VNG Realisatie

Handreiking controle op rechtmatig gebruik Suwinet bij onbekende BSN

Voor Security Officers en gemandateerden van (I)GSD-en

1. Inleiding

Vraag: Mag een Security Officer of gemandateerde zelf gebruik maken van Suwinet bij de controle op misbruik en oneigenlijk gebruik van Suwinet door de medewerkers?
Antwoord: Ja, dat mag onder bepaalde voorwaarden.

In deze handreiking vindt u de juridische onderbouwing van dit antwoord en hoe autorisatie hiertoe vormgegeven kan worden.

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. Hiervoor volgen partijen de verantwoordingsrichtlijn GeVS[i].

Uit deze verantwoordingsrichtlijn vloeit, simpel gezegd, voort dat de interne controle op orde dient te zijn. Het betreft daarbij de uitvoering van de Participatiewet en daaruit voortvloeiend tevens de controle op eventueel onrechtmatig gebruik van Suwinet (en daarmee ook het gebruik van de escape functie). De verantwoordingsrichtlijn GeVS is gebaseerd op de BIO (waarin tevens de AVG-bepalingen zijn verwerkt). Artikel 32 AVG vraagt van gemeenten een passend informatiebeveiligingsbeleid en de daarbij horende maatregelen om dit te waarborgen. Dit is in lijn met de Verantwoordingsrichtlijn.

Controles op het rechtmatig gebruik van Suwinet vinden plaats aan de hand van de logbestanden in de specifieke gebruikersrapportage Suwinet. Deze logbestanden bevatten enkel de geraadpleegde BSN's. Maar als het geraadpleegde BSN niet bekend is, dan is zonder de identificatie op persoonsniveau van het BSN, onrechtmatig gebruik van Suwinet-Inkijk vrijwel niet vast te stellen.

Om aantoonbaar te kunnen voldoen aan artikel 32 AVG is een actieve en regelmatige controle van de logbestanden noodzakelijk. Belangrijk is dat de uitvoering van deze controle onafhankelijk gepositioneerd is ten opzichte van de gebruikers van Suwinet (functiescheiding).
Bij deze controles mag, ter identificatie van het BSN, de Security Officer of een andere gemandateerde, Suwinet-Inkijk raadplegen.

In het volgende hoofdstuk schetsen we eerst de situatie. Daarna gaan we in op de wijze van inbedding van de controle, namelijk door een aparte autorisatierol toe te voegen aan de autorisatiematrix, specifiek voor deze controles. Tenslotte geven we het wettelijk kader weer.

2. Situatieschets

2.1 De uitvoering

Het gebruik van Suwinet is (onder meer) begrensd door de bepaling dat het raadplegen van persoonsgegevens gebonden is aan wettelijke bepalingen: er moet sprake zijn van een noodzaak en/of een gerechtvaardigd doel die ten grondslag ligt aan het verwerken van persoonsgegevens. Vertaald naar de gemeentelijke uitvoeringspraktijk betekent dit dat raadpleging van gegevens alleen is toegestaan wanneer er sprake is van een directe dienstverleningsrelatie met een burger, waarvoor gegevens moeten worden verzameld om te komen tot een besluit. Daarbij mag de gemeente alleen die gegevens raadplegen en vastleggen die relevant zijn voor de (ondersteunings)vraag van de burger (proportionaliteit). Vastlegging vindt plaats in het bedrijfssysteem van de gemeente.

Wanneer een in Suwinet geraadpleegd BSN – alle bevragingen in Suwinet worden gelogd - ook voorkomt in dat bedrijfssysteem, is in ieder geval vastgesteld dat er sprake is of is geweest van een dienstverleningsrelatie en is verder onderzoek naar de rechtmatigheid van de bevraging niet direct voor de hand liggend.

Om verschillende redenen kan het noodzakelijk zijn om toch gegevens te bekijken van een burger wiens BSN (nog) niet voorkomt in het eigen klantenbestand van de gemeente. Omdat het BSN (nog) niet voorkomt in het bedrijfssysteem van de gemeente, is niet direct vast te stellen of er sprake is geweest van een rechtmatige bevraging.

NB.: Een groot gedeelte van de gemeenten werkt met een whitelist, waardoor de toegang tot Suwinet-inkijk beperkt is tot de BSN's van burgers waarmee de gemeente een dienstverleningsrelatie heeft of heeft gehad. Een BSN raadplegen dat niet voorkomt op die whitelist, kan alleen door gebruik te maken van de zogenaamde escape. Er vindt ook logging plaats van gebruik van de escape-functie.

2.2 De Security Officer of gemandateerden

Gemeentelijke Security Officers of andere gemandateerden zien toe op een juist gebruik van Suwinet. Hierbij maken zij gebruik van de door het BKWI beschikbaar gestelde generieke- en specifieke gebruiksrapportages met log-informatie. De rapportage kan signalen bevatten over mogelijk onrechtmatig gebruik. Ook het gebruik van de escapefunctie kan daarop wijzen. Daarom is vaak de meer toegespitste, specifieke rapportage over het gebruik van Suwinet door de Security Officer betrokken bij de interne controle.

2.3 Rapportage en controle

In de specifieke rapportage is aan de hand van de log-informatie te lezen welke medewerker op welk moment een BSN heeft geraadpleegd. Om vast te kunnen stellen waarom een BSN – al dan niet terecht of onterecht - geraadpleegd is, kan de Security Officer of gemandateerde de medewerker vragen naar de reden van een raadpleging. Daarbij doet zich het probleem voor dat medewerkers in de meeste gevallen het BSN niet zullen herkennen of herinneren omdat identificerende gegevens bij dat BSN niet aanwezig zijn in de rapportage. Dit komt geregeld voor bij

een bevraging van een BSN die op zich terecht was, maar die niet heeft geleid tot opname van dat BSN in het bedrijfssysteem.
Denk daarbij bijvoorbeeld aan:

- Onderzoek bij terugvordering op niet aansprakelijke derden;
- Een aanvraag die niet leidde tot een uitkering omdat er geen recht bleek te zijn (afwijzingen, intrekkingen);
- Onderzoek naar de inkomsten van een inwonende 17-jarige die zelf geen subject van bijstand zijn;
- Onderzoek voor het vaststellen van onderhoudsbijdrage waarbij af wordt gezien van het opleggen van een bijdrage;
- (Belasting)signaalafhandeling die betrekking hebben op BSN waarvan de uitkering langer geleden is beëindigd (en die niet meer op de whitelist staan).

Wanneer de Security Officer of gemandateerde de medewerker bevraagt aan de hand van de specifieke gebruikersrapportage, is het voor medewerkers niet mogelijk om het opgevraagde BSN te herkennen en te koppelen aan een persoon. Verdere identificerende gegevens ontbreken in de rapportage. Het is dus niet op voorhand duidelijk voor zowel de medewerker als de Security Officer, welke persoon geraadpleegd is. Dit is wel van belang voor de interne controle en het oordeel of de medewerker de desbetreffende persoon al dan niet rechtmatig heeft geraadpleegd.

2.4 Conclusie

Systematische controle op de logbestanden zelf is van belang om onrechtmatige raadpleging van persoonsgegevens te kunnen achterhalen. Een raadpleging controleren op rechtmatigheid kan alleen wanneer het bevraagde BSN is gekoppeld aan (tenminste) de naam van een klant, zodat bij de betreffende medewerker kan worden achterhaald met welke reden deze raadpleging heeft plaatsgevonden.

3. Controlemogelijkheden

Op grond van de AVG is er de mogelijkheid c.q. de verplichting om passende technische en organisatorische maatregelen te treffen. Het is wettelijk verplicht om alle raadplegingen bij te houden middels logbestanden, zodat onbevoegde toegang kan worden opgespoord en stappen kunnen worden ondernomen.

NB: De Autoriteit Persoonsgegevens (AP) geeft aan dat organisaties – om te voldoen aan de NEN 7510-2 – systematische controle op de logging zelf moeten verrichten. Dit houdt onder meer in dat de organisatie toegang tot de persoonsgegevens van geautoriseerde buiten de behandelrelatie om moet controleren. Deze aanwijzing verwijst naar artikel 32 waarin gesproken wordt over passende technische en organisatorische maatregelen.

De gegevens die via Suwinet te raadplegen zijn, zijn dusdanig gevoelig van aard dat gemeenten hier passende beveiligingsmaatregelen voor dienen te treffen. Gemeenten dienen in het verlengde hiervan de logbestanden regelmatig te controleren op ongeoorloofde raadplegingen.
Raadplegingen zijn alleen geoorloofd wanneer deze noodzakelijk zijn voor de uitvoering van de wettelijke taken binnen de Participatiewet, IOAW en IOAZ.

Om de logbestanden daadwerkelijk te controleren is een uitvraag van het BRP noodzakelijk. Het gaat daarbij om de gevallen waarin een eerdere raadpleging niet heeft geleid tot opname in het klantsysteem. Deze opvraag tijdens de controle is noodzakelijk voor het uitvoeren van het onderzoek. Immers de eerste opvraag door de consulent/medewerker op basis van het Autorisatiebesluit heeft niet direct geleid tot opname in het klantsysteem (die data is direct vernietigd conform de AVG). Echter om zeker te weten dat de eerste opvraging niet onnodig was, is een naam naast het BSN noodzakelijk. Een oplossing kan zijn om de oorspronkelijke data langer te bewaren in afwachting van het onderzoek. Of om gedurende het onderzoek slechts die informatie op te vragen die noodzakelijk is voor het onderzoek (officieel dus een tweede opvraging van dezelfde data in het BRP). De maatregel om vanuit controle een tweede opvraging te doen van slechts één van de gegevens van het BRP (namelijk het gegeven naam) is derhalve minder ingrijpend en richt zich op hetgeen echt noodzakelijk is waardoor voldaan is aan subsidiariteit.

Een tweede opvraging BRP voor het achterhalen van identificerende gegevens bij een onbekend BSN kan op twee manieren:

1) Via Suwinet-Inkijk door een bevraging te doen op de pagina BRP.
   De gemeente kan een aparte autorisatierol aanmaken in de gebruikersadministratie van Suwinet-Inkijk voor bedoelde controle doeleinden.
   Daarbij is van belang dat deze taak wordt opgenomen in het autorisatiebeleid (autorisatiematrix) conform de vastgestelde autorisatieprocedure en rekening houdend met functiescheiding. Op die manier kan de gemeente voldoen aan artikel 32 AVG en indicaties van onrechtmatige toegang of onrechtmatig gebruik van persoonsgegevens controleren en waar nodig actie ondernemen door de verantwoordelijke.

2) Door direct een bevraging in de (gemeentelijke) BRP te doen.
   Het ophalen van identificerende gegevens bij het BSN zoals naam en adres kan de gemeente mogelijk via de eigen BRP-aansluiting terugvinden. Zie ook de verhouding tussen BRP en AVG in hoofdstuk 4, Wettelijk kader.

Tip.

Maak in de Suwi gebruikersadministratie een aparte en goed herkenbare autorisatierol aan met daarin alleen de (beperkte) BRP-pagina. Laat u niet leiden door uitzonderingen. Vaak is alleen de naam en het adres nodig. Dan kunt u volstaan met een autorisatie voor de pagina met beperkte BRP-gegevens.

4. Wettelijk kader

Artikel 32 AVG

Ingevolge artikel 32, eerste lid, van de AVG treft de verwerkingsverantwoordelijke[...], rekening houdend met de stand van de techniek, de uitvoeringskosten, als ook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de recht en vrijheden van personen, passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen [..].
Ingevolge het tweede lid wordt bij de beoordeling van het passende beveiligingsniveau met name rekening gehouden met de verwerkingsrisico's, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig.

De verhouding tussen de BRP en AVG

De AVG is een Europese Verordening. De Verordening heeft rechtstreekse werking in de EU en geldt zonder dat omzetting in nationale wetgeving vereist is. Hierdoor is de AVG ook van toepassing op de verwerkingen die voortvloeien uit de wet BRP. De AVG geeft beperkt ruimte aan de Nederlandse wetgever om bepaalde regels en onderwerpen verder uit te werken. In Nederland staat deze, specifiek voor Nederland, uitwerking in de Uitvoeringswet Algemene Verordening Gegevensbescherming. Deze wet beschrijft in artikel 2 dat 'deze wet' niet van toepassing is op de verwerking van persoonsgegevens die is geregeld bij of krachtens de wet BRP. Met 'deze wet' wordt in dit geval de Uitvoeringswet bedoeld en niet de AVG. De memorie van toelichting van de UAVG beschrijft dat de UAVG niet van toepassing is op de wet BRP, omdat in de wet BRP zelfstandig uitvoering zal worden gegeven aan de verordening, gelet op de bijzondere context waarin de verwerking van persoonsgegevens plaatsvindt[ii].

In de AVG bevinden zich een aantal aanvullende regels voor het verwerken van persoonsgegevens bij de BRP. Het gaat daarbij om situaties die niet in de Wet BRP zelf zijn geregeld. Denk aan het verwerkingsregister, het aanwijzen van een FG en dergelijke. Onverminderd moeten ontvangers van persoonsgegevens uit de BRP zich in zijn geheel aan de AVG houden en/of aan andere specifieke wetgeving zoals de Participatiewet en Regeling SUWI[iii].

Derhalve moeten deze partijen zich ook houden aan artikel 32 AVG. Om zorg te dragen voor een passend beveiligingsniveau en de daarvoor benodigde controles uit te voeren zal de gemeente BRP-gegevens moeten inzien.

De gemeente zelf kan BRP-gegevens van haar eigen inwoners gebruiken, bijvoorbeeld voor de gemeentelijke belastingdienst of de gemeentelijke sociale dienst. De gemeente is verplicht deze gegevensverstrekking in een gemeentelijke verordening vast te leggen (zie art 3.8 BRP)[iv]

Gemeenschappelijke Regelingen vallen onder artikel 3.8 BRP

1. Bij of krachtens gemeentelijke verordening kunnen regels gesteld worden omtrent de verstrekking van gegevens aan overheidsorganen die een orgaan zijn van de gemeente.
2. Aan een overheidsorgaan worden slechts gegevens verstrekt voor zover deze gegevens noodzakelijk zijn voor de goede vervulling van zijn taak[v].

Deze bepaling is niet nieuw voor gemeentelijke sociale diensten. Zoals opgenomen in de Autorisatiebesluiten van de BRP dienen de taken in het geval van een gemeentelijke sociale dienst

en/of regionale sociale dienst opgenomen te zijn in de gemeenschappelijke regeling. Hierdoor zal aan dit vereiste in de praktijk doorgaans al voldaan zijn.

Resteert de vraag wanneer gegevens op grond van de BRP verzocht kunnen worden.

Het samenwerkingsverband ontvangt de gegevens ter uitvoering van de volgende wettelijke taken:

a) Bijstandstaken (Participatiewet, de Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte werkloze werknemers (IOAW), de Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen (IOAZ);
b) Tegemoetkoming kinderopvang (Wet kinderopvang en kwaliteitseisen peuterspeelzalen);
c) Inburgering (Wet Inburgering, Besluit brede doeluitkering sociaal, integratie en veiligheid en de Regeling inburgering oudkomers G25 2006 ;
d) Schuldhulpverlening (Wet gemeentelijke schuldhulpverlening en de Faillissementswet);
e) Arbeidsinschakeling (de Participatiewet, IOAW, IOAZ). Het samenwerkingsverband is slechts bevoegd om gegevens op te vragen voor die taken die bij gemeenschappelijke regeling gedelegeerd zijn aan het samenwerkingsverband.

Het autorisatieverzoek wordt getoetst, waarbij wordt uitgegaan van de beoordelingscriteria zoals deze zijn neergelegd in de Wet BRP en het Besluit basisregistratie personen (Besluit BRP). Onder meer bepalend is of en in hoeverre de verstrekking van de gegevens noodzakelijk is voor de goede vervulling van de taak van de aanvrager. Hierbij wordt steeds de bescherming van de persoonlijke levenssfeer van de personen, van wie de aanvrager gegevens verstrekt wenst te krijgen, gewaarborgd. Aan het autorisatiebesluit kunnen voorschriften en beperkingen worden verbonden in het belang van een zorgvuldige en doelmatige gegevensverstrekking. Het samenwerkingsverband mag tevens op verzoek gegevens opvragen uit de basisregistratie personen. Het samenwerkingsverband beperkt zijn vragen om persoonsgegevens tot de persoonslijsten van ingeschrevenen, waarvan raadpleging noodzakelijk is voor de uitvoering van de hiervoor vermelde taken[vi].

De gemeenten leggen jaarlijks verantwoording af op basis van de Participatiewet en aangezien gemeenten SUWI gebruiken voor de uitvoering van de Participatiewet ook over de Regeling SUWI (de Verantwoordingsrichtlijn). Zoals hiervoor aangegeven komt de oorspronkelijke voort uit de wet BRP en het Autorisatiebesluit. De regeling SUWI, de Verantwoordingsrichtlijn en daarmee ook de AVG bieden gronden voor controle op het juiste gebruik van het BRP.

Normenkaders informatiebeveiliging GeVS

Ingevolge de normenkaders voor de informatiebeveiliging van de GeVS voor afnemers dient de logging gecontroleerd te worden (C.06). De afnemer dient op basis van de vastleggingen evaluatie rapportages op het gebruik/misbruik moeten opstellen. Het monitoren van gebruikers- en beheerdersactiviteiten heeft tot doel ongeautoriseerde toegangspogingen tot Suwinet diensten en ongeautoriseerd gebruik van deze diensten tijdig te signaleren en op basis van de ernst van de signalering acties te ondernemen. *De monitoringsfunctie moet voorbehouden zijn aan een daartoe door de verwerkingsverantwoordelijke geautoriseerde/aangewezen functionaris.*
Norm C.07 geeft aan dat het veilig inrichten en beheersen van identificatie, authenticatie en autorisatie (IAA) voor het gebruik van Suwinet diensten essentieel is in het Suwinet domein. Het is van belang om op basis van rapportages verkregen vanuit deze technisch en organisatorische invalshoeken te evalueren of er zich geen afwijken in de IAA-beheersingsproces voordoen en of er structurele maatregelen noodzakelijk zijn.

Artikel 62. Wet Suwi: Onderlinge gegevensverstrekking door het Uitvoeringsinstituut werknemersverzekeringen, de Sociale verzekeringsbank en de gemeenten

1. Het Uitvoeringsinstituut werknemersverzekeringen, de Sociale verzekeringsbank en de colleges van burgemeester en wethouders verstrekken elkaar uit eigen beweging en op verzoek, kosteloos, alle gegevens en inlichtingen die noodzakelijk zijn voor de uitvoering van de taken die bij of krachtens deze wet of enige andere wet aan het Uitvoeringsinstituut werknemersverzekeringen, de Sociale verzekeringsbank en bij of krachtens de Participatiewet, de Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte werkloze werknemers, de Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen, de Wet gemeentelijke schuldhulpverlening of bij of krachtens andere wetten aan de colleges van burgemeester en wethouders zijn opgedragen, voor zover dit voortvloeit uit de samenwerking, bedoeld in artikel 9.

2. Het Uitvoeringsinstituut werknemersverzekeringen, de Sociale verzekeringsbank en de colleges van burgemeester en wethouders dragen gezamenlijk zorg voor de instandhouding van elektronische voorzieningen voor de verwerking van de gegevens, bedoeld in het eerste lid, voor zover dat noodzakelijk is voor de uitvoering van de taken die bij of krachtens deze wet of enige andere wet aan het Uitvoeringsinstituut werknemersverzekeringen, de Sociale verzekeringsbank en bij of krachtens de Participatiewet, de Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte werkloze werknemers, de Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen of de Wet gemeentelijke schuldhulpverlening aan colleges van burgemeester en wethouders zijn opgedragen. De elektronische voorzieningen hebben mede betrekking op de verwerking van gegevens waarvan de verkrijging en verstrekking door de in de eerste zin genoemde bestuursorganen op grond van enig wettelijk voorschrift is toegestaan.

3. Bij de gegevensverwerking voor de uitvoering van de diensten en taken, bedoeld in artikel 10, zijn het Uitvoeringsinstituut werknemersverzekeringen en de colleges van burgemeester en wethouders gezamenlijke verwerkingsverantwoordelijken als bedoeld in artikel 26 van de Algemene verordening gegevensbescherming voor de verwerking van gegevens voor de uitvoering van taken ten aanzien van dezelfde uitkeringsgerechtigde of werkzoekende.

4. Bij of krachtens algemene maatregel van bestuur worden regels gesteld met betrekking tot het tweede en derde lid in ieder geval met betrekking tot de inrichting, het beheer en de beveiliging van de elektronische voorzieningen.

---

[i] Verantwoordingsrichtlijn GeVS 2020
[ii] Bron: IBD
[iii] Bron: AP
[iv] Bron: RIVG
[v] Bron: Wet BRP
[vi] Bron: Autorisatiebesluit