Vertrouwelijk

# Totaalrapportage Informatiebeveiliging GeVS

## De beveiliging van de GeVS bij gemeenten in 2017

| Datum | Versienummer | Auteur | Opmerking |
|---|---|---|---|
| 8 november 2018 | 1.0 | Jesse Wilzing<br>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. Voor wie is deze rapportage bestemd? Fout! Bladwijzer niet gedefinieerd.

2.4. Over welke organisaties wordt gerapporteerd 4

2.5. 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

# 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.