Totaalrapportage informatiebeveiliging Gemeenschappelijke elektronische Voorziening Suwinet 2022

1. Managementsamenvatting

Dit jaar verschijnt de zesde Totaalrapportage sinds de invoering van de ENSIA-verantwoordingssystematiek door de gemeenten. De Totaalrapportage gaat over de beveiliging van het gebruik van de Gemeenschappelijke elektronische Voorziening Suwinet (hierna GeVS). Met een respons van ruim 99%[1] bij gemeenten en 86%[2] bij andere afnemers is de rapportage representatief. De door een IT-auditor opgestelde assurancerapporten, die onderdeel uitmaken van de transparantierapportage[3], vormen garanties voor de juistheid van de bevindingen.

De Totaalrapportage is een getrouwe afspiegeling, omdat 345 van de 348 partijen[4] die van Suwinet-gebruik maakten en zich moesten verantwoorden, een bruikbare verantwoording hebben aangeleverd.

Net zoals voorgaand jaar, is er sprake van 14 normen waarop gecontroleerd wordt. Deze normen zijn inhoudelijk hetzelfde als in verantwoordingsjaar 2020 en 2021. Ruim driekwart (78,6%[5]) van de gemeenten voldoet in opzet en bestaan aan alle gecontroleerde beveiligingsnormen (in 2021 71,6%). Gemeenten die niet voldoen aan een of meer normen zijn aangeschreven conform het Interventieprotocol Suwinet-ENSIA.

Bij de andere afnemers, het gaat dan om UWV, SVB, DUO, CAK, IND, Dienst Justis en de Nederlandse Arbeidsinspectie, waren er geen partijen zonder bevindingen op opzet, bestaan en werking.[6] Hierbij

[1] Alle gemeenten die dit jaar verantwoording hebben afgelegd hebben dat volledig en duidelijk gedaan.
[2] Zes van de zeven partijen hebben verantwoording afgelegd. Van een van die zes is het transparantierapport nog niet volledig.
[3] Zie voor meer informatie: https://www.bkwi.nl/producten/suwinet-services/suwinet-standaarden/privacy-beveiliging/verantwoordingsrichtlijn-gevs-2022-v1-0/
[4] Op 1 januari 2022 waren er 345 gemeenten. 4 gemeenten hebben over 2022 geen verantwoordingsverplichting vanwege een herindeling in 2023, daarnaast is er 1 gemeente nieuw ontstaan. 341 Gemeenten hebben over 2022 dus een verantwoordingsverplichting. Daarvan hebben 2 gemeenten geen verantwoording afgelegd. Daarnaast hadden 7 andere afnemers een verantwoordingsverplichting te weten; UWV, SVB, DUO, CAK, IND, Dienst Justis en de Nederlandse Arbeidsinspectie. Een van deze partijen heeft geen verantwoording afgelegd.
[5] Aantal gemeenten met nul bevindingen, gedeeld door het aantal gemeenten dat zich moest verantwoorden (over 3 gemeenten bestaat discussie over de trede, deze is buiten de telling gehouden).
[6] 0% van 7 afnemers die een bruikbare verantwoording hebben ingeleverd voldoen aan alle gecontroleerde beveiligingsnormen.

merken we op dat één partij niet heeft aangeleverd. Over verantwoordingsjaar 2021 waren er twee partijen die een rapportage zonder bevindingen hebben aangeleverd. Van één van deze partijen is in de loop van 2023 geconstateerd dat de rapportage niet juist bleek.

Het aantal meldingen van onrechtmatig gebruik van Suwinet bij gemeenten is gedaald van 2 naar 0.

De cijfers bij gemeenten zijn min of meer stabiel gebleven ten opzichte van het voorgaande jaar. Hierbij betreft het een verantwoording over opzet en bestaan. Bij niet-gemeentelijke afnemers is daarnaast ook gekeken naar werking. Bij deze andere afnemers is een zorgwekkende stijging van bevindingen terug te zien, waarbij de rapportage van één partij ontbreekt.

De Domeingroep Privacy & Beveiliging stelt een aparte notitie op voor het Ketenoverleg. In die notitie staan conclusies en aanbevelingen bij deze Totaalrapportage.

2. Inleiding

Deze rapportage bevat een overzicht van de stand van de beveiliging van de GeVS in 2022 bij 341[7] gemeenten en 7 andere afnemers[8]. BKWI stelt deze rapportage samen op verzoek van het Ministerie van Sociale Zaken en Werkgelegenheid. De partijen vertegenwoordigd in het Ketenoverleg bieden de rapportage aan.

Gemeenten leggen verantwoording af over de beveiliging volgens de ENSIA-systematiek[9]. Deze verantwoording is primair gericht aan de gemeenteraad als horizontale toezichthouder, maar het gedeelte dat betrekking heeft op de GeVS wordt, voorzien van een assurancerapport van een IT-auditor, ook doorgestuurd aan BKWI. Andere afnemers leggen verantwoording af via een in-control-verklaring van de bestuurder. Op basis van de verantwoordingsdocumenten stelt het BKWI deze totaalrapportage op. Deze rapportage wordt met de eerdergenoemde conclusies en aanbevelingen van de domeingroep en een bestuurlijke reactie door de partijen in het Ketenoverleg naar de minister van SZW verstuurd.

3. Scope van de rapportage

De rapportage heeft betrekking op de informatiebeveiliging bij de gebruikers (afnemers) van Suwinet. Er dienden 341 gemeenten en 7 andere afnemers verantwoording af te leggen over 2022.

Met ingang van verantwoordingsjaar 2020 is de Baseline Informatiebeveiliging Overheid (BIO) voor alle partijen het uitgangspunt voor de rapportage. Daardoor is de Totaalrapportage uniformer

[7] Er zijn 345 gemeenten in 2022, maar 4 gemeenten hoeven geen verantwoording af te leggen in verband met een herindeling in 2022.
[8] Bronnen en beheerders leggen geen verantwoording af. Dat is vastgelegd in de Verantwoordingsrichtlijn.
[9] Zie www.ensia.nl.

geworden. Alle afnemers verantwoorden zich volgens de Verantwoordingsrichtlijn 2022. Gemeenten en andere afnemers leggen verantwoording af over de normen in tabel 1.

Tabel 1: De 14 beveiligingsnormen BIO voor Suwinet

Norm	Onderwerp
5.1.1	Beleidsregels voor informatiebeveiliging
5.1.2	Beoordeling van het informatiebeveiligingsbeleid
6.1.1	Rollen en verantwoordelijkheden bij informatiebeveiliging
6.1.2	Scheiding van taken
7.2.2	Bewustzijn, opleiding en training ten aanzien van de informatiebeveiliging
9.2.1	Registratie en afmelden van gebruikers
9.2.2	Gebruikers toegang verlenen
9.2.5	Beoordeling van toegangsrechten van gebruikers
9.2.6	Toegangsrechten intrekken of aanpassen
10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen
12.1.1	Gedocumenteerde bedieningsprocedures
12.4.1	Gebeurtenissen registreren
12.4.2	Beschermen van informatie in logbestanden
18.1.4	Privacy en bescherming van persoonsgegevens

Gemeenten verantwoorden zich alleen over opzet en bestaan van de informatiebeveiligingsmaatregelen, de andere afnemers verantwoorden zich ook over de werking daarvan. Er is op dit moment overleg tussen BZK, SZW en VNG over de termijn waarop de gemeenten zich ook over werking gaan verantwoorden.

Onderwerp van de verantwoording is – voor alle afnemers - het veilige gebruik van Suwinet Inkijk, Suwinet Inlezen en/of DKD Inlezen.

Gemeenten gebruiken Suwinet voor SUWI-taken en niet-SUWI-taken. Bij de SUWI-taken gaat het dan om de uitvoering van de Participatiewet, de IOAW en de IOAZ. Bij niet-SUWI-taken gaat het om het gebruik van Suwinet voor RMC[10]-taken, beslaglegging door een gemeentelijke belastingdeurwaarder of adresonderzoek door een afdeling Burgerzaken.

[10] RMC: Regionale Meld- en Coördinatiefunctie voortijdig schoolverlaters

De verhouding van het aantal raadplegingen door gemeenten voor SUWI-taken ten opzichte van niet-SUWI-taken is ongeveer 97:3.

Andere afnemers gebruiken Suwinet alleen voor taken die wettelijk zijn vastgesteld in relevante wetgeving als bijvoorbeeld de Zorgverzekeringswet of Vreemdelingenwet.

4. Voor wie is deze rapportage bestemd?

De Totaalrapportage wordt opgesteld op verzoek van het ministerie van SZW en vastgesteld door het ketenoverleg. Vervolgens wordt de rapportage aangeboden aan de minister van SZW en gedeeld met de Kamer.

5. Wat is het doel van deze rapportage?

Volgens Bijlage I, paragraaf 2.3 van de Regeling SUWI bepalen de SUWI-partijen “één gezamenlijk, transparant en uniform niveau van betrouwbaarheid in termen van beschikbaarheid, integriteit en vertrouwelijkheid” dat wordt vastgelegd in een verantwoordingsrichtlijn.

Die verantwoording is als volgt geregeld:

- Individuele afnemers stellen een transparantierapportage op en richten die aan BKWI
- BKWI maakt op basis hiervan een Totaalrapportage voor het Ketenoverleg en de minister van Sociale Zaken en Werkgelegenheid

De Totaalrapportage geeft een samenvattend beeld van alle ontvangen transparantierapportages van gemeenten en een samenvattend beeld van de rapportages van andere afnemers. De Totaalrapportage beschrijft de feitelijke stand van zaken van de informatiebeveiliging van de GeVS. De rapportage over de bevindingen is geaggregeerd. Bevindingen zijn dus niet te herleiden tot individuele organisaties.

Het verkregen overzicht dient voor de ketenpartijen om het gezamenlijk gerealiseerde niveau van beveiliging te analyseren en waar nodig ondersteunende verbetermaatregelen te nemen.

De Domeingroep Privacy & Beveiliging voorziet de Totaalrapportage van conclusies en aanbevelingen, voordat die aan het Ketenoverleg wordt voorgelegd.

UWV, SVB en VNG formuleren hierop namens het Ketenoverleg een reactie en besluiten gezamenlijk over die conclusies en aanbevelingen. Het geheel wordt door de voorzitter van het Ketenoverleg aangeboden aan de minister van SZW.

De rapportage stelt de Minister van SZW in gelegenheid te interveniëren als blijkt dat de voortgang van individuele gemeenten bij het nemen van verbetermaatregelen onvoldoende is. Dit doet het

ministerie op basis van het Interventieprotocol Suwinet ENSIA 2018. Bij de SUWI-partijen worden eventuele bevindingen besproken in de planning en control cyclus.

6. Hoe is deze rapportage tot stand gekomen?

Voor gemeenten

Voor gemeenten is met ingang van 2017 een nieuwe verantwoordingssystematiek ingevoerd met de naam ENSIA[11], wat staat voor Eenduidige Normatiek Single Information Audit.

Volgens deze systematiek evalueren gemeenten hun informatiebeveiliging met behulp van een vragenlijst, die gebaseerd is op de BIO. Burgemeester en wethouders stellen op basis van een deel van de vragen een in-control-verklaring op, de “collegeverklaring”, die wordt voorzien van een assurancerapport van een IT-auditor[12]. De in-control-verklaring bevat een bijlage, waarin eventuele bevindingen (‘bevindingen”) van de getoetste beveiligingsnormen worden gespecificeerd.

Deze stukken zijn in eerste instantie bedoeld voor horizontale verantwoording aan de gemeenteraad, maar geven ook inzicht in de toepassing van 14 normen uit BIO. Dat maakt ze geschikt voor verticale[13] verantwoording aan de minister van SZW.

Gemeenten hebben zich in 2023 via ENSIA over het verantwoordingsjaar 2022 verantwoord over SUWI-taken (taken die worden uitgevoerd in het kader van de Participatiewet) en niet-SUWI-taken (gebruik van Suwinet voor RMC-taken[14], burgerzaken en belastingdeurwaarders).

Gemeenten dienden de stukken uiterlijk op 1 mei aan te leveren. Twee van de 341 verantwoordingsplichtige gemeenten hebben tot op heden geen verantwoording aangeleverd. Deze gemeenten zijn gemeld bij het ministerie van SZW en zullen door SZW worden benaderd. Ter vergelijking: vorig jaar ontbraken er ook twee verantwoordingen.
Ook de gemeenten die twee jaar achter elkaar of langer bevindingen hebben gemeld, zullen door het ministerie worden benaderd conform het Interventieprotocol.

Voor andere afnemers

Voor de 7 andere afnemers geldt in grote lijnen dezelfde procedure: bestuurders dienen een in-control-verklaring te overleggen, waarin bevindingen per norm zijn opgenomen, met daarbij een assurancerapport.

[11] Voor meer informatie: www.ensia.nl.
[12] De IT-auditor moet tot de NOREA zijn toegelaten (zie Regeling Suwi, artikel 5.22)
[13] Een van de doelen van ENSIA is namelijk om horizontale en verticale verantwoording te combineren en daarmee de verantwoordingslast voor gemeenten zoveel mogelijk te beperken.
[14] Regionale Meld- en Coördinatiefunctie voortijdig schoolverlaters

Zes van de zeven afnemers hebben verantwoording afgelegd en al deze verantwoordingen zijn bruikbaar.

Het uitgangspunt wordt gehanteerd dat aan eventuele bevindingen bij deze afnemers aandacht besteed zal worden in de bij de afnemer gebruikelijke planning & control-cyclus.

Geen weging en interpretatie

BKWI past geen weging toe op de informatie die afnemers aanleveren. De informatie die afnemers aanleveren over de normnaleving wordt één op één overgenomen en BKWI houdt bij het opstellen van deze rapportage ook geen rekening met eventuele interpretatieverschillen van de normen. Om de bruikbaarheid van de rapportage te garanderen wordt een onduidelijke of onvolledige verantwoording[15] van een afnemer niet verwerkt.

Betrouwbaarheid van de Totaalrapportage

Om betrouwbaar te zijn moet de rapportage representatief zijn en moeten de gemelde bevindingen juist zijn. Met een respons van ruim 99%[16] bij gemeenten en 86% bij andere afnemers is de rapportage representatief. De door een IT-auditor opgestelde assurancerapporten, die onderdeel uitmaken van de transparantierapportages, vormen garanties voor de juistheid van de bevindingen.

[15] Dit kan een individuele rapportage betreffen waarbij geen gebruik is gemaakt van voorgeschreven templates of waarbij verplicht aan te leveren stukken ontbreken.
[16] Dit is inclusief gemeenten die een onvolledige of onduidelijke verantwoording hebben afgelegd.

7. Wat is de stand van de informatiebeveiliging bij de afnemers?

Aantallen bevindingen op SUWI-taken per gemeente 2020-2022

Tabel 2 geeft aan hoeveel gemeenten géén bevindingen hebben gerapporteerd bij de uitvoering van SUWI-taken en bij hoeveel gemeenten er 1, 2, 3 of meer bevindingen waren in 2022 en de verantwoordingsjaren 2021 en 2020.

Tabel 2: aantal en percentage bevindingen SUWI-taken 2022, 2021 en 2020 (BIO-normen)

	2022		2021		2020	
Aantal bevindingen	**# Gemeenten**	**%**	**# Gemeenten**	**%**	**# Gemeenten**	**%**
0	268	78,6%	245	71,6%	243	69,2%
1	19	5,6%	25	7,3%	36	10,3%
2	12	3,5%	28	8,2%	23	6,5%
3	12	3,5%	9	2,6%	7	2,0%
4 of meer	28	8,2 %	29	8,5%	32	9,1%
Verantwoording ontbreekt/onduidelijk	2	0,6%	6	1,7%	10	2,8%
Totaal	341	100%	342	100%	355	100%

Aantallen bevindingen van normen bij andere afnemers in 2022, 2021 en 2020

In tabel 3 staat hoeveel andere afnemers geen bevindingen hebben geconstateerd en hoeveel afnemers er 1,2,3,4 of meer bevindingen hebben geconstateerd over verantwoordingsjaren 2022, 2021 en 2020.

Tabel 3: aantal en percentage bevindingen 2022, 2021 en 2020

	2022		2021		2020	
Aantal bevindingen	**# Afnemers**	**%**	**# Afnemers**	**%**	**# Afnemers**	**%**
0	0	0%	2	28,6%	2	33,3%
1	1	14,3%	1	14,3%	1	16,6%
2	0	0%	1	14,3%		
3	0	0%	1	14,3%	1	16,6%
4 of meer	5	71,4%	2	28,6%	1	16,6%
Verantwoording ontbreekt/onduidelijk	1	14,3%	0	0%	1	16,6%
Totaal	7	100%	7	100%	6	100%

Bevindingen van normen bij gemeenten

Tabel 4 geeft per norm aan hoe vaak daarvan afgeweken is bij het gebruik van de GeVS voor SUWI-taken en de drie niet-SUWI-taken. Hierbij wordt opgemerkt dat een beperkt aantal gemeenten gebruik maakt van Suwinet voor niet-SUWI-taken.

Tabel 4: afwijking per norm bij gemeenten per taak in verantwoordingsjaar 2022

Norm	Suwi-taken[17]	BZ[18]	GBD[19]	RMC[20]	Omschrijving norm
5.1.1	17	6			Beleidsregels voor informatiebeveiliging
5.1.2	17	5		1	Beoordeling van het informatiebeveiligingsbeleid
6.1.1	28	11		1	Rollen en verantwoordelijkheden bij informatiebeveiliging
6.1.2	18	7			Scheiding van taken
7.2.2	26	15	3	1	Bewustzijn, opleiding en training ten aanzien van de informatiebeveiliging
9.2.1	28	13	3	2	Registratie en afmelden van gebruikers
9.2.2	24	10	3	1	Gebruikers toegang verlenen
9.2.5	34	12		1	Beoordeling van toegangsrechten van gebruikers
9.2.6	26	11	3	1	Toegangsrechten intrekken of aanpassen
10.1.1	19				Beleid inzake het gebruik van cryptografische beheersmaatregelen
12.1.1	11	5		1	Gedocumenteerde bedieningsprocedures
12.4.1	39	18		1	Gebeurtenissen registreren
12.4.2	11	2			Beschermen van informatie in logbestanden
18.1.4	36	16	3		Privacy en bescherming van persoonsgegevens
Totaal	334	131	15	10	

Op basis van een vergelijking met de gebruikersadministratie constateren we dat sommige gemeenten verantwoording afleggen over Suwi- en niet-Suwitaken terwijl ze geen aansluiting hebben. We constateren ook dat sommige gemeenten geen verantwoording afleggen over Suwi- en niet-Suwitaken terwijl ze wel een aansluiting hadden. In totaal betreft dit zo'n 90 gemeenten.

Bevindingen van normen bij andere afnemers

Onderstaande tabel geeft per norm aan hoe vaak daarvan afgeweken is bij het gebruik van de GeVS voor taken van andere afnemers.

[17] Het gaat hier om de uitvoering van de Participatiewet. Deeltaken, zoals de toetsing van aanvragen en sociale recherche, zijn soms bij verschillende organisaties belegd.
[18] BZ staat voor Afdelingen Burgerzaken. Zij gebruiken Suwinet ook voor niet-SUWI-taken.
[19] BD staat voor Gemeentelijke Belastingdeurwaarders. Zij gebruiken Suwinet ook voor niet-SUWI-taken.
[20] RMC staat voor Regionale Meld- en Coördinatiepunten voortijdige schoolverlaters. Zij gebruiken Suwinet voor taken die niet in de SUWI-wetgeving zijn geregeld. Dat wordt in deze context een niet-SUWI-taak genoemd.

Tabel 5: afwijking per norm bij andere afnemers in verantwoordingsjaar 2022, 2021 en 2020[21]

Norm	2022	2021	2020	Omschrijving norm
5.1.1	1	0	2	Beleidsregels voor informatiebeveiliging
5.1.2	1	1	1	Beoordeling van het informatiebeveiligingsbeleid
6.1.1	2	1	1	Rollen en verantwoordelijkheden bij informatiebeveiliging
6.1.2	4	3	1	Scheiding van taken
7.2.2	3	3	1	Bewustzijn, opleiding en training ten aanzien van de informatiebeveiliging
9.2.1	3	2	1	Registratie en afmelden van gebruikers
9.2.2	5	2	1	Gebruikers toegang verlenen
9.2.5	5	4	1	Beoordeling van toegangsrechten van gebruikers
9.2.6	5	2	1	Toegangsrechten intrekken of aanpassen
10.1.1	2	1	1	Beleid inzake het gebruik van cryptografische beheersmaatregelen
12.1.1	2	1	1	Gedocumenteerde bedieningsprocedures
12.4.1	4	2	3	Gebeurtenissen registreren
12.4.2	2	1	1	Beschermen van informatie in logbestanden
18.1.4	4	2	2	Privacy en bescherming van persoonsgegevens
Totaal	**43**	25	18	

Onrechtmatig gebruik Suwinet bij gemeenten

Voor het gebruik van de via Suwinet ontsloten gegevens is een wettelijke grondslag noodzakelijk. Voor de hierboven beschreven SUWI- en niet-SUWI-taken is die er ook. In tabel 6 staat het verloop van het aantal gemeenten dat heeft gemeld dat Suwinet ook gebruikt wordt voor taken waarvoor geen wettelijke grondslag bestaat. Het gaat daarbij vooral om de inzet van Suwinet bij taken rondom schuldhulpverlening en jeugdzorg.

Tabel 6: verloop aantal meldingen gebruik Suwinet zonder wettelijke grondslag

2022	2021	2020	2019	2018
0	**2**	**6**	**1**	**13**

[21] Deze afwijkingen hebben alleen betrekking op de ingediende verantwoordingen