Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2018–2019

26 448 Structuur van de uitvoering werk en inkomen (SUWI)

Nr. 609

BRIEF VAN DE STAATSSECRETARIS VAN SOCIALE ZAKEN EN WERKGELEGENHEID

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 5 maart 2019

Met deze brief bied ik u de Totaalrapportage over de beveiliging van Suwinet in 2017 aan[1] en informeer ik u over de stappen om het stelsel van gegevensuitwisseling werk en inkomen te moderniseren.

Beveiliging Suwinet

Over de privacy van burgers moet goed worden gewaakt. In de brief van 11 april 2017[2] heeft mijn voorganger u geïnformeerd over de beveiliging van Suwinet bij gemeenten en de daarbij genomen en verder te nemen verbetermaatregelen. Onderzoek van de Inspectie SZW bevestigde dat in 2016 alle gemeenten aan zeven normen voldeden die belangrijk zijn voor een vertrouwelijke omgang met via Suwinet toegankelijke persoonsgegevens. Het gaat bijvoorbeeld om een toereikend informatiebeveiligingsbeleid en een toereikende controle op het raadplegen van gegevens door medewerkers.

Verder is in de periode 2015–2017 het programma «Borging veilige gegevensuitwisseling via Suwinet» uitgevoerd om diverse privacykwetsbaarheden in de keten van gegevensbron tot gegevensafnemer weg te nemen. De maatregelen van het programma zijn ondersteunend en aanvullend aan de maatregelen van gemeenten om aan de zeven beveiligingsnormen te voldoen.

Een aantal maatregelen richtte zich op het beperken van de toegang tot gegevens. Dit kwam tot uitdrukking in het beperken van het aantal medewerkers met toegang tot Suwinet, het beperken van het gebruik van zoeksleutels, het beperken van de gegevens die een medewerker van een persoon kan raadplegen en het beperken van het aantal personen

[1] Raadpleegbaar via www.tweedekamer.nl
[2] Kamerstukken 26 448, nr. 589

kst-26448-609
ISSN 0921 - 7371
's-Gravenhage 2019

waarvan een medewerker gegevens kan raadplegen. Het beperken van de toegang tot de actuele dienstverleningsrelaties van een gemeente in plaats van toegang tot alle Nederlanders geeft bijvoorbeeld voor de gemeente Best het volgende beeld. De gemeente Best heeft 28.954 inwoners en kent bijna 1.100 personen met een actuele dienstverleningsrelatie in het kader van de bijstand. Dit is 3,8% van het aantal inwoners van de gemeente of 0,006% van het inwonersaantal van Nederland.

Andere resultaten van het programma waren 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.

Tot slot is in de hiervoor genoemde brief aangegeven dat het project ENSIA (Eenduidige Normatiek Single Information Audit) voorziet in het realiseren van een werkwijze die de administratieve lasten voor gemeenten bij het jaarlijks afleggen van verantwoording over de informatiebeveiliging voor meerdere registraties en voorzieningen reduceert.[3] Onder de reikwijdte van ENSIA vallen de basisregistraties personen, gebouwen, adressen en ondergrond, het aanvraag- en uitgifte proces van reisdocumenten, het gebruik van DigiD voor identificatie en authenticatie van burgers en het gebruik van gegevens via Suwinet. Met ENSIA komen allereerst de colleges van B&W en de gemeenteraden in positie om hun verantwoordelijkheid voor de informatiebeveiliging te nemen. Aansluitend kom ik in positie om het Interventieprotocol Suwinet (zie bijlage[4]) toe te passen bij gemeenten die afwijken van de aan het Suwinet gestelde beveiligingsnormen.

In de hiervoor genoemde brief is opgemerkt dat de maatregelen een stevige impuls geven aan het beschermen van persoonsgegevens bij het uitwisselen van gegevens via Suwinet en dat incidenten niet altijd kunnen worden voorkomen. Verder is opgemerkt dat het structureel beschermen van persoonsgegevens bij voortduring een grote alertheid en vasthoudendheid van UWV, SVB, gemeenten en het Ministerie van SZW vergen. Ik onderschrijf deze inzet.

Voor het verantwoordingsjaar 2017 hebben gemeenten voor het eerst de ENSIA-systematiek toegepast.[5] De bijgevoegde Totaalrapportage[6] schetst de stand van de beveiliging van Suwinet en is gebaseerd op de verantwoordingen van gemeenten conform de ENSIA-systematiek. Ik merk hierbij op dat het aantal onderzochte beveiligingsnormen ten opzichte van de eerdere onderzoeken van de Inspectie SZW is uitgebreid van 7 naar 11. Gegevens worden namelijk steeds meer direct ingelezen in de eigen applicaties van gemeenten en ook in deze situatie dienen gemeenten het raadplegen van deze gegevens te controleren. De toepassing van ENSIA heeft de volgende afwijkingen van de beveiligingsnormen aan het licht gebracht.

---

[3] Kamerstuk 26 643, nr. 344
[4] Raadpleegbaar via www.tweedekamer.nl
[5] Zie de toelichting op ENSIA in de brief van de Minister van BZK over het verhogen van de informatieveiligheid van de overheid, Kamerstuk 26 643, nr. 574, 16 oktober 2018
[6] Raadpleegbaar via www.tweedekamer.nl

Tabel: Afwijkingen van de beveiligingsnormen per 31 december 2017 bij gebruik door gemeenten van Suwinet voor SUWI-taken betreffende 11 onderzochte normen (bron: Totaalrapportage Beveiliging GeVS 2017)

Afwijkingen	*Aantal gemeenten*	*percentage*
0	173	45,8
1	55	14,6
2	39	10,3
3	36	9,5
4 of meer	63	16,7
onbekend	12	3,2
Totaal	378	100

Het betreft afwijkingen van beveiligingsnormen die gericht zijn op een vertrouwelijke omgang van via Suwinet toegankelijke persoonsgegevens zoals:

- het eenmaal in de 3 jaar actualiseren van het informatiebeveiligingsbeleid Suwinet om richting te geven aan de aard van de te nemen beveiligingsmaatregelen;
- het vaststellen van dit informatiebeveiligingsbeleid door het College van B&W;
- het aan medewerkers toekennen van niet meer toegangsrechten dan noodzakelijk voor de taken van medewerkers;
- het regelmatig beoordelen van de toegekende toegangsrechten door het verantwoordelijke management en
- het controleren van log-informatie om vast te stellen of oneigenlijk gebruik of misbruik is gemaakt van de toegekende autorisaties en het op basis daarvan toepassen van het sanctiebeleid.

De Totaalrapportage geeft inzicht in het aantal afwijkingen per beveiligingsnorm.

Ik vind het belangrijk dat de overheid zorgvuldig omgaat met gegevens van burgers. Deze afwijkingen hebben dan ook mijn aandacht. Allereerst is het aan de gemeenten om de door henzelf geconstateerde afwijkingen voortvarend weg te nemen. Ik merk hierbij op dat de ENSIA-systematiek de colleges van B&W en de gemeenteraden via de zogenoemde Collegeverklaring Informatiebeveiliging ENSIA handvatten biedt om waar nodig verbeterplannen op te stellen en uit te voeren. Ik heb met de VNG afgesproken dat zij gemeenten hierbij ondersteunen. Daarnaast stuurt de VNG een ledenbrief om de urgentie te benadrukken. Verder doet de domeingroep Beveiliging & Privacy Suwinet van UWV, SVB en gemeenten onderzoek naar de oorzaken van de afwijkingen om op basis daarvan ondersteunende maatregelen te kunnen nemen. Te denken valt aan nadere voorlichting over de beveiligingsnormen. Verder heb ik het hiervoor genoemde Interventieprotocol Suwinet toegepast (zie bijlage[7]). Een eerste stap hierin is dat het Bureau Keteninformatisering Werk en Inkomen (BKWI)[8] een zogenoemde Attentiebrief naar 205 gemeenten met afwijkingen heeft gestuurd. Indien bij een volgende verantwoording blijkt dat de afwijkingen niet zijn weggenomen dan zijn verdere mogelijke stappen een (aankondiging van) een aanwijzing conform de wet SUWI en als laatste stap zelfs het afsluiten van Suwinet. Een eerste versie van het Interventieprotocol is in 2015 en 2016 naar aanleiding van de toenmalige onderzoeken van de Inspectie SZW opgesteld en toegepast. 198 gemeenten hebben toen een aankondiging van een aanwijzing ontvangen. Dit heeft er mede toe geleid dat de Inspectie SZW in 2016 concludeerde dat alle gemeenten aan de 7 beveiligingsnormen voldeden. In het vierde kwartaal van 2019 zal ik u informeren over de stand van de beveiliging per 31 december 2018.

[7] Raadpleegbaar via www.tweedekamer.nl

[8] Het BKWI is een afzonderlijk en herkenbaar organisatieonderdeel van het UWV

Modernisering van het stelsel van gegevensuitwisseling werk en inkomen

In de afgelopen jaren heeft de digitalisering van het stelsel werk en inkomen en als onderdeel daarvan de gegevensuitwisseling, een grote vlucht genomen. Deze ontwikkeling was aanleiding om een visie op de toekomst van de gegevensuitwisseling in het werk en inkomen domein te ontwikkelen en vervolgens het programma Toekomst Gegevensuitwisseling Werk en Inkomen te starten om deze visie in de praktijk te brengen. Kernpunt van de visie is dat burgers meer regie krijgen op de dienstverlening en op hun gegevens. Dit betekent dat ik in de eerste plaats burgers beter wil toerusten om zelfstandig, met behulp van gegevens over henzelf en over hun persoonlijke leefsituatie, verantwoordelijkheid te nemen voor (belangrijke) keuzes waar zij voor staan. Zij kunnen bovendien efficiënter werken omdat zij de beschikking krijgen over digitale gegevens over henzelf waarover de overheid beschikt, en deze gegevens hergebruiken in allerlei diensten die zij inroepen van publieke en private partijen. In de tweede plaats verwacht ik dat publieke en private partijen die diensten verlenen aan burgers profiteren van deze ontwikkelingen. Omdat burgers beter worden toegerust, zijn deze partijen minder tijd kwijt voor het begeleiden van deze burgers en voor herstelwerkzaamheden in het geval zij verkeerde informatie aanleveren of een verkeerde keuze maken. De met het programma ingezette beweging sluit aan op de kabinetsbrede strategie op het terrein van digitalisering n.a.v. het regeerakkoord.[9]

Het programma realiseert:
- De benodigde digitale infrastructuur om burgers inzicht te geven in hun persoonlijke situatie en om het voor burgers mogelijk te maken om bij de overheid beschikbare gegevens op digitale wijze in private en publieke diensten te benutten. In 2019 worden de belangrijkste ontwerpkeuzes van deze digitale infrastructuur gemaakt.
- Een afsprakenstelsel dat duidelijk maakt onder welke condities gegevens over burgers door publieke of private partijen digitaal kunnen worden geleverd aan die burger, dan wel door tussenkomst van die burger kunnen worden geleverd aan een andere publieke of private partij. Dit betreft bijvoorbeeld afspraken over de verantwoordelijkheden van burgers, bronhouders en afnemende, dienstverlenende partijen en over een besturingsstructuur die voldoende garanties biedt dat partijen waar tussen gegevens worden uitgewisseld aan de gestelde eisen voldoen. De principes van dit afsprakenstelsel krijgen een plaats in wet- en regelgeving.

Het programma wordt uitgevoerd door mijn ministerie samen met UWV, SVB, VNG, het Inlichtingenbureau (IB) en het BKWI. Daarbij wordt afgestemd met lopende trajecten van onder andere de Agenda Digitale Overheid van mijn collega van BZK. Het programma heeft tot op heden een demo van een Persoonlijke Inkomensomgeving ontwikkeld en met burgers geëvalueerd. De demo bevat realistische fictieve gegevens en maakt zichtbaar hoe het concept van burgers die meer regie krijgen op de dienstverlening in de praktijk vorm gegeven kan worden. In deze demo wordt burgers, bij de gebeurtenissen »ik ga van WW naar bijstand» en «ik ga vanuit bijstand met pensioen» inzicht gegeven in hun financiële situatie en in de financiële consequenties van de verschillende keuzemogelijkheden.

In 2019 gaat het programma het concept van het versterken van regie op dienstverlening en de daarvoor benodigde infrastructuur en afspraken met een afgebakend aantal burgers uit testen om te leren wat op welke

[9] Kamerstuk 26 643, nr. 549, NL-DIGIbeter – Agenda Digitale Overheid, juli 2018

wijze kan werken. Een belangrijk aandachtspunt hierbij is de wijze waarop de dienstverlening aan kan sluiten op de (digitale) vaardigheden van de veelal kwetsbare doelgroep. Allereerst wordt de demo van de Persoonlijke Inkomensomgeving via de bestaande digitale infrastructuur van het IB en het BKWI en aanvullend te realiseren gegevensdiensten gekoppeld aan daadwerkelijke registraties met gegevens over burgers. Een tweede test heeft als doel om burgers in de doelgroep van de Aanvullende Inkomensvoorziening Ouderen (AIO) op het juiste moment duidelijke informatie te geven over hun recht op AIO. Een deel van de potentiële groep rechthebbenden bevindt zich onder de mensen onder de pensioengerechtigde leeftijd die nu al bijstand ontvangen. Verder wordt in samenwerking met het programma I4 Sociaal van de gemeenten Enschede, Groningen, Zwolle en Deventer getest of mensen met een bijstandsuitkering eerder (tijdelijk) werk aanvaarden door inzicht te geven in de financiële gevolgen van het aanvaarden van werk om zo onzekerheid over de toekomstige financiële situatie te reduceren. Met het programma I4 Sociaal wordt ook getest of mensen die op een minimum niveau leven op een eenvoudige en toegankelijke manier kunnen worden geïnformeerd over regelingen die op hun situatie van toepassing zijn. De ervaringen van deze tests worden benut bij het maken van keuzes voor het vorm geven van het afsprakenstelsel en de digitale infrastructuur.

Tot slot merk ik op dat ik verwacht dat het ontsluiten en bewerken van de gegevens waarover burgers, private en publieke partijen beschikken, veel kansen biedt. Denk aan kansen voor burgers om beter zicht te hebben op inkomsten en uitgaven en zo schulden te voorkomen of eerder de stap van een bijstandsuitkering naar werk te maken. Het is hierbij aan de overheid om op een zorgvuldige wijze met gegevens van burgers om te gaan en de waarborgen te realiseren waaronder burgers bij de overheid beschikbare gegevens op digitale wijze in private en publieke diensten kunnen benutten.

De Staatssecretaris van Sociale Zaken en Werkgelegenheid,
T. van Ark