Vereniging van
Nederlandse Gemeenten

Zelftest

Lees onderstaande informatie eerst aandachtig door voorafgaand aan de zelftest

Waarom biedt de VNG de zelftest aan?

Recent heeft de Inspectie SZW de resultaten bekend gemaakt van een onderzoek naar de wijze waarop gemeenten omgaan met persoonsgegevens die zij opvragen via suwinet. De inspectie heeft 80 gemeenten bevraagd op het voldoen aan 7 normen uit het suwi normenkader. Aan alle normen uit het normenkader van suwi moeten gemeenten (al jarenlang) voldoen. De voor het inspectieonderzoek geselecteerde en onderzochte aandachtsgebieden zijn:

- Het informatiebeveiligingsbeleid en beveiligingsplan
- Inrichten en onderhouden van de beveiligingsfunctie en –organisatie (zoals het aanstellen van een security-officer)
- Toegangsbeveiliging, gericht op het voorkomen van ongeautoriseerde toegang tot en gebruik van persoonsgegevens, alsmede de controle op het gebruik.

De resultaten uit het onderzoek zijn schokkend. Opnieuw blijkt dat gemeenten niet goed omgaan met persoonsgegevens van de burger. De staatssecretaris SZW, het College Bescherming Persoonsgegevens, de Tweede Kamer en de VNG hebben geschokt gereageerd. VNG heeft een verbeterplan opgesteld waarin deze zelftest een centrale rol speelt.

Waartoe dient de zelftest?

Met de zelftest kan elke gemeente in kaart brengen of zij inzage in suwinet op maat aanbiedt aan haar medewerkers, of er goed op gebruikt wordt toegezien en hoe de waarborgen daartoe zijn ingebed. Daarmee ziet de gemeente vervolgens aan welke van de zeven door de Inspectie SZW onderzochte normen zij wel of niet voldoet. De einduitkomst kunt u zien als een sterkte / zwakte analyse van uw gemeente. Het biedt richting voor het lokale verbeterpad.

Wat is de relatie tot de Baseline Informatiebeveiliging voor gemeenten?

Op de ALV van 29 november jl. heeft 95% van de gemeenten ingestemd met de resolutie over informatiebeveiliging. Dat betekent dat via een route van zelfregulering de bovengenoemde baseline voor gemeenten het uitgangspunt wordt voor het structureel verbeteren van informatiebeveiliging. In de bijlage bij deze zelftest is aangegeven dat de 7 door de inspectie onderzochte normen een op een terugkomen in de Baseline Informatiebeveiliging. Met het verrichten van de zelftest en de daaruit volgende inzet om de resultaten te optimaliseren, werkt u dus ook aan de implementatie van de Baseline Informatiebeveiliging. U doet geen werk dubbel of voor niets.

Kan direct begonnen worden met het verrichten van de zelftest?

Het verdient aanbeveling om eerst de VNG Ledenbrief van 12 november te lezen met betrekking tot het inspectieonderzoek en de bestuurlijke reactie van de VNG hierop. Daarnaast is het ook goed om eerst een bezoek te brengen aan www.bkwi.nl/veiligsuwinet waar de door de inspectie onderzochte normen worden toegelicht. Na

de zelftest kan de gemeente in kaart brengen wat zij in welke volgorde wil verbeteren en hoe. Hulpmiddelen daarvoor zijn eveneens te downloaden van www.bkwi.nl/veiligsuwinet

Waarom is het noodzakelijk om deze zelftest te doen en wat gebeurt er als we niets doen?

Het is van wezenlijk belang om de situatie van alle gemeenten in beeld te krijgen. Daarnaast is het zo dat een goede zelfanalyse een eerste stap op weg is naar het verbeteren van de lokale situatie. In de tekst die volgt op de vragenlijst ziet u welke volgende stappen u kunt zetten. Als we niets doen zal de situatie niet verbeteren. Gemeenten verliezen dan het vertrouwen van de burger, het rijk en de ketenpartners. Doorontwikkeling van gegevensuitwisseling wordt onmogelijk.Sterker nog, zelfs de huidige uitwisseling kan aan banden worden gelegd. Zonder gegevensuitwisseling is integrale dienstverlening en daarmee het adequaat uitvoeren van de decentralisaties onmogelijk.

Van wie komt deze zelftest?

De zelftest is tot stand gebracht door de VNG, daarbij geadviseerd door BKWI, KING en de Inspectie SZW. De vragenlijst is een directe afgeleide van de door de Inspectie SZW gehanteerde vragenlijst.

Wat vragen we u verder nog te doen?

Wanneer u de vragenlijst hebt ingevuld resulteert dat in een overzicht waarbij u per norm weet of u hieraan wel of niet voldoet. Wanneer u niet aan de norm voldoet, hebt u scherp met welke deelaspecten van de betreffende norm dit te maken heeft. Begin januari zet de VNG via haar website een webapplicatie open. Daarover volgt speciale berichtgeving. Wij vragen de hiertoe aangeschreven gemeentelijke contactpersonen om de situatie van de gemeente in te vullen. Dus per norm of aan deze norm wel of niet voldaan is. In aanvulling hierop vragen we ook om aan te geven of de verbeteraanpak met de gemeenteraad gedeeld zal worden of al gedeeld is. Wij adviseren om dat zo spoedig mogelijk te doen. Alle gemeenteraden zullen vanuit zowel SZW als de VNG geïnformeerd worden over het verbetertraject en opgeroepen worden om hiernaar te vragen bij het college van B&W.

Hoeveel tijd kost het uitvoeren van de zelftest?

Dat hangt ervan af. Als in uw gemeente alles goed geregeld is dan kost de zelftest u tien minuten. Is er weinig tot niets geregeld en de invuller moet dit bij diverse personen en afdelingen nagaan kan dit wel een tot enkele uren in beslag nemen.

Hoe werkt het?

Loop alle deelvragen langs en geef aan of de gemeente er wel of niet aan voldoet. Aan norm wordt pas voldaan wanneer aan alle subnormen wordt voldaan. Zo wordt duidelijk aan welke normen wel of niet voldaan is. Het is een zelftest. De VNG gaat ervan uit dat alle vragen waarvan u aangeeft dat uw gemeente deze scoort, daartoe ook gedocumenteerd materiaal in de organisatie aanwezig is. Wij vragen dit niet op. De Inspectie die op verzoek van de staatssecretaris in 2015 haar onderzoek uit 2012/2013 zal herhalen, zal dit wel doen. Ook is de kans aanwezig dat het College Bescherming Persoonsgegevens bij individuele gemeenten onderzoek zal doen. Het college heeft de bevoegdheid om boetes op te leggen.

Wie is het beste in staat om de vragen te beantwoorden?

Wij denken dat de security officer (hetzij alleen verantwoordelijk voor de sociale dienst, hetzij met een bredere verantwoordelijkheid binnen de gemeente) het beste in staat is om antwoorden op de vragen in te vullen. Hij/zij kan dit niet alleen en zal hiertoe diverse collega's moeten bevragen. Bijvoorbeeld de beleidsmedewerker die het plan heeft geschreven, de applicatiebeheerder die de autorisaties verleent, p&o die functieomschrijvingen opstelt etc.

Wie worden er aangeschreven door de VNG?

Deze zelftest staat op de website van de VNG en BKWI. Iedereen kan er kennis van nemen. Voor het invullen van de webapplicatie met de uitkomsten zullen de security-officers die bij BKWI staan geregistreerd, worden benaderd. Van gemeenten waarvan geen security officer is geregistreerd zal het afdelingshoofd of de directeur van

de (intergemeentelijke) sociale dienst worden aangeschreven. De webapplicatie werkt met een inlogcode waarbij alleen de gegevens van de eigen gemeente kunnen worden gezien.

Wat doen we met de door de gemeenten aangereikte gegevens?

Alle resultaten worden weggeschreven in een bestand. Dit bestand kan alleen worden ingezien door de VNG. In februari of maart wordt de applicatie weer 'dichtgezet'. Op basis van de inhoud van het bestand op dat moment zal een periodieke geanonimiseerde en geaggregeerde voortgangsrapportage worden geschreven. Deze dient als input voor voortgangsoverleg met SZW, CBP en Tweede Kamer. Gemeenten die niet hebben aangeleverd of slecht scoren zullen hierop door de VNG en SZW worden aangesproken. Het is niet uitgesloten dat het CBP ook geaggregeerde informatie zal opvragen in het kader van toezichthoudende activiteiten. De VNG zal niet de gegevens van individuele gemeenten delen of naar buiten brengen. Eind 2014 zal VNG de webapplicatie weer open zetten. U wordt dan gevraagd opnieuw de zelftest in te vullen. Op basis van de resultaten van dat moment levert de VNG opnieuw een voortgangsrapportage aan.

De Inspectie SZW maakt overigens de resultaten bekend van gemeenten die zij in haar steekproef van het onderzoek uit 2012/2013 opnam en in 2015 in haar steekproef op zal nemen.

Wie kijken er mee naar de geaggregeerde resultaten?

Het ministerie / de staatssecretaris van SZW, de Tweede Kamer en het College Bescherming Persoonsgegevens. Ook ketenpartners zoals UWV volgen met meer dan gemiddelde belangstelling de voortgang van het verbetertraject.

Waar kunt u nog meer informatie vinden over het verbetertraject voor veilig gebruik van suwinet door gemeenten?

Dat kan op twee manieren:

- Via een abonnement op het VNG-Weekbericht. Deze maakt u aan op www.vng.nl, kruis hierbij het veld 'Sociale Zaken' aan. Het weekbericht is een digitale nieuwsbrief die u wekelijks op vrijdagavond in uw mailbox ontvangt. Alle voortgangsberichten over het verbetertraject worden hierin opgenomen.
- Via www.bkwi.nl/veiligsuwinet. Vanaf deze site zijn alle verbetertools te downloaden die normsgewijs worden aangeboden. Ook wordt per norm afzonderlijk achtergrondinformatie verschaft.

Voor vragen over informatiebeveiliging in algemene zin (breder dan suwi en de keten van werk en inkomen) verwijzen wij u door naar de Informatie Beveiligingsdienst, ondergebracht bij KING. Zie: https://new.kinggemeenten.nl/informatiebeveiliging

1.3. Het informatiebeveiligingsbeleid en beveiligingsplan zijn goedgekeurd door het management en / of de directie en / of het college van B&W.

☐ Er is een specifiek op suwinet gericht informatiebeveiligingsbeleid of veiligheidsplan aanwezig of er is een suwi-specifieke passage in een algemeen plan aanwezig.

☐ Dit beleid, dit plan of deze passage heeft specifiek betrekking op uw gemeente.

ISD-en let op: elke gemeente in uw samenwerkingsverband dient apart het beleid, plan of de passage te accorderen.

☐ De goedkeuring is formeel vastgelegd. Het beleid, het plan of de passage is ondertekend of van de goedkeuring is expliciet melding gemaakt in het verslag van de betreffende vergadering.

Om aan norm 1.3 te voldoen is het noodzakelijk dat alle drie bovengenoemde eisen is voldaan.

☐ Aan norm 1.3 is voldaan

☐ Aan norm 1.3 is niet voldaan

1.4 Het informatiebeveiligingsbeleid, het beveiligingsplan of de beveiligingspassage worden uitgedragen

☐ Het informatiebeveiligheidsbeleid, het beveiligingsplan of de beveiligingspassage is centraal voor alle gebruikers centraal beschikbaar (het is bijvoorbeeld aan iedereen gemaild of staat op intranet).

☐ Er is het afgelopen jaar minimaal 2x een actie geweest om de gebruikers (opnieuw) te attenderen op het bestaan van het veiligheidsbeleid, -plan of -passage.

Bijvoorbeeld door hernieuwd te wijzen op intranet, te agenderen voor een afdelingsoverleg of te bespreken in functioneringsgesprekken. Wanneer alleen nieuwe gebruikers wordt gevraagd om een geheimhoudingsverklaring te tekenen is dat een goede actie, maar niet voldoende. Het bezoeken van BKWI-bijeenkomsten strekt tot aanbeveling, maar is op zich evenmin voldoende.

Om aan norm 1.4 te voldoen is het noodzakelijk dat aan beide bovengenoemde eisen is voldaan.

☐ Aan norm 1.4 is voldaan

☐ Aan norm 1.4 is niet voldaan

1.5 Het informatiebeveiligingsbeleid, het beveiligingsplan of de beveiligingspassage worden jaarlijks geëvalueerd

☐ De laatste evaluatie is minder dan een jaar oud

☐ De laatste evaluatie is vastgesteld door management en / of directie en / of college van B&W

☐ De evaluatie is een concrete actie van alle direct betrokkenen geweest, schriftelijk vastgelegd en leidt zo nodig tot aanpassen van het informatiebeveiligingsbeleid, het veiligheidsplan of de beveiligingspassage

Om aan norm 1.5 te voldoen is het noodzakelijk dat aan de drie bovengenoemde eisen is voldaan.

☐ Aan norm 1.5 is voldaan

☐ Aan norm 1.5 is niet voldaan

2.2 Functiescheiding

Bij de functiescheiding is het belangrijk dat bij verschillende personen is belegd:

- Uitvoering van taken (het gebruik van suwinet);
- Het beheer van autorisaties (toegang verlenen tot suwinet)
- Kwaliteitszorg en borging van rechtmatig gebruik (controle op gebruik van suwinet);
- Management (beslissen over bevoegdheden van functiegroepen, en/of individuele medewerkers, uitdragen belang goed gebruik, bijsturen na oneigenlijk gebruik, optreden na misbruik suwinet).

☐ Deze scheiding is schriftelijk vastgelegd

☐ Er is een aanvullend document aanwezig waaruit blijkt dat ten aanzien van functiescheiding duidelijke keuzes zijn gemaakt bij het beleggen van taken. Of er is een onderbouwde verklaring waarom zo'n document er niet is en er is een alternatieve aanpak om misbruik te voorkomen (bijvoorbeeld extra controle waar functiescheiding niet of minder goed mogelijk bleek).

Om aan norm 2.2 te voldoen is het noodzakelijk dat aan beide vereisten is voldaan.

☐ Aan norm 2.2 is voldaan

☐ Aan norm 2.2 is niet voldaan

2.3 Security officer

☐ Er is een medewerker verantwoordelijk gemaakt om periodiek – ten minste twee keer per jaar - naar de beveiliging van suwinet kijken

☐ Deze medewerker rapporteert en adviseert periodiek rechtstreeks aan het management en / of de directie en / of het college van B&W

ISD-en let op: het is de bedoeling dat de security officer van de ISD naar elke gemeente apart rapporteert en adviseert.

☐ Dat is vastgelegd in zijn / haar functieomschrijving inclusief takenoverzicht

Om aan norm 2.3 te voldoen is het noodzakelijk dat aan elk van de drie bovengenoemde eisen is voldaan.

☐ Aan norm 2.3 is voldaan

☐ Aan norm 2.3 is niet voldaan

13.1 Autorisatieprocedure

Elke gebruiker van suwinet moet geautoriseerd worden.

☐ Er is een formeel vastgelegde autorisatieprocedure waarin functies aan autorisaties en in het verlengde daarvan aan rollen worden gekoppeld

☐ Het accountbestand wordt meerdere keren per jaar gecontroleerd en aansluitend worden inactieve accounts verwijderd

☐ Er is geen toegang verstrekt buiten de sociale dienst, de gemeentelijke belastingdeurwaarders, burgerzaken en de regionale meld- en coördinatiefunctie bij voortijdig schoolverlaten. Voor het gebruik door gemeentelijke belastingdeurwaarders, burgerzaken en de regionale meld- en coördinatiefunctie bij voortijdig schoolverlaten is een apart contract afgesloten. Het is op dit moment niet geoorloofd om WMO-medewerkers, medewerkers Parkeerbeheer of andere hierboven niet benoemde medewerkers toegang te verstrekken tot suwinet.

Om aan norm 13.1 te voldoen is het noodzakelijk dat aan elk van de drie bovengenoemde eisen is voldaan

☐ Aan norm 13.1 is voldaan

☐ Aan norm 13.1 is niet voldaan

13.5 Controle op toegang en gebruik

☐ Een medewerker van de gemeente vraagt ten minste meerdere keren per jaar bij BKWI een rapportage over het gebruik van suwinet-inkijk op.

Let op: medewerkers van BKWI mogen niet op eigen initiatief aan gemeenten meegeven dat zij opmerkelijkheden constateren in de loggings. Het verdient aanbeveling om bij het opvragen expliciet naar de waarnemingen van BKWI zelf te vragen. Dan is het weergeven van de BKWI-waarneming wel geoorloofd.

☐ De beoordeling van deze rapportage (door wie en langs welke criteria) is centraal belegd

☐ Deze beoordelaar maakt hiervan een schriftelijk verslag

☐ Als uit dit verslag blijkt dat nadere beoordeling gewenst is, wordt vervolgens bij BKWI een specifieke rapportage opgevraagd die vervolgens wordt beoordeeld.

☐ Bij geconstateerd oneigenlijk gebruik c.q. misbruik wordt er ook opgetreden c.q. gesanctioneerd

Om aan norm 13.5 te voldoen is het noodzakelijk dat aan elk van de vijf bovengenoemde eisen is voldaan

☐ Aan norm 13.5 is voldaan

☐ Aan norm 13.5 is niet voldaan

Vraag over transparantie en verantwoording die geen deel uitmaakt van het normenkader

Het is belangrijk om over het gebruik van persoonsgegevens van burgers transparant te communiceren en de daarbij gekozen aanpak te verantwoorden.

☐ De resultaten en de verbeteraanpak zullen binnen maximaal 2 maanden met de gemeenteraad worden gedeeld

Informatie van belang na afloop van het invullen van de vragenlijst

U heeft nu inzicht verkregen in de sterke en verbeterpunten van uw gemeente waar het gaat om veilig en zorgvuldig gebruik van suwinet. Wat kunt u nu vervolgens doen met dit inzicht:

- Deel de einduitkomsten per norm met de VNG via de web enquête die in januari via www.vng.nl zal worden opengesteld. Daarover worden security officers, afdelingshoofden en directeuren van de sociale diensten persoonlijk bericht.
- Ga lokaal aan de slag:
  - Bent u een gemeente die aan 7 normen voldoet? Dan willen wij u vragen om uw kennis en aanpak ter beschikking te stellen. Zie helemaal onderaan de pagina.
  - Bent u een gemeente die aan 4, 5 of 6 normen voldoet? Per niet gescoorde norm is een verbetertool beschikbaar. Zie daarvoor www.bkwi.nl/veiligsuwinet
  - Bent u een gemeente die aan 0,1,2 of 3 normen voldoet? In uw gemeente is veel te verbeteren, zowel qua inrichting van de organisatie als qua werkproces. Op dit moment wordt een stappenplan geschreven die u kan helpen om in de juiste volgorde, met de juiste sleutelfiguren en de meeste treffende toonzetting uw gemeente op het goede spoor te zetten. We hopen het stappenplan nog in 2013 te kunnen opleveren.
- In het eerste kwartaal van 2014 zal de VNG op vijf plaatsen in het land voorlichtingsbijeenkomsten organiseren. De helft van de bijeenkomsten is gericht op de security-officers en de andere helft op die functionarissen van de sociale dienst die op de een of andere manier met HRM-beleid zijn verbonden (afdelingshoofden, teamleiders, hoofd P&O, medewerker P&O etc). In de sessies met de security-officers zullen de verbetertools centraal staan en hoe deze in te zetten. In de sessies over HRM staat het cultuuraspect meer centraal en de wijzen waarop dat in HRM-beleid een plek kan krijgen. Eind december zal hierover meer informatie volgen op de website van de VNG.
- Eind 2014 zet de VNG de webapplicatie weer open. Gemeenten worden opnieuw gevraagd om de stand van zaken door te geven. Wij hopen van harte een ten opzichte van eind 2013 sterk verbeterde situatie te mogen waarnemen.

Neem bij vragen, suggesties of voor het aanleveren van best practices contact op met de VNG:
Beleidsafdeling W&I, Jasja van Ark, Jasja.vanArk@vng.nl, 070-3738696.
Bij zeer technische en inhoudelijk specialistische vragen verwijst de VNG u door naar BKWI.
Bij afwezigheid van de contactpersoon kunt u contact opnemen met de VNG Helpdesk, 070-3738020

Bijlage: koppeling tussen de suwi-normen en de BIG-normen

SUWI	SUWI tekst	BIG	BIG tekst
1.3	Het veiligheidsbeleid en -plan is goedgekeurd door het management en / of de directieen / of het college van B&W.	5.1.1	Informatiebeveiligingsbeleid behoort door het hoogste management te worden goedgekeurd en gepubliceerd. Het document dient tevens kenbaar te worden gemaakt aan alle werknemers en relevante externe partijen.
1.4	Het veiligheidsbeleid, -plan en -passage worden uitgedragen	5.1.1	Informatiebeveiligingsbeleid behoort door het hoogste management te worden goedgekeurd en gepubliceerd. Het document dient tevens kenbaar te worden gemaakt aan alle werknemers en relevante externe partijen.
1.5	Veiligheidsbeleid, - plan of -passage worden jaarlijks geëvalueerd	5.1.2	Het informatiebeveiligingsbeleid behoort met geplande tussenpozen, of zodra zich belangrijke wijzigingen voordoen, te worden beoordeeld om te bewerkstelligen dat het geschikt, toereikend en doeltreffend blijft.
2.2	Functiescheiding	10.1.3	Taken en verantwoordelijkheidsgebieden behoren te worden gescheiden om gelegenheid voor onbevoegde of onbedoelde wijziging of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.
2.3	Security officer	6.1.2	Activiteiten voor informatiebeveiliging behoren te worden gecoördineerd door vertegenwoordigers uit de verschillende delen van de organisatie met relevante rollen en functies.
13.1	Autorisatieprocedure	11.5.1	(niet geheel een match, deels “plusje”). Elke gebruiker behoort over een unieke identificatiecode te beschikken (gebruikers-ID) voor uitsluitend persoonlijk gebruik, en er behoort een geschikte authenticatietechniek te worden gekozen om de geclaimde identiteit van de gebruiker te bewijzen.
13.5	Controle op toegang en gebruik	10.10.2	Er behoren procedures te worden vastgesteld om het gebruik van ITvoorzieningen te controleren. Het resultaat van de controleactiviteiten behoort regelmatig te worden beoordeeld.