Totaalrapportage informatiebeveiliging Gemeenschappelijke elektronische Voorziening Suwinet 2021

1. Managementsamenvatting

Dit jaar verschijnt de vijfde Totaalrapportage sinds de invoering van de ENSIA-verantwoordingssystematiek door de gemeenten. De Totaalrapportage gaat over de informatiebeveiliging van het gebruik van de Gemeenschappelijke elektronische Voorziening Suwinet (hierna GeVS). Met een respons van ruim 99%[1] bij gemeenten en 100%[2] bij andere afnemers is de rapportage representatief. De door een EDP-auditor opgestelde assurance-rapporten, die onderdeel uitmaken van de transparantierapportage, garanderen de juistheid van de bevindingen.

De Totaalrapportage is betrouwbaar, omdat 343 van de 359 partijen[3] die van Suwinet-gebruik maakten en zich moesten verantwoorden, een bruikbare verantwoording hebben aangeleverd.

In 2020 werd voor het eerst over 14 BIO-normen[4] verantwoording afgelegd in plaats van 12 normen die sectorspecifiek waren. Hierdoor kon over verantwoordingsjaar 2020 geen vergelijking worden gemaakt tussen de toename of afname van specifieke normen bij gemeenten ten opzichte van eerdere jaren en waren normen inhoudelijk niet goed vergelijkbaar. In de rapportage over verantwoordingsjaar 2021 kan die vergelijking wel worden gemaakt. Daarnaast kunnen de verantwoordingen van andere afnemers voor het eerst met elkaar worden vergeleken. Net zoals voorgaand jaar, is er sprake van 14 normen waarop gecontroleerd wordt. Deze normen zijn inhoudelijk hetzelfde als in verantwoordingsjaar 2020. Het aantal gemeenten dat aan alle gecontroleerde beveiligingsnormen voldoet ligt op 71,6%[5] (in 2020 69,2, in 2019: 82%, in 2018:

[1] Dit is inclusief gemeenten die een onvolledige of onduidelijke verantwoording hebben afgelegd.
[2] Dit is inclusief een partij die een onvolledige of onduidelijke verantwoording heeft afgelegd.
[3] Op 1 januari 2022 waren er 352 gemeenten. 10 gemeenten hebben over 2021 geen verantwoordingsverplichting vanwege een herindeling in 2022. 342 Gemeenten hebben over 2021 dus een verantwoordingsverplichting. Daarvan hebben 2 gemeenten geen verantwoording afgelegd en 4 een onvolledige/onduidelijke verantwoording. Daarnaast hadden 7 andere afnemers een verantwoordingsverplichting te weten; UWV, SVB, DUO, CAK, IND, Dienst Justis en de Arbeidsinspectie. Over verantwoordingsjaar 2020 was onduidelijkheid over de verantwoordingsverplichting van 1 partij. Daarom is in de Totaalrapportage 2020 verantwoordingen verwerkt van 6 partijen. Inmiddels is er duidelijkheid over de verantwoordingsverplichting van een partij en daarom verantwoorden zich nu 7 partijen.
[4] Baseline Informatiebeveiliging Overheid

[5] Aantal gemeenten met nul bevindingen, gedeeld door het aantal gemeenten dat zich heeft verantwoord (inclusief gemeenten met een onduidelijke/ontbrekende verantwoording).

79,1% en in 2017 45,8%). Het aantal gemeenten dat in twee opeenvolgende jaren niet voldeed aan 2 of meer normen, is 22. Het aantal gemeenten dat voor het derde opeenvolgende jaar 2 of meer bevindingen heeft, is 7.

Het aantal andere afnemers, het gaat dan om UWV, SVB, DUO, CAK, IND, Dienst Justis en de Arbeidsinspectie, dat aan alle gecontroleerde beveiligingsnormen voldoet is 28,6%[6]. In verantwoordingsjaar 2020 was dit 33,3%[7].

Het aantal meldingen van onrechtmatig gebruik van Suwinet, bijvoorbeeld voor Jeugdzorg is gedaald van 6 naar 2.

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 informatiebeveiliging van de GeVS in 2021 bij 342[8] gemeenten en 7 andere afnemers[9]. BKWI stelt deze rapportage samen op verzoek van het Ministerie van Sociale Zaken en Werkgelegenheid.

Gemeenten leggen verantwoording af over de informatiebeveiliging volgens de ENSIA-systematiek[10]. Deze verantwoording is primair gericht aan de Gemeenteraad als horizontale toezichthouder, maar het gedeelte dat betrekking heeft op de GeVS wordt, voorzien van een assurance-rapport van een EDP-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 namens de SUWI-partijen door 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 2021.

[6] 28,6% van 7 afnemers die een bruikbare verantwoording hebben ingeleverd voldoen aan alle gecontroleerde beveiligingsnormen.
[7] Hierbij dient te worden opgemerkt dat zich over 2020 6 partijen verantwoorden.
[8] Er zijn 352 gemeenten in 2021, maar 10 gemeenten hoeven geen verantwoording af te leggen in verband met een herindeling in 2022.
[9] Bronnen en beheerders leggen geen verantwoording af. Dat is vastgelegd in de Verantwoordingsrichtlijn.
[10] Zie www.ensia.nl.

Deze 7 andere afnemers zijn in 2021 voor de tweede keer opgenomen in de rapportage. Met ingang van verantwoordingsjaar 2020 is de Baseline Informatiebeveiliging Overheid (BIO) voor alle partijen het uitgangspunt voor de rapportage. Daardoor wordt de Totaalrapportage uniformer. Over 2019 konden andere afnemers dan gemeenten zich nog verantwoorden op basis van de Verantwoordingsrichlijn 2011 waardoor een vergelijking niet goed mogelijk was. Inmiddels verantwoorden alle afnemers zich volgens de Verantwoordingsrichtijn 2021. 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

Er is één belangrijk verschil in de verantwoording tussen gemeenten en andere afnemers: 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 en SZW 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[11]-taken, beslaglegging door een gemeentelijke belastingdeurwaarder of adresonderzoek door een afdeling Burgerzaken.

De verhouding van het aantal raadplegingen 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 is gericht aan het Ketenoverleg en aan de minister van SZW als verantwoordelijke voor het SUWI-stelsel.

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 transparantie 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 andere afnemers. De Totaalrapportage beschrijft de feitelijke stand van zaken van de informatiebeveiliging van de GeVS. De rapportage over de bevindingen van normen is geaggregeerd. Bevindingen zijn dus niet te herleiden tot individuele organisaties.

Het verkregen overzicht dient voor de ketenpartijen om het gezamenlijke 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.

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

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

Op basis van deze rapportage kan de minister van SZW 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.

De andere afnemers volgen een vergelijkbare procedure, die is geregeld in de Verantwoordingsrichtlijn Informatiebeveiliging GeVS. Deze afnemers leveren een In-control-verklaring aan.

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[12], 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 assurance-rapport van een EDP-auditor. 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 2022 via ENSIA over het verantwoordingsjaar 2021 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 342 verantwoordingsplichtige gemeenten hebben tot op heden geen verantwoording aangeleverd. Deze gemeenten zijn bekend bij het ministerie van SZW. Ter vergelijking: vorig jaar ontbraken er 5 verantwoordingen. Vier gemeenten hebben een onduidelijke of onvolledige verantwoording

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

ingeleverd. Om te voorkomen dat de totaalrapportage onbetrouwbaar wordt is de informatie van deze gemeenten niet verwerkt.
De gemeenten die twee jaar achter elkaar bevindingen hebben gemeld, zullen door het ministerie worden benaderd conform het Interventieprotocol. Ook gemeenten die drie of meer opeenvolgende jaren bevindingen hebben zullen door het ministerie van SZW worden benaderd conform dit protocol.

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 assurance-rapport.

Alle afnemers hebben verantwoording afgelegd en alle verantwoordingen zijn bruikbaar.

Aan eventuele bevindingen bij deze afnemers zal aandacht besteed 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 betrouwbaarheid van de rapportage te garanderen wordt een onduidelijke of onvolledige verantwoording 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%[15] bij gemeenten en 100% bij andere afnemers is de rapportage representatief. De door een EDP-auditor opgestelde assurance-rapporten, die onderdeel uitmaken van de transparantierapportage, garanderen de juistheid van de bevindingen.

[15] Dit is inclusief gemeenten die een onvolledige of onduidelijke verantwoording hebben afgelegd.

7. Wat zegt deze rapportage over de stand van de informatiebeveiliging bij de afnemers?

Aantallen bevindingen op SUWI-taken per gemeente 2017-2021

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 de verantwoordingsjaren 2020 en 2021. Tabel 3 toont de jaren 2019, 2018 en 2017. Deze splitsing is gemaakt omdat zo onderscheid kan worden gemaakt in de jaren dat over 14 BIO-normen verantwoord wordt en de jaren dat over de 12 SUWI-normen verantwoord werd.

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

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

Tabel 3: aantal en percentage bevindingen SUWI-taken 2019, 2018 en 2017 (SUWI-normen)

	2019		2018		2017	
Aantal bevindingen	**# Gemeenten**	**%**	**# Gemeenten**	**%**	**# Gemeenten**	**%**
0	291	82,0%	273	79,1%	170	45,8%
1	10	2,8%	15	4,3%	55	14,6%
2	13	3,7%	17	4,9%	39	10,3%
3	7	2,0%	8	2,3%	36	9,5%
4 of meer	29	8,2%	29	8,4%	63	16,7%
Verantwoording ontbreekt/onduidelijk	5	1,7%	3	0,9%	15	3,2%
Totaal	355	100%	345	100%	378	100%

Aantallen bevindingen van normen bij andere afnemers in 2021 en 2020

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

Tabel 4: aantal en percentage bevindingen 2020 en 2021

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

Verloop bevindingen gemeenten

Er zijn 22 gemeenten die in 2021 en 2020 bevindingen hebben. Deze gemeenten zullen benaderd worden door het ministerie van SZW en met hen zal een ambtelijk overleg worden gevoerd.

Daarnaast zijn er 7 gemeenten die een vooraankondiging tot aanwijzing krijgen van het ministerie omdat ze voor het derde jaar op rij bevindingen hebben.

Verloop bevindingen bij andere afnemers

Er zijn 3 afnemers die voor het tweede jaar op rij bevindingen hebben.

Bevindingen van normen bij gemeenten

Tabel 5 geeft per norm aan hoe vaak daarvan afgeweken is bij het gebruik van de GeVS voor SUWI-taken en de drie niet-SUWI-taken. De norm waarbij de meeste bevindingen op SUWI-taken zijn geconstateerd staat bovenaan, de norm met de minste bevindingen op SUWI-taken staat onderaan. Hierbij moet worden opgemerkt dat een beperkt aantal gemeenten gebruik maakt van Suwinet voor niet-SUWI-taken.

Tabel 5: afwijking per norm bij gemeenten per taak in verantwoordingsjaar 2021

Norm	SUWI-taken[16]	RMC[17]	GBD[18]	BZ[19]	Omschrijving norm
9.2.5	45	2		14	Beoordeling van toegangsrechten van gebruikers
18.1.4	31	1	1	5	Privacy en bescherming van persoonsgegevens
7.2.2	33	3		10	Bewustzijn, opleiding en training ten aanzien van de informatiebeveiliging
12.4.1	45	2	1	13	Gebeurtenissen registreren
12.4.2	25		1	3	Beschermen van informatie in logbestanden
6.1.2	12			4	Scheiding van taken
10.1.1	16			2	Beleid inzake het gebruik van cryptografische maatregelen
9.2.6	26			10	Toegangsrechten intrekken of aanpassen
9.2.2	29	1		6	Gebruikers toegang verlenen
9.2.1	17			8	Registratie en afmelden van gebruikers
12.1.1	24	2		4	Gedocumenteerde bedieningsprocedures
5.1.2	12			4	Beoordeling van het informatiebeveiligingsbeleid
5.1.1	16		2	3	Beleidsregels voor informatiebeveiliging
6.1.1	16	1		6	Rollen en verantwoordelijkheden bij informatiebeveiliging
Totaal	**347**	**12**	**5**	**92**	

We constateren dat sommige gemeenten verantwoording afleggen over niet-Suwitaken terwijl ze geen aansluiting hebben. We constateren ook dat sommige gemeenten geen verantwoording afleggen over niet-Suwitaken terwijl ze wel een aansluiting hadden. Dit zal nader worden onderzocht.

Bevindingen van normen bij andere afnemers

Onderstaande tabel 6 geeft per norm aan hoe vaak daarvan afgeweken is bij het gebruik van de GeVS voor taken bij andere afnemers.

[16] Het gaat hier om de uitvoering van de Participatiewet. Deeltaken, zoals de toetsing van aanvragen en sociale recherche, zijn soms bij verschillende organisaties belegd.
[17] 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.
[18] BD staat voor Gemeentelijke Belastingdeurwaarders. Zij gebruiken Suwinet ook voor niet-SUWI-taken.
[19] BZ staat voor Afdelingen Burgerzaken. Zij gebruiken Suwinet ook voor niet-SUWI-taken.

Tabel 6: afwijking per norm bij andere afnemers in verantwoordingsjaar 2021

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

Onrechtmatig gebruik Suwinet bij gemeenten

Voor het gebruik van Suwinet is een wettelijke grondslag noodzakelijk. Voor de hierboven beschreven SUWI- en niet-SUWI-taken is die er ook. In tabel 7 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. Deze gemeenten zijn namens de minister van SZW schriftelijk verzocht dit gebruik te beëindigen.

Tabel 7: verloop aantal meldingen gebruik Suwinet zonder wettelijke grondslag

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