Verantwoordingsrichtlijn GeVS 2019 (versie 1.2[1])

Doelstelling

Het doel van deze verantwoordingsrichtlijn is het vastleggen van de gezamenlijk te hanteren beveiligingsnormen en van de gezamenlijke afspraken over de wijze waarop partijen verantwoording afleggen en transparantie bieden over de informatiebeveiliging van de GeVS[2].

Iedere partij verantwoordt zich in het jaarverslag en levert daarnaast voor 1 mei een Transparantierapportage[3] aan BKWI. BKWI voegt de afzonderlijke verantwoordingen samen tot één Totaalrapportage[4], die de stelselverantwoordelijke voor de GeVS (de minister van SZW) en het Ketenoverleg[5] inzicht geven in het gemeenschappelijke niveau van privacybescherming[6] en informatiebeveiliging van de GeVS.

Doelgroep

De verantwoordingsplicht is van toepassing op de afnemers (partijen die gegevens opvragen) en op de beheerders van de GeVS, maar niet voor bronhouders (partijen die gegevens leveren). Onder de afnemers vallen zowel SUWI- als niet-SUWI-partijen.

Achtergrond

Toen de Verantwoordingsrichtlijn GeVS 2011 werd opgesteld, waren er nog geen baselines informatiebeveiliging voor overheidsorganisaties, zoals de Baseline Informatiebeveiliging Rijksdienst (BIR) en de Baseline Informatiebeveiliging Gemeenten (BIG). Daarom bevatte de oude verantwoordingsrichtlijn, behalve een beschrijving van het verantwoordingsproces, ook een compleet normenkader op maat gesneden voor de GeVS.

Dat is vanaf 2012 veranderd met de invoering van de BIR en de BIG. Daarom is in 2016 het normenkader uit de vorige verantwoordingsrichtlijn naast deze baselines gelegd en ge-update. Dat heeft twee specifieke normenkaders voor de GeVS opgeleverd – één voor beheerders en één voor

---

[1] Deze versie is vastgesteld door het Ketenoverleg van 22 november 2018

[2] Gemeenschappelijke elektronische Voorzieningen SUWI

[3] Zoals beschreven in criterium C.08 van het Specifieke SUWI-normenkader voor Afnemers en criterium C.09 van het Specifieke SUWI-normenkader voor Beheerders

[4] Zoals beschreven in resp C.09 en C.10 van de in de vorige noot genoemde normenkaders

[5] Het ketenoverleg is het overleg waarnaar verwezen wordt in bij Bijlage I van de Regeling SUWI. Hierin maken het ministerie van SZW, UWV, SVB, VNG, BKWI en Inlichtingenbureau afspraken over onder meer de informatiebeveiliging van de GeVS.

[6] Privacybescherming komt verder niet afzonderlijk aan de orde in deze richtlijn. De AVG kent geen verantwoordingsregime dat vergelijkbaar is met wat in de informatiebeveiliging gebruikelijk is. Wel beschermt een groot aantal normen in de baselines en het Specifieke SUWI-normenkader direct en indirect de verwerking van persoonsgegevens door op de GeVS aangesloten partijen.

afnemers – die bedoeld zijn om in combinatie met de BIR of de BIG te worden gebruikt. De nieuwe, specifieke normenkaders zijn afzonderlijk gepubliceerd.

In april 2017 is het Specifieke SUWI-normenkader voor Afnemers in werking getreden voor gemeenten, die zich daarover verantwoorden volgens de ENSIA-systematiek[7]. Gemeenten hebben begin 2018 voor het eerst verantwoording afgelegd volgens deze nieuwe systematiek en volgens het nieuwe normenkader over verantwoordingsjaar 2017.

Met ingang van 2019 gaan ook de andere afnemers en de beheerders van de GeVS zich verantwoorden over de nieuwe Specifieke SUWI-Normenkaders. Deze verantwoordingsrichtlijn beschrijft dit proces en vervangt de Verantwoordingsrichtlijn GeVS 2011.

Wijzigingen

Er zijn twee belangrijke verschillen met de vorige versie van het normenkader. Het eerste is dat er twee nieuwe normenkaders zijn, die apart worden gepubliceerd op de website van BKWI, hoewel ze formeel onderdeel zijn van deze richtlijn. Het andere is dat het achterliggend onderzoek niet meer wordt beschreven.

Transparantierapportage en Totaalrapportage

Iedere partij die op de GeVS is aangesloten stelt een Transparantierapportage op. Deze rapportage geeft inzicht in de stand van de informatiebeveiliging bij die partij.

BKWI aggregeert de transparantierapportages tot een Totaalrapportage, gericht aan het Ketenoverleg en de minister. De totaalrapportage geeft inzicht in de stand van de informatiebeveiliging van de GeVS.

Gemeenten

Gemeenten verantwoorden zich met ingang van 2017 over informatiebeveiliging volgens de ENSIA-systematiek. Die heeft betrekking op de beveiliging van alle gemeentelijke verwerkingen, niet alleen de GeVS, en is ook op de eerste plaats de verantwoording van het College aan B&W aan de gemeenteraad. Hij is wel zo opgezet dat er een Transparantierapportage bij BKWI wordt ingediend die voldoet aan norm C.08 in het specifieke normenkader voor afnemers.

Die transparantierapportage bestaat uit een incontrolverklaring van het College van Burgemeester en Wethouders, een Suwinet-bijlage met een overzicht van de normen waar niet aan wordt voldaan en een getrouwheidsverklaring van een Register EDP-auditor.

Overige afnemers en beheerders

Voor alle andere partijen bestaat de transparantierapportage uit:

- Een incontrolverklaring van de bestuurder
- Een getrouwheidsverklaring van een Register EDP-auditor
- Een bijlage met een overzicht van de normen waar niet aan wordt voldaan
- Evaluaties van de beleids-, implementatie en beheersingsmaatregelen met betrekking tot opzet, bestaan en werking

[7] ENSIA staat voor Eenduidige Normatiek, Single Information Audit. Dit verantwoordingsstelsel omvat de informatiebeveiliging van gemeenten in het algemeen met specifieke aandacht voor het gebruik van de GeVS.

Totaalrapportage

De verantwoordingsdocumenten over het voorafgaande verantwoordingsjaar van alle aangesloten partijen worden ieder jaar na 1 mei door BKWI verwerkt tot een totaalrapportage, die wordt aangeboden aan het Ketenoverleg.

De totaalrapportage is gebaseerd op de bijlagen bij de incontrolverklaring van Colleges, respectievelijk bestuurders, waarin de normen waarvan wordt afgeweken zijn opgenomen. De totaalrapportage bevat een geaggregeerd overzicht.

De Domeingroep Privacy & Beveiliging stelt een toelichting op bij de rapportage, trekt conclusies en doet aanbevelingen aan het Ketenoverleg. Conclusies en aanbevelingen hebben nooit betrekking op individuele organisaties.

Het doel van de totaalrapportage is om te kunnen beoordelen of de informatiebeveiliging binnen de GeVS uniform is en op het afgesproken niveau ligt en, als dat niet zo is, of daar alleen algemene maatregelen voor nodig zijn. Dergelijke maatregelen zijn ondersteunend en aanvullend op de maatregelen van het Interventieprotocol van de minister van SZW.

De voorzitter van het Ketenoverleg biedt de Totaalrapportage tenslotte, voorzien van een bestuurlijke reactie van SVB, UWV en VNG aan aan de stelselverantwoordelijke, de minister van SZW.

Deadline voor de Transparantierapportage

Op 1 mei van het jaar na het verantwoordingsjaar moeten alle transparantierapportages binnen zijn bij BKWI via ensia@bkwi.nl (gemeenten leveren de verantwoording ook in via de ENSIA-portal)

Interventies

De minister van SZW heeft een interventieprotocol opgesteld en als volgt toegelicht: "*Dit protocol beschrijft de wijze waarop door de minister van SZW gehandeld zal worden bij het niet voldoen aan de verantwoordingsplicht of het niet naleven van het normenkader t.a.v. Suwinet door gemeenten. Het protocol heeft tevens werking op UWV en SVB, waarvoor hetzelfde juridische kader geldt, inclusief aanwijzingsbevoegdheid. De verantwoording over de Suwi-normen door UWV en SVB valt echter samen met de reguliere P&C-cyclus, waardoor er geen aparte procedure hoeft te worden opgesteld. Eventuele interventies zullen dan ook via de instrumenten uit de P&C-cyclus vorm krijgen, zoals de dechargebrief n.a.v. het jaarverslag.*"

Grondslag voor de verantwoording

De wettelijke basis voor de verantwoording door SUWI-partijen is opgenomen in de regeling SUWI art. 5.22 voor gegevensverwerking en artikel 6.4 voor gegevensuitwisseling en uitgewerkt in Bijlage I van de Regeling SUWI behorend bij art. 6.4.

Voor niet-SUWI-partijen is artikel 5.23 van het Besluit SUWI de basis. Dit artikel wordt uitgewerkt in het Aansluitprotocol (Bijlage III van de Regeling SUWI). Het aansluitprotocol voorziet weer in een gegevensleveringsovereenkomst tussen bron, afnemer van SUWI-gegevens en BKWI. Gemeenten kunnen overigens tegelijk SUWI- en niet-SUWI-partij[8] zijn.

[8] Gemeenten worden beschouwd als niet-SUWI-partij als ze de GeVS gebruiken voor taken die niet opgenomen zijn de in Participatiewet, IOAZ of IOAW. Bijvoorbeeld als een afdeling Burgerzaken de GeVS gebruikt om een adres te controleren.

De normenkaders en de verantwoordingsrichtlijn, waarin het uniforme beveiligingsniveau binnen de GeVS en de verantwoording daarover worden beschreven, worden op grond van Bijlage I van de Regeling SUWI door de SUWI-partijen vastgesteld in het Ketenoverleg (Bijlage I, regeling SUWI).

Normenkaders

Normenkaders leggen het gewenste niveau van informatiebeveiliging vast en zijn daarmee de basis voor de verantwoording. Elke organisatie die SUWI-gegevens verwerkt is gehouden aan:

- Het binnen de sector gebruikelijke normenkader (zoals de BIR, de BIG, straks de BIO[9]) of een ander op ISO 27001 en 27002 gebaseerd normenkader.
- Het SUWI (GeVS)-specifieke normenkader voor afnemers of beheerders, naargelang de organisatie afnemer of beheerder is.

Deze normenkaders vormen een geheel, waarbij het sectorbrede normenkader de informatiebeveiliging in het algemeen regelt (object-onafhankelijk) en het specifieke SUWI-normenkader aanvullende maatregelen of verdiepende maatregelen toevoegt voor het object GeVS. De specifieke SUWI-normenkaders worden gepubliceerd op www.bkwi.nl.

Aanpak van de verantwoording

Vorm van de verantwoording[10]

Formats voor de verantwoording voor gemeenten zijn te vinden op www.ensia.nl.

Andere afnemers en beheerders maken gebruik van de bij deze verantwoordingsrichtlijn gevoegde formats voor de incontrolverklaring inzake Informatiebeveiliging GeVS en de bijbehorende bijlage. Voor de getrouwheidsverklaring is geen format opgesteld. Hiervoor geldt als enige eis dat naam en organisatie van de Register EDP-auditor worden vermeld.

Object

Het object van de verantwoording zijn alle verwerkingen van gegevens via de GeVS en alle ICT-voorzieningen die daarvoor worden ingezet overeenkomstig de voor afnemers en beheerders opgestelde normenkaders Het gaat dus niet alleen om de services die door de beheerders van de GeVS ter beschikking worden gesteld, maar ook om het gebruik daarvan, zowel door applicaties als door medewerkers. Daarbij valt naast aan Suwinet-Inkijk ook te denken aan applicaties die gebruik maken van Suwinet-Inlezen en DKD-Inlezen.

Wanneer taken zijn uitbesteed aan derden, zoals samenwerkingsverbanden, zijn die ook object van de verantwoording. Datzelfde geldt voor verwerkingen van gegevens voor SUWI-taken en eventueel niet-SUWI-taken op verschillende plaatsen in dezelfde organisatie.

Het volledig beschrijven van de reikwijdte van het object is dus een belangrijke voorbereidende stap voor de verantwoording.

Scope

Voor afnemers die geen gemeente zijn en voor beheerders wordt met ingang van verantwoordingsjaar 2019 verantwoording gevraagd over opzet, bestaan en werking van alle in het

[9] Baseline Informatiebeveiliging Overheid. Deze baseline vervangt de BIR en de BIG

[10] Zie ook Specifiek Suwinet-normenkader Afnemers, norm C.08, resp. Specifiek Suwinet-normenkader Beheerders, norm C.09

Specifieke SUWI-normenkader voor afnemers, respectievelijk beheerders opgenomen normen gedurende het hele verantwoordingsjaar.

Voor gemeenten is door de Beheerorganisatie ENSIA een groeipad afgesproken: in 2017 hebben ze zich verantwoord over opzet en bestaan van een 11-tal SUWI-normen op 31 december van het verantwoordingsjaar. Deze scope wordt stap voor stap uitgebreid totdat hij gelijk is voor alle afnemers.

Onderzoek

Een Register EDP-auditor onderzoekt of de incontrolverklaring een getrouw beeld geeft. Bij de interpretatie van de normenkaders is het volgende van belang:

- De conformiteitsindicatoren zijn vrijblijvend: ze kunnen behulpzaam zijn bij onderzoek en implementatie, maar invoering is niet verplicht.
- De normen[11] worden *principle based* [12]geïnterpreteerd.
- Er is ruimte voor *comply or explain*: een organisatie kan beargumenteerd afzien van het implementeren van een norm. Het is aan de auditor om de argumentatie te toetsen.

[11] Het normenkader gebruikt hiervoor de afwijkende term “criterium”.

[12] Principle based: de norm kan risicogebaseerd globaal worden ingevuld t.b.v. wat is geregeld. Dit staat tegenover rule based wat dwingend is voorgeschreven, compliancegericht is en niet de risicobeheersing leidend heeft. De nadruk komt daarmee te liggen op het toepassen van de juiste context, de relevante normen daarvoor te selecteren en een beeld weer te geven op basis van de conformiteitsindicatoren.

Format voor de incontrolverklaring inzake informatiebeveiliging GeVS <jaartal>

Het bestuur van <naam organisatie> geeft met deze verklaring aan in hoeverre <naam organisatie> aan het geldende Specifiek SUWI-normenkader 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 Specifieke SUWI-normenkader. De normen zijn geschikt voor het doel van deze verklaring.

Deze verklaring is opgesteld voor het departement dat toeziet op de veiligheid van de Gemeenschappelijke elektronische Voorzieningen SUWI.

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 Specifieke SUWI-normenkader.> <Bij uitzonderingen: De bestuurder verklaart dat niet aan alle geselecteerde normen in het Specifieke SUWI-normenkader 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 aan het Specifieke SUWI-normenkader <Afnemers/Beheerders> Deze bijlage is opgesteld voor het Ministerie van Sociale Zaken en Werkgelegenheid.

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:

SUWI-nummer	Applicatie
…	<Suwinet-Inkijk> of <Suwinet-Inlezen in combinatie met <naam inleesapplicatie>>

>

Wettelijk kader Regeling SUWI § 5.3. Rapportage gegevensverwerking

Artikel 5.22. Verantwoording gegevensverwerking

1. Het UWV, de SVB en het IB rapporteren vóór 15 maart van elk jaar over de opzet en werking van het stelsel van maatregelen en procedures, gericht op het waarborgen van een exclusieve, integere, beschikbare en controleerbare gegevensverwerking.

2. De rapportage wordt vergezeld van een oordeel van een tot de Nederlandse Orde van Register EDP-Auditors toegelaten persoon of van een verklaring van getrouwheid van een dergelijke persoon.

Artikel 6.4. Beveiliging elektronische voorzieningen SUWI

1. Het UWV, de SVB, de colleges van burgemeester en wethouders, het IB en op de gezamenlijke elektronische voorzieningen SUWI aangesloten niet SUWI-partijen dragen zorg voor de beveiliging van de gegevensuitwisselingen die plaatsvinden in het kader van de gezamenlijke elektronische voorzieningen SUWI, tegen inbreuk op de beschikbaarheid, integriteit en vertrouwelijkheid, overeenkomstig hetgeen over de voor het stelsel van maatregelen en procedures te hanteren normen wordt bepaald in bijlage I (â€˜Stelselontwerp & Beveiliging Gezamenlijke elektronische Voorzieningen SUWIâ€™).

2. Het UWV, de SVB, de colleges van burgemeester en wethouders, het IB en op de gezamenlijke elektronische voorzieningen SUWI aangesloten niet- SUWI- partijen geven ieder in een beveiligingsplan aan op welke wijze zij invulling geven aan het eerste lid.

3. Artikel 5.22 is van overeenkomstige toepassing op het gebruik en de inrichting van de gezamenlijke elektronische voorzieningen SUWI.

Bijlage 1 Regeling SUWI

2.3 Uitgangspunt & ketenproduct

Eén gezamenlijk, transparant en uniform niveau van betrouwbaarheid in termen van Beschikbaarheid, Integriteit en Vertrouwelijkheid; de Verantwoordingsrichtlijn Privacy& Beveiliging GeVS

De Verantwoordingsrichtlijn (privacy en beveiliging van de GeVS) is een gezamenlijk product van de SUWI-partijen en de beheerder van de centrale voorziening welke, op basis van de wettelijke voorschriften rondom privacy en beveiliging, vorm en inhoud is gegeven. Het bevat de normen, criteria en vormvereisten op basis waarvan het oordeel dan wel de verklaring van getrouwheid (ex. art 5.22 regeling SUWI) over de privacy en beveiliging van de GeVS in de Jaarverslagen van de op de GeVS aangesloten ontvangende partijen en de beheerder van de centrale voorziening wordt onderbouwd. In het Jaarverslag wordt daartoe een aparte, als zodanig herkenbare, paragraaf gewijd aan de privacy en beveiliging van de GeVS waarin, waar nodig, verbetermaatregelen worden benoemd.

Bij wijziging wordt de Verantwoordingsrichtlijn voor akkoord voorgelegd aan het ketenoverleg, gehoord de Inspectie Werk en Inkomen.