Assurance Rapport
NOREA Richtlijn 3000

Verantwoording betreffende het gebruik van
de Gezamenlijke elektronische Voorzieningen Suwi
(GeVS)

Gemeente Venlo

Opgesteld voor de Gemeenten
Beesel, Bergen, Gennep, Horst aan de Maas, Mook en Middelaar, Peel en Maas en Venray

Uitgebracht door:	3angles B.V.
Auditors:	C.N.A. Beusenberg
Uitgebracht aan:	Gemeente Venlo
Contactpersoon:	J.H.A. Rayer
Datum:	22 februari 2023
Rapportnummer:	2302R.CB80
Versie:	1.1
Status:	Definitief

Inhoud

1 Assurancerapport van de onafhankelijke auditor

1.1 Opdracht

Ingevolge de opdracht van Gemeente Venlo hebben wij een onderzoek uitgevoerd naar de opzet en het bestaan per 31 december 2022 van interne beheersingsmaatregelen voor het waarborgen van de vertrouwelijkheid van de Suwinet-gegevens die worden verwerkt namens de gemeenten Beesel, Bergen, Gennep, Horst aan de Maas, Mook en Middelaar, Peel en Maas en Venray. Deze gemeenten worden in het rapport ten behoeve van de leesbaarheid aangeduid als “samenwerkende gemeenten”.

Wij hebben geen werkzaamheden uitgevoerd met betrekking tot de werking van interne beheersingsmaatregelen en brengen daarover geen oordeel tot uitdrukking.

1.2 Opdrachtomschrijving

Gemeente Venlo voert voor de samenwerkende gemeenten (onderdelen van) Suwi en/of niet Suwi-taken[1] uit. Voor deze dienstverlening wordt gebruik gemaakt van “Suwinet Inkijk” verder te noemen ‘uitbestede Suwi-taken’.

In onderstaande tabel is een samenvatting opgenomen van de Suwinetvoorziening en -diensten uitgevoerd door Gemeente Venlo:

Taak		Inkijk	Inlezen	DKD		Diensten
SUWI-taken						
Participatiewet		√				Uitvoering van de PW, IOAW, IOAZ en Bbz (aanvragen, onderhoud, verhaal, fraudeopsporing, incasso, bezwaar etc.)

Vanaf 2017 passen de gemeenten voor wie deze diensten worden verricht de Eenduidige Normatiek Single Information Audit (ENSIA) toe om invulling te geven aan een gestroomlijnde informatievoorziening over informatieveiligheid. De samenwerkende gemeenten moeten in het kader van ENSIA vaststellen dat aan alle Suwinet vereisten wordt voldaan. Dit kan op basis van de ontvangen assurance rapportages, verantwoordingsinformatie van samenwerkingspartijen en door de samenwerkende gemeenten in eigen beheer uitgevoerde werkzaamheden.

De samenwerkende gemeenten heeft Gemeente Venlo gevraagd door middel van een daarop gericht assurance-rapport aan te tonen dat de vertrouwelijkheid van de verwerkte Suwinet-gegevens wordt gewaarborgd en dat daarmee wordt voldaan aan de gerelateerde Suwinet norm-items voor wat betreft de aan Gemeente Venlo uitbestede Suwi-taken.

[1] Onder het begrip ‘SUWI-taken’ vallen taken die krachtens de wet SUWI, de Participatiewet, de IOAW en de IOAZ aan Colleges van B en W zijn opgedragen (zie de wet SUWI, artikel 62, lid 2)

1.3 Gebruik van deze rapportage

Het Ministerie van Sociale Zaken en Werkgelegenheid (verder: SZW) verwacht van gemeenten dat zij ook in het geval van uitbesteding en / of samenwerking met andere organisaties de bestuurlijke verantwoordelijkheid blijven nemen en daarover verantwoording afleggen. Voorliggende rapportage kan door de gemeenten worden gebruikt om invulling te geven aan deze verantwoordelijkheid.

De gemeente verzoekt - voorafgaand aan de invulling van het self-assessment - aan de serviceorganisatie om middels een assurance-rapport aan te tonen dat de interne beheersingsmaatregelen ter waarborging van de vertrouwelijkheid van de Suwinet-gegevens in opzet en bestaan voldoen aan de criteria. De gemeente neemt deze rapportage vervolgens bij de rapportering in ENSIA in aanmerking en past hierbij de 'carve-out' methodiek toe. Ten slotte stelt de gemeente deze rapportage ter beschikking aan haar ENSIA auditor en wel in het kader van de ENSIA audit werkzaamheden.

In bijlage A is een overzicht opgenomen van de getoetste interne beheersingsmaatregelen en de door ons vastgestelde bevindingen en aanbevelingen.

1.4 Eventueel zelfstandig gebruik van Suwinet gegevens door samenwerkende gemeenten

Indien de samenwerkende gemeenten naast de uitbestede Suwi-taken ook zelfstandig gebruik maken van Suwinet gegevens, zijn zij zelf verantwoordelijk voor het opzetten en implementeren van interne beheersingsmaatregelen ter waarborging van de vertrouwelijkheid van de Suwinet-gegevens. Voor het gebruik van Suwinet en de daarin opgenomen gegevens zijn wettelijke grondslagen vereist. Deze vallen onder de verantwoordelijkheid van de minister van SZW en overige betrokken ministers. Het eventuele zelfstandig gebruik van Suwinet gegevens door de samenwerkende gemeenten is niet in deze assurance-rapportage betrokken en dient door de IT-auditor(s) van de gemeenten te worden onderzocht.

1.5 Verantwoordelijkheden Gemeente Venlo

Gemeente Venlo is verantwoordelijk voor het opzetten en implementeren van interne beheersingsmaatregelen gericht op het waarborgen van de vertrouwelijkheid van Suwinet-gegevens die worden verwerkt voor de gemeente.

De beheersingsmaatregelen voor het veilige gebruik van Suwinet voorzieningen zijn daarbij leidend. De beheersingsmaatregelen zijn opgenomen in paragraaf 1.10. Indien sprake is van Suwinet-inlezen dan wel Suwinet-DKD, wordt van de serviceorganisatie verwacht dat de effectiviteit van de onderliggende General IT-Controls expliciet kan worden aangetoond.

1.6 Onze onafhankelijkheid en kwaliteitsbeheersing

Wij hebben de vereisten van het Reglement Gedragscode ('Code of Ethics') van NOREA nageleefd, welke is gebaseerd op de fundamentele beginselen van integriteit, objectiviteit, deskundigheid en zorgvuldigheid, geheimhouding en professioneel gedrag.

Ons kantoor past het Reglement Kwaliteitsbeheersing NOREA (RKBN) toe en bijgevolg onderhouden we een uitgebreid systeem van kwaliteitscontrole met inbegrip van gedocumenteerd beleid en de procedures met betrekking tot de naleving van de ethische voorschriften, professionele standaarden en de van toepassing zijnde wet- en regelgeving.

1.7 Verantwoordelijkheden van de auditor

We hebben onze opdracht uitgevoerd overeenkomstig Nederlands recht, waaronder NOREA Richtlijn 3000 'Richtlijn Assurance-opdrachten door IT-auditors'.

Onze verantwoordelijkheid is het zodanig plannen en uitvoeren van een assurance-opdracht, dat wij daarmee voldoende en geschikte assurance-informatie verkrijgen voor de door ons af te geven oordelen. Onze assurance-opdracht is uitgevoerd met een redelijke mate van zekerheid, dit betekent een hoge mate maar geen absolute mate van zekerheid waardoor het mogelijk is dat wij tijdens onze assurance-opdracht niet alle afwijkingen ontdekken.

De geselecteerde werkzaamheden zijn afhankelijk van de door de auditor van de organisatie toegepaste oordeelsvorming, met inbegrip van het inschatten van de risico's dat de geselecteerde norm-items niet op afdoende wijze zijn opgezet of niet bestaan. De werkzaamheden bestonden uit een combinatie van het kennisnemen van documentatie, het houden van interviews, het evalueren van de resultaten van de uitgevoerde interne controles en het verrichten van eigen (aanvullende) testwerkzaamheden.

Wij hebben geen werkzaamheden uitgevoerd met betrekking tot de werking van de geselecteerde beheersingsmaatregelen en brengen daarover geen oordeel tot uitdrukking.

Wij zijn van mening dat de door ons verkregen assurance-informatie voldoende en geschikt is om daarop een onderbouwing met een redelijke mate van zekerheid voor onze oordelen te bieden.

1.8 Gehanteerde criteria

Wij hebben bij de uitvoering van onze werkzaamheden gebruik gemaakt van een selectie van beheersingsmaatregelen (gezamenlijk verder aangeduid als ENSIA normenkader) die zijn beschreven in de *'Verantwoordingsrichtlijn Informatiebeveiliging GeVS 2020'* die is vastgesteld door het ketenoverleg van Gezamenlijke elektronische Voorziening Suwinet (GeVS), zoals bekrachtigd door het Ministerie van Sociale Zaken en Werkgelegenheid.

Daarnaast is gebruik gemaakt van de NOREA '*Handreiking ENSIA voor IT-auditors (RE's), versie 4.0 – Update Verantwoordingsjaar 2021, 15 oktober 2021'* (Guidance voor de IT-auditors die zich bezighouden met IT-audits betreffende de Eénduidige Normatiek Single Information Audit (ENSIA) voor gemeenten).

Wij achten deze selectie van beheersingsmaatregelen en de guidance relevant en toereikend voor ons onderzoek.

1.9 Beperkingen

Het 'ENSIA normenkader' is een selectie van beheersingsmaatregelen uit de BIO dat is vastgesteld door het ketenoverleg van de Gezamenlijke elektronische Voorziening Suwinet (GeVS). Wij kunnen niet uitsluiten dat, indien wij aanvullende beheersingsmaatregelen zouden hebben onderzocht wellicht andere onderwerpen zouden zijn geconstateerd die voor rapportering in aanmerking zouden zijn gekomen.

Bovendien is de projectie van oordelen naar de toekomst onderhevig aan het risico dat interne beheersingsmaatregelen bij een serviceorganisatie ineffectief kunnen worden.

1.10 Oordelen

Onze oordelen zijn gevormd op basis van de werkzaamheden zoals ze zijn beschreven in deze rapportage. Per beheersingsmaatregel van de 'Verantwoordingsrichtlijn Informatiebeveiliging GeVS 2020' wordt een oordeel gegeven over de opzet en het bestaan per 31 december 2022.

De criteria waarvan wij gebruik hebben gemaakt, zijn opgenomen in onderstaande tabel. Per beveiligingsrichtlijn hebben wij hieronder vermeld of met redelijke mate van zekerheid wordt voldaan aan de beveiligingsrichtlijn. Om de leesbaarheid van dit rapport te vergroten zijn de conclusies in deze tabel weergegeven als "voldoet" of "voldoet niet". Hierbij moet "voldoet" worden geïnterpreteerd als "Wij zijn van oordeel dat de interne beheersingsmaatregelen die verband houden met de op die regel opgenomen norm volgens de criteria genoemd in hoofdstuk 1.8 in alle materiële opzichten effectief zijn". "Voldoet niet" moet worden geïnterpreteerd als "Wij zijn van oordeel dat de interne beheersingsmaatregelen die verband houden met de op die regel aangegeven norm volgens de criteria genoemd in hoofdstuk 1.8 niet in alle materiële opzichten effectief zijn". De uitspraak voldoet of voldoet niet beperkt zich tot de eigen oordeelsvorming van de auditor.

BIO Control	Beheersingsmaatregel	Oordeel
5.1.1	Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.	Voldoet
5.1.2	Het beleid voor informatiebeveiliging behoort met geplande tussenpozen of als zich significante veranderingen voordoen, te worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.	Voldoet

BIO Control	Beheersingsmaatregel	Oordeel
6.1.1	Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.	Voldoet
6.1.2	Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.	Voldoet
7.2.2	Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.	Voldoet
9.2.1	Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	Voldoet niet
9.2.2	Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.	Voldoet
9.2.5	Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.	Voldoet niet
9.2.6	De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast.	Voldoet

BIO Control	Beheersingsmaatregel	Oordeel
10.1.1	Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersingsmaatregelen te worden ontwikkeld en geïmplementeerd.	Niet van toepassing
12.1.1	Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben.	Voldoet
12.4.1	Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.	Voldoet
12.4.2	Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.	Niet van toepassing
18.1.4	Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.	Voldoet

1.11 Beoogde gebruikers en doel

Onze schriftelijke rapportage is alleen bestemd voor de samenwerkende gemeenten, haar auditor(s), en het Ministerie van SZW en haar auditors, aangezien anderen, die niet op de hoogte zijn van de precieze reikwijdte, aard en doel van de werkzaamheden, de resultaten onjuist kunnen interpreteren. Het doel van de werkzaamheden betreft de gemaakte keuze voor carve-out van SUWI taken.

De rapportage, onderdelen of samenvattingen daarvan mogen niet mondeling of schriftelijk aan derden beschikbaar worden gesteld zonder onze voorafgaande schriftelijke toestemming.

Voor zover het Gemeente Venlo en de samenwerkende gemeenten is toegestaan het rapport aan derden beschikbaar te stellen, zal het rapport origineel, volledig en ongewijzigd beschikbaar worden gesteld. Indien de producten van onze werkzaamheden aan derden ter beschikking worden gesteld, dient erop te worden gewezen dat zonder onze uitdrukkelijke voorafgaande schriftelijke toestemming

geen rechten aan het product kunnen worden ontleend. Het verstrekken van deze toestemming kan omgeven zijn met nadere voorwaarden.

Hillegom, 22 februari 2023

27 Feb 2023 16:32 +0100
Hillegom

C.N.A. Beusenberg
QUALIFIED SIGNATURE

3angles B.V.
C.N.A. Beusenberg RE CISA

Bijlage A- Beschrijving van de testresultaten van de auditor

Deze bijlage is voor Gemeente Venlo bestemd.