VNG Realisatie

Handreiking gebruik Zoeksleutels in Suwinet-Inkijk

voor het gemeentelijk domein Werk en Inkomen

Versie 2.0 mei 2019

Inhoud

1.Inleiding

Het kunnen raadplegen van persoonsgegevens van burgers via Suwinet is essentieel voor het uitvoeren van veel (gemeentelijke) taken zoals de uitkeringsverstrekking en re-integratie van werkzoekenden op grond van de Participatiewet. Deze gegevens zijn per definitie privacygevoelig. Op een enkele bron na[1] dient bij die raadplegingen standaard als zoeksleutel het BSN te worden gebruikt. De medewerker moet dus eerst over dit unieke nummer beschikken voordat hij of zij gegevens van een burger kan inzien. In speciale gevallen kan aan medewerkers de bevoegdheid worden verleend om (ook) gegevens te kunnen raadplegen met een andere zoeksleutel dan het BSN.
Deze handreiking beschrijft welke afwegingen een organisatie behoort te maken voordat zij die bevoegdheid toekent aan zijn medewerker(s).

2.Waarom deze handreiking?

Het beschermen van de privacy van burgers stelt hoge eisen aan de uitvoering van taken waarbij persoonsgegevens worden gebruikt.

Eén van de maatregelen om dat te bereiken is het bewust omgaan met de zoekmogelijkheden in Suwinet-Inkijk; het beperken van het veelvuldig verlenen van bevoegdheden voor andere zoeksleutels dan BSN en het controleren op het gebruik daarvan. Dit om te voorkomen dat persoonsgegevens onnodig of onrechtmatig op andere zoeksleutels dan BSN wordt gezocht. Het kunnen zoeken via andere zoeksleutels maakt het risico groter dat gegevens worden ingezien die niet relevant zijn voor de werkzaamheden van de medewerker. De volgende voorbeelden illustreren dat:

Lies werkt bij een gemeente en heeft uitzicht op het parkeerterrein. Ze ziet een jonge man aankomen in een heel dure auto. Hij komt binnen, noemt zijn naam en zegt een afspraak te hebben. Interessant denkt Lies…..even het kenteken intypen in de RDW via Suwinet-Inkijk. Is die auto van hem? Kan ik mijn collega een tip geven? Lies schendt hiermee de privacy rechten van deze man.

Jan is sociaal rechercheur en mag andere zoeksleutels gebruiken dan BSN. Op een ochtend staat een klantmanager aan zijn bureau: "Jan, wil jij even voor mij opzoeken welke personen op dit adres staan ingeschreven?" Jan kan geen nee zeggen en zoekt het op. Hiermee schendt Jan de privacy van de bewoner(s) op het bewuste adres. Er is geen aanleiding om dit adres te bevragen.

Annelies is klantmanager. Haar man is leraar. Dagelijks rijdt zij na haar werk, op haar fiets naar huis. Het is al meerdere keren voorgekomen dat ze de auto van haar man voor een vreemd huis ziet staan. Hij geeft bijles wiskunde. Annelies vertrouwt het niet en gaat op haar werk via 'zoek in GBA+' kijken wie op dat adres woont om meer over de bewoner(s) uitvinden. Dit is niet werk gerelateerd. Annelies schendt de privacy rechten van de bewoners!

Piet is net gescheiden. Via via hoort hij dat zijn ex een huis heeft gekocht. Dat zint hem niet. Tenslotte ligt hij krom voor haar en kan zelf geen huis betalen. Hij weet het adres en zoekt via het kadaster in Suwinet Inkijk.
Piet schendt hiermee de privacy rechten van zijn ex!

[1] In het Suwi Bedrijven Register is de zoeksleutel niet het BSN. Het betreft hier openbare informatie, er wordt alleen met openbare zoeksleutels gezocht.

3. Welke risico's zijn er verbonden aan het gebruik van 'andere' zoeksleutels?

De bovenstaande voorbeelden leggen een aantal risico's bloot die zich kunnen voordoen bij het gebruik van andere zoeksleutels dan BSN. Het advies is dan ook om autorisaties om die andere zoeksleutels te kunnen gebruiken, beperkt toe te kennen en zodoende verantwoord gebruik te bevorderen.

Nieuwsgierigheid is een menselijke eigenschap. Ook medewerkers hebben een privéleven waaruit vragen naar voren kunnen komen waarop Suwinet Inkijk misschien het antwoord heeft. Het gebruik van Suwinet-Inkijk voor privé doeleinden is misbruik. Het is verboden en ondermijnt het vertrouwen van burgers in de organisaties aan wie zij noodzakelijkerwijs hun gegevens hebben verstrekt. Dat die gegevens worden gebruikt voor privédoeleinden van medewerkers, is een schending van hun privacy.

Privacy risico's kunnen worden beperkt door een adequaat en strikt autorisatiebeleid waarin toezicht, controle en naleving prominent aanwezig zijn. Daardoor is steeds actueel zicht op de bevoegdheden van- en het gebruik door medewerkers. In één oogopslag is aan de hand van een autorisatiematrix zichtbaar waar bevoegdheden zijn belegd. Controle vindt plaats aan de hand van gebruikersrapportages die inzicht bieden in het gebruik van Suwinet en zoeksleutels door individuele medewerkers. Naleving ontstaat wanneer het bewustzijn wordt vergroot. Dit kan onder andere door het een terugkerend onderwerp te maken tijdens werkoverleg en/of intervisie.

4. Autoriseren

Het opvragen van persoonsgegevens mag alleen met gebruik van het Burgerservicenummer (BSN) als zoeksleutel. Wanneer het nodig is daarvan af te wijken, en de mogelijkheid daartoe wordt geboden, geldt dat de gemeente de medewerker expliciet autoriseert voor een aparte zoekpagina[2].

Iedere organisatie heeft de **verplichting** zich aan de beveiligingsnormen te houden zoals die zijn opgenomen in het Normenkader Gezamenlijke Elektronische Voorzieningen SUWI[3]. Dit betekent ook dat iedere organisatie in het beveiligingsplan Suwinet een autorisatiematrix[4] moet hebben opgenomen. Hierin staat beschreven welke taken tot een functieprofiel behoren en welke pagina's binnen Suwinet-Inkijk nodig zijn om deze taken uit te kunnen voeren. Het management van de organisatie heeft als verantwoordelijke goedkeuring gegeven aan de functieprofielen, de autorisatiematrix en het beveiligingsplan Suwinet. De gebruikersbeheerder kent, aan de hand van de autorisatiematrix, de pagina's toe.

Een organisatie die gebruik maakt van Suwinet-Inkijk, is zelf verantwoordelijk voor de toedeling van autorisaties, voert hierop zijn eigen beleid en is hierop aanspreekbaar. Organisaties maken daarbij hun eigen afwegingen, gebaseerd op de wijze waarop zij hun organisatie hebben ingericht en waar, aan welke medewerkers, taken zijn toebedeeld en met welke risico's dat gepaard gaat.
Kortom: er is geen éénduidig gemeentelijk beleid ten aanzien van het toekennen van autorisaties voor het zoeken met zoeksleutels, anders dan BSN.

[2] Zie bijlage 1 voor tabel andere zoeksleutels per bron
[3] Zie www.bkwi.nl
[4] Zie www.bkwi.nl of www.vngrealisatie.nl voor een voorbeeld van een autorisatiematrix.

5.Wanneer wel een andere zoeksleutel?

Welke afwegingen moet een organisatie nu maken om medewerkers een andere autorisatie voor het zoeken met zoeksleutels, anders dan BSN toe te kennen? Feitelijk gaat het dan om het detecteren van wettelijke taken die aan de organisatie zijn opgelegd, waarbij persoonsgegevens nodig zijn die, behalve via het BSN, ook met een andere zoeksleutel zijn op te vragen.

In de regel zal het daarbij gaan om taken die liggen op het terrein van opsporing en verhaal. De volgende voorbeelden dienen ter illustratie:

Pieter is sociaal rechercheur en heeft een melding binnen gekregen dat de heer X samenwoont. Pieter gaat posten bij het huis van de heer X en ziet regelmatig een andere auto voor de deur staan. Een vrouwelijk persoon stapt tegen de avond uit en gaat de volgende ochtend weer weg. Pieter zoekt het kenteken op via Suwinet Inkijk. Dit is toegestaan. Een sociaal rechercheur heeft soms andere zoekmogelijkheden nodig om tot een voorstel te kunnen komen, waarop een besluit kan worden genomen.

Pieter, de sociaal rechercheur, krijgt opnieuw een melding van iemand over een bedrijf met veel zwartwerkers. Pieter gaat er heen en noteert alle kentekens in de omgeving. Vervolgens gaat hij in Suwinet na, wie van de auto-eigenaren een bijstandsuitkering heeft om zo mogelijke fraude op te sporen. Piet schendt nu de privacy van alle auto-eigenaren. We noemen dit ook wel 'niet-proportioneel'.

Een middelgrote gemeente heeft besloten dat alle medewerkers alle voorkomende taken moeten uitvoeren, van intake tot en met terugvordering. Alleen het werk van de sociaal rechercheur is uitbesteed aan een naburige gemeente. De gemeente besluit dat alle medewerkers 'breed' moeten kunnen zoeken in de BRP (voorheen GBA) en RDW. De gemeente neemt hiermee een groot risico. Afwegingen die gemaakt kunnen worden: lopen deze medewerkers vast wanneer zij deze zoeksleutels niet hebben? Hebben alle medewerkers deze zoeksleutels echt nodig? Is het mogelijk bijvoorbeeld het proces verhaal bij enkele medewerkers onder te brengen? Zo nee, waarom niet? Is het misschien mogelijk om de afwijkende zoeksleutels alleen toe te kennen aan enkele senior medewerkers?
Het is verstandig dat deze afwegingen onderbouwd worden vastgelegd. Ook zal de gemeente een strikt controlemechanisme moeten hebben (afspraken/beleid/borgen/naleven).

6.Wat moet U doen?

Een belangrijke stap die u moet nemen is het nalopen van de autorisatiematrix. In een autorisatiematrix is de functie of zijn de functies die een medewerker heeft, vastgelegd. Daarin wordt zichtbaar tot welke gegevens medewerkers met een specifieke functie toegang hebben.

Voorbeelden van autorisatiematrices zijn te vinden op website van BKWI en op de website van VNG-Realisatie.

Dit vereist dat per functie is vastgesteld, welke Suwinet-Inkijk 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.

U kunt zich daarbij afvragen hoeveel medewerkers daadwerkelijk via andere zoeksleutels dan BSN zoeken. Is het echt nodig? Kan het anders? Hoe kunt u borgen dat al deze medewerkers deze risicovolle autorisaties alleen gebruiken voor hun wettelijke taken?

De afwegingen die u behoort te maken zijn:

Stap 1. Voorbereidend:
Analyseer de functie omschrijving en bijbehorende taken

Per functie is vastgesteld, welke Suwinet-Inkijk pagina's gebruikt mogen worden. In deze stap is het van belang om opnieuw te bepalen welke rollen/functies gebruik mogen maken van zoekpagina's met een zoeksleutel anders dan het BSN. Het is raadzaam hier de Security Officer (SO) of een Functionaris Gegevensbescherming (FG), een kwaliteitsmedewerker en de leidinggevende bij te betrekken.

Zoals eerder aangegeven is een functie omschrijving met bijbehorende taken belangrijk om te kunnen bepalen of iemand andere zoeksleutels dan BSN nodig heeft. Enkele voorbeelden:

a. Een medewerker Intake zou voldoende moeten hebben aan het zoeken via BSN.
b. Een sociaal rechercheur of opsporingsambtenaar moet ook via andere zoeksleutels kunnen zoeken.
c. Een medewerker met een breed takenpakket zal misschien meerdere zoeksleutels nodig hebben.

Tip: Maak de afweging of **alle** medewerkers met een breed takenpakket deze risicovolle autorisaties moeten hebben of dat deze bevoegdheid niet bij een kleiner aantal medewerkers kan worden belegd.

Stap 2. Leg vast en documenteer

- Wanneer u een onderbouwde afweging heeft gemaakt wordt dit vastgelegd in een autorisatiebesluit. De onderbouwing laat u ondertekenen en documenteert u. Het fungeert als achtergrondinformatie bij eventuele toekomstige onderzoeken, dan wel rechtszittingen.
- U neemt uw autorisatiebesluit op in de autorisatiematrix van het beveiligingsplan Suwinet en laat beiden opnieuw tekenen door de verantwoordelijken binnen de gemeente.
- U informeert belanghebbenden over het beveiligingsplan en de autorisatiematrix.
- De gebruikersbeheerder voert uit en kent n.a.v. de autorisatiematrix de autorisaties toe.
- De gebruikersbeheerder legt vast wanneer aan welke persoon welke autorisatie is toegekend.

7. Hoe blijft u in control?

Maandelijks stelt het BKWI per organisatie rapportages ter beschikking. 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.

Door op regelmatige basis de maandelijkse **gebruiksrapportage** te analyseren kan misbruik van bevoegdheden vroegtijdig (*maar altijd achteraf*) worden opgespoord. Deze gebruikersrapportage is door de gebruikersbeheerder (of een hiervoor geautoriseerde medewerker) maandelijks via de homepage van Suwinet-Inkijk te downloaden. De gebruiksrapportage[5] toont de activiteiten die de laatste zes maanden in Suwinet-Inkijk plaats hebben gevonden. Zo is het aantal raadplegingen op

[5] De handreiking gebruikersrapportage Suwinet is te vinden op www.vngrealisatie.nl

zoeksleutel anders dan BSN weergegeven. Ook is het mogelijk om de gegevens van de eigen gemeente te vergelijken met de ‘scores’ van andere gemeenten. De gebruiksrapportage zelf bevat geen vertrouwelijke gegevens en kan, indien gewenst, gedeeld worden met collega’s en medewerkers.

Analyse van de gebruiksrapportages kan aanleiding zijn tot het opvragen van een meer gespecificeerde rapportage. Door een **specifieke rapportage** op te vragen bij het BKWI, kunt u bijvoorbeeld achterhalen welke medewerkers welke zoeksleutels hebben gebruikt en wat de frequentie van die opvragingen is.

Er lijken soms argumenten te zijn om de controle achterwege te laten. Die zijn niet altijd valide. Enkele opmerkingen van verschillende organisaties door de jaren heen:

- *Wij zijn zo klein, bij ons gebeurt dat niet;*
- *De medewerkers hebben bij aanstelling hiervoor getekend, dat is toch voldoende?*
- *We kennen onze medewerkers, zij doen dat niet;*
- *De medewerkers zitten dicht op elkaar, ze houden elkaar in de gaten.*

Het is uiteraard van belang dat medewerkers er van op de hoogte zijn dat de raadplegingen die zij doen in Suwinet zichtbaar, en dus controleerbaar zijn. Daarvan gaat ook een preventieve werking uit.

In de specifieke rapportage wordt zowel de naam van de medewerker, als ook – als daar om gevraagd wordt - diens eventuele functiegroep vermeld. **Dit kan alleen wanneer de gebruikersbeheerder functiegroepen heeft ingesteld in de gebruikersadministratie van Suwinet-Inkijk**. Het voordeel van het gebruik van functiegroepen is dat – zeker in grotere organisaties – snel kan worden vastgesteld of een medewerker toegang heeft tot de juiste pagina’s.

Een specifieke rapportage wordt opgevraagd omdat dit een onderdeel is van de control cyclus. Een andere aanleiding voor het opvragen van een specifieke rapportage kan zijn dat de algemene rapportage daartoe aanleiding geeft, bijvoorbeeld omdat er een flinke toename in opvragingen of toename in het gebruik van zoeksleutels anders dan BSN is te zien. U wilt achterhalen wat hier de oorzaak van is.

Omdat het hier om risicovolle autorisaties gaat, raden wij u aan regelmatig, tenminste twee maal per jaar, steekproeven te doen door het opvragen van een specifieke rapportage.

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 BKWI, www.bkwi.nl.

8. Naleving en bewustwording

Hoe zorgt u ervoor dat uw medewerkers alleen een andere zoeksleutel dan BSN gebruiken wanneer hun werkzaamheden daar specifiek om vragen en niet als dat niet nodig is?
Om dat te bereiken is het belangrijk om, naast een stringent beleid ten aanzien van overtredingen, te werken aan de bewustwording bij de medewerkers. Dat kan op vele manieren, zoals deze voorbeelden laten zien:

Bij ons is er eens in de twee maanden een casusbespreking met de mensen die gebruik maken van andere zoeksleutels dan BSN. We bespreken een casus waarbij mogelijk is gezocht met een andere zoeksleutel dan BSN. De rest moet verdiepende vragen stellen en uiteindelijk geeft iedereen om de beurt aan of het nodig was te zoeken met een andere zoeksleutel en komt een gezamenlijke eindconclusie. Pas aan het eind vertelt de indiener hoe hij/zij het heeft gedaan en waarom.

Wij hebben eens per maand een werkoverleg. Een standaard punt op de agenda is de gebruikersrapportage. De Security Officier schuift bij ons aan en stelt vragen over opvallende zaken in de rapportage. Vaak hebben wij hier een antwoord op en weten we wat er is gebeurd. Toch vraagt hij soms rapportages op, op persoonsniveau om te zien wat we hebben gedaan.

Bij ons is een standaard punt van het werkoverleg de wijze waarop wij Suwinet Inkijk gebruiken. De ene keer heeft iemand een vraag over wat wel of niet mag in Suwinet Inkijk, de andere keer horen we wat de opvallende zaken in de lograpportage waren en soms horen we iets over wat in het nieuws is geweest.

Hoe zorgt u ervoor dat men zich bewust blijft van de privacy gevoeligheid van het werken met Suwinet?
U kunt zich afvragen op welke momenten u wel of niet communiceert met medewerkers en wat deze communicatie betekent voor de bewustwording:

- Welk proces hanteert u in geval van een incident? Bespreekt u het breed met alle medewerkers of houdt u het ‘onder de pet’?
- Hoe analyseert u de maandelijkse gebruikersrapportage? Doet u dit alleen, doet u dit met de Security Officer? Of betrekt u de medewerkers hierbij?
- Hoe vaak bespreekt u het beveiligingsplan Suwinet-Inkijk met de medewerkers? Vraagt u hun mening? Waarom wel/niet?
- Legt u uit waarom het zoeken via een andere zoeksleutel dan BSN risicovol is? Herkennen de medewerkers dit? Gaat u in gesprek?

9. Bijlage 1: Overzicht van bronpagina's die toegankelijk zijn op basis van een andere zoeksleutel dan BSN

Bron	Zoekpagina	Beschikbare zoeksleutel(s)
Basisregistratie Personen (voorheen GBA)	Basisregistratie Personen (voorheen GBA), zoeken	Geboortedatum Postcode Huisnummer
	Basisregistratie Personen (voorheen GBA), zoeken+	Geboortedatum Achternaam Geslacht
		Geboortedatum Postcode Huisnummer
		Postcode Huisnummer
Persoonsinformatievoorziening Nederlandse Antillen en Aruba (PIVA)	Persoonsinformatievoorziening Nederlandse Antillen en Aruba (PIVA)	Geboortedatum Achternaam
Basisregistratie Voertuigen (voorheen RDW)	Basisregistratie Voertuigen (voorheen RDW), zoeken (+)	Kenteken voertuig Peildatum Peiltijd
		Achternaam Voorletters Geboortedatum Peil periode
		BSN Peil periode
		Postcode / huisnummer Peilperiode
		Inschrijfnummer KvK Vestigingsnummer Peilperiode
Kadaster	Kadaster, zoeken	Postcode Huisnummer
		Kadastrale gemeentenaam / Gemeentecode Sectie Perceelnummer Deelperceelnummer/Appartementsindex
Suwi Bedrijvenregister (SBR)	Suwi Bedrijvenregister (SBR)	KvK nummer Naam onderneming Straat Huisnummer Postcode Postcode t/m Woonplaats Code economische activiteit Naam contactpersoon
Suwi BedrijvenRegister	SBR Query	Diversen