BUREAU
KETENINFORMATISERING
WERK EN INKOMEN

Totaalrapportage informatiebeveiliging Gemeenschappelijke elektronische Voorziening Suwinet 2023

1. Managementsamenvatting

Voorliggend document betreft de zevende Totaalrapportage sinds de invoering van de ENSIA-verantwoordingssystematiek door de gemeenten. De Totaalrapportage geeft inzicht in de beveiliging van het gebruik van de Gemeenschappelijke elektronische Voorziening Suwi (hierna GeVS) op basis van transparantierapportages die zijn aangeleverd door de afnemers. De door een IT-auditor opgestelde assurancerapporten, die onderdeel uitmaken van de transparantierapportage[1], vormen garanties voor de juistheid van de bevindingen.

De Totaalrapportage is een getrouwe afspiegeling, omdat alle 349 partijen[2] die in 2023 van Suwinet-gebruik maakten en zich moesten verantwoorden een bruikbare verantwoording hebben aangeleverd. Bij 86 gemeenten bleek tijdens de verwerking van de transparantierapportages dat verantwoording over specifieke taken ontbrak (49x) of juist een overbodige verantwoording werd gedaan (37x). Deze gebreken zijn niet cijfermatig verwerkt in de Totaalrapportage.

Net zoals voorgaand jaar, is er sprake van 14 normen waarop gecontroleerd wordt. Deze normen zijn inhoudelijk hetzelfde als in de verantwoordingsjaren 2020, 2021 en 2022.

- De gemeenten scoren iets minder goed dan vorig jaar. Ruim driekwart (76,0%[3]) van de gemeenten voldoet in opzet en bestaan aan alle gecontroleerde beveiligingsnormen (in 2022 78,6%). Gemeenten die niet voldoen aan één of meer normen zijn aangeschreven conform het Interventieprotocol GeVS / Suwinet[4].
- Bij de zeven andere afnemers, het gaat dan om UWV, SVB, DUO, CAK, IND, Dienst Justis en de Nederlandse Arbeidsinspectie, waren er net als in 2022 geen partijen zonder bevindingen op opzet, bestaan en werking. Bij de andere afnemers is er bovendien sprake van een verslechtering in het totaal aantal bevindingen.

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

[1] Zie voor meer informatie: https://bkwi.nl/standaarden/privacy-beveiliging/verantwoordingsrichtlijn-gevs-2022-v10
[2] Op 1 januari 2023 waren er 342 gemeenten. Er waren in 2023 geen herindelingen, dus alle 342 gemeenten hebben een verantwoordingsplicht. Daarnaast hadden 7 andere afnemers een verantwoordingsverplichting te weten; UWV, SVB, DUO, CAK, IND, Dienst Justis en de Nederlandse Arbeidsinspectie.
[3] Aantal gemeenten met nul bevindingen, gedeeld door het aantal gemeenten dat zich moest verantwoorden.
[4] https://bkwi.nl/standaarden/privacy-beveiliging/interventieprotocol-gevs-suwinet

BUREAU
KETENINFORMATISERING
WERK EN INKOMEN

2. Inleiding

Deze rapportage bevat een overzicht van de stand van de beveiliging van de GeVS in 2023 bij 342[5] gemeenten en zeven andere afnemers[6]. Bronnen en beheerders leggen geen verantwoording af. Dat is vastgelegd in de Verantwoordingsrichtlijn. 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 Tweede Kamer.

Gemeenten leggen verantwoording af over de beveiliging volgens de ENSIA-systematiek[7]. Deze verantwoording is primair gericht aan de gemeenteraad als horizontale toezichthouder. Het gedeelte dat betrekking heeft op de GeVS wordt, in de vorm van de zogenoemde Collegeverklaring en een assurancerapport van een IT-auditor, ook doorgestuurd aan BKWI. Andere afnemers sturen aan BKWI een in-control-verklaring van de bestuurder en een assurancerapport van een IT-auditor. 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 342 gemeenten en 7 andere afnemers verantwoording af te leggen over 2023.

Met ingang van verantwoordingsjaar 2020 is de Baseline Informatiebeveiliging Overheid (BIO) voor alle partijen het uitgangspunt voor de rapportage. Daardoor is de Totaalrapportage uniformer geworden. Alle afnemers verantwoorden zich volgens de Verantwoordingsrichtlijn 2022[8]. Gemeenten en andere afnemers leggen verantwoording af over de normen in tabel 1.

[5] Er zijn 342 gemeenten in 2023, er hebben geen herindelingen plaatsgevonden in 2023, dus al deze gemeenten moeten zich verantwoorden.
[6] De zeven andere afnemers: UWV, SVB, CAK, IND, DUO, Justis en de Nederlandse Arbeidsinspectie
[7] Zie www.ensia.nl.
[8] Er is in 2023 geen nieuwe verantwoordingsrichtlijn uitgekomen, afnemers verantwoorden zich daarom conform de Verantwoordingsrichtlijn 2022.

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 de werking van de maatregelen 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 Doorstroompunt[9]-taken, Wet gemeentelijke schuldhulpverlening, beslaglegging door een gemeentelijke belastingdeurwaarder of adresonderzoek door een afdeling Burgerzaken.

[9] Doorstroompunt: Voorheen Regionale Meld- en Coördinatiefunctie voortijdig schoolverlaters (RMC)

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 zoals bijvoorbeeld de Zorgverzekeringswet of Vreemdelingenwet.

4. 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.

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

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

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 de gelegenheid te interveniëren als blijkt dat de voortgang van individuele afnemers bij het nemen van verbetermaatregelen onvoldoende is. Dit doet het Ministerie op basis van het Interventieprotocol GeVS / Suwinet.

5. Hoe is deze rapportage tot stand gekomen?

Voor gemeenten

Voor gemeenten is met ingang van 2017 een verantwoordingssystematiek ingevoerd met de naam ENSIA[10], wat staat voor Eenduidige Normatiek Single Information Audit.

[10] Voor meer informatie: www.ensia.nl.

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[11]. 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[12] verantwoording aan de Minister van SZW.

Gemeenten hebben zich in 2024 via ENSIA over het verantwoordingsjaar 2023 verantwoord over SUWI-taken (taken die worden uitgevoerd in het kader van de Participatiewet, IOAW en IOAZ) en niet-SUWI-taken (gebruik van Suwinet voor Doorstroompunt-taken[13], burgerzaken en belastingdeurwaarders).

Gemeenten dienden de stukken uiterlijk op 1 mei aan te leveren. In een aantal gevallen hebben gemeenten in overleg hun stukken na die datum geleverd of gecorrigeerd. Alle 342 verantwoordingsplichtige gemeenten hebben verantwoording aangeleverd.

Voor andere afnemers

Voor de zeven 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.

Alle zeven afnemers hebben verantwoording afgelegd en al deze verantwoordingen zijn bruikbaar.

Het Ministerie van SZW benadert de gemeenten en de andere afnemers die twee jaar achter elkaar of langer bevindingen hebben gemeld, conform het Interventieprotocol.

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. Om de bruikbaarheid van de rapportage te garanderen wordt een onduidelijke of onvolledige verantwoording[14] van een afnemer niet verwerkt. Dit is niet van toepassing op de verantwoording over 2023.

Betrouwbaarheid van de Totaalrapportage

Om betrouwbaar te zijn moet de rapportage representatief zijn en moeten de gemelde bevindingen juist zijn. Met een respons van 100% bij gemeenten en 100% bij andere afnemers is de rapportage

[11] De IT-auditor moet tot de NOREA zijn toegelaten (zie Regeling Suwi, artikel 5.22)
[12] 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.
[13] Doorstroompunt: Voorheen Regionale Meld- en Coördinatiefunctie voortijdig schoolverlaters (RMC)
[14] Dit kan een individuele rapportage betreffen waarbij geen gebruik is gemaakt van voorgeschreven templates of waarbij verplicht aan te leveren stukken ontbreken.

representatief. De door een IT-auditor opgestelde assurancerapporten, die onderdeel uitmaken van de transparantierapportages, vormen garanties voor de juistheid en volledigheid van de bevindingen.

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

Aantallen bevindingen op SUWI-taken per gemeente 2021-2023

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 normen met bevindingen waren in de verantwoordingsjaren 2023, 2022 en 2021.

Tabel 2: aantal en percentage bevindingen SUWI-taken 2023, 2022 en 2021 (BIO-normen)

	2023		2022		2021	
Aantal bevindingen	**# Gemeenten**	**%**	**# Gemeenten**	**%**	**# Gemeenten**	**%**
0	260	76,0%	268	78,6%	245	71,6%
1	28	8,2%	19	5,6%	25	7,3%
2	10	2,9%	12	3,5%	28	8,2%
3	4	1,2%	12	3,5%	9	2,6%
4 of meer	40	11,7 %	28	8,2 %	29	8,5%
Verantwoording ontbreekt/onduidelijk	0	0,0%	2	0,6%	6	1,7%
Totaal	342	100%	341	100%	342	100%

Aantallen bevindingen van normen bij andere afnemers in 2023, 2022 en 2021

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 2023, 2022 en 2021.

Tabel 3: aantal en percentage bevindingen 2023, 2022 en 2021

	2023		2022		2021	
Aantal bevindingen	**# Afnemers**	**%**	**# Afnemers**	**%**	**# Afnemers**	**%**
0	0	0%	0	0%	2	28,6%
1	1	14,3%	1	14,3%	1	14,3%
2	0	0%	0	0%	1	14,3%
3	0	0%	0	0%	1	14,3%
4 of meer	6	85,7%	5	71,4%	2	28,6%
Verantwoording ontbreekt/onduidelijk	0	0,0%	1	14,3%	0	0%
Totaal	7	100%	7	100%	7	100%

BUREAU
KETENINFORMATISERING
WERK EN INKOMEN

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 2023

Norm	Suwi-taken[15]	BZ[16]	GBD[17]	RMC[18]	WGS[19]	Omschrijving norm
5.1.1	13	3			9	Beleidsregels voor informatiebeveiliging
5.1.2	12	3			7	Beoordeling van het informatiebeveiligingsbeleid
6.1.1	37	15	1		24	Rollen en verantwoordelijkheden bij informatiebeveiliging
6.1.2	16	13	1		9	Scheiding van taken
7.2.2	39	17	1	2	15	Bewustzijn, opleiding en training ten aanzien van de informatiebeveiliging
9.2.1	22	10	1	1	12	Registratie en afmelden van gebruikers
9.2.2	21	17	1		14	Gebruikers toegang verlenen
9.2.5	46	20	1	2	30	Beoordeling van toegangsrechten van gebruikers
9.2.6	26	11	1		15	Toegangsrechten intrekken of aanpassen
10.1.1	21				6	Beleid inzake het gebruik van cryptografische beheersmaatregelen
12.1.1	20	3	1		8	Gedocumenteerde bedieningsprocedures
12.4.1	43	22	1		28	Gebeurtenissen registreren
12.4.2	12				5	Beschermen van informatie in logbestanden
18.1.4	37	18	1		24	Privacy en bescherming van persoonsgegevens
Totaal[20]	365	152	10	5	206	

Ontbrekende- en overbodige verantwoording over taken

Op basis van een vergelijking met de gebruikersadministratie constateert BKWI dat sommige gemeenten verantwoording afleggen over Suwi- en niet-Suwitaken terwijl ze geen aansluiting hebben. BKWI

[15] Het gaat hier om de uitvoering van de Participatiewet, IOAW en IOAZ. Deeltaken, zoals de toetsing van aanvragen en sociale recherche, zijn soms bij verschillende organisaties belegd.
[16] BZ staat voor Afdelingen Burgerzaken. Zij gebruiken Suwinet ook voor niet-SUWI-taken.
[17] BD staat voor Gemeentelijke Belastingdeurwaarders. Zij gebruiken Suwinet ook voor niet-SUWI-taken.
[18] 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.
[19] WGS staat voor Wet Gemeentelijke Schuldhulpverlening.
[20] Aantal aansluitingen per taak (niet elke gemeente heeft een eigen aansluiting, in een aantal gevallen werkt men samen via een samenwerkingsverband en deelt men de aansluiting. De gemeente blijft wel verantwoordelijk): GSD 255, Burgerzaken 178, GBD 1, RMC 34, DKD Inlezen 211, WGS 120

constateert ook dat sommige gemeenten geen verantwoording afleggen over Suwi- en niet-Suwitaken terwijl ze wel een aansluiting hadden. In totaal betreft dit 86 gemeenten (in 2022 was dit in totaal 90). Van deze 86 betrof het 49x een ontbrekende verantwoording en 37x een overbodige verantwoording. Dit laatste heeft veelal te maken hebben met het opzeggen van een aansluiting in de loop van het jaar. Deze gebreken zijn niet cijfermatig verwerkt in de Totaalrapportage.

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. Er is vergeleken met 2021 een ruime verdubbeling te zien in het aantal bevindingen. Dit is deels, maar niet in geheel te verklaren door het compleet zijn van de verantwoording.

Tabel 5: afwijking per norm bij andere afnemers in verantwoordingsjaar 2023, 2022 en 2021[21]

Norm	2023	2022	2021	Omschrijving norm
5.1.1	1	1	0	Beleidsregels voor informatiebeveiliging
5.1.2	2	1	1	Beoordeling van het informatiebeveiligingsbeleid
6.1.1	2	2	1	Rollen en verantwoordelijkheden bij informatiebeveiliging
6.1.2	4	4	3	Scheiding van taken
7.2.2	3	3	3	Bewustzijn, opleiding en training ten aanzien van de informatiebeveiliging
9.2.1	4	3	2	Registratie en afmelden van gebruikers
9.2.2	6	5	2	Gebruikers toegang verlenen
9.2.5	6	5	4	Beoordeling van toegangsrechten van gebruikers
9.2.6	5	5	2	Toegangsrechten intrekken of aanpassen
10.1.1	2	2	1	Beleid inzake het gebruik van cryptografische beheersmaatregelen
12.1.1	4	2	1	Gedocumenteerde bedieningsprocedures
12.4.1	6	4	2	Gebeurtenissen registreren
12.4.2	2	2	1	Beschermen van informatie in logbestanden
18.1.4	6	4	2	Privacy en bescherming van persoonsgegevens
Totaal	**53**	**43**	**25**	

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

BUREAU
KETENINFORMATISERING
WERK EN INKOMEN