VNG Realisatie

Handreiking Suwi autorisaties

voor het gemeentelijk domein Werk en Inkomen

Versie 2.0 mei 2019

Inhoud

1. Inleiding

Het via Suwinet uitwisselen van gegevens tussen gemeenten, SVB, UWV en andere bronnen is om meerdere reden noodzakelijk. Allereerst om burgers beter te kunnen helpen en ten tweede om fraude of misbruik te voorkomen.
De persoonsgegevens die via Suwinet worden uitgewisseld zijn zeer privacygevoelig. Daarom is het van belang dat gebruikers zorgvuldig met de gegevens die via het systeem worden uitgewisseld omgaan. In de praktijk gaat dat niet altijd goed.
Een maatregel om dat te bereiken is het verbeteren van de autorisatiestructuur. Een **fijnmaziger structuur** betekent dat de afstemming tussen de gegevenslevering en de informatiebehoefte van de professional wordt verbeterd (verfijnd). Daarmee wordt voorkomen dat ambtenaren gegevens onnodig raadplegen of meer gegevens onder ogen krijgen dan echt nodig is.
Alle gemeenten moeten hun Suwinet-autorisaties inrichten volgens een fijnmazige autorisatiestructuur in een autorisatiematrix. Wat houdt dat in? Welke werkzaamheden brengt dat met zich mee? Daarover gaat deze handreiking.

2. Doel

Een fijnmaziger autorisatiestructuur bevordert ‘proportionaliteit van gegevenslevering’ en gaat daarmee overmatig gegevensgebruik tegen. De toegang tot gegevens wordt beter afgestemd op wat voor de uitoefening van een taak noodzakelijk is. Niet meer en niet minder. Naast een fijnmaziger autorisatiestructuur vergt dit uiteraard ook een juist gebruik van zoeksleutels.
Deze handreiking is geschreven voor de situatie bij gemeenten. De andere ketenpartijen, SVB en UWV zijn zelf verantwoordelijk voor het treffen van maatregelen ter bevordering van een adequaat autorisatiebeleid.

3. Zoeksleutels

Persoonsgegevens zijn in principe alleen op te vragen via het BSN van de betreffende burger. Maar voor enkele bronnen kan of moet dat met een andere zoeksleutel. Zo werkt het Suwi Bedrijvenregister niet met het BSN en zijn er bij de RDW mogelijkheden om gegevens op te vragen buiten het BSN om, bijvoorbeeld via kenteken of adres. Hiervoor zijn speciale zoekpagina’s ingericht. Zoeken naar persoonsgegevens anders dan op BSN, zijn risicovolle autorisaties. Het advies is om deze beperkt toe te kennen. Medewerkers moeten voor deze zoekpagina’s apart worden geautoriseerd. Voor het omgaan met de zoeksleutels anders dan BSN is een **aparte handreiking** beschikbaar.

4. Wat moet de gemeente doen?

Bij het (her)ijken van het autorisatiebeleid van de gemeente, is het van belang dat de gegevenslevering aan medewerkers in lijn is met de door hun functie ingegeven gegevensbehoefte. Zo is het voor medewerkers die alleen re-integratie doen niet noodzakelijk om ook inkomensgegevens te kunnen inzien.
Door strikt te autoriseren voor alleen de noodzakelijke gegevens voor de uitvoerende taken wordt de gegevenslevering proportioneel.
Via de webapplicatie Suwinet-Inkijk worden gegevens uit verschillende bronnen[1] opgevraagd. De bronhouder bepaalt per wettelijke taak welke gegevensset aan welke organisatie mag worden geleverd. Die gegevens worden getoond op de inkijkpagina's van Suwinet-inkijk. Deze inkijkpagina's bestaan uit bronpagina's en overzichtspagina's:

- Bronpagina: toont de gegevens van één bron
- Overzichtspagina: combineert gegevens van verschillende bronnen

Op de website van het BKWI kunt u in het document **"Overzicht Autorisaties op Suwinet-Inkijk voor GSD"** vinden welke pagina's beschikbaar zijn en welke gegevens die pagina's bevatten. Daarbij worden ook suggesties gedaan voor welk soort uitvoerende taken de pagina's bedoeld zijn.
De werkzaamheden m.b.t het autoriseren zijn incidenteel en structureel van aard:

1. **Voorbereiding (incidenteel):**

a) Inventariseren van de bestaande autorisaties door gebruikersbeheerder
b) Opstellen van een nieuwe autorisatiematrix door gebruikersbeheerder en Security Officer (SO) aan de hand van functies en taken binnen de organisatie.

2. **Implementatie (incidenteel):**
    a) Vaststellen van de nieuwe autorisatiematrix door het MT
    b) Toekennen van autorisaties aan medewerkers door gebruikersbeheerder
3. **Beheer en controle d.m.v. opvragen rapportages (structureel)**
    a) Door management, SO en/of gemandateerde functionaris.

4.1. Voorbereidend: inventarisatie en aanpassing

Een belangrijke maatregel die u moet nemen is het opstellen of aanpassen van de autorisatiematrix. In een autorisatiematrix staan de functies van een medewerker, en tot welke gegevens een specifieke functie toegang heeft. Dit betekent dat na inventarisatie van de situatie per functie moet worden vastgesteld welke Suwinet-pagina's gebruikt mogen worden en welke zoeksleutel daarbij mag worden gehanteerd. Dit is uiteraard afhankelijk van de taken die aan de betreffende medewerkers worden opgedragen.

In sommige situaties vragen medewerkers **meer** gegevens op **dan** voor de uitvoering van hun taak op dat moment **nodig** is. Meestal gebeurt dat onbewust door het opzoeken van één specifiek gegeven via een overzichtspagina (bijvoorbeeld: heeft de klant vorige maand gewerkt?). In voorkomende situaties zal de medewerker een **bronpagina moeten gebruiken** in plaats van de overzichtspagina. Zo krijgt hij niet meer onnodig gegevens onder ogen.
Wij adviseren u daarom om medewerkers die autorisaties krijgen voor overzichtspagina's ook altijd te autoriseren voor de van toepassing zijnde bronpagina's. Op die manier kunnen medewerkers

[1] waaronder die van de BRP, BRV (RDW), GSD, UWV, SVB, Kadaster en DUO

bewust kiezen of ze op dat moment een uitgebreid overzicht van gegevens van de klant nodig hebben of dat slechts gegevens uit één bron kunnen volstaan.

Binnen de Suwinet autorisatiestructuur kunnen gemeenten **zelf autorisatierollen** aanmaken en toewijzen aan bepaalde functies. Die rollen geven toegang tot één of meer pagina's op Suwinet-Inkijk.
Het is aan te raden om bij het opnieuw 'samenstellen' van de rollen per functie, tegelijkertijd opnieuw te bepalen welke rollen/functies gebruik mogen maken van zoekpagina's met een zoeksleutel anders dan het BSN.
Een autorisatiematrix maakt deel uit van het beheerproces op autorisaties. Het vaststellen en bijhouden van een autorisatiestructuur is een gemeentelijke taak die is belegd bij de autorisatiebeheerder. Hij doet dit in overleg met de Security Officer en het management. Een autorisatiematrix maakt in één oogopslag inzichtelijk hoe die autorisatiestructuur is opgebouwd.
Nb. de autorisatieprocedure en de controle op toegang en gebruik is een van de normen uit het Suwinet-normenkader waaraan gebruikers moeten voldoen.
Een eenvoudig en fictief voorbeeld van een autorisatiematrix voor Suwinet-Inkijk van een gemeente vindt u op de website van BKWI en op de website van VNG-Realisatie onder Suwinet.

4.2. Implementatie: vaststellen en toekennen van de autorisaties

Na het samenstellen en (laten) vaststellen van de autorisatiematrix[2], dient deze door het management te worden vastgesteld. Daarna kan de gebruikersbeheerder de gebruikersadministratie Suwinet-Inkijk aanpassen. Via de gebruikersadministratie worden de inkijkpagina's gekoppeld aan een rol en krijgen medewerkers één of meer rollen toebedeeld. Mogelijk moeten bestaande rollen worden aangepast of nieuwe rollen worden aangemaakt, afhankelijk van de bestaande gebruikersadministratie. Medewerkers moeten uiteraard worden voorgelicht over de nieuwe of gewijzigde situatie.
In de **Handleiding Suwinet-Inkijk gebruikersadministratie**, staat informatie over de manier waarop bestaande accounts kunnen worden bewerkt in de gebruikersadministratie. Deze kunt u vinden op de BKWI website.
Het aanpassen van de gebruikersadministratie Suwinet-Inkijk moet door de gemeente zelf en handmatig plaatsvinden. Het is heel vaak niet mogelijk om gebruik te maken van geautomatiseerde overzetting door het BKWI. Dit komt doordat bij iedere gemeente de functies en rollen anders zijn samengesteld. De gemeentelijke rollen in de gebruikersadministratie zijn niet inzichtelijk voor het BKWI, zij kunnen niet zoeken op toegekende pagina's per rol. Daardoor zijn overzettingen door 'zoek en vervang' vaak niet mogelijk.
Gemeenten die al werken met een autorisatiematrix op functies met bijbehorende rollen in Suwinet-Inkijk, kunnen waarschijnlijk de gebruikersadministratie gemakkelijk en snel aanpassen. Andere gemeenten hebben naar verwachting veel meer tijd nodig voor de aanpassingen in de gebruikersadministratie.

[2] Een autorisatiematrix moet onderdeel zijn van het beveiligingsplan van de organisatie (Suwinorm 13.1)

4.3. Beheer en controle

Hoe blijft u in control?
Maandelijks stelt het BKWI per organisatie rapportages beschikbaar. De organisatie is zelf verantwoordelijk voor het ophalen van die rapportages. In de praktijk blijkt dat niet elke gemeente deze rapportages ophaalt. Dat is jammer, want de rapportages geven een goed inzicht in het gebruik door medewerkers. Analyse van de rapportages kan aanleiding geven om meer gespecificeerde rapportages op te vragen.

De maandelijkse **algemene rapportage** bevat geen informatie over bevraagde BSN's of medewerkers die bepaalde gegevens hebben opgevraagd. De rapportage geeft ondermeer een beeld van:

- het aantal raadplegingen per inkijkpagina
- het percentage raadplegingen tussen 19:00 uur en 06:00 uur t.o.v. het totaal aantal raadplegingen
- het percentage raadplegingen op zoeksleutel anders dan BSN
- het aantal raadplegingen van de vijf meest geraadpleegde BSN's
- Het hoogst aantal medewerkers dat een bepaalde BSN heeft geraadpleegd (top 5)
- De top 5 van aantal raadplegingen door een gebruiker
- het percentage geblokkeerde accounts
- het aantal accounts dat tenminste 90 dagen niet is gebruikt
- overzicht hoeveel medewerkers voor welke rol zijn geautoriseerd

De gemeente heeft de mogelijkheid om naast de algemene rapportage ook **specifieke rapportages** op te vragen. Specifieke rapportages geven gedetailleerde informatie over de medewerkers en BSN's. Zo'n rapportage wordt opgevraagd als onderdeel van de control cyclus (bijvoorbeeld steekproeven) of omdat de algemene rapportage daartoe aanleiding geeft (bijvoorbeeld een flinke toename in opvraging of toename in het gebruik van zoeksleutels anders dan BSN).
De specifieke rapportage kan worden aangevraagd door **een hiertoe gemandateerde functionaris**, (bijvoorbeeld een **Interne Controller of Security Officer**) ter ondersteuning van het interne
controleproces. De procedure voor het aanvragen van specifieke rapportages kunt u vinden op de website van het BKWI.

5. Communicatie over proportionaliteit

Medewerkers moeten uiteraard op de hoogte worden gebracht van eventuele wijzigingen.
Het is de bedoeling dat de medewerker alleen de gegevens opvraagt die nodig zijn voor de uitvoering van zijn taak. Een medewerker die enkel voertuiggegevens nodig heeft, kan volstaan met raadpleging van de bronpagina RDW en hoeft geen overzichtspagina handhaving te gebruiken, waar de voertuiggegevens naast vele andere gegevens worden getoond. De verandering in het beperken van het gebruiken van overzichtspagina's betekent dat medewerkers zich bewust moeten worden dat 'less' in veel gevallen 'more' is. Voorlichting en continue in gesprek blijven is daarom essentieel.
In de toekomst wordt het mogelijk dat burgers (met gebruik van hun DigID) zelf kunnen inzien welke organisatie uit welke bron gegevens van hen heeft opgevraagd. Als er dan steeds grote overzichtspagina's zijn opgevraagd is het niet uit te leggen dat een medewerker bijvoorbeeld inkomensgegevens heeft opgevraagd terwijl alleen geverifieerd moest worden of een auto op naam van de klant staat.