# Conclusies en aanbevelingen van de Domeingroep Privacy & Beveiliging bij de Totaalrapportage Informatiebeveiliging GeVS 2019

## Achtergrond

In 2016 zijn de normenkaders voor de informatiebeveiliging van de GeVS (Gemeenschappelijke elektronische Voorziening Suwinet) 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 - ook voor 2019 - betrekking op opzet en bestaan[1] van interne beheersingsmaatregelen voor 11 uit het normenkader geselecteerde normen per 31 december 2019. 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 had de transparantierapportage, naar keuze[2], betrekking op opzet, bestaan en werking van interne beheersmaatregelen voor de 11 in de vorige paragraaf genoemde normen òf op opzet, bestaan en werking van de interne beheersmaatregelen voor de in de Verantwoordingsrichtlijn 2011 opgenomen normen.

BKWI voegt de afzonderlijke transparantierapportages samen tot één uniforme Totaalrapportage, zoals beschreven in de Verantwoordingsrichtlijn. Tot nu toe is dat niet goed mogelijk, omdat andere afnemers dan gemeenten deels over andere normen rapporteren. Daardoor ligt de nadruk in de

[1] “Opzet” en “bestaan” zijn EDP-audit-begrippen. Als de informatiebeveiligingsmaatregelen waarmee een organisatie aan een norm voldoet op een peildatum (in ons geval 31 december van het verantwoordingsjaar) functioneren, voldoet die organisatie in opzet en bestaan aan die norm. Als die maatregelen niet alleen op een peildatum, maar voor een heel tijdvak (in ons geval het hele verantwoordingsjaar) goed functioneren, is er naast opzet en bestaan ook sprake van “werking”. Die wordt bij gemeenten nu nog niet getoetst, bij andere afnemers wel.

[2] Die keuzemogelijkheid was een tegemoetkoming aan de niet-gemeentelijk afnemers in verband met de snel veranderende normenkaders (tot en met 2018 dat uit de Verantwoordingsrichtlijn 2011, in 2019 het Specifieke SUWI-normenkader in combinatie met de BIR en vanaf 2020 de BIO).

Totaalrapportage op bevindingen bij gemeenten, wat een onevenwichtig beeld geeft. Met de introductie van de BIO in 2020 is dit van de baan.

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 algemeen 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 bij gemeenten zo nodig via de toepassing van het Interventieprotocol Suwinet maatregelen nemen gericht op individuele partijen. Bij andere afnemers kan de verantwoordelijke minister binnen de planning- en control-cyclus maatregelen nemen.

## Conclusies

De conclusies in deze paragraaf zijn waar nodig voorzien van een duiding of enkele overwegingen. In algemene zin merkt de domeingroep op dat het bestaan van bevindingen (normafwijkingen) bij de verantwoording niet noodzakelijk betekent dat de informatiebeveiliging niet adequaat 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.

Verder biedt het verantwoordingssysteem dat nu is ingericht organisaties een groot aantal waarborgen voor het tijdig in kaart brengen en herstellen van bevindingen en het terugbrengen van de risico's die daarmee samenhangen. Daarnaast biedt de Totaalrapportage de domeingroep de gelegenheid om algemene maatregelen voor te stellen.

Hoewel nog niet alle normen door alle afnemers worden nageleefd, is er wel een verantwoordingssysteem ontstaan dat zicht geeft op verbeterpunten en waarborgen bevat om de normnaleving te verbeteren. Samen met verbeteringen in de rapportageprocedure, het beter hanteren van de beschikbare formats en de toegenomen ervaring bij gemeenten en hun auditors met de verantwoordingssystematiek, verklaart dit de ten opzichte van 2018 opnieuw verbeterde resultaten.

De conclusies en aanbevelingen die nu volgen hebben uitsluitend betrekking op de deelnemende gemeenten. De 7 overige afnemers zijn dit jaar nog niet meegenomen, omdat ze, zoals hierboven aangegeven, op een andere manier rapporteren. In het algemeen valt wel te vermelden dat 3 van hen geen bevindingen hebben gemeld.

<u>Aantal bevindingen verder gedaald/aantal gemeenten met 0 bevindingen opnieuw gestegen, maar wel minder dan voorgaande jaren</u>

Het valt op dat het aantal gemeenten dat geen bevindingen rapporteert in twee jaar is gestegen van 173 naar 273 naar 291, dus van 45,8% naar 79,1% naar 82%. In vergelijking met de Totaalrapportage van de twee voorgaande jaren valt verder op dat het totale aantal bevindingen bij de SUWI-taken[3] is teruggelopen van 646 naar 266 naar 233.

[3] Dus bij de uitvoering van de Participatiewet.

Aantal gemeenten met meer dan 4 bevindingen vrijwel gelijk

Het aantal gemeenten met 4 of meer bevindingen is, na een halvering tussen 2017 (16,7%) en 2018 (8,4%), in 2019 nagenoeg stabiel gebleven.

Verloop bevindingen per gemeente blijft grillig

Vorig jaar signaleerden we al dat, hoewel het aantal bevindingen gemiddeld genomen over alle gemeenten afneemt, individuele gemeenten soms nieuwe of andere bevindingen melden dan het voorgaande jaar. Dat is ook dit jaar niet veranderd. We hebben bijvoorbeeld vastgesteld dat het aantal gemeenten dat twee jaar achter elkaar twee of meer bevindingen heeft tussen 2018 en 2019 weliswaar gedaald is van 56 naar 21, maar dat 13 van die 21 gemeenten nieuw zijn in het overzicht.

Gebruik Suwinet zonder wettelijke grondslag

In 2018 rapporteerden 13 gemeenten ongevraagd dat zij gebruik hadden gemaakt van Suwinet bij de uitvoering van taken voor schuldhulpverlening of jeugdzorg. Voor dit gebruik bestaat geen wettelijke grondslag dus dat is onrechtmatig en de betreffende gemeenten zijn daarop gewezen. In 2019 was er nog maar één melding van onrechtmatig gebruik.

## Aanbevelingen

Op basis van de bovenstaande bevindingen, die zoals gezegd alleen betrekking hebben op gemeenten, doet de domeingroep de volgende aanbevelingen aan het Ketenoverleg:

1. Ga en blijf in gesprek met afnemers bij bevindingen. Niet-gemeentelijke afnemers, zoals UWV en SVB, hebben in hun P&C-cyclus voldoende gelegenheid om eventuele bevindingen met de systeemverantwoordelijke te bespreken. Het interventieprotocol biedt de stelselverantwoordelijke de mogelijkheid om ook met gemeenten in contact te treden als daar aanleiding toe is.
2. Bepaal een groeipad met een concrete einddatum voor een uniforme verantwoording (op basis van de BIO). De eerste stap daarin zou de uitbreiding van de verantwoording met ‘werking’[4] moeten zijn, de tweede de uitbreiding van de selectie van toe te passen normen. Op die manier ontstaat een compleet beeld van de informatiebeveiliging bij alle afnemers en wordt het beveiligingsniveau uniform, zoals de Regeling SUWI ook voorschrijft. Laat SZW en VNG hiervoor het initiatief nemen in overleg met de DPB: SZW als systeemverantwoordelijke, de VNG als vertegenwoordiger van de gemeenten, voor wie dit groeipad de grootste impact heeft, de DPB namens de overige afnemers.
3. Bepaal een acceptabel niveau van normnaleving voor alle afnemers. Het huidige niveau (bij gemeenten 82%) is niet optimaal, zeker voor een selectie van essentiële normen. Laat ook hier het ministerie en de VNG, in overleg met de DPB het initiatief nemen.
4. Breng de impact van de vorige twee maatregelen in kaart en ondersteun de afnemers bij het volgen van het groeipad en het bereiken van een acceptabel niveau van normnaleving. Het ENSIA-team van de VNG kan hiervoor het initiatief nemen.
5. Laat in de Totaalrapportage ook duidelijk de stand van de informatiebeveiliging bij niet-gemeentelijke afnemers zien. Hier kan BKWI voor zorgen.

[4] Zie de eerste voetnoot, derde zin.