Totaalrapportage informatiebeveiliging GeVS 2019

1. Managementsamenvatting

Dit jaar verschijnt de derde Totaalrapportage over de informatiebeveiliging van de GeVS sinds de invoering van de ENSIA-verantwoordingssystematiek door de gemeenten. De Totaalrapportage is betrouwbaar, omdat 356[1] van de 362 partijen (7 daarvan zijn geen gemeente) die van Suwinet-gebruik maakten een verantwoording hebben aangeleverd.

Het aantal organisaties dat aan alle gecontroleerde beveiligingsnormen voldoet ligt op 82% (in 2018: 79%, in 2017: 46%). Het aantal gemeenten dat in twee opeenvolgende jaren niet voldeed aan twee of meer normen is gedaald van 56 naar 21, maar 13 van die 21 gemeenten kwamen niet voor in de eerdere lijst van 56 gemeenten.

De afwijkingen van de normen voor het autorisatiebeheerproces, functiescheiding en awareness lopen weer iets op, de afwijkingen van de andere 8 normen zijn sterker afgenomen.

Het aantal meldingen van onrechtmatig gebruik van Suwinet, bijvoorbeeld voor schuldhulpverlening is gedaald van 13 naar 1.

De Domeingroep Privacy & Beveiliging komt in een aparte notitie aan het Ketenoverleg met conclusies en aanbevelingen bij deze Totaalrapportage.

2. Inleiding

Deze rapportage bevat een overzicht van de stand van de informatiebeveiliging van de Gemeenschappelijke elektronische Voorziening Suwinet (hierna GeVS) in 2019 bij 355 gemeenten en 7 andere afnemers[2]. BKWI stelt deze rapportage samen op verzoek van het Ministerie van Sociale Zaken en Werkgelegenheid, nu voor de derde keer.

[1] De cijfers in deze rapportage geven de stand van zaken op 12 augustus weer.
[2] Bronnen en beheerders leggen geen verantwoording af. Dat is vastgelegd in de Verantwoordingsrichtlijn.

Uitgangspunt bij de informatiebeveiliging zijn de normen voor de beveiliging van de GeVS die in het programma 'Borging Veilige Gegevensuitwisseling via Suwinet' zijn geactualiseerd. Met ingang van 2020 komen de normen uit de Baseline Informatiebeveiliging Overheid (BIO) hiervoor in de plaats.

Gemeenten leggen verantwoording af over de informatiebeveiliging volgens de ENSIA-systematiek[3]. 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-rapportage van een EDP-auditor, ook doorgestuurd aan BKWI. Deze informatie gebruikt BKWI om deze Totaalrapportage op te stellen, die door het Ketenoverleg met conclusies en aanbevelingen naar de minister van SZW wordt verstuurd.

Daarnaast 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.

3. Scope van de rapportage

Deze rapportage heeft betrekking op de informatiebeveiliging bij de gebruikers (afnemers) van Suwinet. Er dienden 355 gemeenten verantwoording af te leggen over 2019.

De andere 7 op de GeVS aangesloten afnemers zijn dit jaar voor het eerst ook opgenomen. Deze 7 afnemers (UWV, SVB, DUO, CAK, IND, Dienst Justis en Inspectie SZW) zijn verantwoordelijk voor meer dan de helft van de bevragingen van de GeVS in 2019. Hun verantwoordingen zijn niet helemaal vergelijkbaar met die van de gemeenten, omdat een deel van hen[4] zich verantwoord heeft volgens de Verantwoordingsrichtlijn 2011.

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

De komende jaren blijft er nog wel één belangrijk verschil in de verantwoording tussen gemeenten en andere afnemers: gemeenten verantwoording zich alleen over opzet en bestaan van de informatiebeveiligingsmaatregelen, de andere afnemers verantwoorden zich ook over de werking

[3] Zie www.ensia.nl.
[4] In verband met de overgang naar de BIO met ingang van verantwoordingsjaar 2020 heeft de Ketenoverleg de niet-gemeentelijke afnemers hier een keuze in geboden, om tegemoet te komen aan de elkaar snel opvolgende wijzigingen in de verantwoordingsrichtlijn. Voor gemeenten was dat niet nodig, omdat die zich al vanaf 2017 op dezelfde manier verantwoorden (de ENSIA-systematiek).

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. In het geval van gemeenten gaat het bij SUWI-taken om de uitvoering van de Participatiewet, de IOAW en de IOAZ, en bij niet-SUWI-taken om het gebruik van Suwinet voor RMC[5]-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 SUWI-taken.

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 z.g. 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

Deze Totaalrapportage geeft een samenvattend beeld van alle ontvangen transparantierapportages. De Totaalrapportage beschrijft de feitelijke stand van zaken van de informatiebeveiliging van de GeVS bij alle afnemers. De rapportage over de afwijkingen van normen is geaggregeerd. Afwijkingen 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.

[5] RMC: Regionaal Meld- en Coördinatiepunt Vroegtijdige Schoolverlaters

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.

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 eventuele maatregelen om die aanbevelingen uit te voeren. Het geheel wordt door de voorzitter van het Ketenoverleg aangeboden aan de Minister van SZW.

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[6], 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 BIG[7]. Burgemeester & Wethouders stellen op basis van een deel van de vragen een in-control-verklaring op, de “collegeverklaring”, die wordt voorzien van een assurance-rapportage van een EDP-auditor. De in-control-verklaring bevat een bijlage, waarin eventuele afwijkingen (‘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 11 normen uit de BIG en het Specifieke SUWI-normenkader voor Afnemers bij het gebruik van de Suwinet Inkijk, Suwinet Inlezen en DKD Inlezen. Dat maakt ze geschikt voor verticale[8] verantwoording aan de Minister van SZW.

Gemeenten hebben zich in 2020 via ENSIA over het verantwoordingsjaar 2019 verantwoord over SUWI-taken (taken die worden uitgevoerd in het kader van de Participatiewet) en niet-SUWI-taken (gebruik van Suwinet voor RMC-taken[9], burgerzaken en belastingdeurwaarders).

Gemeenten dienden de in-control-verklaring en het assurance-rapport in 2020 uiterlijk op 1 juni aan te leveren (één maand later dan voorgaande jaren in verband met de coronacrisis). Van 5 van de 355 verantwoordingsplichtige gemeenten is tot op heden geen verantwoording ontvangen. Deze gemeenten zijn bekend bij het ministerie. Ter vergelijking: vorig jaar ontbraken er 3 verantwoordingen.

---

[6] Voor meer informatie: www.ensia.nl.
[7] Baseline Informatiebeveiliging Gemeenten
[8] 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.
[9] Regionale Meld- en Coördinatiefunctie voortijdig schoolverlaten

Gemeenten die geen bevindingen rapporteerden hebben inmiddels een brief ontvangen waarin staat dat de verantwoording in orde is. Gemeenten die bevindingen hebben gemeld hebben een brief gekregen waarin die melding wordt bevestigd en is toegelicht wat de vervolgstappen zijn volgens het Interventieprotocol. De gemeenten die twee jaar achter elkaar meer dan twee bevindingen hebben gemeld, zullen door het ministerie worden benaderd conform het Interventieprotocol.

Andere afnemers

Voor de 7 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.

1 van de afnemers heeft hiervoor uitstel gekregen, de anderen hebben zich tijdig volgens de Verantwoordingsrichtlijn 2011, de Verantwoordingsrichtlijn 2019 of het UWV Auditreglement verantwoord.

Aan eventuele bevindingen zal aandacht besteed worden in de bij de afnemer gebruikelijke planning & control-cyclus.

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

Gemeenten

De ENSIA-vragenlijst toetst opzet en bestaan (niet werking) op 31 december 2019 van de interne beheersmaatregelen voor de in de tabel hieronder opgenomen normen uit het Specifiek Suwinet Normenkader Afnemers, aangevuld met een BIG[10]-norm in verband met *awareness*.

Tabel 1: beveiligingsnormen Suwinet Normenkader Afnemers

Norm	Onderwerp
AP	Awareness
B.01	Informatiebeveiligingsbeleid voor Suwinet
B.04	Beveiligingsfunctie Suwinet
B.05	Taken, verantwoordelijkheden en functiescheiding
U.02	Autorisatiebeheerproces

[10] BIG: Baseline Informatiebeveiliging Gemeenten. Het gaat om norm 8.2.2 over *awareness*, die in de ENSIA-systematiek de AP-norm wordt genoemd.

Norm	Onderwerp
U.03	Gebruikersidentificatie en authenticatie
U.11	Encryptie netwerkverbindingen
C.01	Evaluatie van informatiebeveiligingsbeleid Suwinet
C.04	Beoordeling toegangsrechten
C.05	Logging
C.06	Monitoring en rapportage

Andere afnemers

3 Afnemers hebben zich over de hierboven beschreven normen verantwoord, inclusief de werking van de daarvoor getroffen beheersingsmaatregelen. 3 Andere afnemers hebben een ander normenkader als uitgangspunt genomen.

8. Betrouwbaarheid van de Totaalrapportage

Om betrouwbaar te zijn moet de rapportage representatief zijn en moeten de gemelde bevindingen juist zijn. Met een respons van 98% bij gemeenten (86% 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.

Bij de NOREA is twijfel of altijd alle relevante services en taken worden gecontroleerd. Begin dit jaar kwam bijvoorbeeld aan het licht dat 4 gemeenten die deel uitmaken van hetzelfde samenwerkingsverband het gebruik van DKD Inlezen over het hoofd hadden gezien. Hier wordt opnieuw aandacht aan besteed bij de audits over 2020.

9. Uitkomsten

Aantallen afwijkingen op SUWI-taken per gemeente 2017-2019

Tabel 2 geeft aan hoeveel gemeenten géén afwijkingen hebben gerapporteerd bij de uitvoering van SUWI-taken en bij hoeveel gemeenten er 1, 2, 3 of meer afwijkingen waren over de periode 2017-2019.

Tabel 2: aantal en percentage afwijkingen Suwi-taken 2017-2019

	2019		**2018**		**2017**	
Aantal afwijkingen	Aantal gemeenten	%	Aantal gemeenten	%	Aantal 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%
Ontbrekende of onduidelijke verantwoording	5	1,7%	3	0,9%	15	3,2%
	355[11]	**100%**	**345**	100%	**378**[12]	100%

Afwijkingen van normen bij andere afnemers

6 van de 7 afnemers hebben verantwoording afgelegd. 3 van de 6 afnemers meldden geen bevindingen. Door de verschillen in gehanteerde verantwoordingssystematiek zijn de uitkomsten lastig te vergelijken met die van de gemeenten. Ook zijn er extreme verschillen in het gebruik (aantal opvragingen) dat de afnemers van de Suwinet Services maken.

[11] In 2019 waren alle gemeenten verantwoordingsplichtig. In 345 was een aantal gemeenten vrijgesteld van verantwoording vanwege een recente samenvoeging of fusie. Het aantal gemeenten in Nederland is dus niet met 10 gestegen.
[12] In verantwoordingsjaar 2017 is norm C.07 meegenomen, in 2018 en 2019 niet.

Afwijkingen van normen bij gemeenten

Onderstaande tabel geeft per norm aan hoe vaak daarvan afgeweken is bij het gebruik van de GeVS voor SUWI-taken en de drie niet-SUWI-taken. Merk op dat een beperkt aantal gemeenten gebruik maakt van Suwinet voor niet-SUWI-taken. Voor RMC-taken zijn dat er bijvoorbeeld maar 39.

Tabel 3: afwijking per norm verantwoordingsjaar 2019

Norm	SUWI-taken[13]	RMC[14]	BD[15]	BZ[16]	Omschrijving norm
AP	16	3	2	8	Awareness
B.01	20	2	1	10	Informatiebeveiligingsbeleid Suwinet
B.04	16	2	1	12	Beveiligingsfunctie Suwinet
B.05	22	3	1	15	Taken, verantwoordelijkheden en functiescheiding
U.02	40	5	4	17	Autorisatiebeheerproces
U.03	19	2	0	14	Gebruikersidentificatie en -authenticatie
U.11	14	0	0	1	Encryptie netwerkverbindingen
C.01	22	4	2	11	Evaluatie van informatiebeveiligingsbeleid Suwinet
C.04	27	3	4	20	Beoordeling van toegangsrechten
C.05	13	0	1	1	Logging
C.06	24	4	7	20	Monitoring en rapportage
Totaal	**233**	**28[17]**	**23**	**129**	

[13] Het gaat hier om de uitvoering van de Participatiewet. Deeltaken, zoals de toetsing van aanvragen en sociale recherche, zijn soms bij verschillende organisaties belegd.
[14] RMC staat voor Regionale Meld- en Coördinatiepunten Vroegtijdige Schoolverlaters. Zij gebruiken Suwinet voor taken die niet in de SUWI-wetgeving zijn geregeld. Dat wordt in deze context een niet-SUWI-taak genoemd.
[15] BD staat voor Gemeentelijke Belastingdeurwaarders. Zij gebruiken Suwinet ook voor niet-SUWI-taken.
[16] BZ staat voor Afdelingen Burgerzaken. Zij gebruiken Suwinet ook voor niet-SUWI-taken.
[17] Het aantal bevindingen is hier laag, net als in de volgende kolom, omdat er maar een beperkt aantal gemeenten hiervoor Suwinet gebruikt.

Verschuivingen in aantallen afwijkingen bij Suwi-taken over de periode 2017-2019, per norm

In tabel 5 is een vergelijking opgenomen tussen 2019, 2018 en 2017, die laat zien bij welke normen de meeste bevindingen zijn gemeld de afgelopen 3 jaar.

Tabel 4: Verschuivingen in aantallen afwijkingen per norm van 2017 tot 2019

Norm	2019	2018	2017	Omschrijving norm
U.2	40	30	77	Autorisatiebeheerproces
C.4	27	42	84	Beoordeling van toegangsrechten
C.6	24	51	68	Monitoring en rapportage
C.1	22	29	83	Evaluatie van aansluitingsbeleid
B.5	22	13	44	Taken, verantwoordelijkheden en functiescheiding
B.1	20	33	66	Suwinet-aansluitbeleid
U.3	19	18	18	Gebruikersidentificatie en -authenticatie
B.4	16	19	37	Beveiligingsfunctie Suwinet
AP[18]	16	10	N.v.t.	Awareness
U.11	14	13	53	Netwerkverbindingen
C.5	13	15	42	Logging
Totaal	233	266	572	

10. Onrechtmatig gebruik Suwinet

Voor het gebruik van Suwinet is een wettelijke grondslag noodzakelijk. Voor de hierboven beschreven SUWI- en niet-SUWI-taken is die er ook. Over 2018 hebben 13 gemeenten in de transparantierapportage aan BKWI echter – ongevraagd - aangegeven Suwinet ook te gebruiken voor taken waar geen wettelijke grondslag voor is. Het gaat daarbij vooral om inzet van Suwinet bij taken rondom schuldhulpverlening en jeugdzorg. Deze gemeenten is namens de minister van SZW schriftelijk verzocht dit gebruik te beëindigen. Over 2019 is het aantal meldingen van onrechtmatig gebruik gedaald tot 1.

[18] Deze norm was in 2017 ten onrechte niet in de transparantierapportages opgenomen.