Verantwoordingsrichtlijn GeVS 2020

1 Inleiding

Deze Verantwoordingsrichtlijn beschrijft de scope en procedure van verantwoording voor alle partijen die gebruik maken van de GeVS. Volgens het bepaalde in de artikelen 5.22 en 6.4 van de Regeling Suwi moeten UWV, SVB, Colleges van B&W, het Inlichtingenbureau en de op de GeVS aangesloten Suwi en niet Suwi partijen maatregelen treffen gericht op het waarborgen van een exclusieve, integere, beschikbare en controleerbare gegevensverwerking en zich daarover verantwoorden. Deze verantwoordingsrichtlijn bevat de gezamenlijke afspraken van de Suwi-partijen met betrekking tot de te hanteren normen voor informatiebeveiliging en de wijze waarop partijen verantwoording afleggen over de naleving daarvan. De Verantwoordingsrichtlijn GeVS 2020 vervangt de Verantwoordingsrichtlijn GeVS 2019.

De Verantwoordingsrichtlijn GeVS 2020 bestaat uit de volgende onderdelen:

- Doelstelling
- Wijzigingen ten opzichte van de Verantwoordingsrichtlijn GeVS 2019
- Doelgroep voor wie de verplichting geldt
- Een uitwerking van de aanpak
- Bijlage 1: scope van de verantwoording (het uitgewerkte BIO-normenkader).
- Bijlage 2: formats voor de transparantierapportage.

2 Doelstelling

De Suwi partijen bepalen gezamenlijk voor de GeVS het niveau van informatiebeveiliging.
Vanaf 1 januari 2020 geldt de Baseline Informatiebeveiliging Overheid (BIO). De BIO vervangt onder meer de BIG en de BIR en voorziet in een uniform en uitgebreid normenkader informatiebeveiliging voor de gehele overheidssector. Organisaties die de BIO (moeten) implementeren werken daarmee aan het verzekeren van een adequaat niveau van informatiebeveiliging.
Het Ketenoverleg heeft besloten dat vanaf 2020 dit niveau gebaseerd wordt op het normenkader van de BIO en verantwoording op basis daarvan moet plaatsvinden.

Iedere partij verantwoordt zich in het eigen jaarverslag en levert voor 1 mei van het kalenderjaar volgend op het verantwoordingsjaar een Transparantierapportage op aan BKWI ten behoeve van de Totaalrapportage. Aan de hand van de inhoud van de Totaalrapportage kan beoordeeld worden of de

informatiebeveiliging binnen de GeVS adequaat is en of alle afnemers voldoen aan het afgesproken beveiligingsniveau, dat is neergelegd in de specifiek van toepassing zijnde normen uit de BIO.

De beheerders van GeVS (BKWI en IB) verantwoorden zich voor 15 maart van het kalenderjaar volgend op het verantwoordingsjaar op het normenkader van de BIO.

3 Wijzigingen t.o.v. de Verantwoordingsrichtlijn GeVS 2019

Het uitgangspunt van de Verantwoordingsrichtlijn GeVS 2020 is dat de implementatie van de BIO door de organisaties, met een bijbehorend Basis Beveiligingsniveau 2, leidt tot het gewenste gemeenschappelijke beveiligingsniveau. De verantwoording is niet langer gerelateerd aan een specifiek Suwi Normenkader, maar gericht op de naleving van de door de BIO geformuleerde normen en maatregelen specifiek over het gebruik van Suwinet services en/of DKD.

In een bijlage bij deze Verantwoordingsrichtlijn zijn de BIO normen vastgelegd waarover de aangesloten partijen vanaf 2020 specifiek verantwoording moeten afleggen. Daarbij is aansluiting gezocht bij de door de Beheerorganisatie ENSIA reeds afgesproken normen voor gemeenten. Alle afnemers verantwoorden zich over opzet, bestaan en werking van de geselecteerde normen. Echter, voor gemeenten wordt het afgesproken groeipad gevolgd. Gemeenten verantwoorden zich slechts over opzet en bestaan van de normen. Voor 2020 gelden voor de verantwoording veertien BIO-normen die ook reeds onderdeel vormden van het specifieke Suwi normenkader dat geldt tot 2020.

4 Doelgroep voor wie de verplichting geldt

De goedkeuring en vaststelling van deze Verantwoordingsrichtlijn 2020 in het Ketenoverleg impliceert dat de afnemers die vertegenwoordigd zijn in het Ketenoverleg gehouden zijn jaarlijks tijdig een transparantierapportage op te leveren zoals beschreven in dit document inclusief bijlagen.

De verantwoordingsplicht is daarnaast ingevolge het Aansluitprotocol van toepassing op andere partijen die gebruik maken van de GeVS, de niet Suwi-partijen. Op deze wijze kan inzicht worden gegeven in het beveiligingsniveau van het gebruik van de Suwinet-services.

De scope van de verantwoording is de beveiligingsmaatregelen van alle gegevensuitwisselingen via de GeVS. Het gaat niet alleen om de services die door de beheerders van de GeVS beschikbaar worden gesteld, maar ook om het gebruik daarvan zowel door applicaties als door medewerkers. Ook wanneer taken zijn uitbesteed aan derden, zoals samenwerkingsverbanden vallen deze onder de verantwoordingsplicht. Datzelfde geldt voor verwerkingen van gegevens voor SUWI-taken en eventueel niet SUWI-taken op verschillende plaatsen in dezelfde organisatie.

Voor de beheerders (BKWI en IB) geldt tot 2020 een specifiek normenkader voor beheerders dat eveneens zal worden vervangen door de BIO. De verantwoordingsplicht voor beheerders is neergelegd in de SUWI-regeling. De beheerders moeten voor 15 maart van het kalenderjaar volgend

op het verantwoordingsjaar de resultaten van een EDP-audit verstrekken aan de minister van SZW, die daardoor adequaat toezicht kan houden op de informatiebeveiliging bij de beheerders van de GeVS. Deze resultaten maken geen onderdeel uit van de totaalrapportage die eerst in het najaar wordt aangeboden.

De verantwoordingsplicht geldt expliciet niet voor de levering van gegevens door partijen in hun rol van bronhouder.

De minister van SZW heeft een interventieprotocol opgesteld waarin wordt beschreven hoe SZW zal handelen wanneer niet voldaan wordt aan de verantwoordingsplicht of het niet naleven van het normenkader door gemeenten. Het protocol is ook van toepassing op SVB en UWV. De verantwoording over de beveiligingsmaatregelen van gegevensuitwisselingen via de GeVS door SVB en UWV valt echter samen met de reguliere P&C-cyclus, waardoor er geen aparte procedure hoeft te worden opgesteld. Eventuele interventies zullen via de instrumenten uit de P&C-cyclus vorm krijgen, zoals de dechargebrief n.a.v het jaarverslag.

5 Aanpak Verantwoording

Transparantie en verantwoording zijn instrumentele functies ten behoeve van de besturing. Transparantie is het bieden van informatie over sturing, implementatie en beheersingsaspecten van de gebruikte Suwinet services en/of DKD.

Verantwoording is een middel om over de mate van “in control zijn” een verklaring af te geven. Met die verklaring verstrekt de Raad van Bestuur van de ZBO aan de Minister van SZW of het College van B&W aan de Gemeenteraad het signaal greep te hebben op de sturing van de dienstverlening en de informatiebeveiliging.

Iedere afnemende partij verantwoordt zich in het eigen jaarverslag en levert voor 1 mei van het kalenderjaar volgend op het verantwoordingsjaar een Transparantierapportage aan BKWI.

Gemeenten

Gemeenten verantwoorden zich vanaf 2017 over informatiebeveiliging volgens de ENSIA-systematiek, die betrekking heeft op de beveiliging van alle gemeentelijke verwerkingen waarbij gebruik wordt gemaakt van de Suwinet services en/of DKD. De opzet is zodanig dat de op deze wijze tot stand gekomen verantwoording van het College van B&W aan de Gemeenteraad geschikt is om als basis te dienen voor de Transparantierapportage die bij BKWI moet worden ingediend. De transparantierapportage bestaat uit:

- Een in control verklaring van het College van Burgemeester en Wethouders
- Een getrouwheidsverklaring van een Register EDP-auditor.
- Indien van toepassing: een bijlage met een overzicht van de normen waaraan (m.b.t. Suwinet/DKD) niet wordt voldaan.

Op 1 mei van het jaar na het verantwoordingsjaar moeten de transparantierapportages zijn ontvangen door BKWI via ensia@bkwi.nl (levering via de ENSIA-portal).

De formats voor de documenten zijn voor gemeenten ook beschikbaar op www.ensia.nl.

Overige afnemers

Voor alle andere partijen (zowel Suwi- als niet Suwi-partijen) bestaat de transparantierapportage uit:

- Een in control verklaring van de bestuurder
- Een getrouwheidsverklaring van een Register EDP-auditor
- Een bijlage met een overzicht van de normen waaraan niet voldaan wordt

In bijlage 2 zijn formats opgenomen voor de in control verklaring inzake informatiebeveiliging GeVS en de (eventueel) bijbehorende bijlage.

Voor de getrouwheidsverklaring is geen format opgesteld. Hiervoor geldt als enige eis dat de naam en organisatie van de Register EDP-auditor moeten worden vermeld.

Afronding verantwoording

BKWI stelt aan de hand van de verstrekte transparantierapportages een Totaalrapportage op. De Domeingroep Privacy en Beveiliging maakt een toelichting op de bevindingen, trekt conclusies en doet aanbevelingen. De Totaalrapportage wordt voor 1 oktober van het jaar volgend op het verantwoordingsjaar door de voorzitter van het Ketenoverleg aangeboden aan de Minister van SZW.

Bijlage 1: Scope van de verantwoording: normenkader GeVS

Deze bijlage beschrijft aan welke normen (inclusief de bijbehorende subnormen) de interne beheersmaatregelen voor de GeVS worden getoetst en waarover gerapporteerd moet worden in de transparantierapportage. Interne beheersmaatregelen bij gemeenten dienen op de laatste dag van het jaar in opzet en bestaan aan de genoemde normen te voldoen, voor andere afnemers geldt dat voldaan moet worden aan opzet, bestaan en werking van de genoemde normen.

Hoofdstuk	Nummer	Normen
5. Informatiebeveiligingsbeleid	5.1.1.	Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.
5. Informatiebeveiligingsbeleid	5.1.2	Het beleid voor informatiebeveiliging behoort met geplande tussenpozen of als zich significante veranderingen voordoen, te worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.
6. Organiseren van informatiebeveiliging	6.1.1	Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.
6. Organiseren van informatiebeveiliging	6.1.2	Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.
7. Veilig personeel	7.2.2	Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.
9. Toegangsbeveiliging	9.2.1	Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.
9. Toegangsbeveiliging	9.2.2	Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.
9. Toegangsbeveiliging	9.2.5	Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.
9. Toegangsbeveiliging	9.2.6	De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast.
10. Cryptografie	10.1.1	Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.
12. Beveiliging bedrijfsvoering	12.1.1	Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben.
12. Beveiliging bedrijfsvoering	12.4.1	Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en

		informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.
12. Beveiliging bedrijfsvoering	12.4.2	Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.
18. Naleving	18.1.4	Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.

Bijlage 2: formats voor de transparantierapportage

Format voor de incontrolverklaring inzake informatiebeveiliging GeVS <jaartal>

Het bestuur van <naam organisatie> geeft met deze verklaring aan in hoeverre <naam organisatie> aan het normenkader GeVS (bijlage 1 van de Verantwoordingsrichtlijn 2020) voor <afnemers/beheerders> voldoet.

Reikwijdte verklaring
Deze verklaring betreft de verwerkingen van SUWI-gegevens en het gebruik van ondersteunende ICT-voorzieningen door <naam organisatie>, waarover assurance wordt gevraagd van een Register EDP-auditor. De verklaring omvat het gedurende het verantwoordingsjaar <jaartal> in opzet, bestaan en werking voldoen van de beheersingsmaatregelen aan het normenkader GeVS. De normen zijn geschikt voor het doel van deze verklaring. Deze verklaring is opgesteld ten behoeve van de totaalrapportage die door het ketenoverleg aan de minister van SZW wordt aangeboden.

Verklaring bestuurder
<Indien volledig wordt voldaan de normen: De bestuurder verklaart dat bij <naam organisatie> in voor <jaartal> de beoogde en ingerichte beheersingsmaatregelen voldoen aan het normenkader GeVS.> <Bij uitzonderingen: De bestuurder verklaart dat niet aan alle geselecteerde normen in het normenkader GeVS wordt voldaan. De op de uitzonderingen gerichte beheersmaatregelen zijn in een verbeterplan opgenomen, zijn belegd en worden gemonitord>.

[Plaats, datum]

[Bestuurder]

Format voor de bijlage bij de incontrolverklaring inzake informatiebeveiliging GeVS <jaartal>

Deze bijlage is een afzonderlijk onderdeel van de Incontrolverklaring inzake informatiebeveiliging GeVS <jaartal> van <naam organisatie>. Deze verklaring heeft betrekking op het in het verantwoordingsjaar <jaartal> in opzet, bestaan en werking voldoen van de beheersingsmaatregelen van het normenkader GeVS. Deze bijlage is opgesteld ten behoeve van de totaalrapportage die door het ketenoverleg aan de minister van SZW wordt aangeboden.

Onderwerp van de verklaring is het <gebruik / beheer> van de Gemeenschappelijke elektronische Voorzieningen SUWI (GeVS).

Normnaleving

<indien geen afwijkingen van de normen:

Zoals in de bestuurdersverklaring vermeld, voldoen de interne beheersmaatregelen inzake de GeVS voor het verantwoordingsjaar <jaartal> in opzet, bestaan en werking aan alle normen.>

<bij afwijkingen van de normen:

Met uitzondering van de volgende normen voldoen de interne beheersingsmaatregelen voor de GeVS voor verantwoordingsjaar <jaartal> in opzet, bestaan en werking aan alle normen:

Control/maatregel nummer BIO	Applicatie
…	<Suwinet-Inkijk> of <Suwinet-Inlezen in combinatie met <naam inleesapplicatie>>

>