normen uit het toetsingskader van de Inspectie SZW, in 2013, 2014 en 2015.

Het aantal gemeenten dat voldoet aan de normen 1.4, 2.3, 13.1 en 13.5 blijft achter bij het aantal gemeenten dat handelt conform de vereisten van de andere normen. De verschillen nemen in de loop der tijd wel wat af, maar nog steeds kan worden waargenomen dat normen die zich richten op de feitelijke controle van de 'werking' van de beveiliging van het gebruik van Suwinet minder goed scoren dan de meer randvoorwaardelijke normen. Het verrichten van structurele controles kost blijkbaar meer moeite dan het uitvoeren van afgebakende acties zoals het opstellen van een beveiligingplan en het plaatsen daarvan op intranet.

2.4 Overige bevindingen

- *Inzet uitsluitend ten behoeve van Participatiewet?*

Suwinet mag door gemeenten als Suwi-partij, in principe uitsluitend worden ingezet voor de uitvoering van de Participatiewet en aanverwante wetten IOAZ en IOAW. Beleidsterreinen als WMO (Wet Maatschappelijke Ondersteuning) en schuldhulpverlening bijvoorbeeld, mogen geen gebruik maken van Suwinet. Er moeten dus waarborgen aanwezig zijn die gegevens welke via Suwinet worden verkregen, beschermen tegen gebruik voor andere gemeentelijke taken dan waarvoor Suwinet is bedoeld.
Het onderzoek biedt de Inspectie niet de mogelijkheid om met waterdichte conclusies te komen over de werking van deze waarborgen. In een aantal gevallen (ca. 5% van de gemeenten) is vastgesteld dat de waarborgen niet goed functioneren. Oneigenlijk gebruik is geconstateerd voor onder meer Den Haag en Rotterdam. De laatste gemeente had over het gebruik van Suwinet voor andere taken dan de Participatiewet, al vóór het onderzoek van de Inspectie op eigen initiatief contact met het departement gelegd.
Hier manifesteert zich de dynamiek tussen de stuwende (zoals effectiviteit en efficiency) en verankerende (privacy en keuzevrijheid) beginselen zoals beschreven in het WRR rapport i-Overheid. Gemeenten worden geconfronteerd met de overheveling van beleidsterreinen om integraliteit te bewerkstelligen. Maar de regelgeving staat geen integrale gegevensuitwisseling toe.

In tegenstelling tot voorgaande jaren, constateert de Inspectie dat externe partijen, zoals incassobureaus, niet of nauwelijks toegang krijgen tot Suwinet. Acties die hierop zijn ondernomen, lijken te hebben gewerkt

- *Controle op verleende toegangsrechten en gebruik*

Bij norm 13.5 heeft de Inspectie SZW onder meer bekeken of de gemeenten zelf onderzoek doen naar opvallend zoekgedrag van hun medewerkers Diverse gemeenten geven aan dat het beoordelen van alleen de generieke BKWI-rapportages (dat zijn rapportages die BKWI elke maand voor elke gemeente opstelt over het (geanonimiseerde) gebruik van Suwinet) volgens hen daarvoor voldoende is. Dat zijn rapportages die BKWI elke maand voor elke gemeente opstelt De Inspectie is van mening dat een gemeente ook specifieke rapportages (waartoe ook steekproeven op BSN te rekenen zijn) dient op te vragen om echt zicht te krijgen op de vraag wie welke gegevens heeft geraadpleegd. Pas dan kan men ook op accountniveau een controle uitvoeren.

- *Kennis neemt toe*

Hoewel het laatste onderzoek nog maar een jaar geleden heeft plaatsgevonden, merkt de Inspectie dat er door gemeenten in het huidige onderzoek verhoudingsgewijs veel minder vragen over gebruikte begrippen worden gesteld. Begrippen die meestal in het kader van de beveiliging van het gebruik van Suwinet voor zichzelf zouden moeten spreken De inhoudelijke kennis bij de uitvoering neemt derhalve toe

- *Gedrag en cultuur nog vraagtekens*

Uit het huidige onderzoek blijkt nog niet dat er bij alle gemeenten echt een cultuuromslag heeft plaatsgevonden in het denken over de beveiliging van het gebruik van Suwinet, dit ondanks de duidelijk betere scores op de onderzochte normen. De Inspectie signaleert dat diverse gemeenten pas startten met activiteiten op het moment dat het onderzoek van de Inspectie bekend werd (ca een kwart van de gemeenten), of dat gemeenten zich alleen richtten op de 7 normen die de Inspectie in haar onderzoek betrekt (ca. eenvijfde) De andere beveiligingsnormen blijven in de laatstgenoemde situatie dan volledig buiten beeld.

Tevens is er een aantal gemeenten dat nu slechter presteert dan in het vorige onderzoek. Informatiebeveiliging vraagt continue aandacht Het is geen eenmalig project. In bijlage 11 is een overzicht opgenomen waarin de verschillen in normrealisatie over de periode 2014-2015 zijn weergegeven

- *Inlezen-Inkijk*

Het onderzoek van de Inspectie richtte zich op de beveiliging van het gebruik van Suwinet-Inkijk. Een andere voorziening, Suwinet-Inlezen, is buiten beschouwing gebleven Van dat systeem maken echter alleen 3 van de 4 grote steden gebruik Het ontbreken van zicht op het gebruik van gegevens die via Suwinet-Inlezen worden verkregen, is daarmee nog geen wijdverspreide problematiek. Anders ligt dit voor het zogenaamde DKD-Inlezen Ca. 338 gemeenten kunnen in principe de gegevens uit Suwinet-Inkijk namelijk ook verkrijgen via DKD-inlezen DKD staat daarbij voor het digitale klantendossier.

Deze gemeenten hebben daartoe een overeenkomst gesloten met het Inlichtingenbureau (IB) De facto lezen 82 gemeenten ook werkelijk DKD in
Over de beveiling van deze decentrale voorziening doet het onderzoek geen uitspraak. Vanuit het onderzoek van vorig jaar is bekend dat de centrale logging op het gebruik van DKD-Inlezen geen informatie bevat over het gebruik op accountniveau (dus over individuele gebruikers). Dat is technisch niet mogelijk.
Logging tot op accountniveau is een wettelijke verplichting. Uit voorgaande onderzoeken heeft de Inspectie indicaties dat de beschikbare loggegevens niet of nauwelijks worden geraadpleegd Dit betekent dat in de praktijk deze gegevens niet worden geanalyseerd waarmee het de vraag is of gemeenten voldoende controles uitvoeren op het gebruik van DKD-inlezen door individuen
Dat alles roept vragen op over de beveiliging van het gebruik van DKD-Inlezen
De Autoriteit Persoonsgegevens heeft een onderzoek uitgevoerd naar Inlezen. Op basis van dat onderzoek heeft UWV (BKWI) een plan van aanpak opgesteld om de beveiliging van Suwinet-inlezen op dit punt te verbeteren De intentie is om de aanpak via het Programmaplan borging veilige gegevensuitwisseling Suwinet, te verbreden tot DKD-inlezen. Ook het (toekomstig) gebruik van filters waarmee steeds minder makkelijk gegevens kunnen worden opgevraagd die niet strikt noodzakelijk zijn, zal het risico mitigeren.

- *Ontwikkelingen*

Het onderwerp informatiebeveiliging staat al geruime tijd in de belangstelling van de politiek, uitvoering en toezichthouders In dat kader zijn de afgelopen jaren door diverse organisaties dan ook verbetermaatregelen gestart Bijlage 12 bevat een overzicht van deze ontwikkelingen, die deels Suwinet overstijgen.

3 Reactie van de gemeenten op het onderzoek

Alle 393 gemeenten hebben uiterlijk begin februari 2015 een conceptrapportage van bevindingen ontvangen Deze conceptrapportage presenteert voor elke norm de beoordeling van de Inspectie, en bevat een toelichtende onderbouwing voor de normen waaraan niet wordt voldaan

Van de 217 gemeenten die in eerste instantie niet voldeden aan alle 7 normen hebben er 184 gereageerd (92%) op de conceptrapportage.

Van deze 184 gemeenten zijn er 78 die verbetermaatregelen aankondigen De meeste gemeenten benoemen geen concrete acties, maar beloven (binnenkort) aan 7 normen te voldoen Waar concrete acties worden genoemd, betreft dit veelal het evalueren van beleidsplannen, controleren van gebruikersrechten en het rapporteren aan het hoogste management

Als de 78 gemeenten die (al of niet concreet toegezegde) maatregelen hebben doorgevoerd, worden opgeteld bij de gemeenten die volgens het onderzoek al voldoen aan alle 7 normen, dan zou circa 70% van alle gemeenten aan alle onderzochte normen voldoen Uiteraard is dit een aanname omdat op de gebeurtenissen na afsluiting van de onderzoeksperiode geen controle is uitgevoerd

Van de 184 gemeenten die een reactie geven op de conceptrapportage, zijn 38 reacties afkomstig van het College van B&W De resterende reacties komen van de security officer of van de manager of het afdelingshoofd dienstverlening, werk of informatievoorziening.

Van de 184 gemeenten zijn er 64 akkoord met de constateringen zoals beschreven in de conceptrapportage. 120 gemeenten kunnen zich niet vinden in het conceptoordeel, 53 hiervan stuurden extra bewijsmateriaal. Dit grote aantal zal mede te verklaren zijn door het escalatieprotocol waardoor de druk op gemeenten om de 7 normen te halen hoog is. Gemeenten doen daarom hun uiterste best om toch aan alle 7 normen te voldoen

Een aantal gemeenten meldt dat de Inspectie SZW te weinig rekening heeft gehouden met ontwikkelingen die zich na 1 september 2015 hebben voorgedaan. Voor het onderzoek is 1 september 2015 echter het meetmoment.
Om aan dit punt zoveel als mogelijk tegemoet te komen, heeft de Inspectie SZW de situatie nà 1 september 2015 meegewogen indien kon worden aangetoond dat nieuwe ontwikkelingen al vóór 1 september 2015 waren ingezet, niet al te lang na die datum zijn ingevoerd, en er inmiddels ook feitelijk werd gewerkt volgens de beschreven werkwijze.

Gemeenten hebben in hun reactie een aantal redenen gegeven waarom men nog niet voldeed aan bepaalde normen. Meest genoemd daarbij is een reorganisatie of fusie van diverse gemeenten die veel tijd en aandacht vraagt. Ook komt het voor dat de security officer in de onderzoeksperiode ziek of afwezig was en er niet

gecontroleerd kon worden op en/of gerapporteerd kon worden over de beveiliging van Suwinet. Dergelijke problemen mogen volgens de Inspectie de beveiliging van Suwinet niet in de weg staan

De Inspectie SZW heeft naar aanleiding van de opmerkingen van 36 gemeenten op de conceptrapportage de beoordeling bijgesteld Het betrof een positieve bijstelling van één of twee normen Het vaakst werd het oordeel op norm 13.5 (controle op verleende toegangsrechten) aangepast. Andere aanpassingen betroffen normen 1.4, 2 3 en 13 1

Een aantal – veelal kleine – gemeenten verwijst naar het formele karakter van de beoordeling Deze reactie heeft de Inspectie ook bij het vorige onderzoek ontvangen. Zij geven aan dat geen rekening wordt gehouden met het feit dat binnen sommige gemeenten zaken informeel plaatsvinden Dat wil zeggen dat activiteiten wel plaatsvinden, maar niet schriftelijk worden vastgelegd Het gehele onderzoek is – net als in voorgaande jaren – uitgevoerd op basis van schriftelijke vastleggingen. Dit berust op de aanname van de Inspectie dat er altijd iets op papier is terug te vinden van de uitgevoerde activiteiten. Een goede beveiliging vereist ook een goede audittrail

Bij opmerkingen van gemeenten over beoordeelde normen gaat het veelal om norm 13 5 (controle op verleende toegangsrechten) Hierop is in de bevindingen van de Inspectie al ingegaan.

Er zijn 7 gemeenten die tijdens het vorige onderzoek beter scoorden dan in dit onderzoek. De meeste verklaarden dit uit (komende) fusies. De Inspectie vindt dat organisatorische wijzigingen geen invloed mogen hebben op de beveiliging van Suwinet.

4 Bestuurlijke reacties – naschrift Inspectie

- ***Bestuurlijke reacties***

Het **Inlichtingenbureau (IB)** spreekt waardering uit voor het onderzoek van de Inspectie en gaat nader in op een aantal ontwikkelingen om de beveiliging van de gegevens van Suwinet te verbeteren Zo wordt in het jaarplan 2016 van IB ingezet op beperking van gegevensleveringen op basis van de gedachte 'less is more' en op voorlichting ten aanzien van de wettelijke gebruiksdoelen, met name met betrekking tot de verstrekking van dossierpersoon-berichten in het kader van het digitaal klantdossier. IB biedt met informatieproducten, zoals aanvraagtoetssignalen en incasso-ondersteuning bijstandsdebiteuren, ondersteuning van specifieke gemeentelijke werkprocessen op basis van doelbinding, waardoor het voor deze werkprocessen op termijn niet meer nodig is complete generieke klantdossiers te raadplegen via Inkijk-functionaliteit of te importeren via Inlees-functionaliteit

UWV gaat in op het verbeteringstraject. Voor de uitwisseling van gegevens via Suwinet geldt dat VNG, SVB en UWV gezamenlijk uitvoering geven aan het programmaplan 'Borging veilige gegevensuitwisseling via Suwinet'. In dit programma wordt o a gewerkt aan de verbetering van (de benutting van) gebruikersrapportages en logging van gegevensgebruik, een herijking van het normenkader waar partijen zich aan moeten houden, verschillende maatregelen om de gegevensuitwisseling meer proportioneel in te richten (bijv. de doorontwikkeling van filtermogelijkheden) en een ketenbrede awarenesscampagne

UWV constateert daarnaast dat er meer aandacht zou moeten komen voor een integraal veilig gebruik van gegevens, ongeacht de voorzieningen waarmee gegevens worden uitgewisseld. Zo benoemt de Inspectie volgens UWV in het rapport terecht, dat de huidige wet- en regelgeving op het gebied van gegevensuitwisseling niet goed aansluit bij de praktijk van integraal beleid bij gemeenten UWV denkt dat verbeteringen op dit punt ook zullen bijdragen aan een hogere kwaliteit van de privacy en beveiliging van gegevens bij overheidsinstanties Tot slot heeft UWV in een bijlage een aantal inhoudelijke verbeteringen voor de tekst van het rapport aangereikt.

De **VNG** vindt het positief dat het aantal gemeenten dat volledig voldoet aan de normen in een jaar tijd is verdrievoudigd Tevens wijst de VNG erop dat direct na afloop van het onderzoek nog eens 20% van de gemeenten aangeeft dat de beveiliging volledig op orde is gebracht Omdat 90% van de gemeenten al aan de meeste normen voldeed, vertrouwt de VNG erop dat de resterende 30% nu ook snel de noodzakelijke maatregelen zal implementeren.
De VNG wil dat gemeenten bij voorkeur de informatiebeveiliging en borging van de privacy gemeentebreed aanpakken Werken met naast elkaar bestaande sectorale aanpakken zoals die van Suwi is volgens hen suboptimaal vanuit het perspectief van zowel kwaliteit als kosten In dat verband wijst de VNG op de Baseline Informatiebeveiliging Gemeenten (BIG) en de Eenduidige Systematiek Single Informatie Audit (ENSIA)

De VNG is het niet eens met de wijze waarop de Inspectie invulling geeft aan norm 13 5 Volgens VNG valt uit de norm niet af te leiden dat er analyses tot op accountniveau zouden moeten plaatsvinden, en zou primair moeten kunnen worden volstaan met de generieke rapportages van BKWI Ook is nergens bepaald dat de grens voor opvallend afwijkend zoekgedrag zou moeten liggen op het gemiddelde plus de standaarddeviatie Verder constateert VNG dat de gemeenten een steeds breder takenpakket krijgen toebedeeld, zonder dat daar een toereikend informatie-arrangement tegenover staat Concreet wijst de VNG op het ontbreken voor een grondslag om Suwinet te raadplegen voor het gebruik van schuldhulpverlening en de wet Taaleis (nu onderdeel van de Participatiewet). Verder wijst de VNG erop dat het faciliteren van gemeenten met DKD-Inlezen een taak is voor het Inlichtingen-bureau en niet voor BKWI De VNG is met de Inspectie van mening dat de controle op het gebruik van gegevens van DKD-Inlezen kan worden verbeterd Dat kan het beste gebeuren door de partijen die betrokken zijn bij DKD-Inlezen, via de gebruikersoverleggen van gemeenten en de leveranciers van hun applicaties

Divosa vindt het bemoedigend dat gemeenten nu veel beter de zeven essentiele normen uit het normenkader naleven dan voorheen Aan de andere kant vindt Divosa de resultaten nog steeds zorgelijk. Divosa wil graag meer aandacht besteden aan het aspect van integer handelen, zowel in hun bijeenkomsten, als in het programma Vakmanschap, als in directe contacten met de leden Divosa constateert dat de 3D-wetgeving, de wijzigingen van de WBP en de Europese verordening, een omslag vereisen in het denken over privacy Divosa zegt aan te sluiten op de zorgpunten van VNG, waar het gaat om de uitsluiting van toegang tot Suwinet voor gemeentelijke taken als schuldhulpverlening en de Wet taaleis Divosa vindt dit niet uit te leggen aan de burger en de uitvoering Uitsluiting van toegang levert bovendien extra administratieve lasten en bureaucratisering op

- ***Naschrift Inspectie***

De Inspectie stelt vast dat de bestuurlijke reacties vooral betrekking hebben op de richting die de ontwikkeling van de informatievoorziening en de beveiliging daarvan zou moeten nemen. Een grote gemene deler is de opvatting dat er sprake moet zijn van, zoals UWV dat verwoordt "een integraal veilig gebruik van gegevens, ongeacht de voorzieningen waarmee gegevens worden uitgewisseld " VNG wijst in dit verband op de mogelijkheden die BIG en ENSIA bieden. Daarnaast vragen met name VNG en Divosa om verruiming van de mogelijkheden om Suwinet in te zetten voor andere gemeentelijke taken dan sec de uitvoering van de Participatiewet Met name de laatste wens speelt zich af op het scheidvlak van doelmatigheid en doeltreffendheid enerzijds, en de wens om de privacy te beschermen anderzijds Die verruiming overstijgt de verantwoordelijkheid van het ministerie SZW.

VNG heeft kritiek op de operationalisatie die de Inspectie heeft toegepast op norm 13 5 De norm bevat alleen de term controle De Inspectie is van mening dat de controle ook betrekking dient te hebben op de raadplegingen op accountniveau Controle op accountniveau is van belang om een (meer) sluitende controle uit te voeren De huidige generieke rapportages die BKWI voor gemeenten opstelt geven geen informatie over het gebruik op accountniveau Een controle die zich alleen beperkt tot de analyse van de generieke rapportages acht de Inspectie in de huidige situatie dan ook als te beperkt

De Inspectie stelt vast dat de vraag of sprake is van opmerkelijk inloggedrag, alleen kan worden vastgesteld in relatie tot de vraag wat buiten het "normale" ligt In de statistiek hanteert men het begrip standaarddeviatie. Vaker zoeken dan het gemiddelde plus de standdaarddeviatie levert bij een normale verdeling altijd ongeveer 16% van de populatie op Hoewel niet te allen tijde sprake is van een normale verdeling, acht de Inspectie dit een aanvaardbare praktische grens voor de bepaling van wat opvallend is en wat niet

De Inspectie heeft in dit verband gesproken met BKWI en de beleidsdirectie van SZW om de bestaande generieke rapportage aan te passen Deze aanpassing zou betekenen dat de generieke rapportage wordt uitgebreid met informatie op accountniveau en een standaarddeviatie .
De door de Inspectie opgevraagde rapportages naar opvallend zoekgedrag van accounts, is ingezet als hulpmiddel, naast de beoordeling van bewakingsprocessen van de gemeenten. Als een gemeente de bewaking goed heeft ingericht, dan is een enkel afwijkend account dat niet is opgemerkt, geen aanleiding tot afkeuring geweest.

Bijlagen

Bijlage 1 Bestuurlijke reacties

Inspectie SZW
Directie Werk en Inkomen
Programma B
T.a.v. de heer J. Urselmann
Postbus 90801
2509 LV DEN HAAG

Onze referentie:	160158
Uw referentie:	2016-0000094025
Datum:	20 april 2016
Onderwerp:	Suwinet 2015 vervolgstudie 'veilig omgaan met elkaars gegevens'
Van:	Yvette Bommeljé | T 06 - 3730 2337 | ybommelje@divosa.nl

Geachte heer Urselmann,

Wij hebben het concept rapport Suwinet 2015, vervolgonderzoek, van u ontvangen. We geven graag onze reactie. Deze is afgestemd met onze leden via het Algemeen Bestuur, de commissie ICT en afgestemd met de reactie van de VNG.

Algemeen
Het is bemoedigd te zien dat de gemeenten nu veel beter de zeven essentiële normen van het Suwinormenkader naleven dan voorheen. De extra inspanningen van alle betrokken partijen, waaronder ook die van uw Inspectie, hebben daar zeker aan bijgedragen. Aan de andere kant vindt Divosa de resultaten van het onderzoek nog steeds zorgelijk. Uw Inspectie heeft in onze Algemene Ledenvergadering van 5 februari jl. met ons gesproken over onder andere dit onderzoek. De bestuursleden hebben toen aangegeven dat de verbeteringen helaas niet gaan in het tempo en mate die ze hadden verwacht en gehoopt. In Divosaverband gaan we, geïntensiveerd, verder met het onder de aandacht brengen van het onderwerp bescherming persoonsgegevens.

U geeft aan dat de uitslag van het onderzoek bij de individuele gemeenten als een positieve prikkel heeft gewerkt, omdat gemeenten nog na de meting hebben gemeld dat zij tekortkomingen alsnog op orde hebben gebracht. Idealiter zou het niet zo moeten zijn dat Inspectie-onderzoek en het escalatieprotocol de functie hebben als stok achter de deur om het normenkader na te leven. Het belang van bescherming van persoonsgegevens van burgers, zeker van kwetsbare burgers, en de bijbehorende gedragsregels horen in het DNA van de gemeentelijk medewerker te zitten. U wijst terecht op gedrags- en cultuuraspecten die daarvoor belangrijk zijn. Divosa wil dan ook met name aan dit aspect, het integer handelen, prominenter aandacht besteden, zowel in onze bijeenkomsten, het programma Vakmanschap als in de directe contacten met onze leden.

Veilig omgaan met Suwinet staat niet op zichzelf maar is voor Divosa onderdeel van integer omgaan met gegevens van burgers in het brede sociale domein. De nieuwe 3D-wetgeving, de wijzigingen in de Wet Bescherming Persoonsgegevens en de Europese verordening vereisen een omslag in het denken over privacy. Samen met onze partners zoeken wij naar een nieuwe inrichting voor het gegevensverkeer in het sociaal domein met respect voor de privacy voor burgers en gericht op een effectieve dienstverlening.

Aandachtspunten
Graag sluiten wij tenslotte aan bij de zorgpunten die de VNG noemt. Met name de uitsluiting van het gebruik voor de schuldhulpverlening en de Wet Taaleis, notabene onderdeel van de Participatiewet, is niet uit te leggen. Niet aan burgers en niet aan de uitvoering. Dit zadelt alle partijen met onnodige administratieve lasten op, terwijl het rijksbeleid toch juist gericht is op ont-bureaucratisering. We gaan ervan uit dat de wetgever dit snel kan regelen, waarna gemeenten en BKWI een gerichte set gegevens kan ontsluiten voor deze taken.

Het is ons niet bekend of u dit jaar het onderzoek weer herhaalt. Zo ja, dan blijven wij graag betrokken.

Met vriendelijke groet,
Verenigingsbureau Divosa

Mevrouw O.A.A. Bartelds
directeur

Stichting Inlichtingenbureau
Informatieknooppunt Gemeenten

Ministerie van Sociale Zaken en Werkgelegenheid
T.a.v. de waarnemend Inspecteur-Generaal SZW
De heer drs. A. van Dijk
Postbus 90801
2509 LV Den Haag

St. Jacobsstraat 400-420
3511 BT Utrecht
Postbus 19247
3501 DE Utrecht

Telefoon 088 751 37 00
www.inlichtingenbureau.nl
KvK 27244197

Betreft : Reactie op vervolgonderzoek Suwinet 2015: veilig omgaan met elkaars gegevens
Uw kenmerk :
Ons kenmerk : IB16-79
Bijlage(n) :
Datum : 7 april 2016

Geachte heer Van Dijk,

Op uw verzoek reageer ik hierbij op de conclusies van het Suwinet 2015 vervolgonderzoek veilig omgaan met elkaars gegevens. In de eerste plaats wil ik graag mijn waardering uitspreken voor de wijze waarop de Inspectie SZW in een beperkte tijd dit omvangrijke en complexe onderzoek heeft uitgevoerd. Het onderzoek brengt helder in beeld op welke wijze gemeenten uitvoering en invulling geven aan zeven essentiële normen uit het normenkader GeVS. Uw Inspectie stelt terecht vast dat deze normen kunnen gelden als de professionele standaard voor alle SUWI-partijen op het gebied van beveiliging en privacy.

Het Inlichtingenbureau constateert met uw Inspectie dat sprake is van een forse toename van het aantal gemeenten dat aan de afzonderlijke normen voldoet en ook van het aantal gemeenten dat aan alle zeven normen voldoet. Tegelijkertijd moet worden vastgesteld dat een aantal gemeenten nog een eindsprint zal moeten inzetten om aan te sluiten bij de gemeenten die hun privacybescherming en informatiebeveiliging aantoonbaar goed op orde hebben.

Voor het Inlichtingenbureau zijn privacybescherming en informatiebeveiliging kernelementen van de dienstverlening. Zowel aan onze producten als aan het gebruik dat gemeenten daarvan maken stellen wij daarom hoge eisen. In ons jaarplan 2016 wordt ingezet op beperking van gegevensleveringen op basis van de gedachte 'less is more' en op voorlichting ten aanzien van de wettelijke gebruiksdoelen, met name met betrekking tot de verstrekking van dossierpersoon-berichten in het kader van het digitaal klantdossier. Het Inlichtingenbureau biedt met informatieproducten zoals aanvraagtoetssignalen en incasso-ondersteuning bijstandsdebiteuren ondersteuning van specifieke gemeentelijke werkprocessen op basis van doelbinding, waardoor het voor deze werkprocessen op termijn niet meer nodig is complete generieke klantdossiers te raadplegen via Inkijk-functionaliteit of te importeren via Inlees-functionaliteit.

Stichting Inlichtingen*bureau*
Informatieknooppunt Gemeenten

Voor gemeenten is niet altijd duidelijk dat zij DKD-inleesberichten alleen mogen inzetten voor de uitvoering van de Participatiewet. Het Inlichtingenbureau zal in goed overleg met BKWI en de VNG via een communicatiecampagne aandacht besteden aan de werking, gebruik en voorwaarden met betrekking tot het digitaal klantdossier en overige SUWI-gegevens. Specifieke aandachtspunten zijn daarbij privacyaspecten zoals doelbinding, informatiebeveiliging en het creëren van een klimaat waarin alle betrokken partijen (stakeholders) een positief beeld hebben met betrekking tot de verwerking van persoonsgegevens in de SUWI-keten.

Het Inlichtingenbureau vindt het belangrijk om als onafhankelijke instantie gemeenten van advies te kunnen voorzien, zonder daarbij in de rol van toezichthouders te treden. Tegelijkertijd constateren wij dat de doelen van onze stichting, gemeenten en toezichthouders in hoge mate gelijkluidend zijn.

Het gaat er volgens ons met name om op praktische wijze te stimuleren dat centrale en decentrale SUWI-voorzieningen rechtmatig en veilig worden gebruikt. Wij blijven daar in goede samenspraak met uw Inspectie en de Autoriteit Persoonsgegevens graag een bijdrage aan leveren, zodat uiteindelijk ook de laatste gemeenten aantoonbaar zorgvuldig omgaan met persoonsgegevens van burgers.

Met vriendelijke groet,

Drs. R. de Groot
Bestuursvoorzitter Stichting Inlichtingenbureau

Postbus 58285, 1040 HG Amsterdam

Datum
20 APR. 2016

Ons kenmerk
SBK/93652/AM

Aan het Ministerie van Sociale Zaken en Werkgelegenheid,
T.a.v. de waarnemend Inspecteur-Generaal, de heer drs. A. van Dijk
Postbus 90801
2509 LV DEN HAAG

Onderwerp
Bestuurlijke reactie Rapport Suwinet 2015 vervolgonderzoek 'veilig omgaan met elkaars gegevens'

Geachte heer van Dijk,

Met uw brief van 4 april 2016 heeft u ons de conceptrapportage Suwinet 2015 vervolgonderzoek 'veilig omgaan met elkaars gegevens' toegestuurd. U vraagt ons om bestuurlijk op het rapport te reageren.
Naast een algemene reactie op de conclusies uit het rapport, reageren wij (als verantwoordelijke voor het beheer van Suwinet) in deze brief op een aantal specifieke punten die van toepassing zijn op het beheer van Suwinet. In de bijlage vindt u nog een aantal inhoudelijke aanvullingen en correcties op het rapport.

Algemene reactie
Wij vinden het positief dat de Inspectie constateert dat er een significante verbetering heeft plaatsgevonden onder gemeenten wat betreft een veilig gebruik van gegevens die via Suwinet-inkijk worden ingezien. Bijna de helft van alle gemeenten voldeed in 2015 aan de zeven essentiële normen. In 2014 voldeed nog maar 17 procent van de gemeenten aan deze zeven normen en in 2013 werd door bijna de helft van de gemeenten nog aan slechts nul of één norm voldaan.
De bevinding dat bijna de helft van de gemeenten in 2015 voldeed aan de zeven normen, betekent echter ook dat de helft van de gemeenten in 2015 één of meerdere normen nog niet behaalde. Wij vinden het dan ook van groot belang dat gemeenten, en andere overheidsinstanties, structurele verbeteringen blijven doorvoeren om de beveiliging en privacy van gegevens op het gewenste niveau te brengen, en te houden.
Binnen de Suwi-sector wordt hier ook invulling aan gegeven. Voor de uitwisseling van gegevens via Suwinet geldt dat VNG, SVB en UWV gezamenlijk uitvoering geven aan het programmaplan 'Borging veilige gegevensuitwisseling via Suwinet'. In dit programma wordt o.a. gewerkt aan de verbetering van (de benutting van) gebruikersrapportages en logging van gegevensgebruik, een herijking van het normenkader waar partijen zich aan moeten houden, verschillende maatregelen om de gegevensuitwisseling meer proportioneel in te richten (bijv. de doorontwikkeling van filtermogelijkheden) en een ketenbrede awarenesscampagne.
Wel constateren wij dat er meer aandacht zou moeten komen voor een integraal veilig gebruik van gegevens, ongeacht de voorzieningen waarmee gegevens worden uitgewisseld. Zo benoemt de Inspectie in het rapport dat de huidige wet- en regelgeving op het gebied van gegevensuitwisseling, op dit moment niet goed aansluit bij de praktijk van integraal beleid bij gemeenten. Wij denken dat verbeteringen op dit punt ook zullen bijdragen aan een hogere kwaliteit van de privacy en beveiliging van gegevens bij overheidsinstanties.

Beheer van Suwinet
Het onderzoek van de Inspectie ziet toe op het gebruik van gegevens via de voorziening Suwinet-inkijk. De inleesvoorzieningen (Suwinet-inlezen en DKD-inlezen) worden buiten beschouwing gelaten De Inspectie merkt in het rapport wel op dat de beveiliging van het gebruik van gegevens via DKD-inlezen door gemeenten vragen oproept Hierbij wordt verwezen naar het rapport van de Autoriteit Persoonsgegevens en het Plan van Aanpak van UWV om de beveiliging op dit punt te verbeteren. In overleg met het Ministerie van SZW en andere betrokken partijen is besloten om het Plan van Aanpak in eerste instantie toe te passen op de vier afnemers die via BKWI op Suwinet-Inlezen zijn aangesloten Op dit moment zijn wij met de betrokken partijen in overleg om de aanpak te verbreden naar de gemeenten die via het Inlichtingenbureau op DKD-inlezen zijn aangesloten. De verbreding van de scope wordt opgepakt binnen het Programmaplan 'Borging veilige gegevensuitwisseling via Suwinet'

Hoogachtend,

mr. drs B J Bruins
Voorzitter Raad van Bestuur

Bijlage Aanvullingen en correcties op de conceptrapportage

Vereniging van
Nederlandse Gemeenten

Inspectie SZW
drs. A. van Dijk
Postbus 90801
2509 LV 'S-GRAVENHAGE

doorkiesnummer	uw kenmerk	bijlage(n)
(070) 373 8696	2016-0000082407	1
betreft	**ons kenmerk**	**datum**
Suwinet 2015 vervolgonderzoek 'Veilig omgaan met elkaars gegevens'	ECIB/U201600649	20 april 2016

Geachte heer Van Dijk,

Hierbij ontvangt u de bestuurlijke reactie van de VNG op het inspectieonderzoek 'Suwinet 2015, vervolgonderzoek veilig omgaan met elkaars gegevens'. We danken u voor de flexibiliteit ten aanzien van de aanleverdatum van deze bestuurlijke reactie. Dit gaf ons gelegenheid de reactie goed af te stemmen met een aantal belangrijke gemeentelijke gremia. Deze reactie is afgestemd met de G4, de G32 de leden van de VNG-commissies Werk en Inkomen en Divosa en gedeeld met SZW, UWV, BKWI en SVB. . Als bijlage bij de bestuurlijke reactie van de VNG ontvangt u de brief 'Vooraankondiging aanwijzing Rotterdam' die het college van B&W van de gemeente Rotterdam aan staatssecretaris Klijnsma verstuurde. Hierop komen wij later in deze brief terug.

Reactie op hoofdlijnen

Wij danken u voor het toezenden van het concepteindrapport. Wij zijn van mening dat het een goede zaak is dat dit vervolgonderzoek nu is uitgevoerd onder alle gemeenten. Het heeft de reeds op gang gekomen verbeterslag verder verbreed (meer gemeenten verbeteren) en in een stroomversnelling gebracht (gemeenten verbeteren in een hoger tempo). Wij vinden het positief te constateren dat in de onderzoeksperiode 1 september 2014 – 1 september 2015 49% van de gemeenten aan alle 7 onderzochte normen voldoet, na 17% in het jaar ervoor. Dit is een verdrievoudiging.
Wij vinden het ook positief te vernemen dat veel gemeenten na het afsluiten van de onderzoeksperiode zijn blijven verbeteren om aan alle van de 7 onderzochte normen te kunnen voldoen. Dit sluit aan bij de signalen die wij zelf van gemeenten hebben ontvangen. U geeft aan dat in op basis van de door u ontvangen meldingen na afloop van het onderzoek nu in totaal 70% van de gemeenten aan de 7 onderzochten normen zou voldoen. Wij zien hier een duidelijk verband met het handhavingsbeleid van het ministerie en hebben er vertrouwen in dat de resterende 30% nu ook snel het been zal bijtrekken. Uit uw onderzoek bleek immers dat meer dan 90% al aan de meeste onderzochte normen voldeed.

Baseline Informatiebeveiliging Gemeenten (BIG) en Eenduidige Normatiek Single Information Audit (ENSIA)

BIG

Gemeenten willen informatiebeveiliging en borging van de privacy bij voorkeur gemeentebreed aanpakken Werken met naast elkaar bestaande sectorale aanpakken zoals die van suwi is suboptimaal vanuit het perspectief van zowel kwaliteit als kosten Daarom implementeren gemeenten in de volle breedte de Baseline Informatiebeveiliging Gemeenten (BIG) of hebben zij dit reeds gedaan Dit wil niet zeggen dat het Suwi-normenkader daarmee niet relevant meer zou zijn Integendeel, de 7 onderzochte Suwi-normen maken ook onderdeel uit van de BIG Bijvoorbeeld informatiebeveiligingsbeleid en -plan zouden niet apart gerealiseerd moeten worden voor uitsluitend Suwinet, maar is bij voorkeur gemeentebreed van toepassing binnen dit plan wordt specifiek aandacht geschonken aan Suwinet Het is voor ons positief te kunnen constateren dat de toetsing van de inspectie op deze benadering aansluit Samen met UWV en SVB brengen gemeenten de specifieke normenkaders in overeenstemming met de generieke normenkaders zoals BIG en BIR (Baseline Informatiebeveiliging Rijk) Motto daarbij is generiek waar het kan, specifiek waar het moet

ENSIA

Het programma ENSIA richt zich op de vraag hoe de overheid – waaronder gemeenten – zich langs de lijnen van een brede inhoudelijke aanpak het beste kan verantwoorden Voor gemeenten geldt dat zij zich ten principale aan de gemeenteraad verantwoorden Verticaal toezicht naar bevoegd gezag als het ministerie of in het verlengde daarvan de inspectie zou in beeld moeten komen wanneer horizontaal toezicht in voorkomende gevallen niet effectief blijkt ENSIA richt zich erop om gemeenten toe te rusten voor de wijze waarop zij de gemeenteraad zo goed mogelijk van informatie kunnen voorzien Het is voor ons positief te kunnen constateren dat SZW ook voorstander is van de aanpak zoals voorzien door ENSIA en hieraan samen met VNG en gemeenten een wezenlijke bijdrage levert ENSIA zal geïmplementeerd worden per 1 januari 2017

Drie zorgpunten

Mede naar aanleiding van dit onderzoek constateren wij nog wel drie zorgpunten, waarvoor we bestuurlijke aandacht willen vragen Het betreft wettelijke grondslagen voor gegevenswisseling, de toetsing van norm 13 5 en DKD-Inlezen Hieronder werken wij dit verder uit

Zorgpunt 1: Wettelijke grondslagen voor gegevenswisseling

We zien steeds vaker dat gemeenten in het veld van werk en inkomen taken krijgen toebedeeld zonder dat er een passend informatiearrangement bij wordt geboden een wettelijke grondslag en invulling daarvan Conform de Wet Bescherming Persoonsgegevens mogen gemeenten zonder een ingevulde grondslag geen gebruik maken van clientgegevens waarover de overheid reeds beschikt, ook niet via Suwinet Voorbeelden hiervan zijn

- De wet op de gemeentelijke schuldhulpverlening Deze trad in werking op 1 juli 2012 De grondslag voor een AMvB gegevenswisseling is tot op heden ondanks herhaalde verzoeken niet ingevuld Het helpt schuldhulpverleners enorm wanneer de inkomenssituatie van de client snel beschikbaar is Dat verkort de doorlooptijd van trajecten voor clienten en daarmee wachttijden voor trajecten voor andere clienten
- De wet Taaleis (nu onderdeel van de Participatiewet) Deze wet voorziet niet in een grondslag op basis waarvan gemeenten opleidingsgegevens van DUO mogen gebruiken om te bepalen of een client aan de taaleis voldoet of niet Met name opleidingsgegevens met betrekking tot basis- en middelbare school zijn hierbij relevant Deze zijn niet opgenomen in Suwinet Vanaf 1

juli moet het volledige zittend bestand doorgelicht worden Dat is een tijdrovende klus waarbij gemeenten niet kunnen voorkomen dat zij clienten bevragen op gegevens die de overheid al van hen heeft

Het onrechtmatig raadplegen van Suwinet (of een ander systeem) hangt samen met de mate waarin wettelijke grondslagen voor gegevenswisseling goed aansluiten op wettelijke taken Bij een aantal wettelijke taken is daarin nu niet adequaat voorzien Dit heeft als consequentie dat gemeenten in een situatie gebracht worden waar zij ofwel niet aan in dit geval Suwi-normen kunnen voldoen (omdat zij Suwinet hiervoor raadplegen), ofwel de Wet Eenmalige Gegevensuitvraag overtreden (omdat zij de client dubbel bevragen) of hun wettelijke taak niet of onvoldoende uitvoeren (omdat ze noch Suwinet of een ander systeem raadplegen noch de client dubbel bevragen) Gemeenten kunnen het feitelijk niet goed doen

Wij verwijzen hierbij ook naar de bijgevoegde brief van het college van B&W van de gemeente Rotterdam, die aangeeft wat de implicaties zijn van deze situatie voor de gemeente en haar clienten Rotterdam is hierin niet exemplarisch, veel gemeenten hebben hun zorgen hierover mondeling bij de inspectie en de VNG geuit De VNG beschouwt dit als een steeds vaker voorkomend punt van zorg en vraagt het ministerie om bij elke (nieuwe) wettelijke taak te voorzien in een passend informatiearrangement met een daarbij behorende ingevulde wettelijke grondslag

Zorgpunt 2: Toetsing van norm 13.5

Op één punt verschilt de VNG van mening met de inspectie waar het gaat om de interpretatie van de normen Dit betreft norm 13 5 controle op autorisatie en gebruik De VNG is van mening dat gemeenten op een hoger niveau zijn getoetst dan norm 13 5 voorschrijft en op basis van informatie die wel aan de inspectie, maar niet aan gemeenten is verstrekt

- Gemeenten zijn getoetst op het controleren op accountniveau (logginggedrag van individuele medewerkers) De formulering van norm 13 5 luidt de controle op verleende toegangsrechten en gebruik vindt meerdere keren per jaar plaats Dat zou in beginsel ook kunnen door uitsluitend een generieke rapportage te gebruiken
- Daarbij is door de SZW Inspectie informatie gebruikt die aan gemeenten niet ter beschikking wordt gesteld in de generieke of specifieke rapportage Gemeenten beschikken over landelijke gemiddelden van alle gemeenten, van gemeenten met een vergelijkbaar inwoneraantal en van gemeenten met een vergelijkbaar aantal autorisaties De standaarddeviatie (gemiddelde afwijking van het gemiddelde) maakt geen deel uit van deze informatie Gemeenten kunnen in absolute zin zien hoeveel zij afwijken van het gemiddelde, maar niet in hoeverre dit zich verhoudt tot afwijkingen bij andere gemeenten

Vanuit VNG is gemeenten steeds geadviseerd om vanuit kennis van de eigen werkprocessen de afwijkingen van het gemiddelde te interpreteren en zo te beoordelen of deze aanleiding gaf tot nader onderzoek Gemeenten die op deze wijze de controles hebben verricht kunnen daardoor in het betreffende onderzoek niet aan de toets door de inspectie hebben voldaan Daarbij heeft de inspectie de VNG desgevraagd niet duidelijk kunnen maken waarom de grens voor afwijkend opvraaggedrag zou liggen bij meer dan eenmaal de standaarddeviatie van het gemiddelde Dit is de waarde waarop de inspectie getoetst heeft

Hoe nuttig het steekproefsgewijs controleren op accountniveau ook kan zijn, norm 13 5 schrijft dit niet standaard voor Daarmee komen we voor dit punt tot de conclusie dat gemeenten zijn getoetst op een niveau dat verder gaat dan de norm voorschrijft, op een grenswaarde die niet onderbouwd is en met

behulp van informatie waarover zij zelf niet beschikken Wij vragen aan het ministerie om op gemeenten die naar aanleiding hiervan niet aan de norm voldoen dan ook ten aanzien van deze norm niet het escalatieprotocol toe te passen

Zorgpunt 3: DKD-Inlezen

Op pagina 14 beschrijft u onder andere DKD-inlezen U geeft daarbij aan dat UWV ten behoeve van de Autoriteit Persoonsgegevens een plan van aanpak heeft opgesteld voor het verbeteren van de controle op het gebruik van Suwinet- en DKD-inlezen door afnemende partijen Wij hechten eraan om te benoemen dat het faciliteren van gemeenten met DKD-inlezen niet tot de taken van het UWV en BKWI behoort maar tot die van het Inlichtingenbureau Via deze route ontvangen gemeenten gegevens die zij inlezen met behulp van applicaties die betrokken worden uit de markt Wij zijn met UWV en de Inspectie van mening dat controle op het gebruik van ingelezen gegevens meer aandacht behoeft De meest effectieve route om dit te bereiken is in onze beleving echter via partijen die zelf betrokken zijn bij DKD-inlezen Wij bedoelen hiermee de gebruikersoverleggen van gemeenten met de betreffende leveranciers van deze applicaties Wij zijn voornemens om de voorzitters van deze gemeentelijke gebruikersoverleggen hierover aan te schrijven en hopen dat daarmee in samenspraak tussen afnemers en aanbieders controlefunctionaliteiten zullen worden ingeregeld c q verder worden doorontwikkeld en aangescherpt Wij zullen hier alert op blijven

Kortom

Wij beschouwen het onderzoek 'Suwinet 2015, veilig omgaan met elkaars gegevens' als een positieve stimulans voor gemeenten om zich in brede zin te blijven ontwikkelen ten aanzien van informatiebeveiliging en het borgen van privacy Wij zijn verheugd met de vooruitgang die is geconstateerd Tegelijkertijd hebben wij zorgen over de randvoorwaarden waaronder gemeenten van dit systeem gebruik kunnen maken (wettelijk kader), de wijze waarop een van de normen is getoetst (13 5) en tenslotte de wijze waarop de oplossingsrichting ten aanzien van de controle op DKD-Inlezen wordt benoemd

Mocht deze bestuurlijke reactie bij u leiden tot aanvullende vragen of opmerkingen zijn wij uiteraard bereid om deze mondeling verder toe te lichten

Hoogachtend,
Vereniging van Nederlandse Gemeenten

J Kriens
Voorzitter directieraad

Bijlage brief gemeente Rotterdam 'Vooraankondiging aanwijzing Rotterdam'

Gemeente Rotterdam
College van Burgemeester en Wethouders

Bezoekadres: Stadhuis Coolsingel 40
3011 AD Rotterdam
Postadres: Postbus 70012
3000 KP Rotterdam

Website: www rotterdam nl
E-mail: dimbsd@rotterdam nl
Fax: 010 – 267 35 60
Inlichtingen: drs M G C M Castelijns
Telefoon: 010 - 453 35 31
Ons Kenmerk: 16bb2647

Dienst: W&I

Datum: B&W12 april 2016

Betreft: Vooraankondiging aanwijzing Rotterdam

Aan de Staatssecretaris van Sociale Zaken en
Werkgelegenheid, mevrouw Jetta Klijnsma
Postbus 90801
2509 LV DEN HAAG

13 APR 2016

Geachte mevrouw Klijnsma,

In uw brief van 14 maart jl. (kenmerk 2016-0000074974) maakt u bekend dat u voornemens bent een aanwijzing aan de gemeente Rotterdam te geven omdat wij naar het oordeel van de Inspectie SZW niet voldoen aan norm 13 1 uit het Normenkader behorende bij de Verantwoordingsrichtlijn Gezamenlijke elektronische Voorzieningen Suwi (GeVS)
U vraagt aan ons college om binnen acht weken een verklaring toe te sturen, waaruit blijkt dat onze gemeente inmiddels voldoet aan alle zeven door de Inspectie SZW onderzochte normen

Naar aanleiding van uw brief melden wij u dat de gemeente Rotterdam met ingang van 1 mei 2016 zal stoppen met het verlenen van toegang tot Suwinet aan ambtenaren die werkzaam zijn op het gebied van nazorg aan ex-gedetineerden en schuldhulpverlening. Met de effectuering van dit collegebesluit voldoet onze gemeente per 1 mei 2016 aan alle zeven door de Inspectie SZW gestelde normen

Wij betreuren het dat de Inspectie SZW in haar verslag van bevindingen van 25 februari jl niet inhoudelijk ingaat op de door Rotterdam aangedragen (wettelijke) tekortkomingen in de huidige regelgeving Ook in uw brief van 14 maart jl. gaat u daar niet op in Om die reden brengen wij de knelpunten die gemeenten ervaren bij de gegevensuitwisseling nogmaals onder uw aandacht.

Nazorg aan ex-gedetineerden
Zowel door rijk als gemeenten wordt onderkend dat er bij de uitvoering van het convenant tussen de VNG en het Ministerie van V&J inzake de nazorg aan ex-gedetineerden knelpunten in de gegevensuitwisseling zijn Juist om die reden is er een ambtelijke taskforce ingesteld, waarin enkele ministeries (waaronder SZW) en gemeenten (VNG, G4) vertegenwoordigd zijn De taskforce komt op korte termijn met een advies dat gemeenten en de Dienst Justitiële Inrichtingen de mogelijkheid geeft om op rechtmatige wijze persoonsgegevens te verwerken Hopelijk draagt dit advies ertoe bij dat genoemde knelpunten bij de uitvoering van het convenant binnen afzienbare tijd worden opgelost

Wet gemeentelijke schuldhulpverlening (Wgs)
Bij de inwerkingtreding van de Wgs in 2012 is een AMvB in het vooruitzicht gesteld, op grond waarvan het aan gemeenten toegestaan zou zijn om Suwinetgegevens te gebruiken voor de uitvoering van de schuldhulpverlening. Deze regeling is er nog steeds niet, ondanks aandringen van VNG, Divosa en NVVK
Wij verzoeken u te bevorderen dat deze AMvB op korte termijn alsnog tot stand komt. Rotterdam is graag bereid mee te denken over de inhoud van deze regeling

Wet taaleis
Het komt overigens regelmatig voor dat gemeenten een nieuwe wettelijke taak opgedragen krijgen zonder dat er gezorgd is voor een passend informatie-arrangement Het gevolg is dat gemeenten niet over de vereiste informatie beschikken om deze taak goed uit te kunnen voeren
Het hierboven genoemde knelpunt bij de schuldhulpverlening is hiervan een treffend voorbeeld, een ander recent voorbeeld betreft de uitvoering van de Wet taaleis. Bij de uitvoering van deze wet is het noodzakelijk dat de gemeente vaststelt of een bijstandsgerechtigde beschikt over het vereiste opleidingsniveau om vrijstelling van de taaltoets te kunnen verlenen DUO in Groningen beschikt over die informatie Maar in de wet is niet geregeld dat gemeenten daarover kunnen beschikken Het gevolg is dat gemeenten die informatie (nogmaals) bij de betrokken burger moet opvragen Dat is tijdrovend, kost onnodig gemeenschapsgeld en levert irritatie op bij betrokkenen

Uiteraard is privacy een belangrijk goed en ook gemeenten moeten zich aan de wet houden Maar het is ook van belang dat gemeenten beschikken over de juiste tools om de wettelijk aan hen opgedragen taken goed te kunnen uitvoeren Om die reden is het gewenst dat bij ieder voorstel van het rijk voor een nieuwe gemeentelijke taak een passend informatie-arrangement wordt geboden Dit zou standaard bij het (wets)voorstel moeten worden opgenomen. In theorie besteedt het rijk hier wel aandacht aan, maar de praktijk levert steeds weer nieuwe knelpunten op, zie de voorbeelden hierboven

Wij vertrouwen erop u hiermee voldoende te hebben geïnformeerd

Burgemeester en Wethouders van Rotterdam,

De secretaris,

Ph F M Raets

De burgemeester,

A Aboutaleb

BD 8 02

Bijlage 2 Wettelijk kader

Met de inwerkingtreding van de Wet Structuur uitvoeringsorganisatie werk en inkomen (Wet SUWI) in 2002, is het voor UWV, de SVB en gemeenten mogelijk gemaakt om digitaal gegevens van burgers met elkaar uit te wisselen. Deze gegevensuitwisseling vindt plaats via onder andere het Suwinet Miljoenen keren per jaar raadplegen medewerkers van genoemde organisaties persoonsgegevens ten behoeve van vooral het toekennen, continueren en beeindigen van uitkeringen Zij raadplegen daartoe elkaars databestanden, maar ook de bestanden van onder meer de Belastingdienst, de Rijksdienst voor het Wegverkeer, de Dienst Uitvoering Onderwijs (studiefinanciering), het Kadaster en de Gemeentelijke Basisadministratie persoonsgegevens (GBA) Raadpleging vindt plaats op basis van een wettelijke grondslag.
Elektronische gegevensuitwisseling via Suwinet is onmisbaar om de kwaliteit van integrale dienstverlening in de keten Werk en Inkomen aan burgers te borgen. Aangezien via het Suwinet persoonsgegevens te raadplegen zijn, is het van belang dat hiermee zorgvuldig wordt omgegaan De uitkomsten van eerdere onderzoeken gaven aan dat dit niet het geval is Uit het vorige onderzoek van de Inspectie (over 2014) bleek dat verreweg (83%) de meeste gemeenten niet voldeden aan alle 7 belangrijke normen uit het toetsingskader GeVS

Op grond van artikel 62, eerste lid, Wet SUWI, wisselen het UWV, de SVB en gemeenten persoonsgegevens uit in het kader van de uitvoering van hun wettelijke taken.
Deze SUWI-partijen dragen gezamenlijk zorg voor de instandhouding van de Gemeenschappelijke elektronische Voorzieningen SUWI (GeVS) voor de verwerking van gegevens (artikel 62, tweede lid, Wet SUWI)

Het Besluit SUWI en de Regeling SUWI bevatten nadere regelgeving ten aanzien van de GeVS.

Op grond van artikel 5 21, Besluit SUWI, voert het UWV ten behoeve van de gezamenlijke zorg voor de instandhouding van de GeVS een aantal beheertaken uit Het Bureau Keteninformatisering Werk & Inkomen (BKWI) is belast met deze beheertaken

Op grond van artikel 6 4, Regeling SUWI, dragen het UWV, de SVB, de colleges van B&W, het IB en op de GeVS aangesloten niet SUWI-partijen zorg voor de beveiliging van de gegevensuitwisselingen overeenkomstig hetgeen over de voor het stelsel van maatregelen en procedures te hanteren normen wordt bepaald in bijlage I ('Stelselontwerp & Beveiliging Gezamenlijke elektronische Voorzieningen SUWI')
Het UWV, de SVB, de colleges van B&W, het IB en de aangesloten niet SUWI-partijen dienen ieder in een beveiligingsplan aan te geven op welke wijze zij hieraan invulling geven

Op grond van artikel 6 4, derde lid, Regeling SUWI dienen het UWV, de SVB en het IB jaarlijks te rapporteren over het gebruik en de inrichting van de GeVS Deze rapportage gaat vergezeld van een oordeel van een EDP-auditor.

In het Stelselontwerp is opgenomen dat de SUWI-partijen, onderling en gezamenlijk, met het BKWI afspraken maken op de verschillende deelgebieden van informatie-uitwisseling binnen de SUWI-keten. Uiteindelijk vinden de afspraken hun weerslag in diverse concrete producten, zoals de Verantwoordingsrichtlijn Privacy & Beveiliging GeVS.

De Verantwoordingsrichtlijn bevat tevens het Normenkader GeVS. Dit is een praktische vertaling van de eisen op het gebied van beveiliging en privacy.
De Inspectie SZW beschouwt het Normenkader GeVS als de professionele standaard voor alle SUWI-partijen op het gebied van beveiliging en privacy.

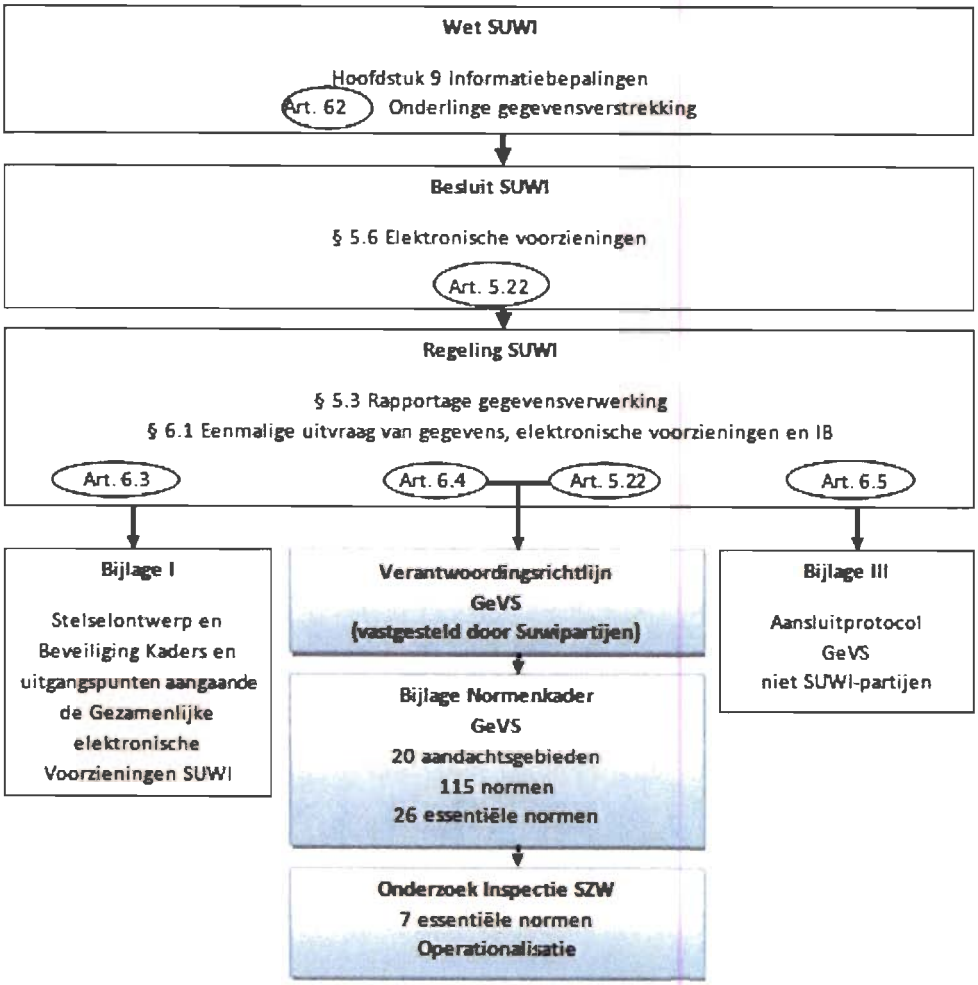
Het normenkader maakt een onderscheid in twintig aandachtsgebieden en maakt tevens een onderscheid in essentiële en niet-essentiële normen. Door SUWI-partijen is aan essentiële normen een zwaarder gewicht toegekend. In de verantwoordingsrichtlijn is bepaald dat een goedkeurend oordeel door een auditor alleen kan worden gegeven, indien uit de bevindingen van alle als essentieel onderkende normen blijkt dat voldaan wordt aan de norm. Bij de overige normen mag er sprake zijn van zgn. niet-materiële tekortkomingen.

De Inspectie heeft in het kader van het onderzoek naar de beveiliging van gemeenten 7 essentiële normen geselecteerd. Deze 7 normen zijn in het kader van dit onderzoek (dat zich richt op de vertrouwelijkheid) de meest relevante.

Organisatie Aandachtsgebieden		Aantal Normen	Aantal essentiële normen	Norm gebruikt in dit onderzoek
1	Organisatorische aspecten	10	6	5
2	Architectuur / Standaarden	4	2	
Ondersteunende processen				
3	Dienstenniveau Beheer	3	-	
4	Capaciteitsbeheer	4	-	
5	Continuïteitsbeheer	5	1	
Beheerprocessen				
6	Configuratiebeheer	4	-	
7	Incident- en probleembeheer	7	2	
8	Wijzigingbeheer	6	3	
9	Testen	6	3	
10	Netwerkbeheer	4	-	
11	Logische toegangsbeveiliging	10	2	2
12	Fysieke beveiliging	2	1	
Functies				
13	Suwinet-Inlezen	10	-	
14	Electronische ketenberichten (EKB's)	5	-	
15	Suwinet-Mail (Ongestructureerde berichten)	6	-	
16	Toegangbeveiliging programmatuur	7	1	
17	Suwinet-Broker	niet verder uitgewerkt	-	
Techniek				
18	Netwerk	8	3	
19	Server	7	-	
20	Koppelingen / koppelpunten	7	2	
Totaal		115	26	7

Tabel: Normenkader GeVS

Van deze 115 normen zijn er 11 (incl. 3 essentiële normen) die alleen betrekking hebben op de beherende taken van BKWI.



Figuur 4 Overzicht toetsingskader

Bijlage 3 Operationalisatie normenkader / werkprogramma

Norm 1.3 Het informatiebeveiligingsbeleid en het beveiligingsplan van het Suwinet zijn goedgekeurd door het management van de Suwi-partij.	
Uitwerking norm	**Controle-activiteiten**
Er is een specifiek op Suwinet gericht informatiebeveiligingsbeleid of veiligheidsplan aanwezig en/of er is een SUWI-specifieke passage aanwezig in een algemeen nformatiebeveiligingsbeleid en -plan *NB We doen geen inhoudelijke beoordeling van het plan en/of de passage*	-Ga na of er een beveiligingsbeleid of -plan is (Let op In ons onderzoek maken we geen onderscheid tussen beide Een beleidsplan vatten we op als beveiligingsplan en andersom) -Ga na of het document specifiek in gaat op Suwinet
Dit beleid, dit plan of deze passage heeft specifiek betrekking op uw gemeente	-Ga na of het stuk over de betreffende gemeente gaat -Ga bij een samenwerkingsverband na of ook de te onderzoeken gemeente wordt genoemd
De goedkeuring van het plan/de passage is formeel vastgelegd Het beleid, het plan of de passage is ondertekend of van de goedkeuring is melding gemaakt in het verslag van de betreffende vergadering	-Ga na of het stuk is getekend door het management òf -Ga na of goedkeuring voor het plan/passage is gegeven door het te bespreken en te accorderen in een vergadering van het management -Ga na of deze accordering is vastgelegd (bijv in de notulen) (Het management is niet gedefinieerd, maar kan zijn betreffende directeur van de gemeente, een MT, het college van B&W, etc In ieder geval moet het stuk zijn goedgekeurd door een ander dan de maker) -Ga de datum na wanneer het plan is goedgekeurd Neem dit expliciet op in de kolom evidence

Norm 1.4 Het informatiebeveiligingsbeleid en het beveiligingsplan van het Suwinet worden uitgedragen in de organisatie	
Uitwerking norm	**Controle-activiteiten**
Het informatiebeveiligingsbeleid, het beveiligingsplan of de beveiligings-passage is aantoonbaar centraal vast-gelegd en beschikbaar voor alle ge-bruikers	-Ga na of het beveiligingsplan, -beleid, -passage centraal beschikbaar is voor alle medewerkers die van Suwinet gebruik maken (staat het bijv op intranet van de gemeente, is het aan alle medewerkers gemaild)
Er is gedurende de onderzoeksperiode minimaal 2x een actie geweest om de gebruikers (opnieuw) te attenderen op het bestaan van het veiligheidsbeleid, -plan of -passage	-Ga na of er acties zijn geweest tussen 1 september 2014 en 1 september 2015 (de onderzoeksperiode) tenminste 2x aandacht is geweest voor het bestaan van het beveili-gingsplan-, -beleid of -passage (gebruik hiervoor bijvoorbeeld hetgeen eventueel in de vastgelegde werkwijze van de gemeente is opgenomen) -Ga na, indien er (nog) geen aandacht voor is geweest, of er voldoende aanwijzingen zijn dat het binnenkort wel zal gebeuren (er is bijv een aankondiging opgesteld, er zijn specifieke data vastgelegd in de door de gemeente overgelegde bewijsstukken, etc) Let op Soms willen gemeenten deze norm invullen door het opsturen van geheimhou-dingsverklaringen Alleen het hebben van een getekende geheimhoudingsverklaring is onvoldoende

Norm 1.5
Het informatiebeveiligingsbeleid en het beveiligingsplan van het Suwinet worden jaarlijks geevalueerd en indien nodig geactualiseerd

N B We doen geen inhoudelijke beoordeling van de evaluatie alleen vaststellen dat er aantoonbaar een evaluatie heeft plaatsgevonden en is vastgesteld

Uitwerking norm	Controle-activiteiten
De laatste evaluatie is minder dan een jaar oud	-Opvragen evaluatie -Controleer de datum van evaluatie -Ga de datum na wanneer het plan is geevalueerd Neem dit expliciet op in de kolom evidence -Datum moet liggen nà 1 september 2014
De laatste evaluatie is vastgesteld door het management	-Opvragen accordering van de evaluatie (bijv evaluatie zelf, notulen, agenda, etc) -Ga na of de accordering is geschied door het management (Het management is niet gedefinieerd, maar kan zijn betreffende directeur van de gemeente, een MT, het college van B&W, etc)
De evaluatie is een concrete actie van alle direct betrokkenen geweest, schriftelijk vastgelegd en leidt zo nodig tot aanpassen van het informatiebeveiligingsbeleid, het beveiligingsplan of de beveiligingspassage	-Opvragen beveiligingsbeleid en -plan, evaluatie en accordering van evaluatie -Ga na of de evaluatie een gezamenlijke actie is geweest van de in de bovengenoemde stukken benoemde functionarissen zoals de security officer, managers, gebruikers, systeembeheerders, etc (we willen uitsluiten dat evaluatie een soloactie is en anderen daar geen weet van hebben) -Raadpleeg de door de gemeente overgelegde bewijsstukken (dat kunnen ook mailwisselingen, goedkeuringsverslagen, etc zijn)

Norm 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 gescheiden zijn belegd - Operationeel beheer - Functioneel beheer - Technisch beheer - Aansturing ICT-leveranciers - Security Officer - Autorisatiebeheer - Eigenaarschap Suwinet	
Uitwerking norm	**Controle-activiteiten**
Er is een schriftelijke vastlegging van de functiescheiding Of er is een onderbouwde verklaring waarom zo'n functiescheiding er niet is en er is een alternatieve aanpak om misbruik te voorkomen (bijv extra controle waar functiescheiding niet of minder goed mogelijk bleek)	-Ga na of in het beveiligingsplan, -beleid of -passage de functiescheiding is opgenomen
In ons onderzoek beperken we ons tot 4 gescheiden functies (i p v de 7 zoals deze in de norm worden genoemd) In principe zijn minimaal de volgende functies bij verschillende personen belegd - uitvoering van taken (het gebruik van Suwinet zoals de klantmanager), - het beheer van autorisaties (toegang verlenen tot Suwinet, de applicatie-beheerder van Suwinet), - kwaliteitszorg en borging van recht-matig gebruik (controle op gebruik van Suwinet, bijvoorbeeld de Security Officer), - management (beslissen over be-voegdheden van functiegroepen, en/of individuele medewerkers, uitdragen belang goed gebruik, bijsturen na oneigenlijk gebruik, optreden na misbruik Suwinet)	-Ga na of minimaal deze 4 functies gescheiden zijn vastgelegd Let op Indien de gemeente minder functies heeft vastgelegd hoeft dit niet automatisch tot een negatieve beoordeling te leiden Zie uitwerking norm in de volgende rij
Er is vastgelegd dat ten aanzien van functiescheiding duidelijke keuzes zijn gemaakt bij het beleggen van taken Of er is een onderbouwde verklaring waarom zo'n functiescheiding er niet is en er is een alternatieve aanpak om misbruik te voorkomen (bijvoorbeeld extra controle waar functiescheiding niet of minder goed mogelijk bleek)	-Ga na of de keuze voor de functiescheiding beargumenteerd is -Ga na, indien er minder functies dan de genoemde 4 zijn gescheiden, of dat logisch is Bijv er is een kleine afdeling waar func-tiescheiding niet goed mogelijk is -Ga na of door de gemeente is herkend dat de functiescheiding niet optimaal is -Ga na of de gemeente extra (controle) maatregelen heeft benoemd om de risico's, gepaard gaande met een beperkte functie-scheiding, te compenseren

Norm 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 geimplementeerd

De Security Officer bevordert en adviseert over de beveiliging van Suwinet, verzorgt rapportages over de status en controleert dat de beveiliging van de Suwinet-maatregelen worden nageleefd, evalueert de uitkomsten en doet voorstellen tot implementatie c q aanpassing van plannen op het gebied van de beveiliging van Suwinet

De Security Officer rapporteert rechtstreeks aan het hoogste management

Uitwerking norm	Controle-activiteiten
De Security Officer is verantwoordelijk gemaakt om periodiek - ten minste 2x per jaar - naar de beveiliging van Suwinet te kijken	-Ga na of er een Security Officer is benoemd binnen de gemeente -Ga na of deze ook specifiek naar de beveiliging van Suwinet zou moeten kijken -Ga na of is vastgelegd dat de Security Officer minimaal 2x per jaar de beveiliging van Suwinet controleert -Ga na of dit is vastgelegd in de functieomschrijving van Security Officer
De Security Officer rapporteert en adviseert periodiek rechtstreeks aan het hoogste management	-Ga na of de Security Officer periodiek rapporteert aan het hoogste management (Het hoogste management is niet gedefinieerd, het gaat erom dat de rapportages van de Security Officer onversneden terecht komen bij het verantwoordelijke management, dus bijv bij een directeur (en niet bij een afdelingshoofd een laag daaronder)
Bovenstaande is vastgelegd in zijn/haar functieomschrijving incl takenoverzicht	-Ga na of er een functieomschrijving is van de Security Officer -Ga na of de taken van de hierboven genoemde 2 rijen in de functieomschrijving terugkomen
Er zijn duidelijk waarneembare en vastgelegde activiteiten van de Security Officer gedurende de onderzoeksperiode	-Ga na of de Security Officer (generieke en/of specfieke) rapportages heeft opgevraagd bij BKWI -Ga na of duidelijk is wat er met rapportages is gebeurd -Ga na of er tussen 1/9/2014 en 1/9/2015 minimaal 1 rapportage van de Security Officer is gestuurd aan het hoogste management -Ga na of de rapportages met geplande periodiciteit, zoals vermeld in de werkwijze van de gemeente, zijn opgeleverd -Ga na of de Security Officer andere activiteiten op het gebied van de beveiliging van Suwinet heeft verricht Raadpleeg hiervoor de door de gemeente overgelegde bewijsstukken (bekijk of er bijv incidenten zijn geweest waar de Security Officer op heeft gereageerd)

Norm 13.1 *De Suwi-partij autoriseert en registreert de gebruikers die toegang hebben tot de Suwinet applicaties op basis van een formele procedure waarin is opgenomen* *-Het verlenen van toegang tot de benodigde gegevens op basis van de uit te voeren functie/taken* *-Het uniek identificeren van elke gebruiker tot één persoon* *-Het goedkeuren van de aanvraag voor toegangsrechten door de manager of een gemandateerde* *-Het tijdig aanpassen of wijzigen van de autorisatie bij functiewijziging of vertrek* *-Het benaderen van de Suwi-databestanden door gebruikers mag alleen plaatsvinden via applicatieprogrammatuur (tenzij sprake is van calamiteiten)*	
Uitwerking norm	***Controle-activiteiten***
Er is een formeel vastgelegde autorisatieprocedure waarin de functies (dus geen personen) aan autorisaties en in het verlengde daarvan aan rollen worden gekoppeld *Vastlegging hiervan geschiedt normaliter in een autorisatiematrix Dit kunnen getekende formulieren zijn, maar ook screenprints van een geautomatiseerd (Role Based Access) systeem zoals Planon*	*-Ga na of er een autorisatieprocedure is* *-Ga na of er een autorisatiematrix is* *-Ga na of met bovenstaande documenten accounts en de toewijzing daarvan (motivatie) tot personen kunnen worden herleid De gemeente moet kunnen aantonen dat medewerkers daadwerkelijk conform hun functie de rollen en de daarbij horende autorisaties toegewezen hebben gekregen* *-Ga na hoeveel medewerkers bevoegdheden kunnen toewijzen en of dit overeenkomt met hun functie (bijv afdelingshoofd, beheerder etc)* *-Ga na of de medewerker die bevoegdheden toewijst (bijv een afdelingshoofd of de beheerder) een andere is dan die de controle uitvoert (bijv de security officer)*
Er vindt controle plaats op inactieve accounts die periodiek worden verwijderd	*-Ga na of er een procedure is voor controle op inactieve accounts* *-Ga na of deze controle minimaal 2x per jaar plaatsvindt* *-Ga na hoeveel medewerkers bij de sociale dienst werken Vergelijk dit met het aantal uitgegeven accounts Indien aantal accounts hoger dan aantal medewerkers achterhaal eventuele verschillen (inactieve accounts, personen met meerdere accounts, medewerkers uit dienst)*
Zware rollen zijn beperkt uitgedeeld *Zie voor meer informatie het document 'Maak optimaal gebruik van de nieuwe gemeentelijke gebruikersrapportages Suwinet'*	*-Ga na of zware rollen beperkt zijn uitgedeeld Dit zijn de rollen waarvan BKWI aangeeft dat het 'risicovolle autorisaties' betreft Beperkt betekent aan een klein aantal medewerkers van de SD Betrek hierbij de verhouding aantal accounts / accounts met speciale bevoegdheden Een indicatie hiervoor is onder meer de verhouding medewerkers sociale dienst / sociale recherche*

	-Ga na of het door de gemeenten opgegeven aantal zware rollen (raadpleeg de door de gemeente overgelegde bewijsstukken) en de opgave van BKWI met elkaar overeen komt *-Indien een gemeente zware rollen 'ruim' heeft ingezet dan hoort daar een verklaring van de gemeente bij waarom zij dat zo hebben gedaan Die verklaring moet in lijn liggen met hetgeen de gemeente in het beveiligingsbeleid en -plan heeft opgesteld* *Zware rollen omvatten* *R1271 (Fraude vorderingen)* *G018 (LRD / GBA zoeken)* *G030 (LRD / GBA zoeken uitgebreid)* *G021 (RDW+ Fraude)* *-Verder kunnen gemeenten in zgn r-rollen samenstellen waarin ook zware autorisaties kunnen voorkomen Ga dit na in de factsheet per gemeente en neem ook deze rollen mee* *-Maak voor bovenstaande gebruik van de loggegevens van BKWI, confronteer dit met het beveiligingsbeleid, -plan of -passage en signaleer eventuele verschillen*
In principe heeft buiten GSD/bijstand-medewerkers slechts een zeer beperkte groep toegang tot Suwinet Deze beperkte groep bestaat uit gemeentelijke belastingdeurwaarders, burgerzaken en de regionale meld- en coordinatiefunctie bij voortijdig schoolverlaters Voor deze groep dient een apart contract te zijn afgesloten met BKWI Dit soort gebruikers zou in de communicatie van de GSD (beveiligingsplan, procedures, autorisatiematrices, etc) niet zichtbaar mogen zijn Voor deze groep geldt dat daar een eigen stroom voor wordt ingericht *Gebruik van Suwinet door overige functionarissen zoals WMO-medewerkers, medewerkers parkeerbeheer of andere hierboven niet benoemde medewerkers is verboden*	*-Loop de autorisatiematrix en de loggegevens van BKWI (generieke rapportage) na op naamgeving van rollen die aanleiding geven door te vragen Denk aan een account met de naam WMO, Deurwaarder, BZ, etc in de naam* *-Vraag de te onderzoeken gemeente om een toelichting bij onduidelijkheden* *-Voor de beperkte groep gebruikers (niet GSD/bijstandaccounts) dient de gemeente afzonderlijke afspraken te maken met BKWI Deze mogen niet voorkomen in de generieke rapportage over het gebruik van Suwinet voor de GSD/Participatiewet*

Norm 13.5 De controle op verleende toegangsrechten en gebruik vindt meerdere keren per jaar plaats -Interne controle op rechten en gebruik van Suwinet -Analyseren van de van het BKWI verkregen informatie over het gebruik van Suwigegevens	
Uitwerking norm	**Controle activiteiten**
Algemeen *Deze norm is soms lastig zwart/wit te beoordelen Bij deze norm geldt niet per definitie dat een negatief oordeel op een deelaspect meteen tot een negatief oordeel leidt op het geheel Probeer de norm in zijn geheel te overzien Maak een duidelijke afweging van hetgeen je hebt gezien Het idee bij deze norm is dat we gevoel willen krijgen of de gemeente ook inhoudelijk kijkt naar de toewijzing van gebruikersrechten en het gebruik van Suwinet Voorbeeld alleen een losstaande vink op een rapportage is wel erg mager Gaat het om meerdere rapportages en heeft de gemeente een procedure hoe zij die controleren dan biedt dat al meer houvast* *Leg wel zelf duidelijk vast wat je hebt waargenomen en wat daarbij je eigen oordeel is Kom je er niet goed uit, leg ook dat vast en bespreek dat met de kwaliteitsborger*	
Een medewerker van de gemeente vraagt ten minste 2x keer per jaar bij BKWI een rapportage over het gebruik van Suwinet-Inkijk op	-Ga in de factsheet per gemeente na wie de gemachtigde en/of Security Officer is van de gemeente -Ga na (in het overzicht per gemeente) of deze persoon tussen 1/9/2014 en 1/9/2015 (de onderzoeksperiode) ten minste 2x een generieke rapportage bij BKWI heeft opgevraagd -Ga na, indien er slechts 1 maal een generieke rapportage is opgevraagd, er voldoende aanwijzingen zijn dat een tweede rapportage wordt opgevraagd (er is bijv al een aankondiging, er zijn specifieke data vastgelegd in de AO, etc)
De beoordeling van deze rapportage (door wie en langs welke criteria) is centraal belegd	-Ga na of er een procedure is aan de hand waarvan deze medewerker de generieke rapportage beoordeelt -Ga na of de criteria in deze procedure (grote verschuivingen, hoge aantallen, verschillen met vergelijkbare gemeenten) voldoende concreet zijn uitgewerkt -Ga na of deze procedure is afgestemd met het management
Deze beoordelaar maakt hiervan schriftelijk verslag	-Ga na of er van deze controle een verslag wordt gemaakt
Als uit dit verslag blijkt dat nadere beoordeling gewenst is, wordt vervolgens bij BKWI een specifieke rapportage opgevraagd die vervolgens wordt beoordeeld	-Controleer het verslag op opvallende zaken -Controleer de generieke rapportage waar het verslag betrekking op heeft -Beoordeel of de medewerker volgens de vastgestelde criteria, terecht wel/geen specifieke rapportage heeft opgevraagd bij BKWI

Er mogen geen opvallende zoekpatronen zijn of, indien dit wel zo is, dient de gemeente daar een duidelijke verklaring voor te geven	-Ga in het document opvallende opvragingen na, en zo ja welke opvallende opvragingen de te onderzoeken gemeente heeft gedaan -Controleer of de gemeente zelf rapporteert en voldoende verklaring geeft over opvallende opvragingen -Bij constatering opvallende patronen navragen bij gemeente of gemeente deze heeft onderkend en daar een mogelijke verklaring voor heeft -Ga na of er andere controlemethoden worden ingezet en hier bewijsstukken voor aanwezig zijn

Bijlage 4 Het Suwinet nader bezien

Algemeen

De Gezamenlijke elektronische Voorzieningen Suwi (GeVS) bestaan uit een geheel van systemen en koppelingen dat door de ketenpartners werk en inkomen wordt gebruikt voor gegevensoverdracht bij de uitvoering van de werknemers- en volksverzekeringen en Participatiewet

GeVS bestaat uit een centrale voorziening (niet in beheer van de afzonderlijke ketenpartners) en decentrale voorzieningen (systemen van de ketenpartners zelf) De centrale voorziening heet Suwinet. Bij decentrale systemen en koppelingen kan gedacht worden aan DKD-Inlezen en het UWV Portal (EROW, SONAR) Deze decentrale voorzieningen blijven in dit onderzoek buiten beschouwing

Het beheer van de centrale voorziening Suwinet wordt verzorgd door BKWI
Deze taak kan opgedeeld worden in de volgende activiteiten

- Ontwikkelen, aanbieden en beheren van de gegevensdiensten van Suwinet
- Beheer van ketenbrede standaarden voor gegevens, architectuur, beheer en beveiliging van Suwinet
- Faciliteren van de ketensamenwerking, ketenadvies en ondersteuning van de dienstverlening door de ketenpartners

Andere organisaties zoals IB en UWV zijn uiteraard beheerder van hun eigen decentrale voorzieningen

Het Suwinet is een belangrijke elektronische voorziening voor gegevensuitwisseling tussen de diverse organisaties Het Suwinet biedt een tiental services (zoals Suwinet-Inkijk, Suwinet-Inlezen en Suwinet-Mail) Hiervan is Suwinet-Inkijk naar omvang van het berichtenverkeer de grootste service.

Suwinet-Inkijk

Suwinet-Inkijk biedt Suwi-partijen de mogelijkheid om gegevens van burgers, die bij andere overheidsorganisaties of in basisregistraties zijn opgeslagen, snel te raadplegen in een webtoepassing. Aangesloten op Suwinet-Inkijk zijn onder andere. UWV, GSD, SVB, Belastingdienst, DUO, RDW en het Kadaster Deze partijen dienen veelal als bron voor de gemeentelijke informatievoorziening. De gemeente is via Suwinet niet altijd of slechts beperkt zelf een bron voor deze organisaties

Suwinet-Inkijk toont op het scherm van de ambtenaar een overzicht van de opgevraagde gegevens van de betreffende burger Het bevat persoonsgegevens van bijna alle Nederlanders
Anders gezegd: om zo'n 450 000 mensen met een uitkering te bedienen heeft een grote groep gemeenteambtenaren die de Participatiewet uitvoeren, toegang tot de gegevens van alle Nederlanders.

In 2015 was de situatie als volgt. Er worden gegevens van bijna 700.000 burgers door 22 000 actieve gebruikers, onder wie 10.000 gemeenteambtenaren, geraadpleegd Daarbij is sprake van 10 miljoen berichtuitwisselingen op maandbasis Dat er gegevens van meer burgers worden geraadpleegd dan er uitkeringsgerechtigden zijn, heeft onder meer te maken met in- en uitstroom in de Participatiewet.

In principe zijn alle gegevens van alle Nederlanders voor de gebruikers opvraagbaar, echter zij mogen alleen opvragen in het kader van de uitvoering van de wettelijke taak Participatiewet, IOAW en IOAZ, en voor zover nodig voor hun taakuitoefening Dit stelt hoge eisen aan de toegangsbeveiliging en vereist een zorgvuldig gebruik De gegevensuitwisseling vindt plaats over het beveiligde netwerk Suwinet Iedere handeling van de gebruiker van Suwinet-Inkijk wordt door BKWI gelogd. BKWI heeft daarvoor een wettelijke taak Op basis van deze logging worden (maandelijks) standaard generieke rapportages opgesteld De rapportage bevat o.a kengetallen waarmee gemeenten een beeld krijgen van hun eigen gebruik van Suwinet-Inkijk Deze rapportages bevatten geen gegevens die tot individuen kunnen worden herleid.

Naast deze standaard door BKWI verstrekte generieke rapportages kunnen gemeenten ook zgn. specifieke rapportages opvragen Deze rapportages worden op verzoek van een, door de gemeente aangewezen gemandateerde, aangevraagd bij BKWI en worden op maat gemaakt voor de gemeente Zo kan de gemeente een controle inrichten tot op accountniveau. Een voorbeeld is een rapportage waarbij alle opvragingen van een gebruiker in een bepaalde periode inzichtelijk worden gemaakt Hierdoor kan er door de deelnemende organisaties gerichte controle op eventueel oneigenlijk gebruik en misbruik plaatsvinden.

Suwinet-Inlezen
Suwinet-Inlezen is een voorziening waarmee niet Suwi-partijen een beperkte set van gegevens afkomstig uit één bron via een bericht op maat in kunnen lezen in hun eigen applicatie die specifiek voor die wettelijke taak is gemaakt Het gaat bij Suwinet-Inlezen om gegevens ten behoeve van niet-Suwi-taken (dus niet Participatiewet, IOAW en IOAZ) Een aanvraag voor toegang tot Suwinet-Inlezen loopt via BKWI. Op dit moment maken slechts drie gemeenten (Amsterdam, Rotterdam en Den Haag) gebruik van Suwinet-Inlezen Dat betreft de ondersteuning van een specifieke activiteit· het leggen van derdenbeslag

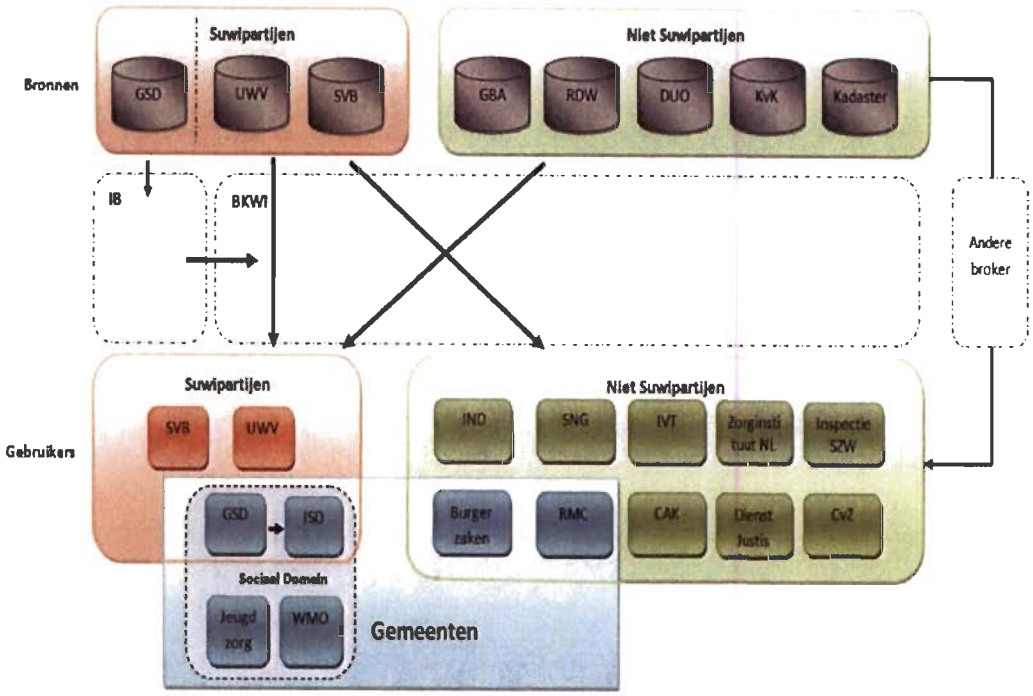
DKD-Inlezen
Waar het gaat om gegevens voor Suwi-taken, is het alternatief van Suwinet-Inkijk het DKD-Inlezen waarmee gemeenten de gegevens in hun eigen applicaties inlezen en kunnen voorinvullen. Met DKD-Inlezen wordt een uitgebreide set van gegevens verstuurd afkomstig uit diverse bronnen die door gemeenten ingelezen kunnen worden in verschillende applicaties. IB is de beheerder van de decentrale voorziening DKD-Inlezen
Op deze vorm van inlezen waren ten tijde van het onderzoek 338 gemeenten aangesloten Van deze groep zijn er 82 gemeenten die DKD-Inlezen ook daadwerkelijk gebruiken Een gemeente dient hiertoe een aanvraag in te dienen bij het Inlichtingenbureau (IB). Onderdeel van de aansluitprocedure DKD is het akkoord op de (grotendeels wettelijke) gebruiksvoorwaarden

In het kader van dit onderzoek naar de beveiliging van Suwinet wordt op decentrale voorzieningen zoals DKD-Inlezen niet ingegaan

Bronnen, gegevensstromen en gebruikers
Gegevens die binnen het domein werk en inkomen aanwezig zijn, mogen alleen worden uitgewisseld met andere organisaties wanneer de wet dit toestaat en er overeenkomsten zijn ondertekend. Zo is gegevensuitwisseling onder meer mogelijk gemaakt voor de Regionale Meld- en Coordinatiefunctie voortijdig schoolverlaten, gemeentelijke deurwaarders en Burgerzaken.

Figuur 5 (deels afgeleid van documentatie van BKWI) geeft de diverse bronnen, afnemers en gegevensstromen binnen GeVS/Suwinet weer.
Het figuur beschrijft ook de speciale positie van gemeenten. Zo is de dienst Werk en Inkomen van de gemeente een zgn. 'Suwi-partij'. Daarnaast zijn er ook andere onderdelen van gemeenten die niet-Suwi-taken uitvoeren en derhalve geen 'Suwi-partij' zijn, maar wel gegevens met behulp van Suwinet raadplegen Ook zijn er onderdelen binnen een gemeente die in het geheel geen verbinding (mogen) hebben met Suwinet.
De situatie van gemeentelijke sociale diensten die onderdeel zijn van een gemeenschappelijke sociale dienst (of de taken uitbesteed hebben aan een andere gemeente) is afzonderlijk weergegeven Dat geldt ook voor het sociaal domein, dat deels gevormd wordt uit de dienst Werk en Inkomen (Suwi-partij) en andere afdelingen die daar buiten vallen.

Door de decentralisatie-operatie sociaal domein, met daarbij de vorming van wijkteams en de invoering van de integrale dienstverlening, is de vraag van diverse gemeenten naar gegevens die via Suwinet te raadplegen zijn, toegenomen Deze aanvullende vraag betreft andere beleidsterreinen en is daarmee breder/omvangrijker dan het wettelijke regime toestaat



Figuur 5. Suwinet, bronnen, gegevensstromen en gebruikers (bron: BKWI)

Legenda

UWV	Uitvoeringsinstituut werknemersverzekeringen
ISD	Intergemeentelijke Sociale Dienst
GSD	Gemeentelijke sociale diensten (uitvoeringsorganisatie van de Participatiewet)
SVB	Sociale verzekeringsbank
GBA	Gemeentelijke Basis Administratie
DUO	Dienst Uitvoering Onderwijs van het Ministerie van Onderwijs, Cultuur en Wetenschappen
RDW	Rijksdienst Wegverkeer
IND	Immigratie- en Naturalisatiedienst van het Ministerie van Veiligheid en Justitie
KvK	Kamer van Koophandel
Justis	Screeningsautoriteit van het Ministerie van Veiligheid en Justitie
RMC	Regionale Meld- en Coördinatiefunctie voortijdig schoolverlaten
IVT	Interventieteams
SNG	Stichting Netwerk Gerechtsdeurwaarders
CAK	Centraal Administratiekantoor AWBZ
WMO	Wet Maatschappelijke Ondersteuning

Bijlage 5 Vragenlijst uitvraag gemeenten (blanco)

Contactgegevens

Gemeente

Functionaris, naam, functie en afdeling

Mailadres

Telefoonnummer

Norm 1.3/1.4/1.5 (beveiligingsbeleid en beveiligingsplan)

Vragen

a. Heeft uw Sociale Dienst een informatiebeveiligings**beleid**?

b. Heeft uw Sociale Dienst een informatiebeveiligings**plan** zoals genoemd in de regeling SUWI?

c Is het plan goedgekeurd door het management van de Sociale Dienst en wanneer?

d Wordt het beleid en het plan uitgedragen in de organisatie?

e. Op welke wijze gebeurt dit?

f. Vindt evaluatie en actualisatie van het informatiebeveiligingsbeleid en het informatiebeveiligingsplan plaats?

g Met welke frequentie en hoe gebeurt dit?

h Worden er werkzaamheden uitgevoerd door bijvoorbeeld een Intergemeentelijke Sociale Dienst (ISD), sociale recherche of ander samenwerkingsverband?

i Zo ja, op welke wijze zijn taken en bevoegdheden, relevant voor het onderwerp informatiebeveiliging, gemandateerd of overgedragen?

Bewijsstukken

- Bovengenoemd informatiebeveiligingsbeleid en beveiligingsplan;
- Stukken waaruit blijkt dat deze:
  - door het management zijn geaccordeerd (bijv een verslag),
  - binnen de organisatie zijn uitgedragen (bijv. verslagen, presentaties, interviews);
  - periodiek worden geevalueerd en geactualiseerd (bijv. verslagen, oude versies en wijzigingen).
- Bij mandatering of overdracht van taken: mandateringsbesluiten, gemeenschappelijke regelingen en contracten

Norm 2.2/2.3 (organisatorische aspecten)

Vragen

a Heeft u taken en verantwoordelijkheden en bevoegdheden t.a v het gebruik van Suwinet beschreven?

b Hoe heeft u deze belegd?

c. Op basis van welke criteria hebben medewerkers:
   i. toegang tot gegevens uit Suwinet?
   ii Zware rollen (zoals bijvoorbeeld de GSD-rollen 018, 021 en 030 en/of eventueel door u zelf samengestelde R-rollen)?
   iii. de mogelijkheid bevoegdheden te verlenen?

d Wat is uw beleid voor de controle van het gebruik?

e Maakt u gebruik van Suwinet-Inlezen?

f Zo ja, wat is het beleid voor veilig gebruik van Suwinet Inlezen? Zo nee, kunt u de hieronder deel 2 van de bij norm 13 gestelde vragen overslaan.

g. Heeft u een security officer aangesteld?
   i. Wat is zijn/haar takenpakket?
   ii Hoe geeft hij/zij hieraan invulling?

Bewijsstukken

- Beschrijving taken en bevoegdheden, hoe deze zijn belegd en hoe met (speciale) bevoegdheden wordt omgegaan,
- Uitgangspunten en richtlijnen voor het gebruik van Suwinet-Inlezen,
- Naam van de security officer, zijn/haar takenpakket en rapportages die door hem/haar in 2014 zijn opgesteld (eventueel geanonimiseerd).

Norm 13.1/13.5 (logische toegangsbeveiliging)

Bij gebruik van Suwinet Inkijk (deel 1):

a. Hoeveel medewerkers hebben toegang tot Suwinet?

b Zijn dit allen medewerkers van de Sociale Dienst of ook medewerkers van andere afdelingen, diensten en/of instellingen?

c Hoeveel hiervan hebben zware rollen en welke?

d. Hoeveel medewerkers (en welke functie hebben deze) kunnen toegangsrechten verlenen en hoe gebeurt dit?

e Hoe, en hoe vaak controleert u de verleende toegangsrechten en het gebruik van Suwinet in de praktijk?

f. Maakt u gebruik van niet-persoonsgebonden accounts (meerdere medewerkers die van 1 account gebruik maken)?

g. Heeft u daarnaast indicaties dat meerdere personen van hetzelfde account gebruik maken?

h Hoe worden bevoegdheden in de praktijk verleend en weer ingetrokken?

i. Gebruikt u voor controle de periodieke rapportages van BKWI? Hoe vaak heeft u deze in 2014 jaar opgevraagd? Controleert u het gebruik ook nog op een andere wijze?

j. Hoe vaak hebt u in 2014 specifieke rapportages opgevraagd bij BKWI (rapportages die tot individuele personen - burgers of medewerkers - herleidbaar zijn)?

Bij gebruik van Suwinet Inlezen (deel 2).

a Hoeveel medewerkers hebben toegang tot gegevens die middels Suwinet Inlezen zijn verkregen?

b Zijn dit allen medewerkers van de Sociale Dienst of ook medewerkers van andere afdelingen, diensten en/of instellingen?

c Hoeveel hiervan hebben zware rollen en welke?

d Hoeveel medewerkers kunnen toegangsrechten verlenen en welke functies hebben deze medewerkers? Hoe gebeurt dit?

e. Hoe, en hoe vaak controleert u het gebruik van Suwinet gegevens in de praktijk?

f Maakt u gebruik van niet-persoonsgebonden accounts (meerdere medewerkers die van 1 account gebruik maken)?

g. Heeft u daarnaast indicaties dat meerdere personen van hetzelfde account gebruik maken?

h Hoe worden bevoegdheden in de praktijk verleend en weer ingetrokken?

i Gebruikt u voor controle vergelijkbare overzichten als de periodieke en specifieke rapportages van BKWI? Hoe vaak heeft u deze het afgelopen jaar opgevraagd? Controleert u het gebruik ook nog op een andere wijze?

Bewijsstukken

- Overzichten van autorisaties, speciale toegangsrechten, controles, incidenten, maatregelen, overige rapportages en relevante mailwisselingen U kunt de bewijsstukken desgewenst anonimiseren

Bijlage 6 Methodologische verantwoording

Representativiteit
Voor dit onderzoek is onderzoek gedaan naar alle 393 gemeenten (peildatum september 2014).

Onderzoekspeildata
Voor het beoordelen van de maatregelen die gemeenten in 2015 hebben getroffen is uitgegaan van de stand van zaken vanaf 1 september 2014 tot 1 september 2015. Maatregelen en documenten, zoals beveiligingsplannen, die na de laatstgenoemde datum tot stand zijn gekomen, zijn in de beoordeling nog meegenomen als aantoonbaar was dat er voor het meetmoment zaken intern wel al bekend waren en nageleefd werden

Methode
Het onderzoek van de Inspectie geeft een beeld van de beveiliging van Suwinet door alle 393 (stand 1 september 2015) gemeenten in Nederland Daarmee kan het onderzoek dienen als basis voor de toepassing van het escalatieprotocol op grond waarvan gemeenten een aanwijzing kunnen krijgen In afwijking van eerdere onderzoeken van de beveiliging van Suwinet is dus geen sprake van een steekproef.

Half juli 2015 hebben 393 Colleges van Burgemeester en Wethouders een brief ontvangen, waarin het onderzoek werd aangekondigd. In de brief werd verzocht om de naam en het e-mailadres van een contactpersoon (bij voorkeur een security officer) door te geven De brief leverde, na schriftelijke en telefonische rappelleringen, 100% respons op
De onderzoeksmethode is verder gelijk aan het vorige onderzoek. De Inspectie stuurde de gemeenten een vragenlijst (bijlage 5) die betrekking had op de naleving van de
7 geselecteerde normen uit het Normenkader GeVS De antwoorden van de gemeenten zijn door de onderzoekers beoordeeld. Veelal leidde dat tot aanvullende vragen Na ontvangst en beoordeling van de reacties op die vragen, werd de conclusie getrokken of (een deel van) de norm wel of niet werd gehaald. In beperkte mate is daarbij sprake van gebruik van door de Inspectie zelf geconstrueerde operationalisaties van de GeVS-normen (zie hiervoor de verduidelijkingen die in het werkprogramma in bijlage 3 zijn opgenomen) Het onderzoek van de Inspectie betreft desk research Er is niet bij de gemeenten zelf onderzocht of de beveiligingsmaatregelen bestaan en werken.
Alleen als alle deelnormen werden behaald, voldoet een gemeente aan een norm. Het conceptoordeel van de onderzoekers werd onderworpen aan een beoordeling door een kwaliteitsgroep Deze kwaliteitsgroep bestond uit drie informatie- en auditdeskundigen
Pas daarna ging het conceptoordeel voor commentaar naar de colleges van B&W van de gemeenten Voor de afhandeling van de reactie van de gemeente op een conceptoordeel gold een gelijksoortige procedure. Daarna werd het onderzoek in de vorm van een definitieve rapportage aan het College van B&W en de Raad van de gemeenten aangeboden

Informatie van BKWI
BKWI logt de gegevens van het gebruik van Suwinet

SUWInet-Inkijk	Logging van gegevens op BSN-niveau per account gemeente/ISD
SUWInet-Inlezen	Logging van gegevens op BSN niveau per gemeente/ISD

Op basis van de loggings maakt BKWI een rapportage. Deze zgn. 'generieke' rapportage is maandelijks door gemeenten opvraagbaar via Suwinet De rapportage bevat onder meer informatie over het totaal aantal opvragingen, het aantal BSN dat is geraadpleegd, het aantal opvragingen binnen en buiten kantooruren, het aantal geslaagde en niet geslaagde inlogpogingen, het aantal actieve en inactieve accounts enz Tevens is de rapportage voorzien van een toelichting. De rapportage bevat geen gegevens op accountniveau die naar natuurlijke personen (gemeentelijke medewerkers) zijn te herleiden.

Gemeenten kunnen dergelijke informatie over het inloggedrag van specifieke medewerkers wel ontvangen van BKWI, maar moeten die dan separaat, als zgn. 'specifieke rapportage' door BKWI laten opstellen

De Inspectie SZW heeft van BKWI van alle geselecteerde gemeenten de generieke rapportages over de periode januari tot september 2015 ontvangen. Ook is van BKWI vernomen welke gemeenten wanneer generieke en specifieke rapportages hebben opgevraagd

De Inspectie SZW heeft bij BKWI ook rapportages opgevraagd die het inloggedrag op 'zware rollen" zichtbaar maken Doel van deze opvraging is opvallend zoekgedrag op te sporen In principe gebruikt een gemeenteambtenaar het BSN om toegang te krijgen tot iemands persoonsgegevens. De beschikbaarheid van zware rollen verhoogt het risico op onrechtmatig gebruik, omdat het gemakkelijker is om op bijv op iemands naam te zoeken, dan op het veel minder publieke BSN.

De logfiles die zijn opgevraagd met betrekking tot de inzet van zware rollen betreffen:
-zoeken op achternaam en geboortedatum,
-zoeken op achternaam (3 letters);
-zoeken op postcode en huisnummer,
-zoeken op kenteken;
-zoeken op postcode buiten postcodegebied

Om te bepalen wanneer er een nadere verklaring nodig is, wordt een onderscheid gemaakt in het aantal opvragingen per account (medewerker met toegang tot Suwinet) en per gemeente
Voor het gebruik per account is navraag gedaan voor alle afwijkingen die groter zijn dan 1x de standaarddeviatie boven het gemiddelde aantal opvragingen
Voor het aantal opvragingen per gemeente is allereerst het aantal opvragingen gedeeld door het bestand Participatiewet. Dat is nodig omdat anders alleen de grote gemeenten worden geselecteerd Vervolgens is het gemiddelde berekend en is gekeken welke gemeenten boven de standaarddeviatie zaten

Ten slotte heeft de Inspectie SZW aan BKWI gevraagd na te gaan of en zo ja hoe vaak gezocht is op het BSN van 100 bekende Nederlanders

Voor een medewerker met toegang tot Suwinet is het verleidelijk om het BSN van een bekende te raadplegen Daarbij valt te denken aan collega's, leidinggevenden, (nieuwe) (ex-)partner, buren, etc Dit soort zoekgedrag is alleen op te sporen door een vergelijking te maken tussen de door de medewerker geraadpleegde BSN en zijn klantenbestand. Wie interessant is voor welke medewerker, is immers vooraf niet bekend. Alleen als er is gezocht op namen van niet-klanten kan een vermoeden rijzen omtrent dit ongewenste zoekgedrag Bij een afwijking kan de medewerker om een verklaring worden gevraagd Bij deze vorm van controle wordt niet ontdekt of een medewerker ten onrechte gegevens opvraagt van een bekende die tevens een uitkering Participatiewet heeft. Er zijn bij dit onderzoek gemeenten geweest die deze controle periodiek en steekproefsgewijs hanteren. De meeste gemeenten hanteren de methode overigens niet

Bij door de Inspectie op bovenstaande wijze vastgesteld opvallend zoekgedrag is aan de contactpersoon van de gemeente gevraagd of men deze 'afwijking' zelf ook heeft geconstateerd en of men hiervoor een verklaring kan geven

Afbakening en beperking
Zoals gezegd vormen de gemeenten de primaire onderzoekseenheden Steeds vaker echter werken gemeenten samen in verbanden die meestal regionale of intergemeentelijke sociale diensten worden genoemd Ook komt het voor dat men een andere gemeente vraagt om de Participatiewet te verzorgen. In het huidige onderzoek is geaccepteerd dat de organisatie van het samenwerkingsverband of de andere gemeente desgewenst optreedt als gesprekspartner voor de participerende gemeenten. Het oordeel over de beveiliging van het samenwerkingsverband is dan het oordeel dat aan elke afzonderlijke deelnemende gemeente wordt toegekend. De gemeente blijft immers verantwoordelijk voor de beveiliging
Slechts bij uitzondering is er een oordeel geveld los van het samenwerkingsverband Dat was bijv het geval voor een aantal gemeenten dat zich uit een samenwerkingsverband gaat terugtrekken
De beveiliging van Suwinet door andere partijen dan gemeenten (bijv. UWV of gemeentelijke deurwaarders), zowel binnen als buiten het domein van werk en inkomen, is niet beoordeeld

Suwinet wordt door gemeenten als Suwi-partij ten principale alleen ingezet voor de uitvoering van de Participatiewet en aanverwante wetten (IOAW en IOAZ) In beperkte mate is inzet voor andere taken (gemeentelijke deurwaarders bijv) mogelijk, maar dan moet daarvoor expliciet een afzonderlijk contract met de bronhouders(s) en BKWI worden afgesloten. De gemeente is in zo'n geval geen Suwi-partij voor deze niet aan de genoemde wetten verbonden toegang. Accounts op basis van een dergelijk contract geven alleen toegang tot een beperkte gegevensset. De beveiliging daarvan is niet in het onderzoek betrokken

In het onderzoek zijn ook geen conclusies getrokken over accounts die gemeenten uitsluitend inzetten ten behoeve van aan de Participatiewet gelieerde taken die *niet* tot de reguliere uitvoering behoren, zoals de bijzondere bijstand. Dergelijke accounts blijven soms bij afzonderlijke gemeenten aanwezig als die de reguliere uitvoering Participatiewet opdragen aan een samenwerkingsverband. Veelal worden ze 'achtergebleven' accounts genoemd.

In bijlage 9 worden de 22 gemeenten die achtergebleven accounts hebben nader toegelicht Deze gemeenten zijn erover geïnformeerd dat er sprake is van achtergebleven accounts en dat het normenkader onverkort ook voor deze accounts van toepassing is

In het licht van het toenemend gebruik van electronische gegevensuitwisseling en de druk om beschikbare gegevens in te zetten ten behoeve van het gehele sociale domein (met name door de decentralisatieoperatie) worden de risico's die gemeenten lopen op oneigenlijk gebruik navenant groter Hoe doelmatig het soms ook lijkt om gegevens aan Suwinet te ontlenen voor andere gemeentelijke taken, het is – zoals gezegd - wettelijk niet toegestaan Het onderzoek biedt de Inspectie niet de mogelijkheid om met waterdichte conclusies te komen over de werking van de schotten die Suwinet moeten beschermen tegen oneigenlijk gebruik voor andere gemeentelijke taken dan waarvoor Suwinet is bedoeld Waar tegen problemen ter zake werd aangelopen, heeft de Inspectie daaraan wel aandacht besteed.

Het onderzoek richt zich op de zgn centrale voorziening Suwinet-Inkijk. Er is geen aandacht voor de eveneens centrale voorziening Suwinet-Inlezen. Bekend is dat er door BKWI geen loggings (kunnen) plaatsvinden op het gebruik van Suwinet-Inlezen door gemeentelijke eindgebruikers Onduidelijk is dus voor BKWI wie wat heeft opgevraagd Daarmee wordt een veiligheidsrisico gelopen omdat er indicaties zijn dat gemeenten dit ook niet vragen aan hun software-leveranciers Suwinet-Inlezen wordt overigens beperkt ingezet (alleen door 3 van de 4 grote gemeenten)

Evenmin is er aandacht voor decentrale voorzieningen, zoals DKD-Inlezen. Dat systeem is een alternatief voor Suwinet-Inlezen, en wordt door 82 gemeenten gebruikt Hiervoor moeten overeenkomsten met IB worden gesloten Dat er bij DKD-Inlezen risico's worden gelopen is voor de Inspectie duidelijk Dit blijkt onder meer uit de gesprekken die de Inspectie (tijdens het vorige onderzoek) heeft gevoerd met software-leveranciers, nadat bleek dat er op DKD-Inlezen net als bij Suwinet-Inlezen, geen centrale logging kan plaatsvinden op het gebruik van gegevens door individuele gemeentelijke medewerkers Die logging zou dan door de gemeenten zelf, in overleg met hun software-leverancier, moeten worden verzorgd wil er niet al op voorhand sprake zijn van een inadequate beveiliging Leveranciers gaven vorig jaar aan dat er door gemeenten waarschijnlijk bijna geen gebruik wordt gemaakt van controlemogelijkheden/logging De risico's blijken ook uit de signalen die de Inspectie ontving van individuele medewerkers die aangeven zich zorgen te maken over de informatiebeveiliging rondom de decentrale voorzieningen

De Autoriteit Persoonsgegevens heeft op dit probleem voor beide vormen van Inlezen gewezen Voor de problemen met de loggings van Suwinet-inlezen heeft UWV (BKWI) een plan van aanpak opgesteld. De intentie is om dit plan van aanpak op termijn te verbreden tot DKD-inlezen.

Omdat bij Suwinet per definitie sprake is van de verwerking van persoonsgegevens dient de Wet bescherming persoonsgegevens (Wbp) in acht te worden genomen (naleving beginselen van doelbinding, proportionaliteit, subsidiariteit etc) Over de naleving van de WBP bij 13 gemeenten en BKWI is in 2014/15 gerapporteerd door het toenmalige CBP (Onderzoek beveiliging van persoonsgegevens via Suwinet, november 2015).

Overige relevante wetgeving is bijv. de Wet eenmalige gegevensuitvraag werk en inkomen (WEU) Deze is niet betrokken in het huidige onderzoek van de Inspectie

Het onderzoek richt zich op 7 essentiele normen Dat is een deel van het totale normenkader dat bestaat uit 115 normen (waarvan 26 essentieel zijn)
Het voldoen aan de 7 normen zegt niets over het voldoen aan de overige normen.
Het onderzoek is uitgevoerd op basis van de door de gemeenten gegeven antwoorden op een standaardvragenlijst en opgestuurde bewijsstukken De Inspectie SZW heeft de betrokken gemeenten niet bezocht en heeft dus niet ter plekke gekeken naar de uitvoering.

Bijlage 7 Overzicht bevindingen gemeenten (393)

Stand 1 september 2015

De volgende gemeenten voldeden aan alle 7 normen

	Aa en Hunze
	Aalsmeer
	Alblasserdam
G32	Almelo
G32	Alphen a/d Rijn
G32	Amersfoort
	Amstelveen
G32	Apeldoorn
	Assen
	Asten
	Bedum
	Beek
	Bergen (NH)
	Bergen op Zoom
	Beverwijk
	Binnenmaas
	Bloemendaal
	Boekel
	Borne
	Boxtel
G32	Breda
	Bronckhorst
	Brummen
	Bunnik
	Buren
	Capelle a/d IJssel
	Castricum
	Cranendonck
	Cromstrijen
	Dalfsen
	De Bilt
	De Marne
	De Wolden
	Den Helder

	Dinkelland
	Doesburg
	Dongen
G32	Dordrecht
	Dronten
	Duiven
	Eijsden-Margraten
G32	Eindhoven
G32	Enschede
	Epe
	Ermelo
	Etten-Leur
	Franekeradeel
	Geldermalsen
	Geldrop
	Gemert
	Gennep
	Giessenlanden
	Goeree Overflakkee
	Gorichem
	Groesbeek
	Gulpen-Wittem
	Haaren
G32	Haarlem
	Haarlemmerliede
G32	Haarlemmermeer
	Halderberge
	Harderwijk
	Hardinxveld-Giessendam
	Harlingen
	Heemskerk
	Heemstede
G32	Heerlen
	Heeze-Leende

G32	Helmond
	Hendrik-Ido-Ambacht
G32	Hengelo
	Het Bildt
	Heumen
	Hillegom
	Hof van Twente
	Hoogeveen
	Hoogezand-Sappemeer
	Horst a/d Maas
	Houten
	IJsselstein
	Kaag en Braassem
	Korendijk
	Krimpen a/d IJssel
	Laarbeek
	Landerd
	Landsmeer
	Leek
	Leerdam
G32	Leeuwarden
	Leeuwarderadeel
G32	Lelystad
	Leusden
	Lingewaal
	Lisse
	Littenseradiel
	Lochem
	Lopik
	Maassluis
	Marum
	Meerssen
	Menameradiel
	Middelburg

	Deurne
	Moerdijk
	Molenwaard
	Neder-Betuwe
	Neerijnen
	Nieuwegein
	Nieuwkoop
G32	Nijmegen
	Noordenveld
	Noordoostpolder
	Noordwijk
	Noordwijkerhout
	Nuth
	Oisterwijk
	Olst-Wijhe
	Ooststellingwerf
	Oostzaan
	Opsterland
G32	Oss
	Oud-Beijerland
	Ouder-Amstel
	Papendrecht
	Peel en Maas
	Renswoude
	Rheden
	Rhenen
	Rijnwaarden
	Roerdalen
	Roermond
G32	Roosendaal

	Heiloo
	Rozendaal
	Rucphen
	Schouwen-Duiveland
	Simpelveld
G32	Sittard-Geleen
	Sliedrecht
	Slochteren
	Sluis
	Smallingerland
	Someren
	Steenbergen
	Steenwijkerland
	Stichtse Vecht
	Strijen
	Súdwest Fryslân
	Terschelling
	Texel
	Teylingen
	Tiel
G32	Tilburg
	Tubbergen
	Tynaarlo
G4	Utrecht
	Utrechtse Heuvelrug
	Vaals
	Valkenswaard
	Veenendaal
	Veere
	Vianen

	Midden-Drenthe
	Vlaardingen
	Vlieland
	Vlissingen
	Voerendaal
	Voorst
	Waalre
	Wageningen
	Waterland
	Weert
	Weesp
	West Maas en Waal
	Westerveld
	Westervoort
	Weststellingswerf
	Wijk bij Duurstede
	Winsum
	Woensdrecht
	Woudenberg
G32	Zaanstad
	Zandvoort
	Zederik
	Zeewolde
	Zeist
	Zevenaar
	Zuidhorn
	Zundert
	Zutphen
	Zwijndrecht
G32	Zwolle

Gemeenten die voldoen aan 6 normen

	Achtkarspelen	1.4
	Albrandswaard	1.4
G32	Alkmaar	13.5
G32	Almere	13.1
	Baarn	1.5
	Barendrecht	1.4
	Barneveld	13.1
	Bergeijk	13.1
	Berkelland	1.4
	Bernheze	1.4
	Bladel	13.1
	Blaricum	1.4
	Boxmeer	13.5
	Brunssum	1.5
	Bunschoten	1.5
	Bussum	13.1
	Cuijk	2.3
	Culemborg	13.5
	Dantumadiel	1.5
	De Ronde Venen	13.5
G32	Delft	2.3
G32	Den Bosch	13.1
G4	Den Haag	13.1
	Dongeradeel	1.5
	Drimmelen	2.3
	Edam-Volendam	13.1
G32	Ede	1.5
	Eemnes	1.4
	Eersel	13.1
	Elburg	1.4
	Ferwerderadiel	1.5
	Geertruidenberg	13.1
G32	Gouda	2.3
	Grave	2.3
	Hardenberg	13.5
	Heusden	13.1

	Hilversum	13.1
	Huizen	1.4
	Kampen	2.3
	Kerkrade	13.1
	Kollumerland	1.5
	Landgraaf	1.5
	Lansingerland	13.5
	Laren	1.4
	Leudal	1.4
	Loon op Zand	13.1
	Losser	13.1
G32	Maastricht	13.1
	Mill	2.3
	Mook en Middelaar	13.1
	Muiden	13.1
	Naarden	13.1
	Nijkerk	13.5
	Nunspeet	13.1
	Oirschot	13.1
	Ommen	13.5
	Onderbanken	1.5
	Oost Gelre	1.4
	Pijnacker-Nootdorp	13.5
	Reusel- De Mierden	13.1
	Ridderkerk	1.4
G4	Rotterdam	13.1
	Scherpenzeel	2.2
	Schiermonnikoog	1.5
	Schijndel	1.4
	Schinnen	1.4
	Soest	1.5
	St. Anthonis	13.5
	Stadskanaal	13.5
	St-Michielsgestel	1.4
	Twenterand	13.1
	Tytsjerksteradiel	1.4

	Veghel	1.4
	Velsen	13.5
G32	Venlo	13.5
	Venray	13.5
	Vught	1.5
	Waalwijk	13.1
	Wijchen	1.5
	Wijdemeren	13.5
	Winterswijk	1.4
	Zeevang	13.1
G32	Zoetermeer	13.1
	Zoeterwoude	13.1
	Zuidplas	13.5

Gemeenten die voldoen aan 5 normen

	Appingedam	1.4	13.1
	Baarle-Nassau	2.3	13.5
	Beemster	2.3	13.5
	Bergen (L)	2.3	13.5
	Best	1.3	13.1
	Beuningen	2.3	13.5
	Bodegraven-Reeuwijk	1.4	2.3
	Borselle	1.4	13.5
	Brielle	2.3	13.5
	Coevorden	2.3	13.1
	Delfzijl	1.4	13.1
G32	Deventer	13.1	13.5
	Diemen	1.5	2.3
	Doetinchem	1.4	1.5
	Drechterland	1.4	2.3
	Echt-Susteren	1.4	13.1
	Enkhuizen	1.4	2.3
	Goirle	1.5	13.1
	Heerenveen	2.2	13.5
	Heerhugowaard	13.1	13.5
	Hollands Kroon	13.1	13.5
	Hoorn	1.4	2.3
	Koggenland	1.4	2.3
G32	Leiden	1.4	13.1
	Leiderdorp	1.4	13.1
	Lingewaard	2.3	13.5
	Loppersum	1.4	13.1
	Maasgouw	1.5	13.5
	Medemblik	1.4	2.3
	Montfoort	1.4	2.3
	Nissewaard	2.3	13.5
	Nuenen c.a.	2.3	13.1
	Oldenzaal	2.3	13.5
	Oosterhout	2.3	13.5
	Opmeer	1.4	2.3
	Oudewater	1.4	2.3
	Overbetuwe	2.3	13.5
	Pekela	1.4	1.5
	Purmerend	2.3	13.5
	Raalte	13.1	13.5
	Renkum	1.4	2.3
	Schagen	13.1	13.5
G32	Schiedam	13.1	13.5
	Son en Breugel	2.3	13.1
	St Oedenrode	2.3	13.1
	Stede Broec	1.4	2.3
	Urk	1.4	13.1
	Veendam	1.4	1.5
	Westvoorne	2.3	13.5
	Wierden	2.3	13.5
	Woerden	1.4	2.3
	Wormerland	2.3	13.5

Gemeenten die voldoen aan 4 of minder normen

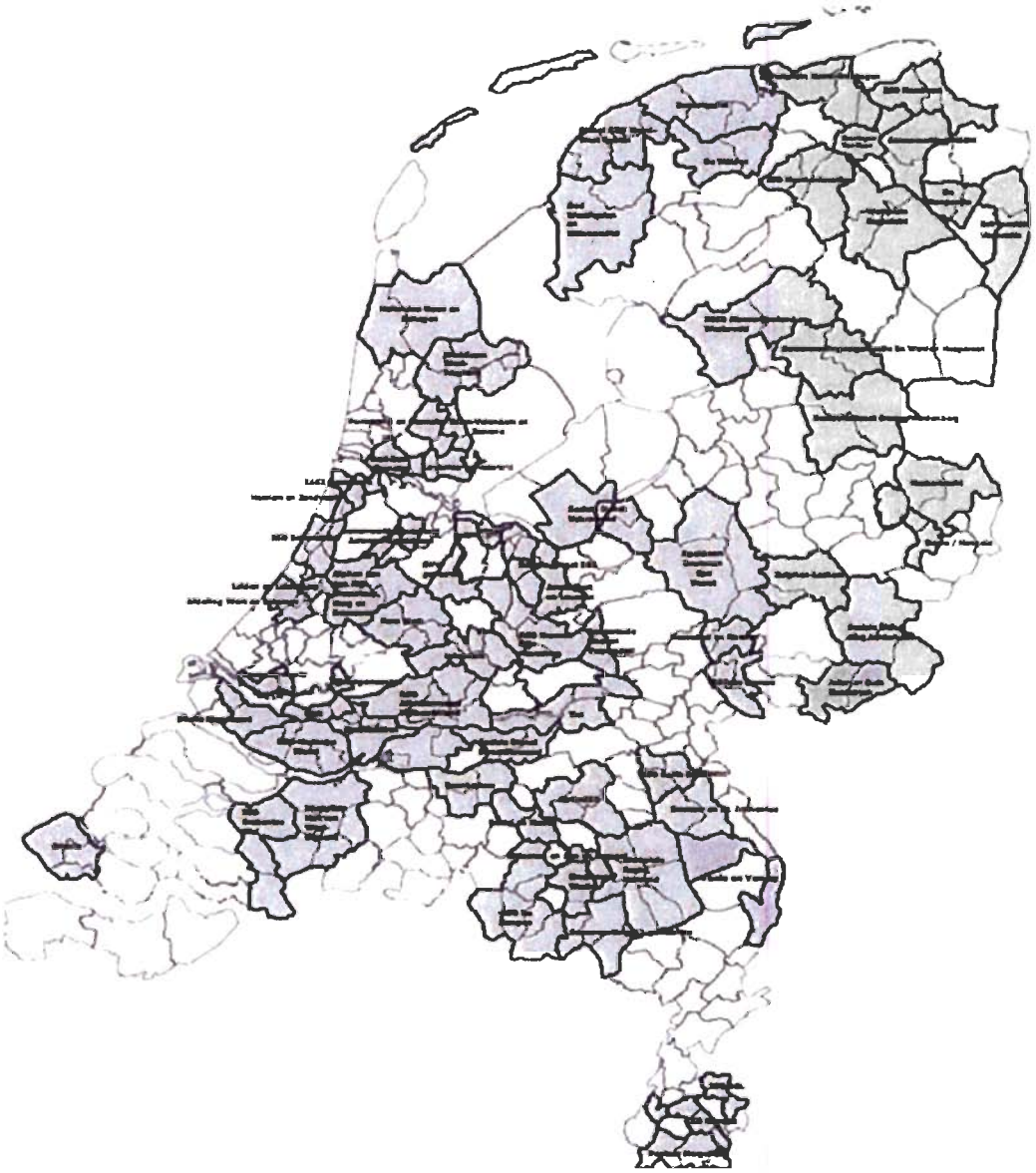
	Alphen-Chaam	1.4	2.3	13.5	
G32	Arnhem	2.3	13.1	13.5	
	Beesel	1.3	1.4	1.5	
	Borger-Odoorn	2.3	13.1	13.5	
G32	Emmen	2.3	13.1	13.5	
	Gilze en Rijen	2.2	2.3	13.1	
	Goes	1.4	13.1	13.5	
	Haaksbergen	1.4	2.3	13.5	
	Haren	1.4	1.5	2.3	
	Hattem	2.2	13.1	13.5	
	Hilvarenbeek	1.4	2.3	13.5	
	Kapelle	1.4	13.1	13.5	
	Katwijk	1.4	2.3	13.5	
	Langedijk	2.2	2.3	13.1	
	Leidschendam-Voorburg	1.4	2.3	13.5	
	Noord-Beveland	1.4	13.1	13.5	
	Oldambt	2.3	13.1	13.5	
	Oldebroek	1.4	13.1	13.5	
	Reimerswaal	1.4	13.1	13.5	
	Rijssen-Holten	2.3	13.1	13.5	
	Terneuzen	1.4	2.3	13.5	
	Veldhoven	2.3	13.1	13.5	
	Voorschoten	1.4	2.3	13.5	
	Waddinxveen	1.5	2.3	13.1	
	Wassenaar	1.4	2.3	13.5	
	Werkendam	2.2	2.3	13.5	
	Woudrichem	2.2	2.3	13.5	
	Aalten	1.5	2.3	13.1	13.5
	Ameland	1.4	1.5	13.1	13.5
	Druten	1.4	2.3	13.1	13.5
G32	Groningen	2.2	2.3	13.1	13.5
	Grootegast	1.5	2.3	13.1	13.5
	Hellevoetsluis	1.4	2.3	13.1	13.5
	Hulst	1.4	1.5	2.3	13.5
	Krimpenerwaard	1.3	1.4	1.5	13.1
	Oude IJsselstreek	1.5	2.3	13.1	13.5

	Putten	1.4	2.2	2.3	13.1			
	Rijswijk (ZH)	1.3	1.4	1.5	2.2			
	Ten Boer	2.2	2.3	13.1	13.5			
	Uden	1.4	2.2	2.3	13.5			
	Uitgeest	1.3	1.4	1.5	13.5			
	Uithoorn	1.4	2.3	13.1	13.5			
	Westland	1.4	2.3	13.1	13.5			
G4	Amsterdam	1.3	1.4	1.5	2.3	13.5		
	Bellingwedde	1.4	2.2	2.3	13.1	13.5		
	De Fryske Marren	1.3	1.4	1.5	2.3	13.5		
	Heerde	1.4	2.2	2.3	13.1	13.5		
	Hellendoorn	1.3	1.4	1.5	2.2	2.3		
	Menterwolde	1.4	1.5	2.3	13.1	13.5		
	Meppel	1.3	1.4	1.5	2.2	2.3		
	Midden-Delfland	1.4	1.5	2.3	13.1	13.5		
	Nederweert	1.4	2.2	2.3	13.1	13.5		
	Tholen	1.4	2.2	2.3	13.1	13.5		
	Vlagtwedde	1.4	2.2	2.3	13.1	13.5		
	Aalburg	1.4	1.5	2.2	2.3	13.1	13.5	
	Eemsmond	1.4	1.5	2.2	2.3	13.1	13.5	
	Montferland	1.3	1.5	2.2	2.3	13.1	13.5	
	Oegstgeest	1.4	1.5	2.2	2.3	13.1	13.5	
	Staphorst	1.3	1.4	1.5	2.2	2.3	13.5	
	Valkenburg	1.3	1.4	1.5	2.3	13.1	13.5	
	Maasdriel	1.3	1.4	1.5	2.2	2.3	13.1	13.5
	Stein (L)	1.3	1.4	1.5	2.2	2.3	13.1	13.5
	Zaltbommel	1.3	1.4	1.5	2.2	2.3	13.1	13.5
	Zwartewaterland	1.3	1.4	1.5	2.2	2.3	13.1	13.5

Bijlage 8 Overzicht score (eerder onderzoek Inspectie en VNG-zelftest)

Aantal normen	Inspectie 2013 (n=80)	VNG-zelftest 2014 (n=274)	Inspectie 2014 (n=78)	VNG-zelftest 2015 (n=259)	Inspectie 2015 (n=393)
7	4%	22%	17%	48%	49%
6	4%	11%	17%	21%	22%
5	10%	16%	14%	13%	13%
4	8%	15%	17%	8%	7%
3	19%	16%	6%	3%	4%
2	11%	7%	9%	3%	3%
1	33%	8%	12%	2%	1%
0	13%	5%	9%	0%	1%

Bijlage 9 Samenwerkingsverbanden en achtergebleven accounts



Samenwerkingsverbanden	Gemeenten	Gemeenten met achtergebleven accounts
Afdeling Werk en Inkomen	Leidschendam-Voorburg, Voorschoten, Wassenaar	
Baanbrekers	Heusden, Loon op Zand, Waalwijk	
BAR	Albrandswaard, Barendrecht, Ridderkerk	
Bel-Combinatie	Blaricum, Eemnes, Laren, Huizen	
Tiel (samenwerking)	Tiel, Neder-Betuwe, Neerijnen, West Maas en Waal	
De Kompanjie	Pekela, Veendam	
Dienst SZW Noard-West Fryslân	Franekeradeel, Harlingen, Het Bildt, Leeuwarderadeel, Menameradiel, Terschelling, Vlieland	
Drechtsteden	Alblasserdam, Dordrecht, Hendrik-Ido-Ambacht, Papendrecht, Sliedrecht, Zwijndrecht	
Ferm Werk	Bodegraven-Reeuwijk, Montfoort, Oudewater, Woerden	
IGSD Steenwijkerland en Westerveld	Steenwijkerland, Westerveld	Gemeente Westerveld heeft 5 achtergebleven accounts die allemaal inactief zijn. Westerveld heeft de uitvoering van de participatiewet uit-besteed aan gemeente Steenwijkerland die 47 actieve accounts heeft.
IASZ Heemstede	Bloemendaal, Haarlemmerliede en Spaarnwoude Heemstede	
ISD BOL	Brunssum, Onderbanken, Landgraaf	
ISD Bollenstreek	Hillegom, Lisse, Noordwijk, Noordwijkerhout, Teylingen	

Samenwerkingsverbanden	Gemeenten	Gemeenten met achtergebleven accounts
ISD Brabantse Wal	Bergen op Zoom, Steenbergen, Woensdrecht	Gemeente Steenbergen heeft 1 achterbleven account dat inactief is. Gemeente Steenbergen heeft de uitvoering uitbesteed aan Bergen op Zoom. Deze heeft 78 accounts.
ISD Cuijk Grave Mill	Cuijk, Grave, Mill en Sint Hubert	
ISD De Kempen	Bergeijk , Bladel, Eersel, Oirschot, Reusel-De Mierden	
ISD Kompas	Nuth, Simpelveld, Voerendaal	
ISD Noordenkwartier	Leek , Marum, Noordenveld	
ISD Noordoost	Appingedam, Delfzijl, Loppersum	
ISWI Aalten en Oude IJsselstreek	Aalten, Oude IJsselstreek	
Noaberkracht	Almelo, Dinkelland, Tubbergen	
OptimISD	Bernheze, Schijndel, Sint-Michielsgestel, Veghel, Boekel	
Orionis	Middelburg, Veere, Vlissingen	
Pentasz Mergelland	Eijsden-Margraten, Gulpen-Wittem, Meersen, Vaals	
RSD Alblasserwaard Vijfheerenland	Giessenlanden, Gorinchem, Hardinxveld-Giessendam Leerdam, Lingewaal, Molenwaard, Zederik	
RSD De Liemers	Duiven, Rijnwaarden, Westervoort, Zevenaar	
RSD Hoeksche Waard	Binnenmaas, Cromstrijen, Korendijk, Oud-Beijerland, Strijen	
RSD Kromme Rijn Heuvelrug	Bunnik, De Bilt, Utrechtse Heuvelrug, Wijk bij Duurstede, Zeist	
Samenwerking A2-gemeenten	Cranendonck , Heeze-Leende, Valkenswaard	
Samenwerkingsorganisatie De Wolden Hoogeveen	De Wolden, Hoogeveen	

Samenwerkingsverbanden	Gemeenten	Gemeenten met achtergebleven accounts
Samenwerking HSSM	Hoogezand-Sappemeer, Slochteren	
Samenwerkingsverband Aalsmeer-Amstelveen	Aalsmeer, Amstelveen	
Samenwerkingsverband IJsselgemeenten	Capelle aan den IJssel, Krimpen aan den IJssel	
Samenwerkingsverband sociale diensten Leiden en Leiderdorp	Leiden, Leiderdorp	
Sociale Dienst BBS	Baarn, Bunschoten, Soest	
Sociale Dienst Bommelerwaard	Maasdriel, Zaltbommel	
Sociale Dienst Oost Achterhoek	Berkelland, Oost-Gelre, Winterswijk	
Sociale Dienst Veluwerand	Ermelo, Harderwijk, Zeewolde	
Werkplein Noord-Groningen	De Marne, Winsum, Bedum	
Stroomopwaarts	Maassluis, Schiedam, Vlaardingen	
Uitvoering. Werk, Zorg, Jeugd, Inkomen Boxtel en Haaren	Boxtel, Haaren	
W&I De Wâlden	Achtkarspelen, Tytsjerksteradiel	
Lekstroom	Houten, IJsselstein, Lopik, Nieuwegein, Vianen	Gemeente Nieuwegein heeft 8 actieve accounts. De accounts worden breed ingezet voor bijna alle mogelijke rollen. Nieuwegein heeft het merendeel van de uitvoering van de Participatiewet uitbesteed aan Werk en Inkomen Lekstroom en deze heeft 76 accounts.
Werkplein Baanzicht	Aa en Hunze, Assen, Tynaarlo	
Werkplein Hart van West-Brabant	Etten-Leur, Halderberge, Moerdijk, Roosendaal, Rucphen, Zundert	

Samenwerkingsverbanden	Gemeenten	Gemeenten met achtergebleven accounts
Werkplein Regio Helmond	Asten, Deurne, Geldrop-Mierlo, Gemert-Bakel Helmond, Laarbeek, Someren	Gemeente Geldrop-Mierlo heeft 12 achtergebleven accounts. De volgende rollen zijn actief: GSD, Bedrijvenregister, Klantbeeld, langdurigheidstoeslag en Klant algemeen+. Gemeente Gemert-Bakel heeft 4 achtergebleven accounts. De volgende rollen zijn actief: GBA, GSD, RWD, Klant algemeen+, Gebruikersadministratie, BD, Participatiewet en inburgering. Gemeente Laarbeek heeft 3 achtergebleven accounts die alle drie inactief zijn. Vanaf 1 januari 2015 is er geen gebruik meer gemaakt van Suwinet door de gemeente. Gemeente Someren heeft 10 achtergebleven accounts. Deze accounts bevatten bijna alle mogelijke rollen. Er is één medewerker die Suwinet nog actief gebruikt en dat is voor Klant-algemeen+ en klantbeeld. Gemeenten Geldrop-Mierlo, Gemert-Bakel, Laarbeek en Someren hebben de uitvoering van de Participatiewet belegd bij gemeente Helmond en deze heeft 114 accounts.

Samenwerkingsverbanden	Gemeenten	Gemeenten met achtergebleven accounts
Wijzer	Bussum, Muiden, Naarden	
Dantumadiel	Dantumadiel, Dongeradeel, Ferwerderdiel, Kollumerland en Nieuwkruisland, Schiermonnikoog	
Samenwerkingsverband Beemster en Purmerend	Beemster, Purmerend	
Samenwerkingsverband Haarlem en Zandvoort	Haarlem, Zandvoort	
Samenwerkingsverband Hollands Kroon en Schagen	Hollands Kroon, Schagen	
Samenwerkingsverband Littenseradiel Súdwest Fryslân	Littenseradiel, Súdwest Fryslân	
Samenwerkingsverband Rhenen, Veenendaal, Renswoude	Renswoude, Rhenen, Veenendaal	
Samenwerkingsverband Brielle Nissewaard	Brielle, Nissewaard	
Samenwerkingsverband Boxmeer St. Anthonis	Boxmeer, Sint Anthonis	Gemeente St. Anthonis heeft 4 achtergebleven accouts waarvan 1 inactief. Deze accounts hebben een groot aantal rollen zoals Langdurigheidstoeslag en Klant algemeen+, maar ook de zware rol R1920. De algemene uitvoering wordt gedaan door de gemeente Boxmeer.

Samenwerkingsverbanden	Gemeenten	Gemeenten met achtergebleven accounts
WerkSaam West-Friesland	Stede Broec , Enkhuizen, Drechterland, Hoorn, Koggenland, Medemblik, Opmeer	Gem. Beemster heeft 6 accounts waarvan 0 actief. Gem. Stede Broec heeft 9 accounts waarvan 4 actief. De accounts worden breed ingezet voor bijna alle mogelijke rollen. Gem. Enkhuizen heeft 18 accounts waarvan 4 actief. De accounts worden breed ingezet voor bijna alle mogelijke rollen. Gem. Drechterland heeft 2 actieve accounts. Deze accounts worden gebruikt voor gsd home, gsd klant algemeen+ en gsd klantbeeld. Gem. Koggenland heeft 12 accounts waarvan 6 actief. Deze accounts worden ingezet voor alle rollen, behalve gsd-rollen. Gem. Medemblik heeft 4 actieve accounts. De accounts worden breed ingezet voor bijna alle mogelijke rollen. Gem. Opmeer heeft 1 actief account. Dit account wordt gebruikt alle mogelijke rollen. Deze gemeenten hebben de uitvoering van de Participatiewet uitbesteed aan Gem. Hoorn. Deze heeft 29 accounts waarvan 15 actief.
GR Het Plein	Lochem , Zutphen	
Rheden en Rozendaal	Rheden, Rozendaal	
Samenwerkingsverband Alpen aan den Rijn, Nieuwkoop, Kaag en Braassem	Alphen aan den Rijn, Nieuwkoop, Kaag en Braassem	

Samenwerkingsverbanden	Gemeenten	Gemeenten met achtergebleven accounts
Bedrijfsvoeringsorg. SWW-gemeenten	Stichtse Vecht, Weesp	
Samenwerkingsverband Borne Hengelo	Borne, Hengelo	Borne heeft 2 achtergebleven accounts waarvan alle accounts inactief zijn. Er is een rol gebruikersadministratie en een rol SCI (Inburgering). Sinds november 2014 of eerder worden de accounts niet meer gebruikt. Gemeente Borne heeft de uitvoering van de Participatiewet uitbesteed aan Hengelo en gemeente Hengelo heeft actieve 93 accounts.
Samenwerkingsverband Amerfoort en Leusden	Amersfoort, Leusden	
Dienst Dommelvallei	Nuenen, Gerwen en Nederwetten, Son en Breugel	
Samenwerkingsverband Groningen en Ten Boer	Groningen, Ten Boer	
Bestuursdienst Ommen-Hardenberg	Hardenberg, Ommen	Gem. Ommen heeft 9 accounts waarvan geen actief is. Er zijn geen GSD-rapportages. Ommen besteedt de uitvoering van de Participatiewet uit aan gem. Hardenberg.
Samenwerkingsverband Eindhoven/Waalre	Eindhoven, Waalre	
Samenwerkingsverband Apeldoorn	Apeldoorn, Brummen, Epe, Voorst	Gem. Voorst heeft 7 achtergebleven actieve accounts die gebruikt worden voor Belastingdienst en verschillende zelfsamengestelde groepen. De algemene uitvoering van de Participatiewet wordt gedaan door gem. Apeldoorn.

Samenwerkingsverbanden	Gemeenten	Gemeenten met achtergebleven accounts
Samenwerkingsverband Borger-Odoorn, Emmen	Borger-Odoorn, Emmen	Gem. Borger-Odoorn heeft 2 actieve achtergebleven accounts. Deze accounts worden gebruikt voor onder meer de Langdurigheidstoeslag. De algemene uitvoering wordt gedaan door gem. Emmen.
Samenwerkingsverband Vlagtwedde Bellingwedde	Bellingwedde, Vlagtwedde	
Samenwerkingsverband Waterland Landsmeer	Landsmeer, Waterland	
Samenwerkingsverband Zaanstad Oostzaan	Zaanstad, Oostzaan	
Samenwerkingsverband Edam-Volendam en Zeevang	Edam-Volendam, Zeevang	
Samenwerking Venray en Venlo	Venray en Venlo	Gem. Venray heeft 14 actieve accounts die vooral gebruikt worden voor GBA, Klant algemeen (+) en GBA volledig. Gem. Venray heeft de uitvoering van de Participatiewet uitbesteed aan gem. Venlo en deze heeft 98 accounts.
Samenwerkingsverband Werkendam en Woudrichem	Werkendam, Woudrichem	

Bijlage 10 Bevindingen landelijk onderzoek per norm en subnorm

In deze bijlage komen de 7 normen afzonderlijk aan bod die door de Inspectie zijn gebruikt om vast te stellen of de beveiliging van Suwinet op orde is Deze normen hebben betrekking op drie clusters. Informatiebeveiligings*beleid*, inrichting en onderhoud van de beveiligings*functie* en -*organisatie*, alsmede logische *toegangs*-beveiliging. In de beschrijving per norm wordt ook ingegaan op operationalisaties die door de Inspectie zijn aangebracht bij de 7 normen uit het GeVS Gemeenten die nog niet voldoen aan alle normen kunnen mede uit de beschrijving in dit hoofdstuk afleiden wat er van ze wordt verwacht In de individuele rapportages aan de gemeenten heeft de Inspectie overigens steeds per niet geaccordeerde norm een motivatie bijgevoegd

Het informatiebeveiligingsbeleid

Het toetsingskader schrijft voor dat gemeenten dienen te beschikken over een informatiebeveiligingsbeleid c q een beveiligingsplan dat specifiek (ook) op Suwinet is gericht Dit dient goedgekeurd te zijn door het management van de gemeente, te worden uitgedragen in de organisatie en jaarlijks te worden geevalueerd/geactualiseerd

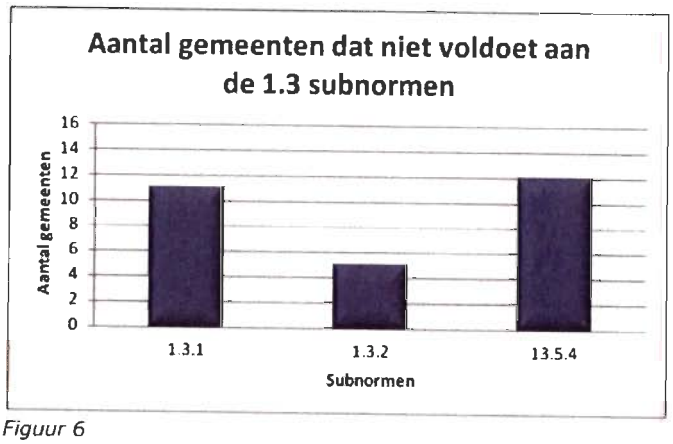
Norm 1.3: Het informatiebeveiligingsbeleid en het beveiligingsplan van het Suwinet zijn goedgekeurd door het management van de Suwi-partij

Deze norm impliceert goedkeuring door het management Door een enkele gemeente is gevraagd naar de operationalisatie van de term management. In de beleidsregels is dit niet verder uitgeschreven. In het onderzoek is uitgegaan van het College van B&W, het managementteam of de manager (directeur/afdelingshoofd) Het is van belang dat de betrokkenheid van de eindverantwoordelijke bij de totstandkoming en de inhoud van het beveiligingsbeleid ook aantoonbaar is (schriftelijk is vastgelegd).
Ook is geaccepteerd dat het management van een samenwerkingsverband heeft geaccordeerd namens de afzonderlijke gemeenten Dit is in afwijking van eerder onderzoek toen de Inspectie nog op het standpunt stond dat het moest gaan om het hoogste management van alle aangesloten gemeenten Bij 11 gemeenten was er geen sprake van een adequate goedkeuring van het beveiligingsplan of -beleid

Bij de beoordeling gaat de Inspectie na, of in geval van een algemeen informatiebeveiligingsbeleid en/of -plan, dat (ook) betrekking heeft op Suwinet Daarvoor moet er tenminste een aparte passage of hoofdstuk aan Suwinet zijn gewijd.
377 gemeenten (96%) van de onderzochte gemeenten beschikt over een goedgekeurd informatiebeveiligingsbeleid of -plan. Dit is een verbetering ten opzichte van 2014 en 2013 Toen scoorde 82% resp 76% van de gemeenten positief

- *Subnormen 1.3*

Van de 16 gemeenten die niet voldoen aan deze norm, falen er 11 op de eerste subnorm (69%), 5 op de tweede subnorm (31%) en 12 op de derde subnorm (75%). Aan de tweede subnorm wordt dus relatief het meeste voldaan, en aan de laatste subnorm het minste.



Figuur 6

1.3.1 Er is een specifiek op Suwinet gericht informatiebeveiligingsbeleid of veiligheidsplan aanwezig en/of er is een SUWI-specifieke passage aanwezig in een algemeen informatiebeveiligingsbeleid en -plan.
1.3.2 Dit beleid, dit plan of deze passage heeft specifiek betrekking op uw gemeente.
1.3.3 De goedkeuring van het plan/de passage is formeel vastgelegd.

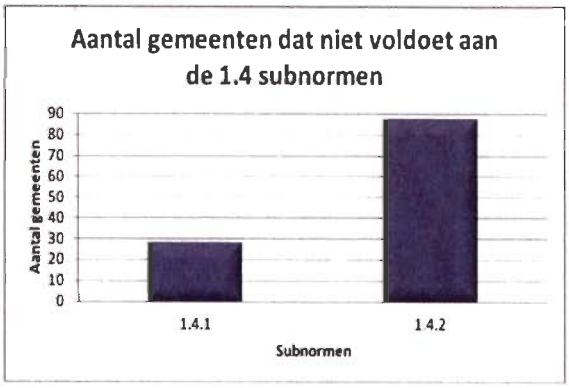
Norm 1.4 Het informatiebeveiligingsbeleid en het beveiligingsplan van het Suwinet worden uitgedragen in de organisatie

Deze norm heeft betrekking op de taak van het management om het bewustzijn van de medewerkers betreffende informatiebeveiliging te stimuleren.
Aan gemeenten is gevraagd aan te tonen dat het beleid en/of plan voor alle betrokkenen (centraal) beschikbaar is, bijvoorbeeld doordat het op het intranet is geplaatst, of via een handboek is verspreid. Daarnaast is gevraagd aan te tonen dat het onderwerp in het afgelopen jaar minimaal 2 keer aan de orde is geweest in overleg, afdelingsvergadering, trainingen en/of presentaties.

Deze norm is relevant omdat medewerkers actief op de hoogte moeten worden gesteld van wat wel en niet mag met Suwinet. De zgn. cultuuraspecten (gedrag, houding) mogen niet worden onderschat. Medewerkers dienen te beseffen dat zij gebruik maken van gevoelige gegevens. 303 Gemeenten (78%) scoren positief op deze norm. Vorig jaar was dit 74% en twee jaar geleden was dit 31%.

- *Subnormen 1.4*

Van de 88 gemeenten die niet voldoen aan deze norm, gaat het bij 28 om de eerste subnorm (32%) en bij 87 (99%) om de tweede subnorm. Bijna alle gemeenten (op één na) voldoen dus niet aan norm 1.4.2.



Figuur 7

1.4.1 Het informatiebeveiligingsbeleid, het beveiligingsplan of de beveiligingspassage is aantoonbaar centraal vastgelegd en beschikbaar voor alle gebruikers.

1.4.2 Er is gedurende de onderzoeksperiode minimaal 2x een actie geweest om de gebruikers (opnieuw) te attenderen op het bestaan van het veiligheidsbeleid.

Norm 1.5 Het informatiebeveiligingsbeleid en/of het beveiligingsplan van het Suwinet wordt jaarlijks geëvalueerd en indien nodig geactualiseerd.

Deze norm ziet erop toe dat na de implementatie van het beveiligingbeleid en/of -plan, deze blijft voldoen aan de meest actuele voorwaarden. In essentie gaat het om de vraag of risico's in voldoende mate in control blijven.
De Inspectie SZW verwacht bij plannen die ouder zijn dan 1 jaar een evaluatie. Als het afgelopen jaar een (nieuw) informatiebeveiligingsplan is vastgesteld wordt dit ook beschouwd als een actualisatie. De evaluatie moet een concrete actie zijn geweest van alle direct betrokkenen (inclusief de gebruikers, deze groep werd soms vergeten) en ook zijn vastgesteld door het management. Zo nodig leidt de evaluatie tot de aanpassing van het informatiebeveiligingsbeleid, -plan of -passage.

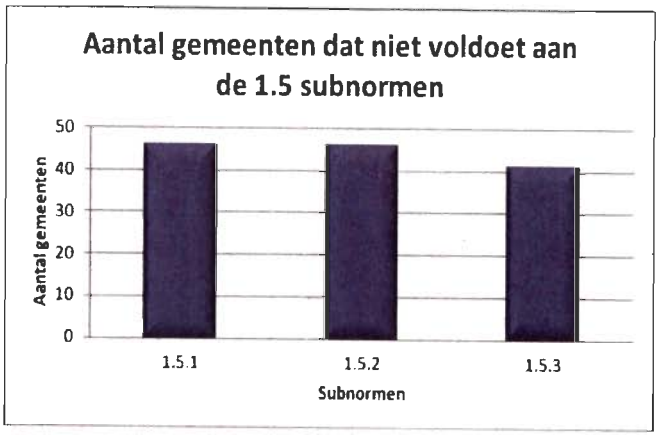
346 Gemeenten (88%) scoren positief. In 2014 was dat 53% en in 2013 was dat 21%.

Waar in oudere onderzoeken over de beveiliging van Suwinet (2009, 2013) regelmatig sprake was van zeer oude beveiligingplannen, kan de laatste jaren worden vastgesteld dat de meeste gemeenten wat dit betreft de zaken op orde hebben. In 2015 zette deze trend zich door. Nog maar 16 gemeenten hebben een plan dat dateert van voor 2013.

In een aantal gevallen gaf de gemeente aan de zelftest van VNG te beschouwen als evaluatie. Dit is als onvoldoende beoordeeld, aangezien de zelftest (evenals dit onderzoek) slechts ingaat op een beperkt aantal normen en geen gebruik maakt van informatie van het BKWI. Bij een zelftest zal de objectiviteit van de uitkomst ook altijd ter discussie staan. De Inspectie SZW verwacht bewijsstukken zoals: plan van aanpak evaluatie, vergaderverslagen, memo's ter beoordeling, documenten als een enquête of anderszins, waaruit blijkt dat de evaluatie breed is uitgezet.

- *Subnormen 1.5*

Van de 47 gemeenten die niet voldoen aan deze norm, gaat het bij 46 om de eerste subnorm (98%), bij 46 om de tweede subnorm (98%) en bij 41 (87%) om de derde subnorm. Als een gemeente niet voldoet aan deze norm, is de kans dus groot dat zij op alle subnormen is afgekeurd.



Figuur 8

1.5.1 De laatste evaluatie is minder dan een jaar oud.
1.5.2 De laatste evaluatie is vastgesteld door het management.
1.5.3 De evaluatie is een concrete actie van alle direct betrokkenen geweest, schriftelijk vastgelegd en leidt zo nodig tot aanpassen van het informatiebeveiligingsbeleid.

Inrichting en onderhoud van de beveiligingsfunctie en -organisatie van Suwinet

Voor de realisatie van een (meer dan) voldoende beveiligingsniveau voor Suwinet is een adequaat ingerichte organisatie een randvoorwaarde. Dit omhelst functiescheiding en de aanstelling van een persoon die de beveiligingsprocedures en -maatregelen in het kader van Suwinet beheert en beheerst (meestal security officer genoemd).

Norm 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.
- operationeel beheer
- functioneel beheer
- technisch beheer
- aansturing ICT-leveranciers
- security officer
- autorisatiebeheer
- eigenaarschap Suwinet

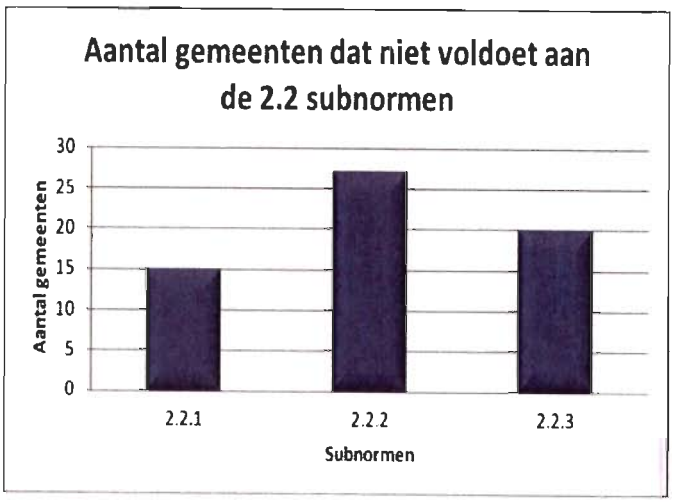
De Inspectie SZW heeft bij deze norm bekeken of de onderscheiden functies van medewerkers schriftelijk zijn vastgelegd, of aan de vraag welke taken waar zijn belegd een heldere overweging ten grondslag ligt, en of er functiescheiding is toegepast. Daarbij is gelet op de splitsing tussen beschikkende, controlerende en uitvoerende taken. Door de functies duidelijk te omschrijven en vast te leggen kan de functiescheiding in opzet worden aangetoond Sommige kleinere gemeenten hebben (door de beperkte omvang van hun ambtelijk apparaat) diverse functies binnen één persoon gecombineerd Indien de gemeente aangeeft zich bewust te zijn van de risico's van het (gedeeltelijk) ontbreken van functiescheiding en aantoonbaar aanvullende maatregelen heeft getroffen, is dit niet als negatief beoordeeld

In het onderzoek heeft de Inspectie SZW zich beperkt tot 4 gescheiden functies, in plaats van de 7 zoals deze formeel in de norm worden genoemd. De operationele, functionele en technische beheerfuncties zijn als één functie meegenomen.
In principe moeten minimaal de volgende functies bij verschillende personen zijn belegd
- uitvoering van taken (het gebruik van Suwinet zoals door de klantmanagers),
- het beheer van autorisaties (toegang verlenen tot Suwinet, de applicatie-beheerder van Suwinet),
- kwaliteitszorg en borging van rechtmatig gebruik (controle op gebruik van Suwinet, bijvoorbeeld de Security Officer);
- management (beslissen over bevoegdheden van functiegroepen en/of individuele medewerkers, uitdragen belang goed gebruik, bijsturen na oneigenlijk gebruik, optreden na misbruik Suwinet).

365 Gemeenten (93%) scoren positief op deze norm. In 2014 was dat 72% en in 2013 was dat 30%.

- *Subnormen 2.2*

Van de 28 gemeenten die niet voldoen aan deze norm, behalen er 15 de eerste subnorm (54%) niet, 27 de tweede subnorm (96%) niet en 20 (71%) de derde subnorm niet. Bij bijna alle gemeenten die niet voldoen aan deze norm gaat het dus om de tweede subnorm.



Figuur 9

2.2.1 Er is een schriftelijke vastlegging van de functiescheiding. Of er is een onderbouwde verklaring waarom zo'n functiescheiding er niet is en er is een alternatieve aanpak om misbruik te voorkomen.

2.2.2 In ons onderzoek beperken we ons tot 4 gescheiden functies (in plaats van de 7 zoals deze in de norm worden genoemd). In principe zijn minimaal de volgende functies bij verschillende personen belegd.

2.2.3 Er is vastgelegd dat ten aanzien van functiescheiding duidelijke keuzes zijn gemaakt bij het beleggen van taken.

Norm 2.3
- De security officer beheert en beheerst beveiligingsprocedures en -maatregelen in het kader van Suwinet, zodanig dat de beveiliging van Suwinet in overeenstemming met wettelijke eisen is geïmplementeerd.
- De security officer bevordert en adviseert over de beveiliging van Suwinet, verzorgt 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.
- De security officer rapporteert rechtstreeks aan het hoogste management.

Het is van belang dat er een medewerker is aangesteld die tot taak heeft te bevorderen en te controleren dat de beveiliging van het Suwinet op orde is. In het toetsingskader wordt voor deze functie de naam security officer gehanteerd. Deze persoon is deskundig op het terrein van informatiebeveiliging, controleert planmatig en periodiek of wordt voldaan aan de regels en analyseert eventuele incidenten. Tevens rapporteert hij aan het hoogste management of het bestuur van de organisatie.

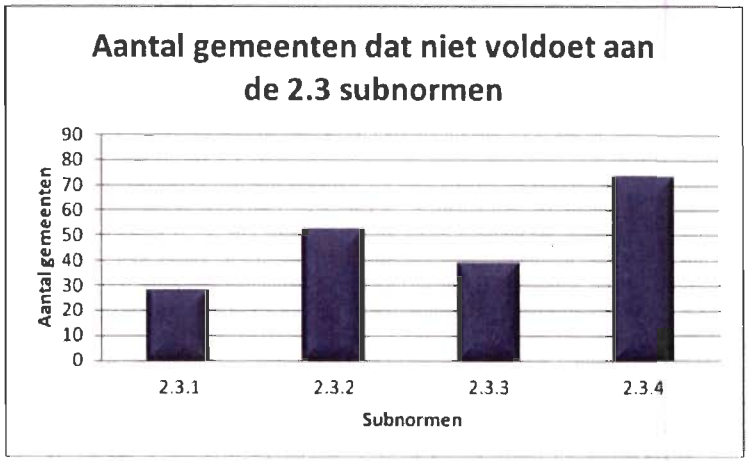
De Inspectie SZW heeft onderzocht of er een persoon aanwezig is die deze taken uitvoert; er dient periodiek – minimaal 2x per jaar – naar de beveiliging van Suwinet te worden gekeken. Daarbij is er niet alleen op gelet of de functie/taken in

de organisatie belegd zijn, maar ook of aan de hand van documenten aantoonbaar was dat de functiegerelateerde taken daadwerkelijk planmatig en periodiek werden uitgevoerd. Ook is gekeken of er een schriftelijke neerslag is van de uitgevoerde controles en van rapportages aan het hoogste management.

303 Gemeenten (78%) scoren positief op deze norm. In het vorige onderzoek scoorde 44% positief op deze norm. In 2013 scoorde 24% voldoende op norm 2.3.

- *Subnormen 2.3*

Van de 91 gemeenten die niet voldoen aan deze norm, zijn er 28 die de eerste subnorm (31%) niet behalen, 52 die niet scoren op de tweede subnorm (57%), 39 die niet voldoen aan de derde subnorm (43%) en 73 die niet voldoen aan de vierde subnorm (80%). Gemeenten scoren dus het minst op de laatste subnorm.



Figuur 10

2.3.1 De Security Officer is verantwoordelijk gemaakt om periodiek - ten minste twee keer per jaar - naar de beveiliging van Suwinet te kijken.
2.3.2 De Security Officer rapporteert en adviseert periodiek rechtstreeks aan het hoogste management.
2.3.3 Bovenstaande is vastgelegd in zijn/haar functieomschrijving inclusief takenoverzicht
2.3.4 Er zijn duidelijk waarneembare en vastgelegde activiteiten van de Security Officer gedurende de onderzoeksperiode.

Logische toegangsbeveiliging

Deze norm behelst de bescherming tegen ongeautoriseerde toegang, gebruik van de informatiehuishouding en uit te wisselen, te verwerken gegevens.

Norm 13.1 De Suwi-partij autoriseert en registreert de gebruikers die toegang hebben tot de Suwinet applicaties op basis van een formele procedure waarin is opgenomen:
- het verlenen van toegang tot de benodigde gegevens op basis van de uit te voeren functies/taken.
- het uniek identificeren van elke gebruiker tot een persoon
- het goedkeuren van de aanvraag voor toegangsrechten door de manager of een gemandateerde.
- het tijdig wijzigen (dus ook intrekken) van de autorisatie bij functiewijziging of vertrek.
- het benaderen van de Suwi-databestanden door gebruikers mag alleen plaatsvinden via applicatieprogrammatuur (tenzij sprake is van calamiteiten).

Er moet op controleerbare wijze worden aangetoond dat huidige of in het verleden verstrekte toegangsrechten tot Suwinet in overeenstemming zijn met het wettelijk kader van Suwinet en de Wet bescherming persoonsgegevens, de uitoefening van een functie, de in de organisatie vastgelegde bevoegdheden rondom het toekennen/ wijzigen/intrekken van Suwinet autorisaties, de in acht te nemen functiescheiding en de richtlijnen rondom het gebruik van Suwinet en de controle op het gebruik (logging)

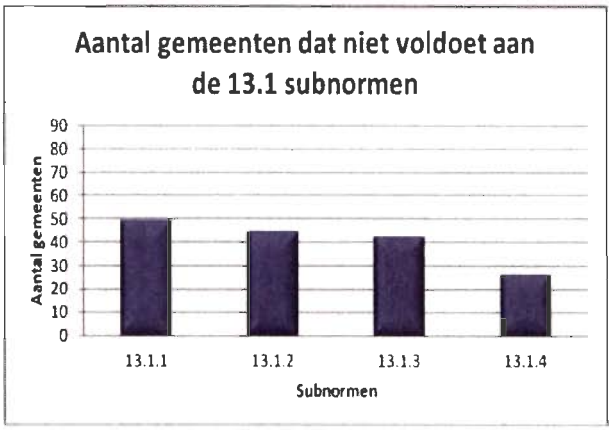
Daartoe is onderzocht of de gemeente beschikt over een autorisatieprocedure en -matrix Bekeken is of alle genoemde stappen (hierboven in kader) in het proces aanwezig zijn, helder zijn beschreven en zijn toegewezen aan bevoegde functionarissen binnen de gemeente.
Ook is bekeken of de autorisatiematrix specifiek ingaat op Suwinet, gebaseerd is op onderkende/aanwezige functieprofielen en aanwezige rollen in Suwinet In een rol wordt in feite vastgelegd tot welke gegevens op Suwinet de gebruiker van de rol wel of juist niet toegang krijgt zonder gebruik van een BSN Zoeksleutels, niet zijnde een BSN, zoals een achternaam, zijn gevoeliger voor misbruik omdat ze veel bekender zijn dan een BSN Dergelijke zoeksleutels behoren tot de zogenaamde zware rollen Door aan te geven welke persoon welke functie(s) uitoefent, kan op een gestandaardiseerde en controleerbare wijze de autorisatie voor een persoon binnen Suwinet worden verleend en gecontroleerd Het toekennen van rollen in Suwinet dient volgens een logische procedure plaats te vinden Hieruit moet duidelijk worden op basis van welke afwegingen, welke medewerker welke gegevens via welke zoeksleutel mag zien. Als de gemeente dit herleidbaar maakt, is dit afdoende
Daarnaast dient er controle op inactieve accounts plaats te vinden, dienen die periodiek te worden verwijderd en zijn zware rollen beperkt uitgedeeld. Bij 42 gemeenten was sprake van onjuist gebruik van zware rollen.

In principe heeft buiten de GSD/bijstand-medewerkers slechts een zeer beperkte groep toegang tot Suwinet. Het betreft de gemeentelijke belastingdeurwaarders, burgerzaken en de regionale meld- en coordinatiefunctie voortijdig schoolverlaten. Voor deze groepen dient een apart contract te worden afgesloten met de bronhouder(s) en BKWI Gebruik van Suwinet door overige functionarissen zoals WMO-medewerkers, medewerkers parkeerbeheer of andere hierboven niet benoemde medewerkers is wettelijk niet toegestaan Toch hadden 28 gemeenten oneigenlijke aansluiting bij Suwinet

301 gemeenten (77%) zijn positief beoordeeld op deze norm. Vorig jaar scoorde 53% voldoende en twee jaar gelden bedroeg dit percentage 38.

- *Subnormen 13.1*

Van de 90 gemeenten die niet voldoen aan deze norm, zijn er 49 (54%) waarvan de eerste subnorm niet is goedgekeurd, 44 waarbij de tweede subnorm (49%) is afgekeurd, 42 die de derde subnorm (47%) niet behalen en 26 die niet voldoen aan de vierde subnorm (29%). Er zijn dus geen subnormen die gemeenten opvallend vaker dan andere subnormen niet behalen.



Figuur 11

13.1.1 Er is een formeel vastgelegde autorisatieprocedure waarin de functies (dus geen personen) aan autorisaties en in het verlengde daarvan aan rollen worden gekoppeld.
13.1.2 Er vindt controle plaats op inactieve accounts die periodiek worden verwijderd.
13.1.3 Zware rollen zijn beperkt uitgedeeld.
13.1.4 In principe heeft buiten GSD/WWB-medewerkers slechts een zeer beperkte groep toegang tot Suwinet.

Norm 13.5 De controle op verleende toegangsrechten en gebruik vindt meerdere keren per jaar plaats.
- interne controle op rechten en gebruik van Suwinet.
- analyseren van de van het BKWI verkregen informatie over het gebruik van Suwi-gegevens.

Deze norm onderstreept het belang van het periodiek controleren of de verleende toegangsrechten in overeenstemming zijn met de vooraf bepaalde uitgangspunten. Zeker voor de zgn. zware rollen is de periodieke controle op uitgave van rechten en gebruik belangrijk. Voor 55 gemeenten kon niet worden aangetoond dat er meerdere controles per jaar hadden plaatsgevonden.

Bij geconstateerde afwijkingen van het reguliere zoekpatroon van gemeentelijke medewerkers, waarbij sprake blijkt te zijn geweest van onregelmatigheden, dienen corrigerende maatregelen te worden genomen. Deze zijn afhankelijk van de soort onregelmatigheden en variëren van beperking van toegangsrechten tot disciplinaire maatregelen bij geconstateerd misbruik van persoonsgegevens.

Het BKWI biedt maandelijks een generieke rapportage aan, waarin geaggregeerde en geanonimiseerde gegevens zijn opgenomen over het loggedrag van medewerkers Met andere woorden· over het zoekpatroon Voor gemeenten is dit – een overigens op zichzelf niet afdoende – handvat bij de controle. Mede op basis van die generieke rapportage kan de gemeente beoordelen of het nodig is om verdere informatie in te winnen bij BKWI in de vorm van een specifieke rapportage, bijv. als er veel wordt gezocht anders dan op BSN of als er veel raadplegingen zijn buiten kantooruren of bij een beperkt aantal gebruikers Een specifieke rapportage kan, in tegenstelling tot een generieke, gegevens bevatten over individuele medewerkers en/of clienten.

De Inspectie heeft het begrip 'meerdere keren' uit de norm geoperationaliseerd in die zin dat er tenminste 2x per jaar controle moet hebben plaatsgevonden Overigens is het minimaal 2x per jaar opvragen van een generieke rapportage geen harde eis voor de beoordeling. Het kwam ook voor dat een gemeente alleen specifieke rapportages opvroeg en daarmee gerichte controles uitvoerde Deze gemeente had een eigen vorm gevonden om de controle in te richten. Tevens kwam het voor dat gemeenten andere vormen van controle hadden gevonden, bijv door het hanteren van een steekproef waarbij opgevraagde BSN naast de BSN van het klantenbestand werd gelegd. Zodra er een BSN is geraadpleegd dat niet behoort bij een klant uit het bestand, moet de betreffende medewerker die het BSN heeft geraadpleegd, over nut en noodzaak een toelichting verschaffen

Op basis van alleen de generieke rapportages is geen sluitende controle uit te voeren. Enkele gemeenten realiseren zich dit niet en denken dat zij van BKWI bericht krijgen als er iets niet goed gaat De Inspectie stelt vast dat dit gelukkig steeds minder vaak voorkomt, en dat voorlichting hieromtrent van VNG en Inspectie heeft gewerkt
De Inspectie SZW verwacht van gemeenten dat zij periodiek en steekproefsgewijs ook specifieke rapportages bij hun controle inzetten (tenzij, zie boven, er een andere adequate vorm van controle wordt toegepast)

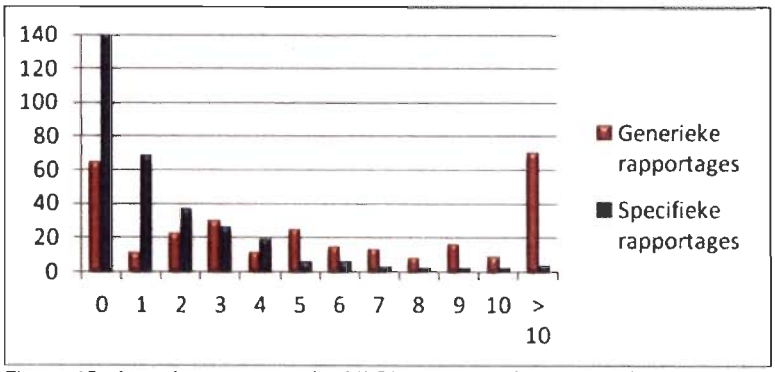
Aanvullend is gemeenten gevraagd of men een verklaring had voor bepaald opvallend zoekgedrag. Dat gedrag is door de Inspectie vastgesteld aan de hand van de bestanden die BKWI verplicht bijhoudt over het inloggedrag van ambtenaren Het zoekgedrag (en vooral de vraag of dat bekend was) is vooral een hulpmiddel in die gevallen waarin de Inspectie twijfelt aan opzet en/of bestaan en werking. Als de Inspectie onzeker is of genomen beveiligingsmaatregelen voldoen, kan waargenomen zoekgedrag de doorslag geven bij de te trekken conclusie. Ongeveer 40 gemeenten hebben geen sluitende verklaring voor opvallend zoekgedrag.

Als verklaring voor opvallende raadplegingen wijzen gemeenten vaak naar handhaving en fraudebestrijding, vooral door de Sociale Recherche. Veelal ontbreekt daarbij een nadere onderbouwing Het beeld ontstaat dat veel gemeenten aannemen dat het wel goed zit als het de Sociale Recherche betreft. Het komt weinig voor dat gemeenten werkelijk zicht hebben op welke gegevens de sociale recherche bij hun werk allemaal van Suwinet afhaalt, en waarom Wel heeft een enkele gemeente

opgemerkt dat hun accounts ingeval van samenwerking met meerdere gemeenten op het gebied van handhaving, werden ingezet voor (klanten van) andere gemeenten. Wat kon verklaren waarom er op hun accounts bovengemiddeld vaak bijv. op een niet-BSN werd gezocht.

297 gemeenten (76%) scoren positief op deze norm. In 2014 scoorde 37% positief en in 2013 scoorde 20% positief.

223 Gemeenten hebben in de periode januari tot september 2015 twee of meer generieke rapportages opgevraagd (figuur 12). Verder is zichtbaar dat gemeenten betrekkelijk weinig gebruik maken van specifieke rapportages van BKWI.



Figuur 12. Aantal gemeenten dat bij BKWI generieke en specifieke rapportages heeft opgevraagd in 2015.

BKWI heeft gemeld dat er door gemeenten na aankondiging van het onderzoek diverse vragen zijn gesteld en rapportages zijn opgevraagd. Voor zover dit plaatsvond voor 1 september 2015 zijn deze bij de beoordeling meegenomen.

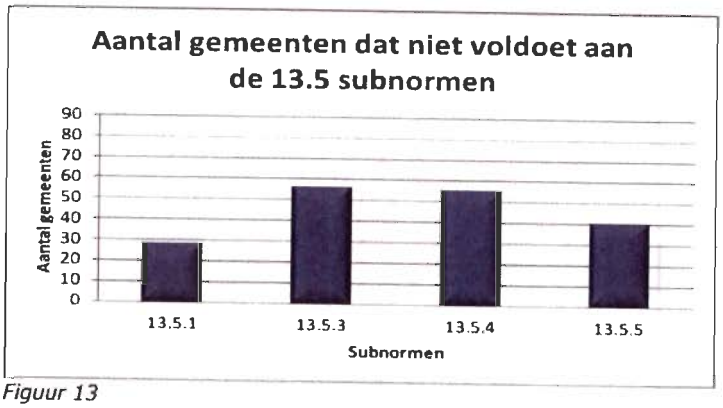
Uit een door de Inspectie aangedragen bestand met de namen van een honderdtal bekende Nederlanders is door BKWI bij één gemeente een raadpleging geconstateerd. Vorig jaar ging het nog om 7 gemeenten. Blijkbaar hebben de eerdere bevindingen van de Inspectie op dit punt voldoende bekendheid gekregen om dit soort misbruik van Suwinet vrijwel te voorkomen. Overigens bleek het bij die ene raadpleging uit 2015 te gaan om een abusievelijke, niet bewuste handeling.

Voor mensen met toegang tot Suwinet kan het overigens interessanter zijn om informatie op te zoeken die hen rechtstreeks raakt. Denk aan de vermogenspositie van de nieuwe vriend van een ex-partner, de nieuwe partner van een dochter, de aspirant kopers van huis/auto etc. De Inspectie kan hierop niet controleren, omdat het uiteraard niet beschikt over de namen van deze personen, laat staan hun BSN. Gemeenten die steekproefsgewijs de BSN van hun klanten vergelijken met door hun medewerkers geraadpleegde BSN, kunnen die controle deels wel uitvoeren. Deels, omdat als wordt gezocht op het BSN van een buur of bekende die wel een uitkering heeft van de gemeente (en daar dus klant is), er geen signaal 'opvallend' wordt afgegeven.

- *Subnormen 13.5*

Hoeveel gemeenten voldoen er niet aan de subnormen van 13.5?
(NB: subnorm 13.5.2 telt niet mee voor de analyse en is derhalve verwijderd.)

Van de 93 gemeenten die niet voldoen aan deze norm, behalen er 28 de eerste subnorm niet (30%), 56 de derde subnorm niet (60%), 55 de vierde subnorm niet (59%) en 40 voldoen niet aan de vijfde subnorm (43%).



Figuur 13

13.5.1 Een medewerker van de gemeente vraagt ten minste 2x keer per jaar bij BKWI een rapportage over het gebruik van Suwinet-Inkijk op.
13.5.3 Deze beoordelaar maakt hiervan schriftelijk verslag.
13.5.4 Als uit dit verslag blijkt dat nadere beoordeling gewenst is, wordt vervolgens bij BKWI een specifieke rapportage opgevraagd die vervolgens wordt beoordeeld.
13.5.5 Er mogen geen opvallende zoekpatronen zijn of, indien dit wel zo is, dient de gemeente daar een duidelijke verklaring voor te geven.

Bevindingen onderzoek 2015 ten opzichte van 2014

Bij het overzicht van de landelijke ontwikkelingen is al ingegaan op de uitkomsten van eerdere onderzoeken. Daarbij is de indeling gehanteerd in de vier groepen die in het escalatieprotocol worden onderscheiden. Onderstaand zijn de resultaten in het onderzoek van nu, en die uit het voorgaande onderzoek, nog eens per norm weergegeven. Een belangrijke constatering is dat binnen de groep die 6, 5 of 4 normen op orde heeft, de gemeenten met 6 behaalde normen het meest voorkomen (21%). Deze zitten dus nog maar 1 norm verwijderd van de optimale score.

Gemeente voldoet aan:	Aantal gemeenten onderzoek 2015 (n=78)	Percentage afgerond	De 393 gemeenten in onderzoek 2016	Percentage afgerond
7 normen	13	17%	192	49%
6 normen	13	17%	85	22%
5 normen	11	14%	52	13%
4 normen	13	17%	27	7%
3 normen	5	6%	16	4%
2 normen	7	9%	11	3%
1 norm	9	12%	6	1%
0 normen	7	9%	4	1%
	78	100%	393	100%

Bijlage 11 Overzicht verschillen normrealisatie

Verbetering in aantal normen waaraan een gemeente voldoet (2015 t.o.v. 2014)	Aantal gemeenten
+7	4
+6	6
+5	3
+4	5
+3	16
+2	5
+1	34
0	30
-1	3
-2	2
-3	2
TOTAAL	108

Bijlage 12 Ontwikkelingen

Informatievoorziening en -beveiliging zijn constant in ontwikkeling. Door het Ministerie van SZW zijn per brief van 5 februari 2015 diverse verbetermaatregelen aangekondigd (punt 1 t/m 4) Hieronder worden de activiteiten beschreven

1 Aanpak informatieveiligheid overheden

Door aanname van de Resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' geven gemeenten aan dat zij verder werken aan informatieveiligheid, onder andere door de zogenoemde Baseline Informatiebeveiliging Nederlandse Gemeenten uit te voeren Samen met de minister van BZK en de VNG wordt gewerkt aan de inrichting van een verantwoording informatiebeveiliging voor gemeenten waar de verantwoording over het Suwinet onderdeel van is.

De brief van de minister van BZK aan de Tweede Kamer van 18 december 2014 over informatieveiligheid bij de overheid geeft aan dat de verantwoording over informatieveiligheid aan vernieuwing en bundeling toe is, en de administratieve lasten voor gemeenten kunnen worden teruggedrongen Het doel van het recent gestarte ENSIA (Eenduidige Normatiek Single Information Audit) project is om een zo effectief en efficient mogelijk ingericht verantwoordingsstelsel voor informatieveiligheid te ontwikkelen dat in 2017 door alle gemeenten kan worden gebruikt
Het verantwoordingsstelsel is erop gericht om verantwoording af te leggen over informatieveiligheidsaspecten zoals deze verwoord zijn in de BIG maar ook over onder andere de normensets Suwinet.
De Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) is in 2013 vastgesteld door gemeenten De tactische baseline spreekt niet van aandachtsgebieden maar van hoofdbeveiligingscategorieen/secties en subcategorieen/secties en gebieden. De BIG kan worden beschouwd als een algemene richtlijn voor de informatiebeveiliging van alle gemeentelijke systemen Door één van de werkgroepen binnen het programmaplan is een concept van een nieuwe 'Suwinet-normenkader afnemers' opgesteld Daarbij zijn alle normen die gelijk zijn aan de BIG uit het bestaande normenkader

2 Aanpak verbetering gebruik Suwinet bij gemeenten

In november 2015 zijn de colleges van burgemeester en wethouders en de gemeenteraden door de staatssecretaris geinformeerd over het escalatieprotocol Het onderzoek van de Inspectie heeft ook een plek in het escalatieprotocol. Gemeenten die nog niet voldoen aan de 7 geselecteerde normen zullen allereerst een aankondiging tot aanwijzing ontvangen In de tweede helft van 2016 zal de Inspectie op deze groep een steekproef uitvoeren, conform een verzoek van de staatssecretaris. Mede afhankelijk van het resultaat kan dan een aanwijzing volgen

3 Programma 'Borging veilige gegevensuitwisseling via Suwinet'

Per brief van 8 november 2013 kondigde de staatssecretaris een privacy impact assessment naar het Suwinet aan. Dit omvat het wettelijk kader voor de gegevensuitwisseling via Suwinet evenals de keten die loopt van de aanlevering van gegevens door bronleveranciers, het transporteren van gegevens naar afnemers tot en met het gebruik van de gegevens door afnemers De uitkomst is dat in de afgelopen jaren een aantal samenhangende kwetsbaarheden is ontstaan die elkaar op een negatieve manier beinvloeden en daarmee tot privacyrisico's leiden UWV, SVB en VNG hebben op verzoek aangegeven welke maatregelen zij gaan treffen.

Om te zorgen voor een duidelijke sturing op de keten Werk en Inkomen en Suwinet, is vanuit de Suwipartijen UWV, SVB en de gemeenten (VNG) na 11 februari 2014 het zgn. Opdrachtgeversberaad van start gegaan. Hiermee is meer helderheid ontstaan over de verantwoordelijkheden voor de instandhouding van Suwinet, en zijn betere afspraken rondom privacy en beveiliging mogelijk geworden. Begin oktober 2014 heeft het Opdrachtgeversberaad het programmaplan 'Borging veilige gegevensuitwisseling Suwinet' aangeboden aan de bewindslieden van het ministerie van SZW. De maatregelen die de Suwi-partijen nemen, zijn geordend naar de mate van prioriteit en de volgtijdelijkheid van de maatregelen De maatregelen zijn daartoe in vier categorieen onderverdeeld

Categorie 1. Prioritaire maatregelen randvoorwaardelijk voor categorie 4
1 Ontwikkeling en invoering van een meer fijnmazige autorisatiestructuur bij gemeenten.
2 Verbetering logging en gebruiksrapportages

Categorie 2· Prioritaire maatregelen met een meer autonoom karakter
3 Ontwikkeling en vaststelling aansluitvoorwaarden en gebruiksvoorwaarden Suwinet-Inlezen
4 Ketenbrede awareness-campagne

Categorie 3. Onderzoeksmaatregelen die duiden of en hoe richtlijnen en beleid aanpassing behoeven
5 Beleid inzake misbruik van gegevens door medewerkers
6. Herijking normenkader en verantwoordingsrichtlijn Suwi in het licht van BIR/BIG
7. Telewerken en doorlevering van gegevens

Categorie 4· Vervolgmaatregelen op maatregelen categorie 1
8. Beperking zoekmogelijkheden in Suwinet-Inkijk
9 Beperking toegang Suwinet tot personen relevant voor werkzaamheden medewerker
10 Analyse van gegevens van bepaalde risicoklassen

De maatregelen waarvoor de Suwi-partijen het ministerie van SZW vragen om het initiatief te nemen zijn
11 Herijken van wet- en regelgeving SUWI
12 Levering van informatie in plaats van gegevens
13 Transparantie naar de burger
14 Afsluitbeleid

Aanvullend op het programmaplan is begin dit jaar een implementatieplan gemeenten opgesteld. Dit plan richt zich op het overdragen van de producten uit het programmaplan naar de gemeenten. Het implementatieplan richt zich primair op de eerste tien maatregelen. De looptijd is tot en met 2016

De Inspectie verwacht dat de diverse producten kunnen bijdragen aan een veiliger gebruik van Suwinet Mogelijkheden om de beveiliging verder te verbeteren ziet de Inspectie verder in het gebruik van standaardfunctieprofielen, het koppelen van standaardrapportages aan de eigen uitkeringspopulatie, het signaleren van opvragingen buiten deze groep, het signaleren bij opvragingen van bekende Nederlanders (of lokale bekenden) en het ontwikkelen van een richtlijn/methodiek met betrekking tot de controle van het gebruik van Suwinet door de sociale recherche Deze zijn ook deels al verwerkt in het programmaplan

4 Toekomstverkenning gegevensuitwisseling

Een voor Suwinet relevante verbetermaatregel betreft de 'Toekomstverkenning gegevensuitwisseling'.
Samen met UWV, SVB, VNG en het Inlichtingenbureau is gestart met de verkenning van een toekomstbeeld voor gegevensuitwisseling. Wet- en regelgeving SUWI betreffende gegevensverwerking en –uitwisseling wordt herijkt aan de toenemende gegevensuitwisseling tussen beleidsterreinen Vertrekpunt is wetswijziging in 2016, na de evaluatie van de wet SUWI in 2015 Wet- en regelgeving kan echter eerder wijzigen als dit randvoorwaardelijk is voor de maatregelen van het programma 'Borging veilige gegevensuitwisseling via Suwinet'

Vervolg Inlezen·
De Autoriteit Persoonsgegevens heeft in 2015 een onderzoek uitgevoerd naar Inlezen. Constatering daarbij was dat ook bronhouders zich moeten verantwoorden over hoe een veilig gebruik van gegevens die worden verwerkt in eigen applicaties (via Inlezen) is geborgd. UWV heeft naar aanleiding van dit onderzoek een plan van aanpak – borgen van een adequaat beveiligingsniveau voor het gebruik van gegevens via (Suwinet en DKD) Inlezen – opgesteld (30 oktober 2015).
Het plan kent 3 stappen
-aanscherpen aansluit- en gebruiksvoorwaarden,
-de beoordeling van de periodieke verantwoordingsrapportage en
-het melden door BKWI aan het bevoegd gezag
Vanaf 2017 dienen deze stappen te zijn ingevoerd Het plan heeft relaties met het hiervoor beschreven ENSIA project.

Bijlage 13 Publicaties van de Inspectie SZW – directie Werk en Inkomen

2016

R16/01	Kansen op uitstroom
R16/02	Suwidienstverlening en de governance SVB
R16/03	Literatuurstudie Integrale dienstverlening

2015

R15/01	Gemeentelijke aandacht voor verdringing door bijstandsgerechtigden
R15/02	Suwinet 'veilig omgaan met elkaars gegevens'
R15/03	Buitenspel, De uitvoering voor jongeren in de WW of bijstand
R15/04	Arbeidsomstandigheden van gedetacheerde medewerkers in de Sociale Werkvoorziening
R15/05	Verkennende studie. Signalen en klachten over toegankelijkheid van dienstverlening in het sociale domein
R15/06	Beschut werken
R15/08	Verordeningen Tegenprestatie – inventarisatie –
R15/09	Verkennende studie Werkgeversperspectief
R15/10	Verkennende studie Verwerken van meldingen en signalen over inkomsten. 'Minder gemist!'

2014

R14/01	Handhaving tijdens de Dienstverlening
R14/02	Kansen voor oudere Ww-ers (45+)!
R14/03	Afspraken en resultaten regionaal arbeidsmarktbeleid
R14/04	Ken uw klanten
R14/05	De boete belicht
R14/06	Uitvoering van de WWB voor jongeren (18-27 jaar)

2013

R13/01	De Sociale Verzekeringsbank; Veranderprogramma SVB Tien
R13/02	De invloed van ontheffingen op de arbeidsparticipatie van WWB'ers
R13/03	Regierol gemeenten bij regionaal arbeidsmarktbeleid
R13/04	Over signaal, sanctie en incasso
R13/05	Dienstverlening aan oudere (45+) bijstandsgerechtigden
R13/06	Van schoolgaand kind tot zelfstandig jongere ACTIEF OP WEG NAAR WERK
R13/07	Verordeningsplicht gemeenten maatschappelijke participatie kinderen
R13/08	De burger bediend in 2013
R13/09	Voor wat hoort wat, Een beschrijving van de uitvoering van de tegenprestatie naar vermogen door gemeenten

[redacted]

De Inspectie SZW maakt deel uit van
het Ministerie van Sociale Zaken en
Werkgelegenheid

Inspectie SZW
Postbus 820 | 3500 AV Utrecht
Telefoon 0800 5151
(gratis)
www inspectieszw nl

Mei 2016