Inspectie SZW
Ministerie van Sociale Zaken en Werkgelegenheid

Veilig gebruik Suwinet 2013

Een onderzoek naar de beveiliging van gegevens die worden uitgewisseld binnen het Suwinet door gemeenten.

Nota van bevindingen

Colofon

Programma	B
Projectnaam	(PIn27/On) Veilig gebruik Suwinet
Versie	2.0 definitief
Datum	26 augustus 2013
Nummer	

Inhoud

1 Samenvatting en conclusies

1.1 Aanleiding en achtergrond

Bij eerdere onderzoeken van de rechtsvoorganger van de Inspectie SZW is melding gemaakt van gebrekkige beveiliging van persoonsgegevens en incidenteel gebruik van misbruik of oneigenlijk gebruik van daarvan. In 2012 stelde de inspectie vast dat gemeenten de afgelopen jaren maatregelen hebben getroffen om de beveiliging van de gegevensuitwisseling van Suwinet te verbeteren, maar dat verdere verbetering noodzakelijk lijkt.

De toenmalige Staatssecretaris van SZW (De Krom) heeft in juni 2012 een brief geschreven aan alle gemeenten in Nederland, waarin hij gemeenten waarschuwt voor de soms matige beveiliging van de gegevens die zij verwerken bij het verrichten van hun taken in de sociale zekerheid.[1] Hij wijst de gemeenten op hun verantwoordelijkheid voor het gebruik van persoonsgegevens door medewerkers van de gemeenten. Verder kondigt hij met deze brief een vervolgonderzoek van de Inspectie SZW aan naar de beveiliging van Suwinet.

Hij heeft de inspectie SZW gevraagd om in 2013 onderzoek te doen naar de beveiliging van Suwinet door gemeenten.[2] De inspectie heeft ingestemd met dit verzoek.

1.2 Onderzoeksvragen

Het verzoek van de staatssecretaris luidt:
Geef een representatief beeld van de mate waarin gemeenten voldoen aan de eisen die worden gesteld aan de beveiliging van uitwisseling van informatie die wordt uitgewisseld binnen het Suwinet en geef hierover een oordeel.

Het gevraagde onderzoek dient bij te dragen aan het verbeteren van de beveiliging van het Suwinet door in een nota van bevindingen een representatief beeld te geven van de mate waarin de beveiliging van het Suwinet door gemeenten op orde is.
Op basis van de bevindingen per gemeente kan de staatssecretaris besluiten nadere maatregelen te treffen om de beveiliging van Suwinet in betrokken gemeente(n) op orde te doen brengen.

De centrale vraag in het onderzoek is als volgt geformuleerd:
In welke mate voldoen gemeenten aan de eisen van vertrouwelijkheid die worden gesteld aan de beveiliging van informatie die wordt uitgewisseld binnen het Suwinet in 2012?[3]

De deelvragen van dit onderzoek zijn:
1. *Voldoen gemeenten aan de wettelijke verplichtingen inzake de informatiebeveiliging? (o.a. actueel beveiligingsplan)*
2. *Op welke wijze hebben gemeenten de verantwoordelijkheden in de organisatie belegd (o.a. rol security officer, rol verantwoordelijk management)*
3. *Worden de bevoegdheden aan medewerkers conform de voorwaarden verstrekt?*

[1] Brief van 8 juni 2012 aan de Colleges van B&W van de gemeenten in Nederland, kenmerk RUA/UO/2012/6612
[2] Brief d.d. 28 juni 2012, kenmerk RUA/A/2012/9996.
[3] Met vertrouwelijkheid wordt bedoeld dat een gegeven alleen te benaderen is door iemand die gemachtigd is het gegeven te benaderen en voor de uitvoering van zijn wettelijke taken nodig heeft.

4. *In hoeverre vragen gemeenten algemene en/of specifieke rapportages op bij BKWI (op basis van logfiles) over het gebruik van Suwinet?*

1.3 Toetsingkader

De inspectie gaat in dit onderzoek uit van de essentiële normen voor het waarborgen van de vertrouwelijkheid, opgenomen in het Normenkader GeVS (Gezamenlijke elektronische Voorzieningen SUWI)[4]. Deze hebben betrekking op:

- Het informatiebeveiligingsbeleid en het informatiebeveiligingsplan voor Suwinet;
- De inrichting en onderhoud van de beveiligingsfunctie en de beveiligingsorganisatie van Suwinet (waar onder de aanstelling van een security officer);
- De logische toegangsbeveiliging, gericht op het voorkomen van ongeautoriseerde toegang tot en gebruik van persoonsgegevens.

1.4 Onderzoeksmethoden

Voor dit onderzoek is een zuiver aselecte steekproef getrokken van 80 uit de 415 gemeenten in Nederland, in het jaar 2012.
Aangezien dit een representatieve steekproef is van voldoende omvang kan de inspectie op grond van de bevindingen bij de steekproefgemeenten algemeen geldende uitspraken doen over alle gemeenten.

Waar een gemeente uit de steekproef samenwerkt met één of meer andere gemeenten op het gebied van sociale zaken binnen een intergemeentelijke sociale dienst of anderszins heeft het onderzoek zich gericht op het samenwerkingsverband. Lees hiervoor ook paragraaf 4.3, Samenwerking in de uitvoering.

De beoordelingen van de inspectie zijn gebaseerd op de antwoorden die de steekproefgemeenten hebben gegeven naar aanleiding van de vragenlijst en op de bijbehorende bewijsstukken die gemeenten hebben ingezonden. [5]

Verder heeft de inspectie gebruik gemaakt van de BKWI-rapportages over het gebruik van Suwinet per steekproefgemeente over de periode november 2011 tot en met oktober 2012.

Tenslotte heeft de inspectie (geanonimiseerde) gegevens uit de logfiles van de desbetreffende gemeenten opgevraagd bij BKWI. Zie voor een uitgebreidere beschrijving van de onderzoekmethode bijlage 2.

[4] Het Normenkader GeVS maakt deel uit van de Verantwoordingsrichtlijn GeVS. Zie hiervoor verder bijlage 3, Wettelijk Kader.

[5] Zie voor de vragenlijst bijlage 5.

1.5 Conclusies

CENTRALE VRAAGSTELLING:

In welke mate voldoen gemeenten aan de eisen van vertrouwelijkheid die worden gesteld aan de beveiliging van informatie die wordt uitgewisseld binnen het Suwinet in 2012?

Antwoord:

4% van de onderzochte gemeenten voldoet aan alle zeven door de inspectie getoetste normen inzake de informatiebeveiliging en voldoen daarmee op deze punten aan hun wettelijke verplichtingen.

	Aantal gemeenten	Percentage van het totaal aan tal gemeenten
Gemeente voldoet aan 7 normen	3	4%
Gemeente voldoet aan 6 normen	3	4%
Gemeente voldoet aan 5 normen	8	10%
Gemeente voldoet aan 4 normen	6	8%
Gemeente voldoet aan 3 normen	15	19%
Gemeente voldoet aan 2 normen	9	11%
Gemeente voldoet aan 1 norm	26	33%
Gemeente voldoet aan 0 normen	10	13%
Totaal	80	100% [6]

DEELVRAAG 1
Voldoen gemeenten aan de wettelijke verplichtingen inzake de informatiebeveiliging? (o.a. actueel beveiligingsplan)

Antwoord:
85% van de steekproefgemeenten kon een informatiebeveiligingsplan voor Suwinet overleggen. Dat wil niet zeggen dat de toegezonden beveiligingsplannen alle actueel zijn. De inspectie heeft vastgesteld van wanneer de plannen dateren. De datering van de informatiebeveiligingsplannen loopt uiteen van september 2005 tot december 2012. De gemiddelde leeftijd van de plannen is ruim vier jaar. 21% van de beveiligingsplannen is jonger dan 2 jaar.

In 24% van de gevallen was het informatiebeveiligingsplan niet voorzien van een formele goedkeuring.

Bij 69% van de gemeenten kon met de door hen aangeleverde informatie onvoldoende worden aangetoond dat het beveiligingsplan binnen de gemeente actief is uitgedragen.

[6] Door afrondingsverschillen tellen de cijfers in deze tabellen niet altijd op tot exact 100%.

79% van de gemeenten evalueert (en waar nodig: actualiseert) het beveiligingsplan niet regelmatig (ten minste eens in de twee jaar).

Bij gemeenten bestaat nogal eens het misverstand dat een beveiligingsbeleid- of plan voor de GBA ook voor Suwinet zou gelden, terwijl aan Suwinet andere en specifieke eisen worden gesteld, die afwijken van de maatregelen voor de GBA.

DEELVRAAG 2
Op welke wijze hebben gemeenten de verantwoordelijkheden in de organisatie belegd (o.a. rol security officer, rol verantwoordelijk management)

Antwoord:
Circa 30% van de gemeenten voldoet aan de norm dat de taken, verantwoordelijkheden en bevoegdheden ten aanzien van het gebruik, de inrichting, het beheer en de beveiliging van Suwinet-gegevens, applicaties, processen en infrastructuur zijn beschreven en duidelijk gescheiden zijn belegd (functiescheiding). Voor deze gemeenten geldt met andere woorden dat zij voldoende duidelijk hebben aangetoond waarom welke functionarissen welke autorisaties hebben binnen Suwinet. Er zijn dan onder andere functiebeschrijvingen en er wordt gewerkt met een autorisatiematrix zodat duidelijk is wie welke (zware) rollen heeft.

Voor de gemeenten die niet voldoen aan de norm, geldt dat deze vaak geen functiescheiding hebben vastgelegd of dit niet volledig hebben gedaan. Er wordt dan wel aangegeven dat men binnen de gemeente met diverse functies werkt, maar functiebeschrijvingen ontbreken of zijn onvoldoende gedetailleerd. Ook zijn er gemeenten die duidelijk hebben vastgelegd welke personen welke autorisaties hebben in Suwinet, echter niet waarom ze dan deze autorisatie nodig hebben. Verder constateert de inspectie dat binnen sommige gemeenten dezelfde functionarissen verschillende autorisaties hebben zonder dat duidelijk wordt gemaakt waarom dit zo is. De inspectie constateert dat de meeste gemeenten niet in staat zijn aantoonbaar te maken wie welke taken met betrekking tot Suwinet uitvoert en op basis waarvan dit is vastgesteld. In deze gevallen is dientengevolge ook niet vast te stellen of er sprake is van voldoende functiescheiding.

De inspectie heeft vastgesteld dat 58% van de gemeenten een security officer heeft aangemeld bij BKWI. Bij de aangemelde security-officers blijkt in de praktijk meestal sprake van een beperkte taakopvatting. Veelal is er sprake van een formele aanstelling, waarbij er maar weinig invulling wordt gegeven aan de functie. Een van de taken van een SO is om het hoogste management te adviseren over de beveiliging van Suwinet; bij de onderzochte gemeenten heeft de inspectie niet gezien dat aan deze adviesfunctie enige invulling werd gegeven.

DEELVRAAG 3
Worden de bevoegdheden aan medewerkers conform de voorwaarden verstrekt?

Antwoord:
32 van de 80 onderzochte gemeenten (38%) waren in staat om aan de inspectie een geformaliseerde, correcte en in gebruik zijnde autorisatieprocedure en autorisatiematrix te verstrekken.

De 48 gemeenten die niet voldeden aan deze norm (60%), zijn te verdelen in een drietal groepen:

1. gemeenten die geen autorisatieprocedure en geen autorisatiematrix met betrekking tot Suwinet hebben.

Dit betreft vaak gemeenten met een klein tot zeer klein aantal mensen die gebruik moeten maken van Suwinet. De gemeente beschouwt dan deze procedure als te bureaucratisch. Men vertrouwt dan meer op het bestaan van onderling toezicht.
Het risico bestaat nu dat er fouten worden gemaakt in het verlenen van autorisatie aan personen (onterechte toegang) en/of in het toekennen van Suwinet-rollen aan een bepaald persoon (doorbreking van functiescheiding).

2. gemeenten die wel een formele autorisatieprocedure hebben, maar geen specifieke Suwinet-autorisatiematrix.
   Het risico bestaat nu dat er fouten worden gemaakt in het toekennen van Suwinet rollen aan een bepaald persoon (doorbreking van functiescheiding).

3. gemeenten die wel een formele autorisatieprocedure en autorisatiematrix Suwinet hebben, maar dat in de autorisatiematrix Suwinet: ·
   - of geen functies staan vermeld, maar afdelingen
   - of geen Suwinet rollen staan vermeld, maar uit te voeren taken in tekst

   Het risico bestaat hier ook dat er fouten worden gemaakt in het toekennen van Suwinet-rollen aan een bepaald persoon (doorbreking van functiescheiding).

DEELVRAAG 4
In hoeverre vragen gemeenten algemene en/of specifieke rapportages op bij BKWI (op basis van logfiles) over het gebruik van Suwinet?

Circa een derde van de onderzochte gemeenten voldoet aan de norm dat er meerdere keren per jaar plaats controle plaatsvindt op verleende toegangsrechten en op het gebruik, zodanig, dat die werkwijze ook voor de Inspectie is te herleiden. Een voorbeeld hiervan zijn gemeenten die steekproefsgewijs periodiek alle opvragingen van een medewerker aan de hand van de eigen WWB populatie controleren en eventuele verschillen nader uitzoeken. Ook worden hiervoor de standaard overzichten van BKWI gebruikt en incidenteel een specifieke rapportage opgevraagd.

Van de overige gemeenten geeft circa de helft aan de controle aan de hand van de standaard BKWI overzichten uit te voeren, maar kan niet aangeven waarop precies wordt gelet. Van deze controles zijn in het algemeen geen aantekeningen of rapportages beschikbaar zodat de Inspectie niet kan herleiden hoe deze controles hebben plaatsgevonden. In veel gevallen hadden deze gemeenten het door de Inspectie gesignaleerde afwijkende zoekgedrag zelf niet geconstateerd en konden dat ook niet verklaren. Zo kunnen gemeenten meestal niet aangeven waarom de zoeksleutel op kenteken wordt gebruikt terwijl het autobezit ook via de 'standaard' ingang (Burgerservicenummer) is te zien. Hoge aantallen raadplegingen op postcode/huisnummer worden regelmatig verklaard door de huishoudinkomenstoets waarbij gecontroleerd is of er op het opgegeven adres ook andere personen met een inkomen wonen. Hoewel deze verklaring plausibel lijkt, is dit door de betreffende gemeenten op account/medewerkerniveau niet verder gecontroleerd. Of deze verklaring in alle geconstateerde gevallen een rol speelt blijft dus onduidelijk. Andere verklaringen zijn: verhaal waarvoor personen buiten de gemeente moeten worden gezocht of controle op naam omdat het BSN bij de eerste contacten niet bekend is. Ook voor deze verklaringen is geen nadere onderbouwing aangetroffen.

De andere gemeenten, circa een derde van het totaal gaven aan deze controle niet of zeer beperkt uit te voeren, of hierbij kwam de inspectie zelf tot deze conclusie.

De inspectie heeft ook gecontroleerd of binnen gemeenten gegevens van 100 willekeurig geselecteerde bekende Nederlanders zijn geraadpleegd, iets wat eveneens kan wijzen op oneigenlijk gebruik.
Bij 14 van de 80 onderzochte gemeenten (18%) zijn in 2012 gegevens van bekende Nederlanders met gebruikmaking van Suwinet-Inkijk geraadpleegd, zonder dat hiervoor een goede reden is gegeven. Eén van deze gemeenten heeft hiervoor een plausibele verklaring gegeven. De overige dertien konden de raadplegingen niet verklaren.

Enkele gemeenten geven aan in het verleden met behulp van de overzichten van BKWI, misbruik of oneigenlijk gebruik te hebben geconstateerd en hiervoor maatregelen te hebben genomen.

OVERIGE BEVINDINGEN

Inlezen

Gemeenten hebben de mogelijkheid om naast het online opvragen van gegevens via Suwinet-Inkijk ook gegevens van burgers op te kunnen vragen en direct over te nemen in de eigen systemen, het zogenoemde 'Suwinet Inlezen'. Het voordeel hiervan is dat deze gegevens direct voor verdere administratieve handelingen kunnen worden gebruikt en niet nogmaals hoeven te worden ingevoerd.
De via Suwinet-inlezen opgevraagde gegevens worden echter niet gelogd en zijn, nadat deze zijn overgenomen in het gemeentelijke systeem, ook vanuit deze omgeving te benaderen. Toegangsbeheer, logging, controles etc. dienen dan ook in deze omgeving te zijn ingericht. Gegevens over het gebruik worden niet opgenomen in de centrale logfiles van BKWI en zijn evenmin opgenomen in de reguliere maandrapportages over het gebruik van Suwinet.

Van de 80 gemeenten in de steekproef geven er 6 aan gebruik te maken van de mogelijkheid van Suwinet-Inlezen en hebben de betreffende vragen hierover ingevuld.
De BKWI-website vermeldt dat inmiddels meer dan de helft van de gemeenten gebruik maakt van systemen die gegevens kunnen inlezen via Suwinet."
Geen van deze gemeenten heeft op voldoende wijze aangegeven op welke manier de waarborgen rondom het gebruik van Suwinet Inlezen gestalte hebben gekregen.

De inspectie heeft geprobeerd via BKWI een actueel beeld over het gebruik van Suwinet Inlezen te verkrijgen. Doordat een centrale registratie rondom het gebruik van Suwinet Inlezen ontbreekt, is de Inspectie niet in staat de door gemeenten verstrekte antwoorden, met betrekking tot het geen gebruik maken van Suwinet Inlezen, te valideren.

In alle gevallen ontbreekt een sluitende aanpak bij het gebruik van Suwinet Inlezen. Het is de inspectie niet duidelijk geworden op welke wijze gemeenten de toegangsrechten voor het gebruik van deze gegevens verlenen en hoe zij de controle op het gebruik hiervan uitvoeren.

Monitor zorgvuldig gebruik Suwinet

In het kader van de campagne zorgvuldig gebruik Suwinet is gebruik gemaakt van een monitor van BKWI. De monitor 'Gebruik Suwinet' geeft voor elke sociale dienst in Nederland een indicatie van de wijze waarop Suwinet gebruikt wordt. De scores worden weergegeven in een overzicht per gemeente met groen, oranje of rood, afhankelijk van de mate waarin de scores op de indicatoren om aandacht vragen.

Een goede score op de monitor-indicatoren wil niet zeggen dat daarmee wordt voldaan aan het normenkader. Er zijn veel meer aspecten waaraan de informatiebeveiliging moet voldoen. De resultaten van de monitor kunnen wel aanleiding geven tot verder onderzoek door de gemeente.

Uit de contacten die de inspectie gedurende de looptijd van dit onderzoek met gemeenten heeft gehad, is naar voren gekomen dat er bij gemeenten veel misverstand is over de duiding van de scores op de indicatoren.
In het bijzonder de hoofdconclusie op de monitor, bijvoorbeeld "Status per 1 oktober 2012, 80% op orde" wordt nogal eens onjuist geïnterpreteerd; gemeenten maken hieruit op dat zij met 80% goed presteren, terwijl het beperkte aantal indicatoren van de monitor slechts een zeer beperkt gedeelte van dat terrein bestrijkt.

Uit de onderzoeksresultaten van de inspectie blijkt dat er weinig overeenkomst is tussen de mate waarin gemeenten in dit onderzoek voldoen aan de zeven normen met betrekking tot vertrouwelijkheid en de scores op de BKWI-monitor.

De uitkomsten van de BKWI-monitor blijken een ander, gunstiger beeld te geven over de informatiebeveiliging door gemeenten dan uit het onderzoek van de inspectie naar voren komt. Dit geldt met name bij gemeenten die slechts aan enkele normen voldoen. Een voorbeeld hiervan is dat de 10 gemeenten waarbij de inspectie constateerde dat aan geen van de zeven essentiële normen werd voldaan gemiddeld 68% op orde scoorden op de BKWI-monitor.

Samenwerking in de uitvoering

Een aanzienlijk aantal gemeenten werkt samen voor wat betreft de uitvoering van de WWB en aanverwante sociale voorzieningen. Onder de 80 gemeenten waarop het onderzoek zich heeft gericht, bevonden zich 30 gemeenten die op een of andere manier samenwerken.

Uit haar contacten met gemeenten in de loop van dit onderzoek is bij de inspectie het beeld ontstaan dat deze vormen van samenwerking in veel gevallen tot gevolg hebben dat de individuele gemeenten nauwelijks verantwoordelijkheid voelen voor de uit wet- en regelgeving voortvloeiende eisen op het gebied van de privacy bij de uitvoering van de WWB, omdat zij de verantwoordelijkheid voor de uitvoering hebben overgedragen. Volgens de inspectie ontslaat zo'n overdracht een gemeente echter niet van de taak om zich ervan te vergewissen dat de overgedragen taak naar behoren wordt uitgevoerd, ook waar het gaat om de privacyaspecten daarvan.

Integriteits- en geheimhoudingsverklaringen

Als onderdeel van hun beveiligingsbeleid hanteren veel gemeenten een geheimhoudingsverklaring die door hun medewerkers moet worden ondertekend. Andere gemeenten laten hun medewerkers daarnaast of in plaats daarvan een integriteitverklaring ondertekenen, die inhoudt dat de ondertekenaar verklaart op integere wijze

te zullen omgaan met de verleende toegang tot gemeentelijke informatiesystemen. Ook zijn er gemeenten die niet dit soort verklaringen laten tekenen, maar hun medewerkers alleen een ambtseed laten afleggen. De ambtseed is echter niet van toepassing op ingehuurd personeel.

Het valt de inspectie op dat niet alle gemeenten die een geheimhoudings- of integriteitverklaring hanteren, zo'n verklaring ook laten ondertekenen door extern (ingehuurd) personeel. Hoewel dergelijke externen net als de ambtenaren zijn gebonden aan de wettelijk regels en eisen ter zake van het gebruik van (persoons-)gegevens, kan juist voor hen een integriteitverklaring een meerwaarde kan hebben. Zij hebben vaak geen ambtelijke achtergrond van waaruit de wettelijke bepalingen hun bekend kunnen zijn, en een ambtseed die hen aan hun verplichtingen zou kunnen herinneren, wordt door hen niet afgelegd.

2 Inleiding

2.1 Introductie

Overheidsorganisaties zoals het Uitvoeringsinstituut Werknemersverzekeringen (UWV) inclusief UWV WERKbedrijf, de Sociale Verzekeringsbank (SVB) en gemeenten wisselen onderling grote hoeveelheden gegevens van burgers uit.
Miljoenen keren per jaar raadplegen hun medewerkers via de elektronische voorziening Suwinet-persoonsgegevens voor met name het toekennen en intrekken van uitkeringen. Zij raadplegen daartoe elkaars databestanden en ook de bestanden van onder meer de Belastingdienst, de Rijksdienst voor het Wegverkeer, DUO (studiefinanciering) en het Kadaster. Al met al is elektronische gegevensuitwisseling via Suwinet een onmisbaar onderdeel geworden voor de kwaliteit van integrale dienstverlening aan burgers.

Burgers moeten er op kunnen rekenen dat overheidsinstanties en hun medewerkers zorgvuldig met hun persoonsgegevens omgaan. Daarom is Suwinet beveiligd en gelden voor toegang en het gebruik ervan door medewerkers strikte regels en eisen.

Bij eerdere onderzoeken van de toenmalige Inspectie Werk en Inkomen is melding gemaakt van gebrekkige beveiliging van persoonsgegevens en incidenteel misbruik of oneigenlijk gebruik daarvan. De inspectie constateerde in 2012 opnieuw dat de beveiliging bij met name (inter-)gemeentelijke sociale diensten (in deze nota verder te noemen 'gemeenten') onder de maat is.[7] De inspectie stelde vast dat de gemeenten de afgelopen jaren maatregelen hebben getroffen om de beveiliging van de gegevensuitwisseling via Suwinet te verbeteren, maar dat bij veel gemeenten verdere verbetering noodzakelijk lijkt.

De toenmalige Staatssecretaris van SZW (De Krom) heeft in juni 2012 een brief geschreven aan alle gemeenten in Nederland, waarin hij gemeenten waarschuwt voor de soms matige beveiliging van de gegevens die zij verwerken bij het verrichten van hun taken in de sociale zekerheid.[8] Hij wijst de gemeenten op hun verantwoordelijkheid voor het gebruik van persoonsgegevens door medewerkers van de gemeenten. Verder kondigt hij met deze brief een vervolgonderzoek van de Inspectie SZW aan naar de beveiliging van Suwinet.

De huidige staatssecretaris van SZW, heeft de inspectie SZW gevraagd om in 2013 onderzoek te doen naar de beveiliging van Suwinet door gemeenten.[9] De inspectie heeft ingestemd met dit verzoek.

[7] Gegevensuitwisseling WWB/WIJ", Inspectie Werk en Inkomen, december 2011.
[8] Brief van 8 juni 2012 aan de Colleges van B&W van de gemeenten in Nederland, kenmerk RUA/UO/2012/6612
[9] Brief d.d. 28 juni 2012, kenmerk RUA/A/2012/9996.

2.2 Doelstelling

Het verzoek van de staatssecretaris luidt:
Geef een representatief beeld van de mate waarin gemeenten voldoen aan de eisen die worden gesteld aan de beveiliging van uitwisseling van informatie die wordt uitgewisseld binnen het Suwinet en geef hierover een oordeel.

Het gevraagde onderzoek dient bij te dragen aan het verbeteren van de beveiliging van het Suwinet door in een nota van bevindingen een representatief beeld te geven van de mate waarin de beveiliging van het Suwinet door gemeenten op orde is.

Op basis van de bevindingen per gemeente kan de staatssecretaris besluiten nadere maatregelen te treffen om de beveiliging van Suwinet in betrokken gemeente(n) op orde te doen brengen.

2.3 Probleemstelling en onderzoeksvragen

Bescherming van persoonsgegevens houdt onder meer in dat deze gegevens op een veilige manier worden verzameld, verwerkt en gedeeld.

Een veilige manier van omgaan met persoonsgegevens wil zeggen dat er door de gemeente procedures en processen zijn ingericht die de vertrouwelijkheid, integriteit en continuïteit van de gebruikte systemen waarborgen.
Om een uitspraak te doen over de mate waarin gemeenten voldoen aan alle wettelijke eisen rond informatiebeveiliging van Suwi-gegevens, zou bij elke onderzochte gemeente een zogenoemde IT-audit moeten worden uitgevoerd. [10]
Het uitvoeren van een dergelijke IT-audit, die enkele dagen per gemeente zou kosten, valt buiten de mogelijkheden van dit onderzoek. Daarom heeft de inspectie dit onderzoek, in samenspraak met de betrokken beleidsdirectie, beperkt tot het aspect waarvan zij denkt dat zich hierbij de grootste risico's voordoen, namelijk het aspect 'vertrouwelijkheid'.
Met vertrouwelijkheid wordt bedoeld dat een gegeven alleen te benaderen is door iemand die gemachtigd is het gegeven te benaderen en voor zijn wettelijke taken nodig heeft.

De centrale vraag in het onderzoek is als volgt geformuleerd:
In welke mate voldoen gemeenten aan de eisen van vertrouwelijkheid die worden gesteld aan de beveiliging van informatie die wordt uitgewisseld binnen het Suwinet in 2012?

De deelvragen van dit onderzoek zijn:
1. *Voldoen gemeenten aan de wettelijke verplichtingen inzake de informatiebeveiliging? (o.a. actueel beveiligingsplan)*
2. *Op welke wijze hebben gemeenten de verantwoordelijkheden in de organisatie belegd (o.a. rol security officer, rol verantwoordelijk management)*
3. *Worden de bevoegdheden aan medewerkers conform de voorwaarden verstrekt?*
4. *In hoeverre vragen gemeenten algemene en/of specifieke rapportages op bij BKWI (op basis van logfiles) over het gebruik van Suwinet?*

[10] IT-auditing is het vakgebied dat zich bezighoudt met het beoordelen van de automatisering van de organisatie en de organisatie van de automatisering. IT-auditing is een specialisme binnen het auditing-vakgebied. Het specialisme wordt meer en meer gevraagd bij uitvoering van accountantscontroles.

2.4 Normenkader

De inspectie gaat in dit onderzoek uit van de essentiële normen voor het waarborgen van de vertrouwelijkheid, opgenomen in het Normenkader GeVS (Gezamenlijke elektronische Voorzieningen SUWI)[11]. De in dit onderzoek door de inspectie gehanteerde normen hebben betrekking op een drietal aandachtsgebieden:

- Aandachtsgebied 1, Het informatiebeveiligingsbeleid en het informatiebeveiligingsplan voor Suwinet;
- Aandachtsgebied 2, De inrichting en onderhoud van de beveiligingsfunctie en de beveiligingsorganisatie van Suwinet (waaronder de aanstelling van een security officer);
- Aandachtsgebied 3, De logische toegangsbeveiliging, gericht op het voorkomen van ongeautoriseerde toegang tot en gebruik van persoonsgegevens.

In het normenkader wordt onderscheid gemaakt tussen essentiële en niet-essentiële normen. Door de SUWI-partijen is aan essentiële normen een zwaarder belang toegekend dan aan niet-essentiële normen. In de Verantwoordingsrichtlijn is bepaald dat een goedkeurend oordeel door een IT-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.

In bijlage 4 is een overzicht opgenomen aan welke essentiële normen de inspectie heeft getoetst.

2.5 Onderzoeksmethode en reikwijdte uitspraken

Voor dit onderzoek is een zuiver aselecte steekproef getrokken van 80 uit de 415 gemeenten in Nederland, in het jaar 2012.
Aangezien dit een representatieve steekproef is van voldoende omvang kan de inspectie op grond van de bevindingen bij de steekproefgemeenten algemeen geldende uitspraken doen over alle gemeenten.

Waar een gemeente uit de steekproef samenwerkt met één of meer andere gemeenten op het gebied van sociale zaken binnen een intergemeentelijke sociale dienst of anderszins heeft het onderzoek zich gericht op het samenwerkingsverband. Lees hiervoor ook paragraaf 4.3 Samenwerking in de uitvoering.

De beoordelingen van de inspectie zijn gebaseerd op de antwoorden die de steekproefgemeenten hebben gegeven naar aanleiding van de vragenlijst en op de bijbehorende bewijsstukken die gemeenten hebben ingezonden. [12]
Verder heeft de inspectie gebruik gemaakt van de BKWI-rapportages over het gebruik van Suwinet per steekproefgemeente over de periode november 2011 tot en met oktober 2012.

[11] Het Normenkader GeVS maakt deel uit van de Verantwoordingsrichtlijn GeVS. Zie hiervoor verder bijlage 3, Wettelijk Kader.
[12] Zie voor de vragenlijst bijlage 5.

Tenslotte heeft de inspectie (geanonimiseerde) gegevens uit de logfiles van de desbetreffende gemeenten opgevraagd bij BKWI.

Zie voor een uitgebreidere beschrijving van de onderzoekmethode bijlage 2.

3 Bevindingen normenkader

3.1 Beleidsplan, Uitdragen en Actualiseren (normen 1.3, 1.4 en 1.5)

Norm
Norm 1 van het normenkader schrijft voor dat de gemeente dient te beschikken over een informatiebeveiligingsbeleid en een Suwinet-beveiligingsplan:

- 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 het beveiligingsplan van het Suwinet worden jaarlijks geëvalueerd en indien nodig geactualiseerd.

Doel
Het informatiebeveiligingsbeleid dient volgens norm 1.3 goedgekeurd te zijn door het management van de organisatie. Daarmee wordt aangegeven dat het management betrokken is bij de totstandkoming en de inhoud van het beveiligingsbeleid. Het management is immers verantwoordelijk voor de uitvoering van het beveiligingsbeleid.
Een belangrijke taak van het management ligt in het vergroten van de bewustwording van de medewerkers rond informatiebeveiliging. Daarom schrijft norm 1.4 voor dat het informatiebeveiligingsbeleid en –plan worden uitgedragen in de organisatie. Na het implementeren van de maatregelen dient de naleving ervan te worden bewaakt. Bovendien dient te worden nagegaan of het geïmplementeerde pakket maatregelen blijft voldoen aan de beveiligingseisen en - randvoorwaarden en of de relevante risico's voldoende gereduceerd worden. In norm 1.5 is voorgeschreven dat het informatiebeveiligingsbeleid en –plan jaarlijks worden geëvalueerd en indien nodig geactualiseerd.

Operationalisatie
In de vragenlijst heeft de inspectie gevraagd of de gemeente beschikt over een informatiebeveiligingsbeleid en –plan zoals genoemd in de regeling SUWI en dit aan de inspectie toe te zenden.

In de regel is een beveiligingsbeleid tactisch/strategisch van aard. Hierin komen onderwerpen aan de orde te komen als:

- hoe men omgaat met functieomschrijvingen,
- functiescheiding,
- thuiswerken,
- werken op eigen apparaten,
- social media, etc.

In het beveiligingsplan wordt het beleid verder geconcretiseerd en wordt aandacht te worden besteed aan:

- het toekennen van autorisaties (begeleid met een autorisatiematrix)

- de rollen en functies van de diverse medewerkers waaronder die van de Security Officer
- Wie op welke gronden wie welke autorisaties toekent;
- wie de uitgegeven autorisaties en het gebruik hiervan beoordeelt en hoe hij/zij dit uitvoert.

Om een algemene indruk te krijgen van de inrichting van de informatiebeveiliging van SUWI-gegevens bij de gemeente is onder andere nagegaan of het informatiebeveiligingsbeleid en –plan specifiek betrekking hebben op SUWI of dat er in algemeen stuk een aparte passage of hoofdstuk aan SUWI is gewijd. Verder is gelet op de vraag of er in het beveiligingsbeleid of plan aandacht is besteed aan het toekennen van autorisaties, de rollen/functies van de diverse medewerkers waaronder de Security Officer, wie op welke gronden autorisaties toekent, wie de uitgegeven autorisaties en het gebruik hiervan beoordeelt en hoe hij dit uitvoert.
Indien werkzaamheden zijn uitbesteed (bijvoorbeeld ISD, samenwerkingsverband, sociale recherche) dan is ook nagegaan of in het informatiebeveiligingsbeleid en –plan melding gemaakt wordt van de uitbestede werkzaamheden en of er aanvullende verklaringen zijn waarmee de aannemer zich bekend en akkoord verklaart met het informatiebeveiligingsbeleid en –plan (contracten, Service Level Agreements etc.).

Ten behoeve van de beoordeling van de naleving van norm 1.3 is gevraagd of het plan is goedgekeurd door het management van de gemeente en wanneer dat is gebeurd. Bewijsstukken hiervan zijn opgevraagd, bijvoorbeeld een verslag waaruit blijkt dat het management de documenten heeft geaccordeerd.

Voorts is in verband met de beoordeling van norm 1.4 aan de gemeente de vraag gesteld of het beleid en het plan worden uitgedragen in de organisatie en op welke wijze dat gebeurt. Aanwijzingen hiervoor kunnen bewijsstukken zijn waaruit blijkt dat het beleid en het plan voor alle betrokkenen centraal beschikbaar zijn. Bijvoorbeeld op intranet, in een handboek etc. Ook gevraagd is naar verslagen van (werk)overleggen, afdelingsvergaderingen, trainingen, heisessies, functionerings- en beoordelingsgesprekken etc. waarin het beleid en plan aan de orde zijn gekomen.

Bij het onderzoek is deze norm door de inspectie zodanig geoperationaliseerd, dat er sprake dient te zijn van ten minste twee wijzen waarop het informatiebeveiligingsbeleid en het Beveiligingsplan SUWI in de organisatie worden uitgedragen, waarbij er ook sprake is van cyclisch uitdragen, waarbij plan en/of beleid met enige regelmaat aan de orde komen.

Ten slotte is in het kader van norm 1.5 gevraagd of evaluatie en actualisatie van het informatiebeveiligingsbeleid en het informatiebeveiligingsplan plaatsvindt en op welke wijze en met welke frequentie dat gebeurt. Nagegaan is met welk tijdsinterval het beleid en plan zijn bijgesteld en gevraagd is om schriftelijke bewijsstukken van evaluaties en actualisaties.
In afwijking van de tekst van norm 1.5, die een jaarlijkse evaluatie en actualisatie voorschrijft, heeft de inspectie bij deze norm een termijn van twee jaar gehanteerd, binnen welke het beleid en/of plan zouden moeten zijn geëvalueerd en geactualiseerd.

Bevindingen
De meerderheid van onderzochte gemeenten beschikt over een informatiebeveiligingsplan en heeft dit als bijlage bij de vragenlijst aan de inspectie gezonden.
15% van de gemeenten kon geen beveiligingsplan overleggen, hoewel gemeenten verplicht zijn om daarover te beschikken.

Dat is opmerkelijk omdat uit gegevens van de toenmalige Inspectie Werk en Inkomen blijkt dat in 2009 alle gemeenten in Nederland over een beveiligingsplan beschikten. [13]

Uit de antwoorden op de gestelde vragen is gebleken dat een formeel onderscheid tussen een informatiebeveiligingsbeleid en een informatiebeveiligingsplan niet altijd goed te maken is. De toegezonden informatiebeveiligingsplannen bevatten vaak onderdelen van informatiebeleidsplannen en vice versa. Verder werd in een aantal gevallen het informatiebeleidsplan met betrekking tot de Gemeentelijke Basisadministratie (GBA) toegezonden, waarin geen aandacht werd besteed aan SUWI. Gelet op het bovenstaande heeft de inspectie de gegevens van zowel het informatiebeveiligingsbeleid als de –plannen in het onderzoek betrokken en geen formeel onderscheid hierin aangebracht. In het vervolg wordt dan ook alleen over beveiligingsplannen gesproken, waar dan zowel beveiligingsbeleid als beveiligingsplannen worden bedoeld.

Bij gemeenten leeft nogal eens het misverstand dat een beveiligingsbeleid of -plan voor de GBA ook voor Suwinet zou gelden, terwijl aan Suwinet andere en specifieke eisen worden gesteld, die afwijken van de maatregelen voor de GBA.

In 24% van de gevallen was het informatiebeveiligingsplan niet voorzien van een formele goedkeuring. Er kon door de gemeente geen stuk worden overlegd met een datum, handtekening, naam en functie op het plan zelf of een apart document (beslisstuk of verslag van een vergadering) waaruit bleek dat er goedkeuring door het management verleend is.

Bij 69% van de gemeenten kon met de door hen aangeleverde informatie onvoldoende worden aangetoond dat het beveiligingsplan binnen de gemeente actief is uitgedragen. Deze organisaties konden bijvoorbeeld geen verslagen van werkoverleggen, afdelingsvergadering, presentaties of andere stukken overleggen waaruit blijkt dat het informatiebeveiligingsbeleid regelmatig aan de orde is geweest.

Uit de antwoorden op de vragenlijst en de toegezonden stukken is verder gebleken dat 79% van de gemeenten het beveiligingsplan niet regelmatig (ten minste eens in de twee jaar) evalueert en zo nodig actualiseert.

De toegezonden informatiebeveiligingsplannen lopen in datering uiteen van september 2005 tot december 2012. De gemiddelde leeftijd van de plannen is ruim vier jaar. 21% van de beveiligingsplannen is jonger dan 2 jaar.

3.2 Functiescheiding, (norm 2.2)

De norm
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 gescheiden zijn belegd. Dan gaat het om:

- Operationeel beheer

[13] De Staatssecretaris van Sociale Zaken en Werkgelegenheid heeft in 2009 alle 96 gemeenten die destijds geen informatiebeveiligingsplan hadden overlegd aan de Inspectie Werk en Inkomen, verzocht om binnen vier maanden alsnog een beveiligingsplan op te sturen. (Brief van de Staatssecretaris van SZW, d.d. 24 juni 2009, kenmerk RUA/UO/2009/13304). Alle gemeenten hebben hieraan gehoor gegeven.

- Functioneel beheer
- Technisch beheer
- Aansturing ICT-leveranciers
- Security Officer
- Autorisatiebeheer
- Eigenaarschap Suwinet

Doel
Een randvoorwaarde voor het realiseren van een minimaal beveiligingsniveau voor Suwinet is een goed ingerichte organisatie. Alleen indien dit is gerealiseerd, kan de beveiliging van het Suwinet voldoende worden beheerst. Norm 2.2 handelt over de functiescheiding. Door de in de norm genoemde functies duidelijk te beschrijven (welke taken, verantwoordelijkheden en bevoegdheden vallen onder de diverse functies) en (gescheiden) te beleggen wordt invulling gegeven aan het scheiden van beschikkende, uitvoerende en controlerende taken. Populair gezegd: zorg ervoor dat de slager niet zijn eigen vlees keurt.
Alleen indien de diverse functies duidelijk zijn omschreven en vastgelegd kan de functiescheiding aantoonbaar worden gemaakt. Vastlegging en omschrijven is dus een randvoorwaarde.

Operationalisatie
Om inzicht te krijgen in de inrichting van de functiescheiding binnen de gemeente is gevraagd of, en zo ja op welke wijze, taken, verantwoordelijkheden en bevoegdheden zijn beschreven. De inspectie heeft de inrichting op een aantal aspecten beoordeeld. Gekeken is of de diverse functies schriftelijk zijn vastgelegd, of er een heldere overweging ten grondslag ligt aan welke taken waar zijn belegd en of er functiescheiding is toegepast. Bij deze laatste norm is gelet op het onderscheid tussen de beschikkende en uitvoerende taken (normaliter bepaalt het afdelingshoofd wie welke autorisaties krijgt en vindt uitvoering hiervan plaats door een applicatiebeheerder) en het onderscheid tussen de uitvoerende en controlerende taak (dat de medewerker niet zichzelf controleert).
Sommige gemeenten hebben (bijvoorbeeld door beperkte omvang) diverse functies binnen één persoon gecombineerd. Dit soort gevallen leidt niet automatisch tot een negatieve bevinding indien de gemeente blijk geeft zich hier bewust van te zijn en aantoonbaar aanvullende maatregelen heeft getroffen.

Bevindingen
Circa 30% van de gemeenten voldoet aan deze norm. Voor deze gemeenten geldt dat zij voldoende duidelijk hebben aangetoond waarom welke functionarissen welke autorisaties hebben binnen Suwinet. Er zijn dan onder andere functiebeschrijvingen en er wordt gewerkt met een autorisatiematrix zodat duidelijk is wie welke (zware) rollen heeft.

Voor de gemeenten die niet voldoen aan de norm, geldt dat deze vaak geen functiescheiding hebben vastgelegd of dit niet volledig hebben gedaan. Er wordt dan wel aangegeven dat men binnen de gemeente met diverse functies werkt, maar functiebeschrijvingen ontbreken of zijn onvoldoende gedetailleerd. Ook zijn er gemeenten die duidelijk hebben vastgelegd welke personen welke autorisaties hebben in Suwinet, echter niet waarom ze dan deze autorisatie nodig hebben. Verder constateert de inspectie dat binnen sommige gemeenten dezelfde functionarissen verschillende autorisaties hebben zonder dat duidelijk wordt gemaakt waarom dit zo is. De inspectie constateert dat de meeste gemeenten niet in staat zijn aantoonbaar te maken wie welke taken met betrekking tot Suwinet uitvoert en op basis waarvan dit is

vastgesteld. In deze gevallen is dientengevolge ook niet vast te stellen of er sprake is van voldoende functiescheiding.

3.3 Security Officer (norm 2.3)

De norm
De Security Officer beheert en beheerst beveiligingsprocedures en -maatregelen in het kader van Suwinet, zodanig dat de beveiliging van Suwinet overeenkomstig wettelijke eisen is geïmplementeerd.

- De Security Officer bevordert en adviseert over de beveiliging van Suwinet, verzorgt rapportages over de status, controleert dat m.b.t. 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.

Doel
In het normenkader is bepaald dat organisaties die gebruik maken van Suwinet een medewerker dienen aan te stellen die specifiek tot taak heeft te bevorderen en te controleren dat de beveiliging van het Suwinet op orde is.
In het normenkader wordt voor deze functie de term 'Security Officer' gebruikt. Deze Security Officer (SO) is deskundig op het terrein van informatiebeveiliging, controleert planmatig en periodiek of wordt voldaan aan de regels en analyseert eventuele beveiligingsincidenten. Hij of zij rapporteert hierover aan het management of bestuur van de organisatie.

De Bijlage XIV bij de Regeling SUWI (die gold van 1 januari 2002 tot 15 september 2008) bevatte daarover de volgende passage: "De Suwi-organisatie kan een aantal taken op het gebied van informatiebeveiliging toewijzen aan bijvoorbeeld een Security Officer of aan een coördinatiepunt Informatiebeveiliging. In het vervolg wordt het begrip Security Officer gehanteerd voor de functie die een aantal coördinerende en uitvoerende taken op het gebied van informatiebeveiliging uitvoert. De organisatorische invulling van deze functie (of taken) kan per Suwi-organisatie verschillen." De norm aangaande de SO is na intrekking van Bijlage XIV in de Verantwoordingsrichtlijn GeVS gehandhaafd.

De Verantwoordingsrichtlijn, met name het daarin opgenomen Normenkader, gaat ervan uit dat de beveiliging van de persoonsgegevens bij de SUWI-organisaties gestructureerd wordt vormgegeven; het Normenkader stelt daartoe eisen met betrekking tot opzet, bestaan en werking van een goed georganiseerde, permanente beveiliging.

Operationalisatie
De inspectie heeft onderzocht of in een gemeente een SO aanwezig is, en zo nee, of daar een coördinatiepunt aanwezig was, dat de in de norm genoemde taken van de SO uitvoert. Daarbij heeft de inspectie er niet alleen op gelet of de functie of de taken in opzet in de organisatie belegd waren, maar met name ook of aan de hand van documenten aantoonbaar was dat functie en/of taken daadwerkelijk planmatig en periodiek werden uitgevoerd. Met name heeft de inspectie daarbij bezien of er schriftelijke neerslag was van uitgevoerde controles en van rapportages direct aan het hoogste management.

Bevindingen
Uit gegevens van BKWI blijkt dat 58% van de gemeenten een Security Officer had. Er is echter meestal sprake van een beperkte taakuitoefening. Vaak is er sprake van een formele aanstelling, waarbij er maar weinig invulling wordt gegeven aan de functie. Een van de taken van een SO is om het hoogste management te adviseren over de beveiliging van Suwinet; bij de onderzochte gemeenten heeft de inspectie nauwelijks gezien dat aan deze adviesfunctie enige invulling werd gegeven.
76% van de gemeenten voldoet niet aan norm 2.3.

3.4 Autorisatiestructuur (norm 13.1)

Norm
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 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)

Doel
Deze norm is van belang om op een **controleerbare** wijze aan te kunnen tonen dat huidige of in het verleden verstrekte toegangsrechten tot Suwinet in overeenstemming zijn (waren) met:

- het wettelijke kader van Suwinet / 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 noodzakelijke functiescheiding tussen:
    - het schriftelijk toekennen / wijzigen / intrekken van autorisaties (door de manager)
    - het veranderen (inbrengen, wijzigen of verwijderen) van autorisaties in Suwinet-systeem (door de applicatiebeheerder)
    - het controleren van de verleende Suwinet-autorisaties (door de Security Officer voor Suwinet)
- de noodzakelijke informatiebeveiligingsrichtlijnen rondom het gebruik van Suwinet en de controle op het gebruik (logging).
- De achterliggende norm is dat persoonsgegevens alleen gebruikt mogen worden voor het doel waarvoor ze zijn verzameld. Dit betekent dat gegevens in Suwinet door gemeenten in het algemeen alleen gebruikt worden voor de rechtmatige uitvoering van de WWB.

Operationalisatie
Om zicht te krijgen op hoe bovenstaande procedures in de praktijk werken, heeft de inspectie bij de Security Officer Suwinet van betreffende gemeente c.q. aangewezen contactpersoon de volgende zaken opgevraagd:

- schriftelijk vastgelegde en geformaliseerde autorisatie procedure voor toegang tot het Suwinet
- schriftelijk vastgelegde en geformaliseerde autorisatiematrix voor het gebruik van Suwinet

Indien een autorisatie procedure is verstrekt door de desbetreffende gemeente, dan is gekeken of deze autorisatieprocedure voldoet aan de eisen van volledigheid:

- zijn alle noodzakelijke stappen in dit proces aanwezig,
- duidelijk beschreven en
- toegewezen aan bevoegde functionarissen binnen de gemeente.

Indien een autorisatiematrix is verstrekt door betreffende gemeente, dan is gekeken of deze autorisatiematrix:

- specifiek ingaat op Suwinet
- gebaseerd is op onderkende / aanwezige functie (profielen)
- gebaseerd is op aanwezige rollen in Suwinet

Volgens de inspectie SZW dient een juiste Suwinet autorisatiematrix van een gemeente inzicht te geven in welke functie (profielen) standaard welke rollen in Suwinet dienen te krijgen. Door ook nog 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 (welke medewerker mag welke gegevens zien) dient volgens een logische procedure plaats te vinden. Hieruit moet duidelijk worden: op basis van welke afwegingen, welke medewerker, welke gegevens mag zien. Als de gemeente dit herleidbaar maakt is dit afdoende. Hierbij is het mogelijk dat dit op schrift of (deels) in een geautomatiseerd systeem is vastgelegd.

Bevindingen
30 van de 80 onderzochte gemeenten (38%) waren in staat om aan de inspectie een geformaliseerde, correcte en in gebruik zijnde autorisatieprocedure en autorisatiematrix te verstrekken.

De 48 gemeenten die niet voldeden aan deze norm (60%), zijn te verdelen in een drietal groepen:

4. gemeenten die geen autorisatieprocedure en geen autorisatiematrix met betrekking tot Suwinet aan de inspectie hebben overlegd.

   Dit betreft vaak gemeenten met een klein tot zeer klein aantal , dat gebruik moet maken van Suwinet. De gemeente beschouwt dan deze procedure als te bureaucratisch. Men vertrouwt dan meer op het bestaan van onderling toezicht.
   Het risico bestaat nu dat er fouten worden gemaakt in het verlenen van autorisatie aan personen (onterechte toegang) en/of in het toekennen van Suwinet rollen aan een bepaald persoon (doorbreking van functiescheiding).

5. gemeenten die wel een formele autorisatieprocedure hebben, maar geen specifieke Suwinet autorisatiematrix.
   Het risico bestaat nu dat er fouten worden gemaakt in het toekennen van Suwinet rollen aan een bepaald persoon (doorbreking van functiescheiding).

6. gemeenten die wel een formele autorisatieprocedure en autorisatiematrix Suwinet hebben, maar waar in de autorisatiematrix Suwinet:

   - of geen functies staan vermeld, maar afdelingen
   - of geen Suwinet rollen staan vermeld, maar uit te voeren taken in tekst

Het risico bestaat hier ook dat er fouten worden gemaakt in het toekennen van Suwinet-rollen aan een bepaald persoon (doorbreking van functiescheiding).

3.5 Controle (norm 13.5)

Norm
Norm 13.5 luidt als volgt:

- De controle op verleende toegangsrechten en het 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.

Doel
Deze norm benadrukt het belang van periodieke controle of de verleende toegangsrechten in overeenstemming met de vooraf bepaalde uitgangspunten zijn. Hiernaast schrijft deze norm voor dat de controle of het gebruik van Suwinet plaatsvindt conform de wettelijke vereisten. Indien afwijkingen worden geconstateerd dienen corrigerende maatregelen te worden genomen. Deze zijn in grote mate afhankelijk van de geconstateerde afwijkingen en variëren van het beperken van de toegangsrechten tot disciplinaire maatregelen bij geconstateerd misbruik van persoonsgegevens.

Voor deze controle kunnen in eerste instantie de verleende toegangsrechten via de applicatie die het toegangsbeheer voor Suwinet-Inkijk regelt worden beoordeeld. Voor het daadwerkelijk gebruik van Suwinet-inkijk stelt BKWI standaard overzichten beschikbaar waarmee een eerste indicatie van afwijkend gedrag kan worden gesignaleerd. Hiernaast bestaat de mogelijkheid om aan BKWI te vragen specifieke overzichten (bijvoorbeeld opvragingen op postcode en/of per medewerker) op te stellen waarmee beter inzicht in het gebruik kan worden verkregen.

Operationalisatie
BKWI maakt iedere maand voor elke gemeente een zogenoemde periodieke rapportage over het gebruik van Suwinet-Inkijk. Deze rapportage bevat onder andere informatie over het aantal raadplegingen van Suwinet-Inkijk, het aantal geraadpleegde BSN's, het aantal raadplegingen binnen en buiten kantooruren, het aantal inlogpogingen en het aantal actieve en inactieve accounts. Deze rapportage bevat geen direct herleidbare persoonsgegevens. De geïnteresseerde gemeente kan deze rapportage zelf opvragen via Suwinet.
Daarnaast kan een gemeente bij BKWI een specifieke rapportage aanvragen, ter ondersteuning van het interne controleproces of bijvoorbeeld wanneer op basis van

een periodieke rapportage of van eigen waarneming een vermoeden bestaat van misbruik of oneigenlijk gebruik van gegevens vanuit Suwinet-Inkijk. De specifieke rapportages kunnen, in tegenstelling tot de reguliere rapportages, gegevens bevatten over individuele medewerkers of cliënten. De specifieke rapportages mogen dan ook alleen worden opgevraagd door een door de gemeente geautoriseerde persoon, meestal een intern controleur of een security officer.

Om zicht te krijgen op hoe de controleprocedures bij de gemeenten in de praktijk werken, heeft de inspectie de daadwerkelijk verleende toegangsrechten en reguliere rapportages beoordeeld.
Aan BKWI is gevraagd om over 2012 per gemeente ook inzicht te geven in het aantal raadplegingen op postcode/huisnummer (ook buiten het eigen postcodegebied), kenteken en naam/geboortedatum. Het gebruik van deze ingangen is uitsluitend mogelijk met de zogenaamde 'zware rollen' en is standaard niet noodzakelijk voor het raadplegen van persoonsgegevens van een cliënt van wie het Burgerservicenummer (BSN) normaliter bekend is. Een BSN is immers een voorwaarde voor het aanvragen van een WWB-uitkering.

Zware autorisaties, ook wel genoemd zware rollen, zijn autorisaties met uitgebreidere zoekmogelijkheden dan alleen op BSN. Dat kan bijvoorbeeld zijn zoeken op postcode en huisnummer of zoeken op kenteken. Voor verreweg de meeste medewerkers zijn deze zware rollen niet nodig voor de uitvoering van hun taken. Een kleine minderheid van de medewerkers van gemeenten, namelijk de medewerkers die betrokken zijn bij bijvoorbeeld handhaving of opsporing zal deze rollen echt nodig hebben.

Het te ruim verstrekken van zware autorisaties vergroot het risico op onrechtmatige raadplegingen van de bestanden omdat het voor een medewerker eenvoudiger is om, zonder te beschikken over hun BSN, gegevens van personen te raadplegen die voor hem of haar van belang zijn. Te denken valt aan het raadplegen van gegevens van collega's, leidinggevenden, (ex)-partners, familieleden, kennissen, buren, verkopers van woningen waarin de medewerker geïnteresseerd is, etc.

De inspectie heeft gemeenten waar opvallend vaak met zware rollen is gezocht als opvallend gekenmerkt.

Hiernaast heeft de inspectie gecontroleerd of binnen gemeenten de BSN van 100 willekeurig geselecteerde bekende Nederlanders is geraadpleegd, iets wat eveneens kan wijzen op oneigenlijk gebruik. Omdat op voorhand legitiem zoekgedrag op bekende Nederlander onwaarschijnlijk werd geacht, en omdat het gaat om een beperkt aantal waarnemingen, zijn alle gevonden opvragingen per account en gemeente onderzocht.
De inspectie gaat er hierbij vanuit dat het zoeken op een bekende Nederlander een indicator is voor de mate waarin Suwinet oneigenlijk en/of onrechtmatig wordt gebruikt.

De desbetreffende gemeenten is gevraagd of zij dit zoekgedrag ook al hadden geconstateerd en of dit noodzakelijk was om de rechtmatigheid van een WWB uitkering te kunnen waarborgen.

De inspectie heeft vastgesteld of een gemeente het daadwerkelijk gebruik van Suwinet minstens 2 keer per jaar controleert en dit inzichtelijk kan maken.

Bevindingen

Circa een derde van de onderzochte gemeenten voert de controle conform norm 13.5 uit op een wijze die ook voor de Inspectie is te herleiden. Een voorbeeld hiervan zijn gemeenten die steekproefsgewijs periodiek alle opvragingen van persoonsgegevens van een medewerker aan de hand van de eigen WWB populatie controleren en eventuele verschillen nader uitzoeken. Ook worden hiervoor de standaard overzichten van BKWI gebruikt en incidenteel een specifieke rapportage opgevraagd.

Van de overige gemeenten geeft circa de helft aan de controle aan de hand van de standaard BKWI overzichten uit te voeren maar deze kunnen niet aangeven waarop precies wordt gelet. Van deze controles zijn in het algemeen geen aantekeningen of rapportages beschikbaar zodat de Inspectie niet kan herleiden hoe deze controles hebben plaatsgevonden. In veel gevallen hadden deze gemeenten het door de Inspectie gesignaleerde afwijkende zoekgedrag zelf niet geconstateerd en konden dat ook niet verklaren. Zo kunnen gemeenten meestal niet aangeven waarom de zoeksleutel op kenteken wordt gebruikt terwijl het autobezit ook via de 'standaard' ingang (BSN) is te zien. Als verklaring voor de grote aantallen raadplegingen op postcode/huisnummer wordt regelmatig genoemd dat deze te maken zouden kunnen hebben met de huishoudinkomenstoets, waarbij gecontroleerd is of er op het opgegeven adres ook andere personen met een inkomen wonen. Hoewel deze verklaring plausibel lijkt, is dit door de betreffende gemeenten op account-/medewerkerniveau niet verder gecontroleerd. Of deze verklaring in alle geconstateerde gevallen een rol speelt blijft dus onduidelijk. Andere verklaringen zijn: verhaal waarvoor personen buiten de gemeente moeten worden gezocht of controle op naam omdat het BSN bij de eerste contacten niet bekend is. Ook voor deze verklaringen is geen nadere onderbouwing aangetroffen.

De andere gemeenten, circa een derde van het totaal gaven aan deze controle niet of zeer beperkt uit te voeren, of hierbij kwam de inspectie zelf tot deze conclusie.

De inspectie heeft ook gecontroleerd of binnen gemeenten gegevens van 100 willekeurig geselecteerde bekende Nederlanders zijn geraadpleegd, iets wat eveneens kan wijzen op oneigenlijk gebruik.
Bij 14 van de 80 onderzochte gemeenten (18%) zijn in 2012 gegevens van bekende Nederlanders met gebruikmaking van Suwinet Inkijk geraadpleegd, zonder dat hiervoor een goede reden is gegeven. Eén van deze gemeenten heeft hiervoor een plausibele verklaring gegeven. De overige dertien konden de raadplegingen niet verklaren.

Een aantal gemeenten geeft aan in het verleden met behulp van de overzichten van BKWI, misbruik of oneigenlijk gebruik te hebben geconstateerd en hiertegen maatregelen te hebben genomen.

Uit gegevens van BKWI blijkt dat 20% van de gemeenten op de peildatum 1 oktober 2012 het laatste half jaar geen periodieke rapportage bij BKWI had opgevraagd.
80% heeft in het half jaar daarvoor de periodieke rapportage minimaal één keer opgevraagd.
21% van de gemeenten heeft in de periode november 2011 tot en met oktober één of meer specifieke rapportages opgevraagd.

4 Overige Bevindingen

4.1 Inlezen

Gemeenten hebben de mogelijkheid om naast het online opvragen van gegevens via Suwinet Inkijk ook gegevens van burgers op te kunnen vragen en direct over te nemen in de eigen systemen, het zogenoemde 'Suwinet Inlezen'. Het voordeel hiervan is dat deze gegevens direct voor verdere administratieve handelingen kunnen worden gebruikt en niet nogmaals hoeven te worden ingevoerd. Hiermee worden fouten voorkomen en de efficiency bevorderd. Er zijn zgn. "Aansluit- & gebruiksvoorwaarden inlezen en voorinvullen via Gezamenlijke elektronische Voorzieningen SUWI (GeVS) ten behoeve van SUWI-taken" opgesteld. Ook is er een aantal matrices beschikbaar waarin staat aangegeven welke gegevens een GSD mag gebruiken voor inlezen.

De via Suwinet inlezen opgevraagde gegevens worden echter niet gelogd en zijn, nadat deze zijn overgenomen in het gemeentelijke systeem, ook vanuit deze omgeving te benaderen. Toegangsbeheer, logging, controles etc. dienen dan ook in deze omgeving te zijn ingericht. Gegevens over het gebruik worden niet opgenomen in de centrale logfiles die via BKWI te benaderen zijn en zijn evenmin opgenomen in de reguliere maandrapportages over het gebruik van Suwinet.

Bij het onderzoek heeft de Inspectie aan gemeenten gevraagd welke waarborgen voor het gebruik van Suwinet Inlezen zijn getroffen. Hierbij gaat het om dezelfde waarborgen die gelden voor het gebruik van de online mogelijkheid via Suwinet Inlezen, de door de Inspectie gestelde vragen zijn daarom identiek.

Bevindingen
Van de 80 gemeenten geven 6 gemeenten aan gebruik te maken van de mogelijkheid van Suwinet Inlezen. Uit de gegeven antwoorden leidt de inspectie af dat in een aantal gevallen het vermoeden bestaat dat het hierbij niet gaat om het inlezen van gegevens uit Suwinet maar het inlezen van signalen uit de samenloopapplicatie van het Inlichtingenbureau. Hoewel deze gegevens deels voor hetzelfde doel kunnen worden gebruikt (detecteren van fraude) gaat het hierbij om een andere methodiek waarvoor andere beheersmaatregelen zijn getroffen. De risico's die bij het gebruik van Suwinet-Inkijk spelen zijn hierbij niet aan de orde.

Verder heeft geen van de gemeenten op voldoende wijze aangegeven op welke manier de waarborgen rondom het gebruik van Suwinet Inlezen gestalte hebben gekregen.

Hiernaast heeft de Inspectie geprobeerd via BKWI een actueel beeld over het gebruik van Suwinet Inlezen te verkrijgen. Doordat een centrale registratie rondom het gebruik van Suwinet Inlezen ontbreekt, is de Inspectie niet in staat de door gemeenten verstrekte antwoorden, met betrekking tot het geen gebruik maken van Suwinet Inlezen, te valideren.

In alle gevallen ontbreekt een sluitende aanpak bij het gebruik van Suwinet Inlezen. Het is de inspectie niet duidelijk geworden op welke wijze gemeenten de toegangsrechten voor het gebruik van deze gegevens verlenen en hoe zij de controle op het gebruik hiervan uitvoeren.

4.2 Monitor zorgvuldig gebruik Suwinet

BKWI, een zelfstandig onderdeel van UWV, is de organisatie die in opdracht van de Minister van Sociale Zaken en Werkgelegenheid verantwoordelijk is voor het technisch beheer van het centrale deel van Suwinet en zorgt voor de verdere ontwikkeling ervan.

Sinds september 2011 voert BKWI de campagne "Zorgvuldig Gebruik Suwinet". Deze campagne heeft BKWI opgezet in samenwerking met het ministerie van SZW, Divosa en de Vereniging Nederlandse Gemeenten (VNG) om het bewustzijn omtrent privacy en beveiliging bij gemeenten te vergroten.

De campagne bestaat uit workshops voor gemeenten en de zogenoemde 'monitor Gebruik Suwinet'. In de workshops besteedt BKWI aandacht aan het belang van zorgvuldig gebruik van Suwinet voor burgers en gemeenten en wat er op het gebied van informatiebeveiliging van Suwinet geregeld hoort te zijn.
De 'monitor Gebruik Suwinet' geeft voor elke sociale dienst in Nederland een indicatie van de wijze waarop Suwinet gebruikt wordt. Hiervoor gebruikt BKWI een aantal indicatoren gebaseerd op bij BKWI beschikbare informatie uit de logfiles en de gebruikersadministratie. De scores worden weergegeven in een overzicht per gemeente met groen, oranje of rood, afhankelijk van de mate waarin de scores op de indicatoren om aandacht vragen. Het overzicht is uitsluitend beschikbaar voor de desbetreffende sociale dienst.
Daar waar bij een gemeente de indicator op rood staat, vindt een persoonlijk gesprek met een van de accountmanagers van BKWI plaats. Voor gemeenten die het rode waarschuwingslicht negeren is een escalatieprocedure opgesteld in samenwerking met Divosa, VNG en SZW. Tot dusver is de escalatieprocedure bij één gemeente gehanteerd.

Volgens BKWI toonde de monitor aan het eind van de campagne dat 289 gemeenten van de 415 gemeenten de score op de beveiligingsindicatoren het afgelopen jaar hebben verbeterd.

Een goede score op de monitor-indicatoren wil niet zeggen dat daarmee wordt voldaan aan het normenkader. Er zijn veel meer aspecten waaraan de informatiebeveiliging moet voldoen. De resultaten van de monitor kunnen wel aanleiding geven tot verder onderzoek door de gemeente.

Uit de contacten die de inspectie gedurende de looptijd van dit onderzoek met gemeenten heeft gehad, is naar voren gekomen dat er bij gemeenten veel misverstand is over de duiding van de scores op de indicatoren.
In het bijzonder de hoofdconclusie op de monitor, bijvoorbeeld "Status per 1 oktober 2012, 80% op orde" wordt nogal eens onjuist geïnterpreteerd; gemeenten maken hieruit op dat zij met 80% goed presteren, terwijl het beperkte aantal indicatoren van de monitor slechts een zeer beperkt gedeelte van dat terrein bestrijkt.

De toelichtende teksten op de BKWI-monitor: 'Wilt u in 3 minuten weten hoe het er voor staat in uw gemeente? Of uw gemeente optimaal gebruik maakt van deze mogelijkheden? Heeft uw gemeente de beveiligingsmaatregelen goed voor elkaar?' dragen bij aan dit misverstand.

Uit de onderzoeksresultaten van de inspectie blijkt dat er weinig overeenkomst is tussen de mate waarin gemeenten in dit onderzoek voldoen aan de zeven normen met betrekking tot vertrouwelijkheid en de scores op de BKWI-monitor.

De 12 gemeenten waarbij de inspectie constateerde dat aan geen van de zeven essentiële normen werd voldaan, scoren op de BKWI monitor gemiddeld 68% op orde.

De 35 gemeenten die aan slechts één of twee normen voldoen, scoren op de BKWI-monitor gemiddeld 60% op orde.

De 3 gemeenten die in het onderzoek van de inspectie aan alle zeven essentiële normen voldeden scoren op de BKWI-monitor respectievelijk 90%, 90% en 100% en op orde.

4.3 Samenwerking in de uitvoering

Een aanzienlijk aantal gemeenten werkt samen voor wat betreft de uitvoering van de WWB en aanverwante sociale voorzieningen. Onder de 80 gemeenten waarop het onderzoek zich heeft gericht, bevonden zich 30 gemeenten die op een of andere manier samenwerken.

De meeste van die gemeenten werken samen in openbare lichamen die daartoe zijn opgericht op grond van de Wet gemeenschappelijke regelingen (WGR). Zo'n openbaar lichaam heeft krachtens de WGR eigen rechtspersoonlijkheid. De organen van deelnemende gemeenten delegeren hun bestuursbevoegdheden aan desbetreffende organen van het openbaar lichaam; een college van burgemeester en wethouders delegeert zijn bevoegdheden aan het dagelijks bestuur van een openbaar lichaam.

Andere gemeenten werken samen op grond van een gemeenschappelijke regeling waarbij een gemeenschappelijk orgaan wordt ingesteld; zo'n gemeenschappelijk orgaan heeft geen rechtspersoonlijkheid.

Een derde vorm van samenwerking is een gemeenschappelijke regeling waarin een centrumgemeente wordt aangewezen, die de uitvoering op zich neemt. Daarbij worden twee varianten aangetroffen: a. een tweepartijenovereenkomst waarin een van de twee gemeenten als centrumgemeente wordt aangewezen, die de uitvoering op zich neemt, en b. een meerpartijenovereekomst waarin een gemeente als centrumgemeente wordt aangewezen, die de uitvoering op zich neemt.

Uit haar contacten met gemeenten in de loop van dit onderzoek is bij de inspectie het beeld ontstaan dat deze vormen van samenwerking in veel gevallen tot gevolg hebben dat de individuele gemeenten nauwelijks verantwoordelijkheid voelen voor de uit wet- en regelgeving voortvloeiende eisen op het gebied van de privacy bij de uitvoering van de WWB, omdat zij de verantwoordelijkheid voor de uitvoering hebben overgedragen. Volgens de inspectie ontslaat zo'n overdracht een gemeente echter niet van de taak om zich ervan te vergewissen dat de overgedragen taak naar behoren wordt uitgevoerd, ook waar het gaat om de privacyaspecten daarvan.

Daarnaast werkt een aantal gemeenten samen op het gebied van de sociale recherche. Dit gebeurt op dezelfde manier als hierboven beschreven, maar minder vaak.

Sommige gemeenten voeren wel zelf de WWB uit, maar werken voor wat betreft de sociale recherche samen in WGR-verband. Andere gemeenten werken op het terrein van de uitvoering van de WWB samen in een gemeenschappelijke regeling, en werken op het gebied van de sociale recherche samen in een anders samengestelde gemeenschappelijke regeling.

4.4 Integriteits- en geheimhoudingsverklaringen

Gemeenten maken bij de uitvoering van de WWB en andere socialezekerheidswetten gebruik van Suwinet. Zij dienen zich bij de uitvoering van hun taken te houden aan de in diverse wetten (WWB, Wet SUWI, Awb, WBP) opgenomen bepalingen over het gebruik van (persoons-)gegevens. In deze wetten zijn ook bepalingen opgenomen, die medewerkers van gemeenten verplichten tot geheimhouding van hetgeen zij weten over de persoon of zaken van een ander. Die bepalingen zijn overigens ook van toepassing voor bijvoorbeeld ingehuurd personeel. Daardoor zijn de medewerkers gehouden tot geheimhouding en tot rechtmatige verwerking (waaronder raadpleging) van deze gegevens.

Gemeenten dienen te beschikken over een beveiligingsplan Suwinet; dat is (idealiter) gebaseerd op een informatiebeveiligingsbeleid. Het beveiligingsbeleid ten aanzien van Suwinet maakt bij veel gemeenten deel uit van een organisatiebreed informatiebeveiligingsbeleid. Het bewustzijn van medewerkers op elk niveau binnen de organisatie over de noodzaak van beveiliging en van de zorgvuldige verwerking van persoonsgegevens, is een zeer belangrijke voorwaarde om beveiliging effectief te laten functioneren. Daarom moet aandacht worden besteed aan het vergroten of op peil houden van het beveiligingsbewustzijn van medewerkers.

Als onderdeel van hun beveiligingsbeleid hanteren veel gemeenten een geheimhoudingsverklaring die door hun medewerkers moet worden ondertekend. Andere gemeenten laten hun medewerkers daarnaast of in plaats daarvan een integriteitsverklaring ondertekenen, die inhoudt dat de ondertekenaar verklaart op integere wijze te zullen omgaan met de verleende toegang tot gemeentelijke informatiesystemen. Ook zijn er gemeenten die niet dit soort verklaringen laten tekenen, maar hun medewerkers alleen een ambtseed laten afleggen. De ambtseed is echter niet van toepassing op ingehuurd personeel.

Het valt de inspectie op dat niet alle gemeenten die een geheimhoudings- of integriteitsverklaring hanteren, zo'n verklaring ook laten ondertekenen door extern (ingehuurd) personeel. Hoewel dergelijke externen net als de ambtenaren zijn gebonden aan de wettelijk regels en eisen ter zake van het gebruik van (persoons-)gegevens, kan juist voor hen een integriteitsverklaring een meerwaarde kan hebben. Zij hebben vaak geen ambtelijke achtergrond van waaruit de wettelijke bepalingen hun bekend kunnen zijn, en een ambtseed die hen aan hun verplichtingen zou kunnen herinneren, wordt door hen niet afgelegd.

Bijlagen

Bijlage 1

Overzicht bevindingen gemeenten:

Gemeente	Norm 1.3 E	Norm 1.4.E	Norm 1.5 E	Norm 2.2 E	Norm 2.3 E	Norm 13.1 E	Norm 13.5 E	Aantal normen voldoende	Score op BKWI-monitor
Alblassersdam	Ja	Nee	Nee	Nee	Nee	Nee	Nee	1	50%
Alphen aan den Rijn	Ja	Ja	Nee	Nee	Ja	Nee	Nee	3	93%
Alphen-Chaam	Ja	Ja	Nee	Nee	Nee	Ja	Nee	3	64%
Baarle-Nassau	Nee	Nee	Nee	Nee	Nee	Nee	Nee	0	64%
Bergambacht	Ja	Nee	Nee	Ja	Ja	Ja	Nee	4	100%
Bergen NH	Ja	Ja	Ja	Ja	Ja	Nee	Nee	5	50%
Boarnsterhim	Ja	Nee	Nee	Nee	Nee	Nee	Nee	1	43%
Bodegraven-Reeuwijk	Ja	Nee	Nee	Nee	Nee	Nee	Nee	1	79%
Boekel	Ja	Nee	Nee	Ja	Nee	Nee	Nee	2	64%
Borger-Odoorn	Ja	Nee	Nee	Nee	Nee	Nee	Nee	1	36%
Borsele	Ja	Ja	Ja	Ja	Ja	Ja	Ja	7	86%
Brielle	Nee	Nee	Nee	Nee	Nee	Nee	Nee	0	71%
Brunssum	Ja	Ja	Ja	Nee	Ja	Nee	Ja	5	86%
Bunschoten	Nee	Nee	Nee	Nee	Nee	Nee	Nee	0	57%
Dalfsen	Nee	Nee	Ja	Nee	Nee	Nee	Nee	1	57%
De Marne	Ja	Nee	Nee	Nee	Nee	Ja	Nee	2	64%
De Ronde Venen	Nee	Nee	Ja	Ja	Nee	Nee	Nee	2	50%
De Wolden	Ja	Ja	Ja	Ja	Ja	Ja	Nee	6	86%
Den Haag	Ja	Nee	Ja	Ja	Nee	Nee	Nee	3	64%
Diemen	Ja	Nee	Nee	Nee	Nee	Nee	Nee	1	93%
Eemnes	Ja	Ja	Ja	Nee	Ja	Nee	Nee	4	57%
Enkhuizen	Ja	Nee	Nee	Nee	Nee	Nee	Nee	1	64%
Ermelo	Nee	Nee	Nee	Nee	Nee	Nee	Nee	0	57%
Etten-Leur	Nee	Nee	Nee	Nee	Nee	Nee	Nee	0	86%
Franekeradeel	Ja	Nee	Nee	Nee	Nee	Ja	Nee	2	79%
Geertruidenberg	Ja	Nee	Nee	Ja	Ja	Ja	Ja	5	64%
Gennep	Ja	Nee	Nee	Ja	Ja	Ja	Ja	5	79%
Haarlem	Ja	Ja	Ja	Ja	Ja	Ja	Nee	6	50%
Heemskerk	Ja	Nee	Nee	Nee	Nee	Nee	Nee	1	71%
Heerhugowaard	Ja	Nee	Ja	Nee	Nee	Ja	Nee	3	71%
Heiloo	Ja	Ja	Nee	Nee	Nee	Nee	Nee	2	21%

Gemeente	Norm 1.3 E	Norm 1.4.E	Norm 1.5 E	Norm 2.2 E	Norm 2.3 E	Norm 13.1 E	Norm 13.5 E	Aantal normen voldoende	Score op BKWI-monitor
Hilversum	Nee	Nee	Nee	Nee	Nee	Ja	Nee	1	93%
Hof van Twente	Ja	Nee	Nee	Nee	Nee	Nee	Nee	1	50%
Hoogeveen	Ja	Nee	Nee	Nee	Nee	Nee	Nee	1	86%
Huizen	Ja	Ja	Ja	Nee	Ja	Nee	Nee	4	79%
Korendijk	Nee	Nee	Nee	Nee	Nee	Nee	Ja	1	57%
Laarbeek	Ja	Nee	Nee	Ja	Nee	Nee	Nee	2	50%
Leerdam	Ja	Nee	Nee	Nee	Nee	Nee	Nee	1	50%
Liesveld	Ja	Nee	Nee	Nee	Nee	Nee	Nee	1	50%
Maasgouw	Ja	Nee	Nee	Nee	Nee	Nee	Nee	1	64%
Marum	Ja	Ja	Nee	Nee	Nee	Ja	Nee	3	71%
Middelburg	Ja	Nee	Nee	Ja	Nee	Ja	Nee	3	50%
Midden-Drenthe	Ja	Nee	Nee	Nee	Nee	Nee	Nee	1	36%
Moerdijk	Nee	Ja	Ja	Nee	Nee	Ja	Nee	3	100%
Neerijnen	Nee	Nee	Nee	Nee	Nee	Nee	Nee	0	64%
Noord-Beveland	Ja	Nee	Nee	Nee	Nee	Nee	Nee	1	21%
Noordenveld	Ja	Ja	Nee	Nee	Nee	Ja	Nee	3	71%
Ooststellingwerf	Ja	Nee	Nee	Nee	Nee	Ja	Nee	2	79%
Oostzaan	Ja	Ja	Nee	Ja	Ja	Nee	Ja	5	71%
Opsterland	Ja	Nee	Nee	Nee	Nee	Nee	Nee	1	86%
Oude IJsselstreek	Ja	Nee	Nee	Nee	Nee	Nee	Nee	1	71%
Oudewater	Ja	Ja	Ja	Ja	Nee	Ja	Nee	5	71%
Peel en Maas	Ja	Nee	Nee	Ja	Nee	Ja	Nee	3	79%
Rijswijk	Ja	Ja	Nee	Ja	Ja	Ja	Ja	6	86%
Roermond	Ja	Ja	Ja	Ja	Ja	Ja	Ja	7	79%
Schermer	Nee	Nee	Nee	Nee	Nee	Nee	Nee	0	64%
Schinnen	Ja	Nee	Nee	Nee	Nee	Nee	Nee	1	57%
Schoonhoven	Ja	Nee	Nee	Ja	Ja	Ja	Nee	4	100%
Sint-Oedenrode	Nee	Nee	Nee	Nee	Nee	Nee	Nee	0	57%
Soest	Nee	Nee	Nee	Nee	Nee	Nee	Nee	0	93%
Stadskanaal	Ja	Ja	Ja	Ja	Ja	Ja	Ja	7	100%
Strijen	Nee	Nee	Nee	Nee	Nee	Nee	Ja	1	57%
Ten Boer	Ja	Ja	Nee	Nee	Nee	Ja	Nee	3	86%
Texel	Nee	Nee	Nee	Nee	Nee	Nee	Nee	0	71%
Tubbergen	Nee	Ja	Nee	Ja	Ja	Ja	Ja	5	79%
Twenterand	Ja	Ja	Ja	Nee	Nee	Nee	Ja	4	57%
Tynaarlo	Ja	Ja	Nee	Ja	Nee	Ja	Nee	4	71%
Utrecht	Nee	Nee	Nee	Ja	Ja	Ja	Nee	3	71%
Utrechtse Heuvelrug	Ja	Nee	Nee	Nee	Nee	Nee	Nee	1	79%
Vlissingen	Ja	Nee	Nee	Nee	Nee	Ja	Ja	3	64%
Wageningen	Ja	Nee	Nee	Ja	Nee	Nee	Ja	3	79%
Waterland	Ja	Nee	Nee	Nee	Nee	Nee	Nee	1	64%

Gemeente	Norm 1.3 E	Norm 1.4.E	Norm 1.5 E	Norm 2.2 E	Norm 2.3 E	Norm 13.1 E	Norm 13.5 E	Aantal normen voldoende	Score op BKWI-monitor
Westervoort	Ja	Ja	Nee	Nee	Nee	Nee	Nee	2	79%
Weststellingwerf	Ja	Nee	Nee	Ja	Ja	Ja	Ja	5	71%
Winsum	Ja	Nee	Nee	Nee	Nee	Ja	Nee	2	57%
Zederik	Ja	Nee	Nee	Nee	Nee	Nee	Nee	1	50%
Zijpe	Nee	Ja	Nee	Nee	Nee	Ja	Ja	3	50%
Zoeterwoude	Ja	Ja	Ja	Nee	Nee	Nee	Nee	3	50%
Zundert	Ja	Nee	Nee	Nee	Nee	Nee	Nee	1	64%
Zwijndrecht	Ja	Nee	Nee	Nee	Nee	Nee	Nee	1	50%

	Norm 1.3E	Norm 1.4E	Norm 1.5E	Norm 2.2E	Norm 2.3E	Norm 13.1E	Norm 13.5E
Aantal gemeenten dat voldoet aan de norm	61	25	17	24	19	30	16
Aantal gemeenten dat niet voldoet aan de norm	19	55	63	56	61	50	64
% gemeenten dat voldoet aan de norm	76%	31%	21%	30%	24%	38%	20%
% gemeenten dat niet voldoet aan de norm	24%	69%	79%	70%	76%	62%	80%

	Aantal gemeenten	Percentage van het totaal aan tal gemeenten
Gemeente voldoet aan 7 normen	3	4%
Gemeente voldoet aan 6 normen	3	4%
Gemeente voldoet aan 5 normen	8	10%
Gemeente voldoet aan 4 normen	6	8%
Gemeente voldoet aan 3 normen	15	19%
Gemeente voldoet aan 2 normen	9	11%
Gemeente voldoet aan 1 norm	26	33%
Gemeente voldoet aan 0 normen	10	13%
Totaal	80	100% [14]

[14] Door afrondingsverschillen tellen de cijfers in deze tabellen niet altijd op tot exact 100%.

Bijlage 2
Methodologische verantwoording

Representativiteit
Voor dit onderzoek is een zuiver aselecte steekproef getrokken van 80 uit de 415 gemeenten in Nederland, in het jaar 2012. Hiermee kunnen uitspraken worden gedaan over alle gemeenten in Nederland met 95% betrouwbaarheid en een onnauwkeurigheidsmarge van 10%.
Met andere woorden: Als de inspectie in deze nota constateert dat bijvoorbeeld 60% van de steekproefgemeenten niet voldoet aan Norm 13.1, dan betekent dit dat met een betrouwbaarheid van 95% gesteld kan worden dat landelijk gezien 60±10%, dus tussen de 50 en 70% van de gemeenten niet voldoen aan Norm 13.1.

Onderzoekspeildata
Voor het beoordelen van de maatregelen die gemeenten in 2012 hebben getroffen is de inspectie uitgegaan van de stand van zaken op 1 oktober 2012. Maatregelen en documenten, zoals beveiligingsplannen, die na deze datum tot stand zijn gekomen, acht de inspectie onvoldoende van toepassing op het gehele kalenderjaar 2012, en zijn dan ook niet in de beoordeling betrokken.

Reikwijdte uitspraken
Bescherming van persoonsgegevens houdt onder meer in dat deze gegevens op een veilige manier worden verzameld, verwerkt en gedeeld.
Om een uitspraak te doen over de mate waarin gemeenten voldoen aan alle wettelijke eisen rond informatiebeveiliging van Suwi-gegevens, zou bij elke onderzochte gemeente een zogenoemde IT-audit moeten worden uitgevoerd. [15]
Het uitvoeren van een dergelijke IT-audit, die enkele dagen per gemeente zou kosten, valt buiten de mogelijkheden van dit onderzoek. Daarom heeft de inspectie dit onderzoek, in samenspraak met de betrokken beleidsdirectie, beperkt tot het aspect waarvan zij denkt dat zich hierbij de grootste risico's voordoen, namelijk het aspect 'vertrouwelijkheid'. [16]
Het Normenkader bestaat uit totaal 115 subnormen. Hiervan heeft de inspectie er 7 geselecteerd en beoordeeld. Dit zijn weliswaar belangrijke normen, met grote invloed op de totale informatiebeveiliging van een gemeente, maar 108 subnormen zijn niet beoordeeld. Het al dan niet voldoen aan één van de zeven door de inspectie beoordeelde normen, zegt niet automatisch iets over het voldoen aan de overige normen.

Benadering gemeenten
In december heeft de inspectie een brief gestuurd aan de Colleges van B&W van de 80 steekproefgemeenten waarmee het onderzoek is aangekondigd en toegelicht. Aan de colleges is verzocht om de naam en het mailadres van een contactpersoon (bij voorkeur de security officer) aan de inspectie door te geven. In de brief is gewezen op het verplichte karakter van deelname aan dit onderzoek. De brief leverde uiteindelijk (na schriftelijke en telefonische rappeleringen 100% respons op.

Aan de functionaris die door het college is aangewezen is per e-mail een vragenlijst toegestuurd. De antwoorden op de vragenlijst zijn door medewerkers van de inspec-

[15] IT-auditing is het vakgebied dat zich bezighoudt met het beoordelen van de automatisering van de organisatie en de organisatie van de automatisering. IT-auditing is een specialisme binnen het auditing-vakgebied. Het specialisme wordt meer en meer gevraagd bij uitvoering van accountantscontroles.

[16] Met vertrouwelijkheid wordt bedoeld dat een gegeven alleen te benaderen is door iemand die gemachtigd is het gegeven te benaderen en voor zijn wettelijke taken nodig heeft.

tie beoordeeld, in samenhang met reeds over de gemeente bekende informatie die de inspectie via BKWI heeft betrokken. In vrijwel alle gevallen leidde bestudering van de stukken tot aanvullende vragen, die per e-mail aan de contactpersoon van de gemeente zijn voorgelegd.
Na ontvangst van de antwoorden op de aanvullende vragen en eventuele bewijsstukken is de informatie van en over gemeenten beoordeeld door medewerkers van de inspectie, aan de hand van de tekst van de beoordeelde normen en een daarop gebaseerd werkprogramma. De resultaten van de beoordelingen zijn besproken en afgestemd in een team van kwaliteitsborgers, waarin onder andere een extern ingehuurde gecertificeerde IT-auditor zitting had.

De resultaten van de beoordelingen zijn in mei 2012 in concept verzonden aan de Colleges van B&W van de steekproefgemeenten, in afschrift aan de contactpersonen. De inspectie heeft de gemeente de mogelijkheid geboden te reageren op de concept versies van de beoordelingen en eventueel nog aanvullende documenten op te leveren.
Na ontvangst van de reacties van gemeenten of het verstrijken van de reactietermijn zijn in juni 2013 de definitieve beoordelingen aan de Colleges van B&W van de gemeenten verzonden.

Samenwerkende gemeenten
Een aanzienlijk aantal gemeenten werkt samen voor wat betreft de uitvoering van de WWB en aanverwante sociale voorzieningen. Onder de 80 gemeenten waarop het onderzoek zich heeft gericht, bevonden zich 30 gemeenten die op een of andere manier samenwerken.
Waar een gemeente samenwerkt met één of meer andere gemeenten op het gebied van sociale zaken binnen een intergemeentelijke sociale dienst of anderszins heeft het onderzoek zich gericht op het samenwerkingsverband. Lees hiervoor ook paragraaf 4.3, Samenwerking in de uitvoering.

Informatie van BKWI
Het BKWI is verplicht om gegevens te loggen waarmee het gebruik van Suwinet-Inkijk per medewerker van onder andere gemeentelijke gemeenten kan worden nagegaan. Deze logging bevat informatie over wie (welke gebruiker) welke gegevens over welk BSN heeft geraadpleegd. Op basis van deze logging worden periodieke rapportages opgesteld. Deze rapportages, die maandelijks door gemeenten opvraagbaar zijn via Suwinet, bevatten onder meer informatie over het totale aantal opvragingen, het aantal burgerservicenummers dat is geraadpleegd, het aantal opvragingen binnen en buiten kantooruren, het aantal geslaagde en niet geslaagde inlogpogingen, het aantal actieve en inactieve accounts etc.
De rapportages bevatten geen naar natuurlijke personen herleidbare informatie.

De inspectie heeft BKWI verzocht om te kunnen beschikken over de rapportages van de periode november 2011 tot en met oktober 2012 van alle 80 steekproefgemeenten. De inspectie heeft deze gegevens ontvangen en gebruikt als aanvullende informatie bij de beoordeling van de gemeentelijke informatiebeveiliging op het gebied van Suwi.

Voorts heeft de inspectie bij dit onderzoek bij BKWI ook rapportages opgevraagd waarmee het inloggedrag op de zogenaamde zware rollen zichtbaar kan worden gemaakt.
De bedoeling hiervan was om opvallend zoekgedrag op te sporen, en te bezien of de gemeente dat gedrag zelf ook als zodanig herkende en/of er goede verklaringen

voor heeft gevonden, dan wel of er adequate maatregelen zijn genomen om soortgelijk gedrag in de toekomst te voorkomen.
Het opvallend vaak raadplegen van Suwinet met zware rollen, kan immers wijzen op onrechtmatig gebruik (bijvoorbeeld uit nieuwsgierigheid of met een ander motief raadplegen van buren, familie, andere verkeersdeelnemers etc.)
De logfiles die zijn opgevraagd betreffen het zoekgedrag op zware rollen. Namelijk op naam en geboortedatum (normaliter wordt gezocht op BSN om toegang te krijgen tot iemands persoonsgegevens), op postcode en huisnummer (idem, gewoonlijk wordt gezocht op BSN) en op kenteken (voor het vaststellen van het bezit van voertuigen kunnen via het BSN de gegevens van het RDW worden ingezien, hiervoor is kenteken niet nodig)
Om te bepalen wanneer er wel, en wanneer er niet sprake is van gebruik dat nader onderzoek behoeft heeft de inspectie onderscheid gemaakt naar het gebruik per account (per medewerker met toegang tot Suwinet) en per gemeente. Voor het gebruik per medewerker zijn alle logfiles meegenomen van medewerkers die meer dan 1x dan wel 2x de standaardafwijking overtreffen van (boven) het gemiddeld aantal keren dat in 2012 op de geselecteerde zware rol is gezocht. De keuze voor 1x dan wel 2x de standaardafwijking is voornamelijk om praktische redenen toegepast. Sommige logfiles zijn zo omvangrijk dat het voor de inspectie een te zware belasting zou zijn om alles boven 1x de standaardafwijking mee te nemen.
Voor het aantal keren dat er per gemeente is geraadpleegd is het bovenstaande geen goede oplossing. Grotere gemeenten zullen a priori immers vaker zoeken dan kleinere gemeenten. Daarom heeft de inspectie het aantal keren dat vanuit eenzelfde gemeente is ingelogd op de onderzochte zware rol, gedeeld door het aantal WWB-ers per gemeente. Daarna is het gemiddelde berekend en is de bovenomschreven selectiemethode toegepast om de uitschieters te selecteren.

Tenslotte heeft de inspectie aan BKWI gevraagd na te gaan of en zo ja hoe vaak gezocht is op het BSN van bekende Nederlanders. Normaliter zal niet vaak sprake zijn van noodzakelijk zoekgedrag op een bekende Nederlander. Voor de logfiles die over het zoeken op bekende Nederlander zijn opgevraagd heeft de inspectie een honderdtal namen van willekeurig gekozen bekende Nederlanders aan BKWI opgegeven en heeft BKWI aangegeven hoe vaak gegevens van één of meerdere bekende Nederlanders uit de lijst van 100 door één of meer steekproefgemeenten zijn geraadpleegd. De inspectie gaat er hierbij vanuit dat het zoeken op een bekende Nederlander een indicator is voor de mate waarin Suwinet oneigenlijk en/of onrechtmatig wordt gebruikt. De premisse is dat het voor een medewerker met toegang tot Suwinet verleidelijker is om BSN van die personen te raadplegen die voor hem of haar van meer belang zijn. Te denken valt aan het raadplegen van gegevens van collega's, leidinggevenden, (ex)-partners, familieleden, buren, verkopers van woningen waarin de medewerker geïnteresseerd is, etc. Overigens is dit soort zoekgedrag door gemeenten op te sporen door een vergelijking te maken tussen de door de medewerker geraadpleegde BSN en zijn of haar werkvoorraad. Bij afwijkingen kan de medewerker een verklaring worden gevraagd. Er zijn binnen dit onderzoek gemeenten aangetroffen die deze controle periodiek en steekproefsgewijs hanteert.

Bij opvallend zoekgedrag is aan de contactpersonen van gemeenten gevraagd een verklaring hiervoor te geven.

Bijlage 3, Wettelijk kader

Op grond van de Wet SUWI en de WWB wisselen UWV, SVB en gemeenten (de SUWI-partijen) persoonsgegeven uit in het kader van de uitvoering van hun wettelijke taken. Met het oog daarop dragen de SUWI-partijen zorg voor de instandhouding van de gemeenschappelijke elektronische voorzieningen SUWI (GeVS) voor de uitwisseling van die gegevens. Vanaf de inwerkingtreding van de Wet SUWI droeg deze voorziening de naam Suwinet. Het Besluit SUWI en de Regeling SUWI bevatten nadere regelgeving ten aanzien vande GeVS. Met name wordt in het kader van dit onderzoek genoemd artikel 6.4, tweede lid, van de Regeling SUWI, dat onderr andere gemeenten verplicht in een beveiligingsplan aan te geven hoe zij zorgdragen voor de beveiliging van de gegevensuitwisseling via de GeVS, overeenkomstig hetgeen over de voor het stelsel van maatregelen en procedures te hanteren normen wordt bepaald in bijlage I bij de Regeling SUWI (Stelselontwerp & Beveiliging Gezamenlijke elektronische Voorzieningen SUWI). Naast de Wet SUWI en de daarop berustende regelgeving is de Wet bescherming persoonsgegevens (WBP) van toepassing als algemene wet op de gebieden die niet geregeld zijn.

In bijlage 1 bij de Regeling SUWI is bepaald dat de SUWI-partijen en BKWI gezamenlijk een "Verantwoordingsrichtlijn privacy en beveiliging GeVS" ontwikkelen; deze verantwoordingsrichtlijn bevat ook een normenkader GeVS (verder: het Suwinet-normenkader). De Verantwoordingsrichtlijn is gericht tot de SUWI-partijen die zich op grond van artikel 6.4, derde lid van de Regeling SUWI verantwoorden over het gebruik en de inrichting van de GeVS, te weten het UWV, de SVB en het IB. Het Suwinet-normenkader is een praktische vertaling van de eisen op het gebied van beveiliging en privacy bij het gebruik van de GeVS, waarin mede gebruik is gemaakt van professionele standaards zoals de Code voor Informatiebeveiliging en het rapport "Beveiliging van persoonsgegevens", gepubliceerd door de toenmalige Registratiekamer als Achtergrondstudies en Verkenningen nr. 23.

In het normenkader wordt onderscheid gemaakt tussen essentiële en niet-essentiële normen. Door de SUWI-partijen is aan essentiële normen een zwaarder belang toegekend dan aan niet-essentiële normen. In de Verantwoordingsrichtlijn is bepaald dat een goedkeurend oordeel door een IT-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 beschouwt het Suwinet-normenkader als de professionele standaard voor alle SUWI-partijen op het gebied van beveiliging en privacy van Suwinet.

Bijlage 4, Door de inspectie gehanteerde normen

De inspectie heeft de gemeenten in de steekproef beoordeeld op de volgende zeven essentiële normen:

Aandachtsgebied 1. Beveiligingsbeleid en beveiligingsplan

- *Norm 1.3*: Het informatiebeveiligingsbeleid en het beveiligingsplan van het Suwinet zijn goedgekeurd door het management van de Suwi-partij.
- *Norm 1.4*: Het informatiebeveiligingsbeleid en het beveiligingsplan van het Suwinet worden uitgedragen in de organisatie.
- *Norm 1.5*: Het informatiebeveiligingsbeleid en het beveiligingsplan van het Suwinet worden jaarlijks geëvalueerd en indien nodig geactualiseerd

Aandachtsgebied 2. Organisatie

- *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

- *Norm 2.3*: De Security Officer beheert en beheerst beveiligingsprocedures en maatregelen in het kader van Suwinet, zodanig dat de beveiliging van Suwi overeenkomstig wettelijke eisen is geïmplementeerd.
    - De Security Officer bevordert en adviseert over de beveiliging van Suwinet, verzorgt rapportages over de status, controleert dat m.b.t. 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

Aandachtsgebied 13. Logische toegangsbeveiliging

- *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 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

- *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

Bijlage 5, Vragenlijst voor gemeenten

Contactgegevens

Gemeente

Functionaris, naam, functie en afdeling

Mailadres

Telefoonnummer

Norm 1 (beveiligingsbeleid en beveiligingsplan)

Vragen:

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

b. Heeft uw Sociale Dienst een informatiebeveiliging**splan** 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 geëvalueerd en geactualiseerd (bijv. verslagen, oude versies en wijzigingen).
- Bij mandatering of overdracht van taken: mandateringsbesluiten, gemeenschappelijke regelingen, contracten en periodieke evaluaties.

Norm 2 (organisatorische aspecten)

Vragen:

a. Heeft u taken en verantwoordelijkheden en bevoegdheden beschreven?

b. Hoe heeft u deze belegd?

c. Op basis van welke criteria hebben medewerkers:
   i. toegang tot gegevens uit Suwinet?

   ii. Zware rollen / speciale toegangsrechten (zoals bijvoorbeeld de GSD-rollen 018, 021 en 030)?

   iii. de mogelijkheid bevoegdheden te verlenen?

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

e. Maakt u gebruik van SuwinetInlezen?

f. Zo ja, wat is hiervoor uw beleid? Zo nee, kunt u de hieronder bij norm 13 gestelde vragen (deel 2) 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 SuwinetInlezen;
- Naam van de security officer, zijn/haar takenpakket en rapportages die door hem/haar in 2012 zijn opgesteld (eventueel geanonimiseerd).

Norm 13 (logische toegangsbeveiliging)

Vragen:

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 speciale toegangsrechten (vergelijkbaar met zware rollen, zie norm 2) en welke?

d. Hoeveel medewerkers (en welke functie hebben deze) kunnen toegangsrechten verlenen en hoe gebeurt dit, zowel formeel als feitelijk?

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 (zowel formeel als feitelijk) verleend en weer ingetrokken?

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

j. Hoe vaak hebt u het afgelopen jaar 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 speciale toegangsrechten (zware rollen, zie norm 2) en welke?

d. Hoeveel medewerkers kunnen toegangsrechten verlenen en welke functies hebben deze medewerkers? Hoe gebeurt dit, zowel formeel als feitelijk?

e. Hoe, en hoe vaak controleert u het gebruik van Suwinetgegevens 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 (zowel formeel als feitelijk) verleend en weer ingetrokken?

i. Gebruikt u voor controle vergelijkbare overzichten als de periodieke 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.