Postbus 58285, 1040 HG Amsterdam

Datum

20 DEC. 2018

Ons kenmerk

SBK/98574/AM

Bijlage

Aan de staatssecretaris van Sociale zaken en Werkgelegenheid
Mevrouw drs. T. van Ark
Postbus 90801
2509 LV Den Haag

Onderwerp

Begeleidende brief Totaalrapportage Informatiebeveiliging GeVS 2017

Geachte mevrouw Van Ark,

Namens de SVB, VNG en UWV bied ik u de Totaalrapportage Informatiebeveiliging GeVS aan. De rapportage biedt een totaalbeeld van de stand van de informatiebeveiliging in de SUWI-keten, waar het de gegevensverwerkingen betreft die via de Gezamenlijke elektronische voorzieningen SUWI (GeVS) plaatsvinden. De Totaalrapportage is opgesteld op basis van individuele rapportages van de afnemers van de GeVS, de zogenaamde transparantierapportages. Organisaties die gebruik maken van de GeVS zijn verplicht om transparantie te bieden en verantwoording af te leggen over het gebruik van de GeVS. Met de Totaalrapportage heeft de keten zelf een instrument in handen om zicht te krijgen op de naleving van beveiligingsnormen en risico's in kaart te brengen. Op basis hiervan kan de keten zelf, indien nodig, passende maatregelen treffen. Dit is een aanvulling op al bestaande mechanismen om de privacy en informatiebeveiliging bij gegevensverwerkingen te borgen.

Dit jaar is de Totaalrapportage voor het eerst opgesteld. In de bijgevoegde, eerste Totaalrapportage zijn uitsluitend bevindingen van de gemeenten opgenomen. De verplichting voor de gebruikers van de GeVS om transparantierapportages aan te leveren aan het BKWI is voor gemeenten versneld in werking getreden. Deze verplichting geldt vanaf het verantwoordingsjaar 2017 al voor gemeenten, via een herijkt Specifieke SUWI-Normenkader Afnemers. Het BKWI (Bureau Keteninformatisering Werk en Inkomen, organisatieonderdeel van UWV en beheerder van het centrale deel van de GeVS) stelt op basis van de individuele transparantierapportages de Totaalrapportage op. De versnelde inwerkingtreding voor gemeenten hangt samen met de invoering van de ENSIA-systematiek in 2017. In de Totaalrapportage en de bijgevoegde reactie van de VNG wordt hier meer toelichting over gegeven. SVB en UWV verantwoorden zich nog op de oude manier, op basis van het SUWI-Normenkader dat momenteel voor deze partijen geldt. De verantwoording van SVB en UWV aan het Ministerie van SZW verloopt via de reguliere cycli van planning & control. Vanaf het verantwoordingsjaar 2019 werken ook de SVB en UWV met het herijkte Specifieke SUWI-Normenkader Afnemers. De transparantierapportages van deze partijen worden dan ook opgenomen in de Totaalrapportage.

De VNG heeft naar aanleiding van de Totaalrapportage een bestuurlijke reactie opgesteld. Deze reactie is afgestemd met en wordt onderschreven door de SVB en UWV. Deze partijen nemen deel aan het Ketenoverleg, het bestuurlijke overleg over de GeVS. De adviezen en aanbevelingen van de Domeingroep Privacy en Beveiliging, een adviesorgaan van het Ketenoverleg, zijn hier ook in meegenomen. In de bijlagen vind u de bestuurlijke reactie van de VNG, de adviezen en aanbevelingen van de Domeingroep Privacy en Beveiliging en de Totaalrapportage. In de bijlagen vind u ook meer informatie over de maatregelen die we zullen treffen of al getroffen hebben.

De ketenpartijen zijn tevreden dat er nu een instrument bestaat om een compleet beeld te krijgen van de stand van de informatiebeveiliging in de gehele SUWI-keten bij de inzet van de GeVS. Tegelijkertijd realiseren we ons dat we hier ook serieus gevolg aan moeten geven. En dat gaan we ook doen. Een zorgvuldige verwerking van persoonsgegevens en een goede informatiebeveiliging van de GeVS staan hoog op onze agenda en hebben onze voortdurende aandacht. Hierover hebben we ook nauw contact met het Ministerie van SZW. Ik hoop u hierbij voldoende te hebben geïnformeerd.

Hoogachtend,

Jose L[illegible]eroms (voorzitter van het Ketenoverleg Werk en Inkomen)

Minister Sociale Zaken en Werkgelegenheid

Datum
18 december 2018
Bijlage(n)
1

Onderwerp
Ter informatie stand van zaken totaalrapportage informatiebeveiliging GeVS (Gezamenlijke elektronische Voorzieningen Suwi) 2017

Geachte mevrouw van Ark,

Met deze brief willen wij u informeren over de totaalrapportage die is verschenen en een beeld geeft over de stand van zaken van de informatiebeveiliging van de Gezamenlijke elektronische Voorzieningen Suwi[1],GeVS) over 2017 bij gemeenten.

Uit de rapportage blijkt dat er stappen zijn gezet. De afgelopen jaren is er veel aandacht besteed aan de bewustwording om Suwinet veilig en zorgvuldig te gebruiken. Bijvoorbeeld door het programma 'Borging veilige gegevensuitwisseling via Suwinet'. De rapportage laat zien dat er nog werk aan de winkel is. Vooral de controle van logging en systeemgebruik, de beoordeling van toegangsrechten en het actualiseren van informatiebeveiligingsbeleid vragen aandacht. Gemeenten zijn primair verantwoordelijk om de verbeteringen die naar voren zijn gekomen uit de totaalrapportage door te voeren. De VNG ondersteunt hierbij vanuit de rol van vertegenwoordiger van gemeenten. Vanuit de keten wordt er ook actie ondernomen naar aanleiding van de bevindingen die naar voren zijn gekomen en mogelijke verbeteringen worden in de komende periode door de ketenpartijen nader gezamenlijk uitgewerkt.

Proces

In 2016 zijn de normenkaders voor de informatiebeveiliging van de GeVS herzien en geldt het normenkader voor gemeenten als afnemer. In 2017 is de ENSIA-verantwoordingssystematiek voor informatiebeveiliging bij gemeenten ingevoerd. Via ENSIA geven gemeenten invulling aan de afspraken in het normenkader. Het uitgangspunt van ENSIA is het horizontale verantwoordingsproces aan de gemeenteraad. Dit vormt de basis voor het verticale

[1] Suwinet is de digitale infrastructuur die is ontwikkeld door en om ervoor te zorgen dat, de Suwi-partijen (UWV, SVB en gemeenten) gegevens met elkaar kunnen uitwisselen voor de uitoefening van hun wettelijke taak. De gegevens die getoond worden zijn vastgelegd in de wettelijke taak die de afnemende organisatie uitvoert en bepaalt welke gegevens van welke burgers mogen worden geraadpleegd. Het betreffen gegevens over onder meer uitkeringen, werk, re-integratie en opleidingen.

Vereniging van Nederlandse Gemeenten
Nassaulaan 12 Den Haag | Postbus 30435 | 2500 GK Den Haag
070 - 373 83 93 | info@vng.nl

verantwoordingsproces aan nationale partijen die een rol hebben in het toezicht op informatieveiligheid. Gemeenten lopen in de keten voorop in het verantwoorden over de herziene normenkaders. Voor de andere SUWI-partijen (UWV en SVB) bestond voor 2017 nog geen verplichting tot het leveren van een transparantierapport aangezien de herziene normenkaders nog niet van kracht waren voor de andere partijen. Zij leggen verantwoording af via de bestaande wijze en reguliere P&C cycli.

De totaalrapportage geeft een weergave over de verantwoording betreffende de opzet en bestaan van interne beheersingsmaatregelen bij gemeenten voor 11 geselecteerde[2] normen.
Gemeenten hebben aan de hand van de zelfevaluatie ENSIA gerapporteerd over de mate waarin zij voldoen aan de 11 normen in scope. Zij hebben hierover aan de hand van een door het college opgestelde verklaring gerapporteerd aan de gemeenteraad en BKWI[3]. Deze rapportage is van assurance voorzien door een IT auditor. Namens het ministerie van SZW verzendt BKWI een brief aan gemeenten als eerste stap van het SUWI interventieprotocol over verbetermaatregelen wanneer dit aan de orde is.

Bevindingen
Met deze totaalrapportage is voor het eerst in het bestaan van de GeVS een compleet beeld van de door SZW geformuleerde normen voor afnemers. Meer dan 99% van de gemeenten heeft al in het eerste jaar dat de ENSIA-verantwoordingssystematiek van kracht was een transparantierapportage ingeleverd. Tegelijkertijd wordt er geconstateerd dat er verbeteringen kunnen en moeten worden aangebracht om aan alle normen te voldoen en de verantwoording over de GeVS bij gemeenten op het juiste niveau te krijgen. Vooral de beoordeling van toegangsrechten, het actualiseren van informatiebeveiligingsbeleid en controle van logging en systeemgebruik vragen aandacht.

Duiding
Bij de duiding van de rapportage is het van belang de onderstaande elementen mee te nemen:

- De transparantierapportage geeft een beeld van de stand van de informatiebeveiliging bij gemeenten als het gaat om SUWI-taken. Het beeld van de niet-SUWI-taken is veel minder volledig en geeft niet voldoende zekerheid om er conclusies aan te verbinden. Mede omdat die pas laat aan de verantwoordingssystematiek is toegevoegd.
- Het is duidelijk dat de normnaleving niet voldoende is. Er is wel een verantwoordingssysteem ontstaan dat zicht geeft op verbeterpunten en waarborgen bevat om de normnaleving te verbeteren. Ook is er een interventieprotocol dat voorziet in situaties waarin de normnaleving bij individuele gemeenten over een langere periode te wensen overlaat.
- Waar de totaalrapportage nog onvoldoende zicht op geeft, zijn de oorzaken van niet-naleving van de normen. Het is duidelijk dat bepaalde afwijkingen met elkaar samenhangen.

Risico's
De geconstateerde afwijkingen geven aan dat er verbeteringen nodig zijn. Het betekent niet automatisch dat de informatiebeveiliging zelf in het geding is. De controle op autorisaties kan

---

[2] De selectie is aangereikt door de toezichthouder. Vervolgens is vanuit de ENSIA-beheerorganisatie waarin naast het ministerie van BZK en de gemeenten een aantal toezichthouders samenwerken, waaronder het ministerie van SZW vanuit de rol van systeemverantwoordelijke voor de GeVS, gekeken op welke wijze de aangereikte normenset geplaatst kon worden in het verantwoordingsstelsel. In overleg met de toezichthouder en NOREA (beroepsorganisatie van IT-auditors).

[3] Het BKWI (Bureau Keteninformatisering Werk en Inkomen, organisatieonderdeel van UWV en beheerorganisatie van het centrale deel van de GeVS) voegt de afzonderlijke transparantierapportages samen tot een totaalrapportage, zoals beschreven in het genoemde normenkader. Deze wordt aangeboden aan het Ketenoverleg Werk en Inkomen bestaande uit SVB, UWV en de VNG, nadat het heeft kennisgenomen van de aanbevelingen van de Domeingroep Privacy & Beveiliging (adviesorgaan voor het Ketenoverleg). Deze totaalrapportage geeft een geaggregeerd beeld van de stand van de informatiebeveiliging van de GeVS. Op grond hiervan kan het Ketenoverleg, mocht daar aanleiding toe zijn, algemene, niet op individuele partijen, gerichte maatregelen nemen om de informatiebeveiliging op het overeengekomen niveau te krijgen.

bijvoorbeeld maandelijks plaatsvinden maar wanneer die niet beschreven is in een formeel vastgestelde procedure, is er toch sprake van een afwijking van een norm.

Domeingroep Privacy en Beveiliging (adviesorgaan voor het Ketenoverleg)
Op basis van de transparantierapportages heeft de domeingroep Privacy en Beveiliging een advies opgesteld:

Aanbevelingen
1. De betrouwbaarheid van de verantwoording over niet-SUWI-taken kan en moet beter.
2. Geef de betrokken partijen eerst de gelegenheid om de rol te gaan spelen die ze in het systeem hebben, zoals de toezichthoudende rol van de Gemeenteraad, alvorens hierin aanpassingen aan te brengen.
3. Start onderzoek dat afwijkingen en samenhang van normen verklaart en zicht biedt op passende, effectieve interventies, waar die nodig zijn.

Vervolg
De primaire verantwoordelijkheid om de noodzakelijke verbeteringen door te voeren ligt bij gemeenten waarbij de VNG ondersteuning biedt. Daarnaast is er het afgelopen jaar gewerkt aan het optimaliseren van de verantwoordingssystematiek.

Om gemeenten te ondersteunen wordt er in het voorjaar van 2019 een webinar georganiseerd over de normen uit de rapportage en de verantwoording hierover naast de reguliere communicatie. Voor praktische handreikingen over de verantwoording met betrekking tot Suwinet en ondersteuning, bijvoorbeeld de keuzehulp Suwinet verantwoording, kunnen gemeenten terecht op www.vngrealisatie.nl/ensia.

Daarnaast wordt er in januari gestart met een onderzoek samen met een aantal gemeenten dat de afwijkingen van de normen verklaart en daarmee zicht biedt op passende en effectieve interventies waar deze nodig zijn. De bevindingen die hieruit voortkomen worden gedeeld met alle gemeenten zodat gemeenten deze kunnen inzetten binnen hun eigen organisatie. Vanuit de keten wordt er ook actie ondernomen naar aanleiding van bevindingen die naar voren zijn gekomen en mogelijke verbeteringen worden in de komende periode door de ketenpartijen nader gezamenlijk uitgewerkt.

Toekomstige gegevensuitwisseling Werk en Inkomen
Sinds de totstandkoming van het huidige stelsel gegevensuitwisseling binnen het domein Werk en Inkomen zijn een aantal veranderingen opgetreden. Denk daarbij onder meer aan nieuwe techniek, vergaande borging van privacy en de groeiende behoefte aan integrale dienstverlening. Om ervoor te zorgen dat de burger meer regie heeft op de eigen gegevens en dat de burger centraal komt te staan in de dienstverlening binnen Werk & Inkomen is het programma Toekomst Gegevensuitwisseling Werk & Inkomen gestart. In de komende jaren wordt er stapsgewijs vorm en inhoud gegeven aan een toekomstbestendig stelsel voor gegevensuitwisseling onder leiding van het ministerie van Sociale Zaken en Werkgelegenheid.

De VNG heeft bestuurders en raadsleden via een ledenbrief opgeroepen om aandacht te hebben voor een zorgvuldig gebruik van Suwinet en de verantwoording hierover via ENSIA. De VNG ondersteunt gemeenten hierbij.

Hoogachtend,
Vereniging van Nederlandse Gemeenten



Conclusies en aanbevelingen bij de Totaalrapportage Informatiebeveiliging GeVS 2017 van de Domeingroep Privacy & Beveiliging

Achtergrond

In 2016 zijn de normenkaders voor de informatiebeveiliging van de GeVS herzien en in 2017 is de ENSIA-verantwoordingssystematiek voor informatiebeveiliging bij gemeenten ingevoerd. In de normenkaders is geregeld dat alle partijen ieder jaar een zogenoemde transparantierapportage over de informatiebeveiliging ter beschikking stellen aan BKWI. Gemeenten vullen dit in met de ENSIA-systematiek.

De transparantierapportages van gemeenten hadden voor 2017 betrekking op opzet en bestaan van interne beheersingsmaatregelen voor 11 uit het normenkader geselecteerde normen per 31 december 2017. Deze selectie is gemaakt door het ministerie van SZW als systeemverantwoordelijke voor de GeVS en afgestemd met het Ketenoverleg.

Voor de andere op de GeVS aangesloten partijen bestond voor 2017 nog geen verplichting tot het leveren van een transparantierapportage, omdat de herziene normenkaders voor hen nog niet van kracht waren. De Totaalrapportage voor 2017 heeft dus alleen betrekking op gemeenten.

BKWI voegt de afzonderlijke transparantierapportages samen tot een Totaalrapportage, zoals beschreven in het genoemde normenkader. De Domeingroep Privacy & Beveiliging stuurt de Totaalrapportage met conclusies en aanbevelingen naar het Ketenoverleg, dat de rapportage vervolgens met een bestuurlijke reactie van VNG, SVB en UWV aanbiedt aan de minister van SZW..

Deze Totaalrapportage geeft een geaggregeerd beeld van de stand van de informatiebeveiliging van de GeVS. Op grond hiervan kan het Ketenoverleg, mocht daar aanleiding toe zijn, algemene, niet op individuele partijen gerichte maatregelen nemen om de informatiebeveiliging op het overeengekomen niveau te krijgen. De minister van SZW kan zonodig via de toepassing van het Interventieprotocol Suwinet maatregelen nemen gericht op individuele partijen.

Bevindingen

Met deze Totaalrapportage is voor het eerst in het bestaan van de GeVS een compleet beeld van de informatiebeveiliging bij gemeenten beschikbaar gekomen. Meer dan 99% van de gemeenten heeft al in het eerste jaar dat de ENSIA-verantwoordingssystematiek van kracht was een Transparantierapportage ingeleverd. Er is dus veel bereikt!

Wel blijkt uit de ervaringen van het eerste jaar dat er nog een aantal verbeteringen nodig is. Allereerst is de verantwoording over de informatiebeveiliging van niet-SUWI-taken[1] nog niet

[1] Het gaat om het gebruik van de GeVS door afdelingen Burgerzaken, gemeentelijke belastingdeurwaarders en RMCs, regionale meld- en coördinatiecentra vroegtijdig schoolverlaten, voor taken die niet in de SUWI-wetgeving zijn geregeld.

representatief. Hierbij kan een rol spelen dat dit onderwerp pas laat aan de verantwoordingssystematiek is toegevoegd. Ook is het gebruik van de GeVS voor niet-SUWI-taken veel minder frequent[2] dan dat van de SUWI-taken en doorgaans elders in de organisatie is belegd.

Een andere observatie is dat de normnaleving voor SUWI-taken nog niet maximaal is: voor 2017 meldt 54% van de gemeenten één of meer afwijkingen van de 11 geselecteerde normen[3] [4].

Duiding

Betrouwbaarheid

De Totaalrapportage geeft een representatief beeld van de stand van de informatiebeveiliging op basis van de geselecteerde normen bij gemeenten als het gaat om SUWI-taken. Het beeld van de niet-SUWI-taken is veel minder volledig en daarmee minder betrouwbaar. Daarbij moet worden opgemerkt dat de GeVS veel minder intensief gebruikt wordt voor niet-SUWI-taken (3,5% van de opvragingen door gemeenten).

Werking van het verantwoordingsysteem

Hoewel niet alle normen worden nageleefd, is er wel een verantwoordingssysteem ontstaan dat zicht geeft op verbeterpunten en waarborgen bevat om de normnaleving te verbeteren. Daartoe behoren de jaarlijkse zelfevaluatie, de Collegeverklaring en de getrouwheidsverklaring van een onafhankelijke IT-auditor, waarmee verantwoording wordt afgelegd aan de gemeenteraad en aan de minister van SZW. Daarnaast is er een interventieprotocol dat voorziet in het nemen van maatregelen door de minister van SZW indien van normen wordt afgeweken en verbetering te lang op zich laat wachten.

Oorzaken van niet-naleving

Waar de Totaalrapportage nog onvoldoende zicht op geeft, zijn de oorzaken van niet-naleving van normen.

Het is evident dat bepaalde afwijkingen met elkaar samenhangen. Om logging te kunnen controleren (norm C.06), moet die bijvoorbeeld wel beschikbaar zijn (C.05). Een afwijking op C.05 leidt dus automatisch tot een afwijking op C.06.

Er zijn ook correlaties denkbaar tussen de grootteklasse van een gemeente en bepaalde afwijkingen. Onderzoek kan dit soort verbanden zichtbaar maken en zo bijdragen aan effectieve interventies.

Risico's

Gebreken bij de verantwoording betekenen nog niet automatisch dat de informatiebeveiliging zelf in het geding is. De controle op autorisaties kan bijvoorbeeld maandelijks plaatsvinden, maar als die niet beschreven is in een formeel vastgestelde procedure, is er toch sprake van een afwijking van een norm.

---

[2] De niet-SUWI-taken zijn goed voor ongeveer 3,5% van de gemeentelijke raadplegingen via de GeVS.

[3] Het in het rapport *SUWInet 2016 Stand van zaken na ontvangst in-control verklaringen gemeenten* van de Inspectie SZW beschreven onderzoek meldde geen afwijkingen, maar verschilde in belangrijke opzichten van het onderzoek waarop deze Totaalrapportage is gebaseerd. Zo zijn de onderzochte normen tussen beide rapportages ingrijpend herzien en is het aantal onderzochte normen uitgebreid (er waren er 7 en er zijn er 4 toegevoegd, onder andere op het gebied van controle van logging). Ook is de scope van het onderzoek uitgebreid naar niet-SUWI-taken en het gebruik van Suwinet- en DKD-Inlezen. Verder ging het bij het onderzoek van de inspectie om desk research bij een aselecte steekproef van gemeenten. Bij de voorbereiding van de Totaalrapportage is bij iedere gemeente onderzoek gedaan door een IT-auditors.

Zeker bij de introductie van een nieuwe verantwoordingssystematiek zullen dat soort situaties zich eerder voordoen en ligt het in de lijn van de verwachting dat die snel hersteld worden.

Verder biedt het verantwoordingssysteem dat nu is ingericht, zoals eerder aangegeven, een groot aantal waarborgen voor het tijdig in kaart brengen en herstellen van normafwijkingen en terugbrengen van de risico's die daarmee samenhangen.

Aanbevelingen

1. De betrouwbaarheid van de verantwoording over niet-SUWI-taken kan en moet beter. Zie erop toe dat de in de bijlage beschreven maatregelen worden genomen.
2. Geef de betrokken partijen eerst de gelegenheid om de rol te gaan spelen die ze in het systeem hebben, zoals de toezichthoudende rol van de Gemeenteraad, alvorens hierin aanpassingen aan te brengen.
3. Start onderzoek dat afwijkingen en samenhang van normen verklaart en zicht biedt op passende, effectieve interventies, waar die nodig zijn.

Conclusie

Met de ENSIA-systematiek en de Totaalrapportage is er voor het eerst een compleet overzicht in de stand van de informatiebeveiliging van de GeVS bij gemeenten. Daarmee is voor het eerst integrale stuurinformatie beschikbaar, in ieder geval voor de normnaleving bij SUWI-taken. Hiermee beschikt de SUWI-keten, hoewel er nog een aantal verbeteringen in mogelijk en nodig zijn, nu al over een belangrijk instrument om het gemeenschappelijke informatiebeveiligingsniveau te bewaken en risico's op dit vlak te beheersen

Bijlage: Verbetermaatregelen

Op basis van de ervaringen met de toepassing van ENSIA en de door gemeenten opgestelde en aan BKWI geleverde verantwoordingsinformatie zijn en worden de volgende maatregelen genomen.

Maatregelen in ENSIA-verband:

1. Verbeteren van de via de ENSIA-tooling ondersteunde zelfevaluatie betreffende de vragenlijst en de guidance daarbij (VNG in afstemming met SZW en BKWI: afgerond) (gemeenten zijn per 1 juli 2018 gestart met de zelfevaluatie over 2018).

2. Verbeteren van de algemene formats voor de Collegeverklaring en het Assurancerapport en de specifieke bijlage 2 Suwinet bij de Collegeverklaring (SZW, BKWI, VNG en beroepsvereniging NOREA: afgerond).

3. Verbeteren van de Handreiking ENSIA voor Gemeenten en het daarbij ontwikkelen van een spreadsheet voor het bij elkaar brengen van de verantwoordingsinformatie voor: SUWI-taken en evt. niet-SUWI-taken, inkijken en/of inlezen, eigen organisatie en/of organisatie(s) waaraan taken zijn uitbesteed (VNG in afstemming met NOREA, SZW en BKWI: afgerond).

4. Verdere communicatie/educatie voor gemeenten (VNG: communicatie via nieuwsbrieven, website, bijeenkomsten is doorlopende activiteit).

5. Verbeteren van de handreiking voor de IT-auditors waarbij is afgesproken dat de IT-auditors voortaan gaan beoordelen of de Collegeverklaring voldoet aan het afgesproken format en ook zelf het format van de Assuranceverklaring gaan naleven (NOREA in afstemming met VNG, SZW, BKWI: afgerond).

6. Verdere communicatie/educatie voor de groep ENSIA-auditors (NOREA: bijeenkomst in oktober en communicatie via website, nieuwsbrieven is een doorlopende activiteit).

Maatregelen SZW en BKWI op basis van via ENSIA al dan niet ontvangen verantwoordingsinformatie:

1. Benaderen van de 3 gemeenten over de nog ontbrekende ENSIA-verantwoording (BKWI en SZW).

2. BKWI stuurt brieven aan individuele gemeenten over onduidelijke en ontbrekende onderdelen van verantwoordingsinformatie met het verzoek om contact op te nemen met BKWI om dit door te spreken (BKWI in afstemming met SZW en UWV).

3. SZW informeert gemeenten via de algemene nieuwsbrief Gemeentenieuws over de opbrengst van het eerste jaar ENSIA (na ontvangst van de Totaalrapportage).

Totaalrapportage Informatiebeveiliging GeVS

De beveiliging van de GeVS bij gemeenten in 2017

Datum	Versienummer	Auteur	Opmerking
8 november 2018	1.0	Jesse Wilzing Marc Woltering	

Samenvatting

Achtergrond

In 2018 stelt het BKWI op verzoek van het Ministerie van Sociale Zaken en Werkgelegenheid voor het eerst een totaalrapportage op over de informatiebeveiliging binnen de Gemeenschappelijke elektronische Voorziening SUWI (GeVS). Uitgangspunt hiervoor zijn de in het programma 'Borging Veilige Gegevensuitwisseling via Suwinet' geactualiseerde normen voor de beveiliging van de GeVS. Gezien de afwijkende opzet van het 'oude' en het 'nieuwe' normenkader hebben de ketenpartijen UWV, SVB, VNG, IB en BKWI in overleg met het Ministerie van SZW ervoor gekozen om deze eerste rapportage te beperken tot de op de GeVS aangesloten gemeenten. In verband met de invoering van de verantwoordingssystematiek ENSIA in 2017, is het 'nieuwe' Suwinet specifieke normenkader voor afnemers namelijk als eerste voor gemeenten geldig verklaard. De overige aangesloten partijen volgen met ingang van het verantwoordingsjaar 2018. UWV (inclusief BKWI), SVB en IB hebben over het verantwoordingsjaar 2017 volgens het voor hen geldende 'oude' normenkader, via de jaarverslagen verantwoording aan de minister van SZW afgelegd.

Via de in 2017 ingevoerde ENSIA-systematiek hebben de Colleges van B&W verantwoording afgelegd over de informatiebeveiliging van de GeVS. Allereerst is deze verantwoording gericht aan de Gemeenteraad en zijn gemeenten met afwijkingen van de normen als eerste zelf aan zet om de noodzakelijke verbetermaatregelen te nemen. Daarnaast hebben de gemeenten een afslag van de verantwoordingsinformatie over de GeVS aan het BKWI verstrekt. Op basis van deze informatie intervenieert de minister van SZW als blijkt dat de voortgang van individuele gemeenten bij het nemen van verbetermaatregelen, onvoldoende is. Hiervoor heeft de minister van SZW het Interventieprotocol ENSIA Suwinet vastgesteld.

Deze totaalrapportage beschrijft de feitelijke stand van zaken van de informatiebeveiliging van de GeVS bij gemeenten. Het verkregen overzicht dient voor de ketenpartijen om het gezamenlijke gerealiseerde niveau van beveiliging te analyseren en waar nodig ondersteunende

verbetermaatregelen te nemen. Verder dient de Totaalrapportage om de minister van SZW jaarlijks over de beveiliging van de GeVS te informeren.

Gemeenten hebben zich in 2018 via ENSIA over het verantwoordingsjaar 2017 verantwoord over SUWI-taken (taken die worden uitgevoerd in het kader van de Participatiewet) en niet-SUWI-taken (gebruik van Suwinet voor RMC-taken[1], burgerzaken en belastingdeurwaarders).

In 2018 ontving het BKWI van bijna alle gemeenten hun verantwoording. Van drie gemeenten is tot op heden geen verantwoording ontvangen. Deze gemeenten zijn bekend bij het ministerie en conform het interventieprotocol zal het ministerie in overleg treden met deze gemeenten. De afwijkingen van de normen bij gemeenten zijn geaggregeerd. Afwijkingen zijn dus niet te herleiden tot individuele gemeenten.

Afwijkingen
Bij 173 gemeenten is geen sprake van afwijkingen van de normen. Dat is 45,8%. Bij 55 gemeenten (14,6%) is sprake van één afwijking en bij 39 (10,3%) is sprake van 2 afwijkingen. Bij 36 gemeenten is sprake van 3 afwijkingen en bij 63 (16,7%) is sprake van 4 of meer afwijkingen.
Deze afwijkingen hebben bij SUWI-taken vooral betrekking op de beoordeling van toegangsrechten, het actualiseren van informatiebeveiligingsbeleid en controle van logging en systeemgebruik.

[1] Regionale Meld- en Coördinatiefunctie voortijdig schoolverlaten

Inhoudsopgave

1. Inleiding 4

2. Achtergrond bij deze rapportage 4

2.1. Wettelijk kader 4

2.2. Doel 4

2.3. Over welke organisaties wordt gerapporteerd 4

2.4. Onderwerp van de verantwoording 5

3. Hoe is deze rapportage tot stand gekomen? 7

3.1. Verantwoording door gemeenten via ENSIA 7

3.2. Procesverantwoording gemeenten 7

4. Bevindingen 8

4.1. Aantallen gemeenten met afwijkingen bij SUWI-taken 8

4.2. Type afwijkingen bij SUWI-taken 8

4.3. Niet-SUWI-afwijkingen 9

4.4. Verhouding tussen gebruik voor SUWI- en niet-SUWI-taken 10

1. Inleiding

Gemeenten verantwoorden zich over de beveiliging van de GeVS op basis van de normen die zijn vastgelegd in de Baseline Informatiebeveiliging Gemeenten (BIG) aangevuld met het Specifieke SUWI-Normenkader Afnemers. Onderdeel van de verantwoordingsinformatie is een bijlage met eventuele afwijkingen van normen. Op basis van deze afwijkingen stelt het BKWI deze totaalrapportage op. Deze rapportage geeft inzicht in de mate waarin gemeenten voldoen aan de beveiligingsnormen.

2. Achtergrond bij deze rapportage

2.1. Wettelijk kader

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 rapporteren over hun informatiebeveiliging aan BKWI (criterium C.08 van het Specifiek SUWI-Normenkader voor Afnemers), de transparantierapportage
- BKWI maakt een totaalrapportage voor Ketenoverleg en de Minister SZW (criterium C.10 van het Specifiek SUWI-Normenkader voor Beheerders)

Gemeenten verstrekken de transparantierapportage via de ENSIA-verantwoordingssystematiek.

Deze totaalrapportage geeft een samenvatting van alle op tijd ingeleverde rapportages.

2.2. Doel

Deze rapportage biedt inzicht in de stand van de informatiebeveiliging van de GeVS bij gemeenten. Het verkregen overzicht dient voor de ketenpartijen om het gezamenlijke gerealiseerde niveau van beveiliging te analyseren en waar nodig ondersteunende verbetermaatregelen te nemen. Verder dient de Totaalrapportage om de minister van SZW jaarlijks over de beveiliging van de GeVS te informeren.

De rapportage geeft geen inzicht in de stand van zaken bij individuele gemeenten.

2.3. Over welke organisaties wordt gerapporteerd

Deze rapportage geeft een samenvattend beeld van de verantwoordingen van alle gemeenten. Vanaf verantwoordingsjaar 2019 zal deze rapportage ook een beeld geven van de beveiliging van de GeVS bij afnemers UWV en SVB en beheerders Inlichtingenbureau en BKWI. De rapportage bevat dan ook

de verantwoording van alle niet-SUWI-afnemers die zijn aangesloten op de GeVS. Het gaat dan om de IND, CAK, Inspectie SZW, dienst Justis en DUO. Het nieuwe normenkader en de bijbehorende verantwoordingsrichtlijn zijn dan ook op hen van toepassing.

2.4. Onderwerp van de verantwoording

Gemeentelijke afnemers verantwoorden zich met ingang van 2017 over het Specifieke SUWI-Normenkader Afnemers.

2.4.1 Verantwoording voor gemeenten

Gemeenten leggen als eerste verantwoording af over het Specifiek SUWI-Normenkader Afnemers. Zij hanteren hierbij de ENSIA-systematiek. De verantwoording van gemeenten bestaat uit een getekende verklaring van het College van B&W en een bijlage met eventuele bevindingen bij het gebruik van de GeVS. De verantwoording bevat verder een assuranceverklaring, opgesteld door een auditor.

In de ENSIA-systematiek, worden opzet en bestaan (op termijn uit te breiden met werking) van de volgende normen getoetst:

BIG	Suwinet	Onderwerp
5.1.1	B.01	Informatiebeveiligingsbeleid
6.1.2	B.04	Interne organisatie beveiliging
6.1.3 en 10.1.3	B.05	Functiescheiding
8.2.2 en 11.2.1	U.02	Autorisatiebeheer
11.2.1 en 11.5.2	U.03	Identificatie en authenticatie
12.3.1	U.11	Beveiliging van netwerk verbindingen
5.1.2 en 6.1.1	C.01	Bijstelling informatiebeveiligingsbeleid
11.2.4	C.04	Beoordeling toegangsrechten
10.10.1	C.05	Logging
10.10.1 en 10.10.2	C.06	Controle van logging
10.10.2	C.07	Controle van systeemgebruik

Deze selectie van normen correspondeert met de 7 essentiële normen uit het "oude" normenkader waaraan de Inspectie SZW tussen 2013 en 2017 de beveiliging van Suwinet bij gemeenten heeft getoetst. Daarnaast zijn een aantal normen naar aanleiding van eerder onderzoek van de Autoriteit Persoonsgegevens geselecteerd.

De verantwoording heeft betrekking op deze normen bij het gebruik van Suwinet-Inkijk, Suwinet Inlezen en DKD-Inlezen, voor zover de gemeente – of een andere partij namens die gemeente, zoals een samenwerkingsverband of een RMC – daar gebruik van heeft gemaakt.

2.4.2 SUWI- en niet-SUWI-taken bij gemeenten

Binnen gemeenten kan Suwinet gebruikt worden voor SUWI-taken en niet-SUWI-taken. SUWI-taken hebben betrekking op de uitvoering van de Participatiewet. Voorbeelden zijn:

- verwerkingen van uitkeringsaanvragen
- Bijzondere Bijstand
- Sociale recherche

Soms brengen gemeenten deze taken deels of geheel onder bij samenwerkingsverbanden, soms voeren gemeenten deze taken allemaal zelf uit.

De niet-SUWI-taken vallen uiteen in:

- adrescontrole door afdelingen Burgerzaken
- raadplegen van werkgeversgegevens ten behoeve van invordering door gemeentelijke belastingdeurwaarders
- controle van inkomensgegevens ten behoeve van de Regionale Meld- en Coördinatiefunctie voortijdig schoolverlaten (RMC).

Gemeenten moeten verantwoording afleggen over de informatiebeveiliging voor alle SUWI- en niet-SUWI-taken, ook als ze die uitbesteden.

3. Hoe is deze rapportage tot stand gekomen?

3.1. Verantwoording door gemeenten via ENSIA

Voor gemeenten is met ingang van 2017 een nieuwe verantwoordingssystematiek ingevoerd met de naam ENSIA[2], 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 en het Specifieke Suwinet-normenkader Afnemers. Burgemeester & wethouders stellen op basis van een deel van de vragen een zogenoemde Collegeverklaring ENSIA (In Control-verklaring) op. Die wordt voorzien van een Assurance-verklaring van een EDP-auditor. Zie nadere informatie op www.ensia.nl.

De Collegeverklaring en het Assurancerapport zijn bedoeld voor de verantwoording aan de gemeenteraad en de informatieverstrekking aan het BKWI.

3.2. Procesverantwoording gemeenten

Gemeenten dienden voor 1 mei 2018 hun verantwoording te uploaden via www.ensia.nl. Op 1 juni 2018 hadden 359 gemeenten dit gedaan. Op 4 juni is aan 19 gemeenten een brief verzonden met het verzoek de verantwoording alsnog aan te leveren. Op 1 oktober ontbrak nog van 3 gemeenten de verantwoording. De namen van deze gemeenten zijn bekend bij het ministerie.

Alle gemeenten met een afwijking op een of meerdere normen ontvingen rond 1 oktober 2018 een zogenaamde Attentiebrief, met het verzoek maatregelen te treffen zodat deze afwijking(en) worden opgelost. Het betrof 193 gemeenten. Indien uit de verantwoording over 2018 blijkt dat deze afwijking niet is opgelost dan zal het ministerie handelen conform het interventieprotocol.

Bij 9 gemeenten is sprake van een verantwoording die dermate onduidelijk is dat niet kan worden vastgesteld of er sprake is van afwijkingen.

In samenspraak met het ministerie en de VNG is er voor gekozen om alle gemeenten via nieuwsbrieven te informeren over alle onduidelijkheden, ontbrekende zaken of onduidelijke formuleringen die zijn geconstateerd in de bijlage. Daarnaast ontvangen de gemeenten waar sprake is van een incomplete of onduidelijke verantwoording een brief. Om de kans op herhaling te voorkomen is de indeling van en toelichting op de bijlage verbeterd.

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

4. Bevindingen

4.1. Aantallen gemeenten met afwijkingen bij SUWI-taken

In onderstaande diagram staat het aantal gemeenten dat 0,1, 2, 3 of meer dan vier afwijkingen heeft. 45,8% van de gemeenten heeft 0 afwijkingen op SUWI-taken. 16,7% heeft meer dan 4 afwijkingen op SUWI-taken.

Bij 12 gemeenten kon niet worden vastgesteld of er sprake is van afwijkingen omdat de verantwoording ontbreekt of onduidelijk is.

Afwijkingen	Aantal	Percentage
0	173	45,8%
1	55	14,6%
2	39	10,3%
3	36	9,5%
4 of meer	63	16,7%
Onbekend	12	3,2%
Totaal	**378**	**100%**

4.2. Type afwijkingen bij SUWI-taken

In onderstaande tabel staat het aantal afwijkingen per norm voor de SUWI-taken. Zo is inzichtelijk hoe vaak van een specifieke norm is afgeweken.

De normen zijn gesorteerd op het aantal keren dat ervan is afgeweken.

Norm	Aantal afwijkingen	Omschrijving norm
C.4	84	Beoordeling toegangsrechten
C.1	83	Bijstelling informatiebeveiligingsbeleid
U.2	77	Autorisatiebeheer
C.7	74	Controle van systeemgebruik
C.6	68	Controle van logging
B.1	66	Informatiebeveiligingsbeleid
U.11	53	Beveiliging van netwerkverbindingen
B.5	44	Functiescheiding
C.5	42	Logging
B.4	37	Interne organisatie beveiliging
U.3	18	Identificatie en authenticatie
Totaal	646	

De 646 afwijkingen hebben betrekking op 193 gemeenten.

4.3. Niet-SUWI-afwijkingen

In de volgende tabel is te lezen hoeveel afwijkingen zijn aangetroffen per norm bij de verschillende niet-SUWI-taken.

Een voorbehoud bij deze gegevens is op zijn plaats. Uit de contract- en gebruikersadministraties van UWV en BKWI blijkt dat niet alle gemeenten die Suwinet gebruiken voor niet-SUWI-taken zich daarover hebben verantwoord. De uitkomsten zijn dus niet representatief voor alle gemeenten.

Norm	RMC[3]	BD	BZ	Omschrijving norm
B.1	3	18	30	Informatiebeveiligingsbeleid
B.4	4	16	26	Interne organisatie beveiliging
B.5	4	17	30	Functiescheiding
				Autorisatiebeheer
U.2	4	17	29	Identificatie en authenticatie
U.3	3	7	22	Encryptie van verbindingen
U.11	2	16	26	Bijstelling informatiebeveiligingsbeleid
				Beoordeling toegangsrechten
C.1	4	19	29	Logging
C.4	6	19	30	Controle van logging
C.5	2	5	18	Controle van systeemgebruik
C.6	4	20	35	Informatiebeveiligingsbeleid
C.7	2	22	33	Interne organisatie beveiliging
Totaal	38	176	308	

De 308 afwijkingen bij afdelingen Burgerzaken hebben betrekking op 66 gemeenten.[4]
De 176 afwijkingen bij gemeentelijke belastingdeurwaarders hebben betrekking op 47 gemeenten.[5]
De 38 afwijkingen bij RMC-centra hebben betrekking op 15 gemeenten.[6]

4.4. Verhouding tussen gebruik voor SUWI- en niet-SUWI-taken

Onderstaande tabel geeft de verhouding tussen het aantal raadplegingen voor SUWI-taken (uitvoering Participatiewet, IOAZ, IOAW) en niet-SUWI-taken weer.

Taak		Raadplegingen	Percentage
SUWI		660.054	96,4%
niet-SUWI	Belastingdeurwaarders	12.094	1,8%
	Burgerzaken	6.832	1,0%
	RMC	5.969	0,9%
Totaal		684.949	100,0%

Bron: BKWI *Suwinet Services - Gebruik en prestaties - september 2018*

[3] RMC staat voor RMC-taken, BD heeft betrekking op de taken van gemeentelijke belastingdeurwaarders, BZ op de taken waarvoor afdelingen Burgerzaken Suwinet gebruiken.
[4] Volgens de administratie van het BKWI maken 263 gemeenten gebruik van Suwinet bij hun afdeling Burgerzaken.
[5] Volgens de administratie van het BKWI maken 115 gemeenten gebruik van Suwinet voor de uitvoering van taken door gemeentelijke belastingdeurwaarders.
[6] Volgens de administratie van het BKWI maken 24 gemeenten gebruik van Suwinet voor RMC-taken.