Ministerie van Sociale Zaken en Werkgelegenheid

> Retouradres Postbus 90801 2509 LV Den Haag

Aan het College van Burgemeester en Wethouders

Postbus 90801
2509 LV Den Haag
Parnassusplein 5
T 070 333 44 44
F 070 333 44 00
www.rijksoverheid.nl

Contactpersoon
mw. mr. A. van Splunter
T 070 333 53 99
AvSplunter@minszw.nl

Onze referentie
2015-0000252205

Datum 19 november 2015
Betreft Veilig gebruik van SUWInet

In deze brief vraag ik uw aandacht voor het gebruik van gegevens via SUWInet. Over de privacy van burgers moet goed worden gewaakt. Zeker door overheden die toegang hebben tot veel gevoelige persoonsinformatie. Daarom vind ik het van groot belang dat u zorgvuldig omgaat met de informatie van burgers die u tot uw beschikking heeft. Wat betreft het gebruik van SUWInet kan dat nog verbeterd worden, mede omdat met de eerder in gang gezette verbeteracties nog onvoldoende resultaat is bereikt. De bescherming van persoonsgegevens is een grondrecht en het is niet acceptabel dat de overheid hierin tekortschiet. U dient er voor te zorgen dat burgers in uw gemeente erop kunnen vertrouwen dat u zorgvuldig met gegevens om gaat en dat de beveiliging op orde is.

De Inspectie SZW heeft in 2014 bij 78 gemeenten een vervolgonderzoek uitgevoerd naar de beveiliging van het gebruik van gegevens via SUWInet. Uit het onderzoek volgt dat er 13 gemeenten (17%) zijn die voldoen aan de 7 door de Inspectie SZW onderzochte normen voor de beveiliging van SUWInet. Er zijn 7 gemeenten (9%) die aan geen enkele onderzochte norm voldoen. Daarnaast heeft de Inspectie SZW 43 gemeenten onderzocht die ook bij het vorige onderzoek in 2013 in de steekproef zaten. Daar waar in 2013 er 2 gemeenten aan alle 7 normen voldeden, voldoen nu 6 gemeenten aan de 7 normen. De gemiddelde score van deze groep steeg van 2,4 naar 4,7 normen. Deze verbetering is groter dan de resultaten vanuit het landelijke beeld. In de bijlage bij deze brief vindt u een overzicht van de resultaten per gemeente.

Naar aanleiding van de resultaten van het onderzoek van de Inspectie SZW heb ik het College Bescherming Persoonsgegevens (CBP) geïnformeerd. Het CBP heeft aangegeven direct een onderzoek te starten bij de gemeenten die aan geen enkele norm voldoen[1]. Het CBP kan handhavend optreden en een last onder dwangsom opleggen.

[1] Met uitzondering van één gemeente waar de Inspectie SZW een herhalingsonderzoek gaat uitvoeren.

De Inspectie SZW is bij alle gemeenten met een onderzoek naar de beveiliging van SUWInet gestart. De Inspectie SZW gaat in dit onderzoek wederom uit van zeven essentiële normen voor het waarborgen van vertrouwelijkheid, opgenomen in het Normenkader Gezamenlijke elektronische Voorzieningen SUWI (GeVS)[2]. Indien uit het onderzoek volgt dat uw gemeente niet voldoet aan 7 essentiële normen dan treedt het escalatieprotocol 'afsluiten SUWInet' in werking en loopt u, met als ultimum remedium, het risico te worden afgesloten van het gebruik van SUWInet. Het escalatieprotocol is als bijlage toegevoegd aan deze brief.

Wanneer alle stappen van het escalatieprotocol zijn doorlopen en geen enkele financiële prikkel heeft bijgedragen aan structurele verbetering van de informatiebeveiliging, resteert geen andere mogelijkheid dan afsluiten. Met afsluiten zijn ook kosten gemoeid: er moeten alternatieve wijze van gegevenswisseling worden opgezet, de dienstverlening wordt hierdoor arbeidsintensiever en trager en het risico op beroeps- en bezwaarprocedures van cliënten neemt hierdoor toe. Tegelijk moet worden gewerkt aan verbetering om weer aangesloten te kunnen worden.

In het algemeen overleg met de Tweede Kamer op 24 juni jl. is veel aandacht besteed aan de beveiliging van SUWInet. In de reactie op het aanvalplan beveiliging SUWInet van D66 heb ik onder meer aangegeven[3]:

1. *Gemeente afsluiten van SUWInet die hun zaken niet op orde hebben*
   Het onderzoek van de Inspectie SZW zal uitwijzen in hoeverre iedere gemeente aan de 7 essentiële beveiligingsnormen voldoet. Een gemeente die nalaat om de beveiliging op orde te brengen, zal in een aantal stappen, als ultimum remedium, worden afgesloten van het gebruik van SUWInet.

2. *Aanpassen systeem SUWInet zodat medewerkers alleen toegang hebben tot gegevens van eigen cliënten en conform de motie Ulenbelt-Van Weyenberg niet breder dan op burgerservicenummer kunnen zoeken*
   In 2015 wordt de toegang van medewerkers tot de gegevens van personen die cliënt zijn van de betreffende organisatie beperkt. Om het aantal de gegevens dat een medewerker van een persoon kan raadplegen te beperken, wordt in 2015 een aantal aanvullende inkijk-pagina's ontwikkeld. In 2016 volgt het beperken van de toegang van medewerkers tot de gegevens van cliënten die medewerkers zelf behandelen.

3. *Meer bekendheid geven aan de mogelijkheid in bepaalde gevallen gegevens binnen SUWInet af te schermen, in het bijzonder adressen van personen in een blijf-van-mijn-lijf huis*
   Ik vind het van groot belang dat de gegevens van personen die verblijven in een blijf-van-mijn-lijf-huis geheim blijven. Gemeenten moeten speciale aandacht besteden aan het beschermen van gegevens van kwetsbare groepen. In overleg met de Federatie Opvang, het UWV en de VNG wordt bekeken in hoeverre er aanvullende maatregelen nodig zijn voor het afschermen van gegevens.

---

[2] Het Normenkader GeVS maakt deel uit van de Verantwoordingsrichtlijn GeVS. Het normenkader bevat in totaal 115 normen.

[3] Kamerstukken II, 2014-2015, 26448, nr. 537 .

In de verzamelbrieven van juni en november 2015 heb ik uw aandacht gevraagd voor de verplichte jaarlijkse verantwoording over het gebruik van SUWInet. In de wet- en regelgeving SUWI is geregeld dat iedere organisatie die van SUWInet gebruik maakt, moet aantonen dat het stelsel van de door zijn organisatie genomen maatregelen voldoet aan het SUWI-normenkader. In het jaarverslag geeft het college van burgemeester en wethouders aan op welke wijze zij sturing heeft gegeven aan de beveiliging van SUWInet en, indien nodig, welke maatregelen er zijn getroffen indien er sprake is van tekortkomingen. Het verdient aanbeveling om de sturing op de beveiliging van SUWInet te plaatsen binnen de bredere sturing op de informatieveiligheid. Naast voldoende bestuurlijke aandacht wil ik u in overweging geven om de gemeentesecretaris te belasten met de dagelijkse sturing op de informatieveiligheid.

Datum

Onze referentie
2015-0000252205

Alle gemeenten krijgen lograpportages van de beheerder van Suwinet BKWI. Uit eerder onderzoek van de Inspectie SZW is gebleken dat gemeenten moeite hebben met het naleven van deze norm. Daarom vraag ik extra uw aandacht voor naleving van deze norm. Lograpportages geven inzicht in het gebruik van gegevens via SUWInet door medewerkers en vormen een belangrijk instrument om oneigenlijk gebruik van SUWInet te signaleren.

Tot slot wil ik uw aandacht vragen voor het leveren van gegevens via SUWInet aan incassobureaus of andere derden. Op grond van de Wet bescherming persoonsgegevens is het toegestaan om een derde partij als bewerker gegevens te laten verwerken, waarbij het college van B&W verantwoordelijke blijft. Hiervoor dient een bewerkersovereenkomst te worden gesloten. In het geval een gemeente een incassobureau inschakelt mogen alleen die gegevens worden verstrekt aan het incassobureau die nodig zijn voor het incassobureau om de vorderingen te kunnen innen. Daarbij is het niet toegestaan dat incassobureaus toegang krijgen tot meer gegevens dan noodzakelijk voor de uitoefening van hun taak. Op grond hiervan is toegang tot SUWInet, waar veel meer gegevens van (alle) burgers zijn in te zien, niet toegestaan. In de notitie 'uitbesteden en toegang tot SUWInet' die de VNG heeft opgesteld, kunt u hierover meer informatie vinden.

Het escalatieprotocol is tot stand gekomen in samenwerking met VNG, SVB en UWV. De bescherming van de persoonsgegevens is een grondrecht en het is niet acceptabel dat de overheid hierin tekort schiet. Dit betekent dat gemeenten, ondersteund door de VNG, met hoge urgentie door moeten pakken en de beveiliging van SUWInet op orde moeten brengen.

Paralel aan deze brief informeer ik de gemeenteraden over het veilig gebruiken van SUWInet.

De Staatssecretaris van Sociale Zaken
en Werkgelegenheid,

Jetta Klijnsma

Bijlage 1

Overzicht bevindingen gemeenten (78)

Gemeente	Norm 1.3	Norm 1.4	Norm 1.5	Norm 2.2	Norm 2.3	Norm 13.1	Norm 13.5	Aantal normen Voldoende
Aalten	x	x	x	x		x		5
Alblasserdam	x	x	x	x		x	x	6
Albrandswaard	x	x	x	x		x		5
Alkmaar								0
Assen	x	x	x	x	x	x	x	7
Baarle-Nassau								0
Barendrecht	x	x	x	x		x		5
Binnenmaas	x	x	x	x	x	x	x	7
Blaricum	x	x		x	x	x		5
Boekel	x	x	x	x	x	x	x	7
Boxmeer	x	x	x	x				4
Breda	x	x	x	x	x	x	x	7
Brielle								0
Brummen								0
Bunnik	x							1
Buren	x	x				x	x	4
Cranendonck				x	x	x	x	4
Dantumadiel	x	x	x	x		x		5
Den Haag	x	x		x	x			4
Deurne	x	x		x	x			4
Deventer	x		x	x			x	4
Dinkelland				x	x	x	x	4
Ede	x	x				x		3
Geldrop-Mierlo	x	x		x	x			4
Giessenlanden	x	x	x	x	x		x	6
Groesbeek	x	x	x	x				4
Heemskerk	x	x						2
Heemstede	x	x	x	x	x	x	x	7
Heerenveen								0
Helmond	x	x		x	x			4
Hendrik-Ido-Ambacht	x	x	x	x		x	x	6
Het Bildt	x	x	x	x	x	x		6
Heumen	x					x		2
Hof van Twente	x							1
Houten	x	x	x	x	x	x	x	7

Gemeente	Norm 1.3	Norm 1.4	Norm 1.5	Norm 2.2	Norm 2.3	Norm 13.1	Norm 13.5	Aantal normen Voldoende
Kampen	x	x		x		x	x	5
Krimpen aan den IJssel	x							1
Laren	x	x		x	x	x		5
Leek	x	x	x	x	x	x	x	7
Lelystad	x	x		x	x	x	x	6
Leusden	x	x		x	x	x	x	6
Lingewaard		x						1
Meerssen				x				1
Molenwaard	x	x	x	x	x		x	6
Nieuwkoop	x	x	x	x	x	x		6
Noordwijkerhout	x	x		x		x		4
Oisterwijk	x		x					2
Oldebroek	x		x	x	x	x	x	6
Ommen				x		x		2
Papendrecht	x	x	x	x		x	x	6
Reusel-De Mierden	x	x	x	x	x	x	x	7
Rheden	x	x	x	x	x			5
Rhenen	x							1
Roerdalen	x			x		x	x	4
Scherpenzeel	x					x		2
Schijndel	x	x	x	x	x	x	x	7
Schinnen	x							1
Schoonhoven	x	x	x	x	x		x	6
Sluis	x			x				2
Súdwest Fryslân		x	x					2
Texel	x	x	x	x		x		5
Twenterand	x	x	x	x	x			5
Tynaarlo	x	x	x	x	x	x	x	7
Urk	x	x	x	x	x	x		6
Veldhoven	x							1
Venray				x				1
Vlaardingen	x	x	x	x	x	x	x	7
Vught	x		x			x		3
Waalre	x	x	x	x	x		x	6
Wassenaar	x		x	x				3
Weert	x	x	x	x				4
Werkendam								0

Gemeente	Norm 1.3	Norm 1.4	Norm 1.5	Norm 2.2	Norm 2.3	Norm 13.1	Norm 13.5	Aantal normen Voldoende
West Maas en Waal	x		x	x				3
Weststellingwerf	x	x	x	x	x	x	x	7
Wierden	x		x	x				3
Wormerland	x	x		x	x	x		5
Woudenberg								0
Zevenaar	x	x	x	x	x	x	x	7
Totaal onderzoek 2013	76%	31%	21%	30%	24%	38%	20%	Gem. 2.4
Totaal onderzoek 2015	82%	63%	53%	72%	44%	53%	37%	Gem. 3.9

Gemeenten in kleur zaten ook in het vorige onderzoek van de Inspectie SZW.

Bijlage 2

Escalatieprotocol afsluiten SUWInet

In dit protocol wordt beschreven uit welke stappen het "escalatieprotocol afsluiten SUWInet" bestaat. Iedere stap in het protocol is erop gericht om te bewerkstelligen dat tekortkomingen in de beveiliging van SUWInet worden weggenomen. Als ultimum remedium is het mogelijk om een gemeente af te sluiten van het gebruik van SUWInet. Afsluiting van het gebruik van SUWInet heeft vergaande consequenties voor de burger. Hij moet zijn gegevens opnieuw aanleveren en wordt daarmee onevenredig belast.

STAP 1 Zelfevaluatie (vrijwillig)
Gemeenten kunnen via een zelftest van de VNG onderzoeken of wordt voldaan aan de normen uit het SUWI-normenkader. De zelftest is een analyse die aangeeft op welke onderdelen uit het SUWI-normenkader aanpassingen of verbeteringen aangebracht moeten worden. De zelftest is daarmee een instrument van en voor gemeenten *zelf* om invulling te geven aan de verantwoordelijkheid voor de beveiliging van de gegevens die via SUWInet worden ontvangen. Het verdient aanbeveling om de uitkomsten van de zelftest in het College van B&W te agenderen en het (eventuele) verbeterplan dat daaruit volgt door het College van B&W te laten vaststellen en hierover de gemeenteraad te informeren. Maatregelen kunnen ook worden opgenomen in het jaarlijks verplicht op te stellen beveiligingsplan en/of het verslag over de verantwoording.

STAP 2 Jaarverslag (bestaande wettelijke verplichting)
Op grond van de SUWI wet-en regelgeving[1] is geregeld dat iedere gebruiker van Suwinet, dat wil zeggen het UWV, de SVB en de colleges van B&W voor de SUWI-taken aantoont dat het stelsel van de door zijn organisatie genomen maatregelen voldoet aan het SUWI-normenkader. Het jaarlijkse verslag over het gebruik van SUWInet moet ieder jaar worden vastgesteld. Het aantonen gebeurt door in te gaan op opzet, bestaan, werking en controleerbaarheid van het stelsel van maatregelen en procedures gericht op de gegevenshuishouding in relatie tot SUWInet. De rapportage dient te worden bevestigd met een oordeel (van getrouwheid) van een tot de Nederlandse Orde van Register EDP-Auditor toegelaten persoon. De verantwoording over de informatiebeveiliging biedt het college van B&W en de gemeenteraad een handvat om hun verantwoordelijkheid voor informatiebeveiliging en bescherming van persoonsgegevens in te vullen. Daarnaast kunnen burgers er vertrouwen aan ontlenen dat gemeenten de aan hen toevertrouwde gegevens zorgvuldig verwerken.

STAP 3 Onderzoek van de Inspectie SZW
De Inspectie SZW houdt toezicht op de wijze waarop het UWV, de SVB, en de colleges van burgemeester en wethouders bij de uitvoering van de aan hen opgedragen taken samenwerken. Het toezicht van de inspectie is onafhankelijk en signalerend. De aard en intensiteit van het toezicht hangen af van de kwaliteit van de uitvoering en de risico's die zich in de uitvoering voordoen. De risico's betreffende de informatiebeveiliging van SUWInet bij gemeenten wordt betrokken bij het opstellen van het jaarplan van de Inspectie. De mate waarin gemeenten hebben aangetoond dat de beveiliging van SUWInet op orde is, zal leidend zijn voor de intensiteit van onderzoek door de inspectie. Onderzoeken van de Inspectie SZW naar de beveiliging van SUWInet richten zich op de 7 normen uit het SUWI-normenkader. Uit het onderzoek van de Inspectie SZW volgt welke gemeenten niet aan alle 7 (essentiële) normen voldoen. Voor gemeenten die niet voldoen aan de 7 essentiële normen treedt stap 4 in werking. Het College Bescherming Persoonsgegevens zal worden geïnformeerd over de resultaten van het onderzoek van de Inspectie SZW.

STAP 4 Aankondiging tot een aanwijzing
De gemeente die niet aan alle 7 essentiële normen voldoet ontvangt een aankondiging tot een aanwijzing. De gemeente ontvangt dan een brief waarin het voornemen tot een aanwijzing wordt aangekondigd. De gemeente krijgt in deze fase een laatste mogelijkheid om de beveiliging van

[1] Artikel 5.22 besluit SUWI en artikel 5.22 en 6.4 van de Regeling SUWI.

SUWInet op orde te brengen. In deze aankondiging zal een termijn worden genoemd, die afhankelijk is van de specifieke situatie in de betreffende gemeente. Na de genoemde termijn zal de gemeente moeten aangeven of de onrechtmatige situatie is hersteld en wordt voldaan aan alle 7 essentiële normen. Afhankelijk van de situatie kan het voorkomen dat een gemeente nog niet aan 1 norm kan voldoen. Met deze gemeente worden nadere afspraken gemaakt over de termijn waarbinnen alsnog aan deze norm wordt voldaan.

STAP 5 Aanwijzing tot het op orde brengen van de beveiliging van SUWInet
Een gemeente die geen verantwoordelijkheid neemt voor de beveiliging van SUWInet en ook na de aankondiging van de aanwijzing geen orde op zaken heeft gesteld, zal een aanwijzing ontvangen. Een mogelijke aanwijzing kan zijn dat een gemeente wordt verplicht om, na een daartoe door SZW gestelde termijn, door middel van een audit aan te tonen dat de beveiliging van SUWInet op orde is. Dit is een relatieve milde aanwijzing. Dit kan aan de orde zijn als de gemeente verbeteringen heeft doorgevoerd, maar nog een aantal punten niet heeft opgelost. Ook kan een aanwijzing worden gegeven waarin de gemeente wordt opgedragen om een externe deskundige in te huren om de beveiliging van SUWInet op orde te brengen. De Minister van SZW bepaalt aan welke voorwaarden de externe deskundige dient te voldoen en welk resultaat bereikt dient te worden, voordat de gemeente weer zelfstandig de uitvoering ter hand kan nemen. De kosten voor het uitvoeren van een audit of het inhuren van één of meerdere externe deskundigen zijn volledig voor rekening van de gemeente. Dit zal aan de orde zijn als de gemeente er blijk van heeft gegeven het herstellen van de onrechtmatigheden niet zelfstandig uit te kunnen voeren.

STAP 6 Treffen van noodzakelijke voorziening tot het afsluiten van SUWInet
Indien een gemeente zelfs de aanwijzing niet opvolgt, zal de Minister van SZW zelf in de zaak voorzien. Zo kan de Minister zelf een externe deskundige aanstellen en bij een gemeente installeren, uiteraard op kosten van die gemeente.[2] In situaties waarin er een acuut en reëel risico is op grove schendingen van de privacy van burgers, kan het geboden zijn een gemeente (tijdelijk) van SUWInet af te sluiten. De minister van SZW zal op dat moment aan de beheerder vragen om de verleende autorisaties voor SUWInet in te trekken. Dit betekent dat er geen mogelijkheid meer is voor gemeenten om gegevens in te zien. Gemeenten zullen wel gegevens kunnen blijven leveren. Het afsluiten van SUWInet heeft tot gevolg dat gemeenten zelf informatie van hun burgers zullen moeten vragen, of via individuele overeenkomsten met andere partners in de keten moeten betrekken. Voor zover die partners op grond van staande wetgeving niet zijn gehouden deze gegevens kosteloos te verstrekken, kunnen ook hiervoor kosten in rekening worden gebracht.

Toezicht College Bescherming Persoonsgegevens
De minister kan op ieder moment in het proces of wanneer daartoe aanleiding is het College Bescherming Persoonsgegevens informeren en vragen om handhavend op te treden. Het College Bescherming Persoonsgegevens maakt vervolgens een zelfstandige afweging of het overgaat tot het verrichten van een onderzoek.

Het CBP kan een last onder dwangsom opleggen indien uit onderzoek van het CBP blijkt dat gemeenten niet voldoen aan de Wet bescherming persoonsgegevens. Een andere mogelijkheid is het opleggen van een boete. De wet die regelt dat het College Bescherming Persoonsgegevens (CBP) de bevoegdheid heeft om aan verantwoordelijken en bewerkers bestuurlijke boetes op te leggen voor overtredingen van de Wet bescherming persoonsgegevens (Wbp) en andere specifieke dataprotectieregels is door de Eerste Kamer aanvaard en zal vermoedelijk op 1 januari 2016 in werking treden. De boete kan maximaal € 810.000 bedragen.

[2] Gedacht kan worden aan bijvoorbeeld inhuur vanuit ABD-topconsult.