

> Retouradres Postbus 90801 2509 LV Den Haag

De Voorzitter van de Tweede Kamer
der Staten-Generaal
Binnenhof 1 A
2513 AA S GRAVENHAGE

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

Onze referentie
2017-0000044390

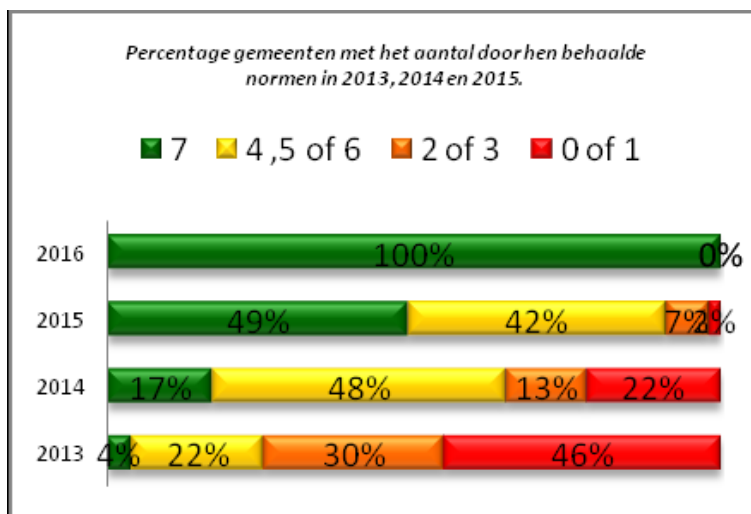
Bijlagen
1. Rapport SUWInet 2016
Stand van zaken na ontvangst
in-control verklaringen
gemeenten
2. Rapport PIA Toegang
persoonsgegevens SUWInet
3. Bestuurlijke reacties UWV,
SVB en VNG op Rapport PIA

Datum 11 april 2017
Betreft SUWInet

Met deze brief bied ik u het rapport 'SUWInet 2016 Stand van zaken na ontvangst in-control verklaringen gemeenten' van de Inspectie SZW aan en informeer ik u over de stand van zaken van het Programma 'Borging veilige gegevens-uitwisseling via Suwinet'. Verder informeer ik u over de motie Ulenbelt - van Weyenberg¹ inzake het beperken van de toegang tot gegevens via SUWInet tot gegevens van relevante personen en stuur ik u daarbij het Privacy Impact Assessment (PIA) Toegang persoonsgegevens SUWInet.

Beveiliging van Suwinet bij gemeenten

Over de privacy van burgers moet goed worden gewaakt. De Inspectie SZW heeft op mijn verzoek in 2016 een vervolgonderzoek gedaan naar de beveiliging van SUWInet bij gemeenten die in 2015 nog niet voldeden aan de zeven belangrijkste beveiligingsnormen. Ik ben verheugd dat de inspectie concludeert dat alle gemeenten aan de zeven belangrijkste normen voldoen. Onderstaande figuur laat de voortgang in de afgelopen jaren zien.



¹ Kamerstukken 26448, nr. 513, 28 mei 2014

In 2013 signaleerde de inspectie ernstige tekortkomingen in de beveiliging van SUWInet bij gemeenten. Aangespoord en ondersteund door de VNG hebben gemeenten in de afgelopen jaren de beveiliging van SUWInet verbeterd. Om alle gemeenten daar toe te zetten heb ik in 2015 het 'Escalatieprotocol afsluiten SUWInet' opgesteld. In 2016 heb ik dit protocol toegepast en de gemeenten die nog niet aan de zeven belangrijkste normen voldeden een aankondiging tot een aanwijzing gestuurd. Betrokken gemeenten hebben vervolgens de beveiliging verder verbeterd en aan mij verklaard dat de beveiliging op orde is gebracht. Op mijn verzoek heeft de inspectie in 2016 het bijgevoegde vervolgonderzoek gedaan en daarbij een steekproef van 65 gemeenten getrokken uit de 198 gemeenten die in het onderzoek van 2015 niet aan de zeven belangrijkste normen voldeden. Ik stel vast dat de inspectie met dit onderzoek de verklaringen van de gemeenten onderschrijft. Ondanks deze mooie resultaten blijft het nodig om de vinger aan de pols te houden.

Datum

11 april 2017

Onze referentie

2017-0000044390

Van belang is dat gemeenten hun verantwoordelijkheid voor de beveiliging van SUWInet structureel invullen. Een belangrijke waarborg hierbij is de jaarlijkse verantwoording over de beveiliging van SUWInet zoals vastgelegd in de Regeling SUWI. Hierbij is de gemeenteraad de eerst aangewezen partij om de informatiebeveiliging te controleren. Met ingang van het verantwoordingsjaar 2017 zal ik alle colleges van B en W aan deze verantwoordingsplicht houden. Het project ENSIA (Eenduidige Normatiek Single Information Audit) voorziet hierbij in een werkwijze die de administratieve lasten voor gemeenten bij het afleggen van verantwoording over de informatiebeveiliging voor meerdere registraties en voorzieningen reduceert.² Onder de reikwijdte van ENSIA vallen de basis-registraties personen, gebouwen en adressen, het aanvraag- en uitgifte proces van reisdocumenten, het gebruik van DigiD voor identificatie en authenticatie van burgers en het gebruik van gegevens op het terrein werk en inkomen via SUWInet.

Programma Borging veilige gegevensuitwisseling via Suwinet

Dit programma heeft zich in de afgelopen twee jaar gericht op het wegnemen van privacykwetsbaarheden in de keten van gegevensbron tot gegevensafnemer. De maatregelen van het programma zijn ondersteunend en aanvullend aan de maatregelen die gemeenten hebben genomen om aan de zeven belangrijkste beveiligingsnormen te voldoen.

Een aantal maatregelen richt zich op het beperken van de toegang tot gegevens. Dit komt tot uitdrukking in het beperken van het aantal medewerkers met toegang tot SUWInet, het beperken van de gegevens die een medewerker van een persoon kan raadplegen, het beperken van het aantal personen waarvan een medewerker gegevens kan raadplegen en het beperken van het gebruik van zoekleutels. Andere resultaten van het programma zijn het verbeteren van de rapportages over het gebruik van gegevens ten behoeve van een snellere en meer gerichte controle achteraf, een uniform sanctiebeleid bij geconstateerd misbruik van gegevens, het herijken van de beveiligingsnormen en het realiseren van middelen om de bewustwording betreffende een zorgvuldig gebruik van gegevens te bevorderen. Om op bestuurlijk niveau de bewustwording te versterken over de voorwaarden die gelden bij een aansluiting op SUWInet worden aanvullend zogenoemde aansluitvoorwaarden ter ondertekening voorgelegd.

² Brief Minister van BZK, 18 december 2014

De door het programma ontwikkelde producten zijn voor een deel reeds bij de op SUWInet aangesloten organisaties geïmplementeerd. Om gemeenten te ondersteunen bij het implementeren van de producten van het programma is met ingang van afgelopen september, voor de duur van een jaar, een team van vijf accountmanagers bij VNG/KING gestart.

Datum

11 april 2017

Onze referentie

2017-0000044390

Verder is onderzocht op welke wijze burgers inzage wordt geboden in de gegevens die via SUWInet worden uitgewisseld. Dit heeft ertoe geleid dat betrokken organisaties op hun websites op uniforme en begrijpelijke wijze algemene informatie gaan opnemen over de gegevensuitwisseling via SUWInet. Verder gaan zij ervoor zorgen dat burgers op digitale wijze hun inzagerecht kunnen uitoefenen waar het gegevens betreft die over burgers via SUWInet zijn uitgewisseld. Deze maatregelen worden als onderdeel van het implementeren van de Algemene Verordening Gegevensbescherming gerealiseerd en daarbij afgestemd op de wijze waarop de organisaties inzage geven in andere gegevensverwerkingen en -uitwisselingen en de wijze waarop overheidsbreed de inzage in gegevens wordt vormgegeven. De Algemene Verordening Gegevensbescherming betreft Europese wetgeving die met ingang van 25 mei 2018 van toepassing is.

Privacy Impact Assessment (PIA) Toegang persoonsgegevens Suwinet

Ik heb u eerder geïnformeerd dat UWV, SVB en VNG het beperken van de toegang tot het aantal personen waarvan een medewerker gegevens kan raadplegen, onderzoeken en dat deze onderzoeken van een PIA worden voorzien.³ Hierbij stuur ik u het rapport en bestuurlijke reacties van UWV, SVB en VNG daarbij. Het rapport wijst uit dat aan de 'achterkant' goede maatregelen zijn genomen om de privacy rondom het raadplegen van gegevens via SUWInet beter te waarborgen. Denk hierbij aan de controle op het gebruik van gegevens en het waar nodig sanctioneren van misbruik. De onderzoekers merken op dat redenerend vanuit het bestaande wettelijke kader en de aanstaande Algemene Verordening Gegevensbescherming stappen moeten worden gezet om de toegang tot gegevens aan de 'voorkant' te beperken.

Het rapport wijst uit dat SVB en gemeenten, met als vertrekpunt een toegang tot alle Nederlanders, stappen in de goede richting zetten door de toegang te beperken tot actuele dienstverleningsrelaties. Hierbij passen SVB en gemeenten het instrument 'whitelist' toe. Bij de SVB betekent dit dat een medewerker via SUWInet toegang zal hebben tot ongeveer 400.000 personen op een totaal van 4 miljoen personen waarvoor de SVB diensten verleent. De SVB gaat deze stap in 2017 zetten. Voor een gemeente betekent het beperken van de toegang tot actuele dienstverleningsrelaties dat een medewerker toegang zal hebben tot alle bijstandsgerechtigden van de betreffende gemeente. Ter illustratie: de gemeente Best heeft 28.954 inwoners en kent bijna 1.100 personen met een actuele dienstverleningsrelatie. Dit is 3,8% van het aantal inwoners van de gemeente of 0,006% van het inwonersaantal van Nederland. Gemeenten gaan deze stap in 2017 zetten. Gezien het complexe ICT-landschap en de brede en diverse wet- en regelgeving en dienstverlening van UWV is het toepassen van één whitelist bij UWV niet mogelijk. In de bijgevoegde bestuurlijke reactie licht UWV de aanpak toe. De eerste maatregel die UWV neemt betreft het uitsluiten dat medewerkers gegevens van personen kunnen raadplegen die niet tot de kring van verzekerden van de werknemersverzekeringen horen, denk hierbij aan personen onder de 18 jaar en boven de AOW-gerechtigde leeftijd. UWV gaat in de toekomst applicaties toepassen waarin medewerkers alleen de gegevens van personen zien die tot de

³ Kamerstukken 26 448, nr. 530, 30 juni 2015 en nr. , 28 juni 2016

'caseload' van een medewerker behoren. Daar waar een dergelijke applicatie niet mogelijk is, zal UWV de toegang op proces- of afdelingsniveau beperken. In april 2017 ontvang ik van UWV een plan van aanpak met de concrete korte, middellange en lange termijn maatregelen. Verder gaat UWV deze maatregelen integreren in het UWV Informatieplan⁴.

Datum

11 april 2017

Onze referentie

2017-0000044390

Tot slot

De hiervoor beschreven maatregelen geven een stevige impuls aan het beschermen van persoonsgegevens bij het uitwisselen van gegevens via SUWInet. Incidenten kunnen echter altijd voorkomen. Het structureel beschermen van persoonsgegevens zal bij voortduring een grote alertheid en vasthoudendheid vergen van UWV, SVB, gemeenten en mijn ministerie.

De Staatssecretaris van Sociale Zaken
en Werkgelegenheid,

Jetta Klijnsma

⁴ Kamerstukken 26448, nr. 575, 13 september 2016