Bijlage

De Suwi-partijen UWV, SVB en de VNG hebben per brief (van 7 oktober 2014) aan de minister en de staatssecretaris van SZW het programmaplan Borging Veilige Gegevensuitwisseling Suwinet aangeboden. Dit programmaplan omvat een samenhangend pakket aan (aanvullende) maatregelen, gericht op het borgen van veilige gegevensuitwisseling en betere bescherming van persoonsgegevens. De maatregelen dragen bij aan het wegnemen van de gesignaleerde kwetsbaarheden.

- Programmaplan Borging Veilige Gegevensuitwisseling Suwinet

Het ministerie van SZW heeft met instemming gereageerd op dit plan. Op basis hiervan zijn de Suwi-partijen gezamenlijk aan de slag gegaan met de uitwerking van de maatregelen. Onder aansturing van een binnen VNG ingerichte centrale programma-organisatie gingen zes werkgroepen van start, vertegenwoordigers van alle partijen nemen hieraan deel. Het programma opereert onder de gezamenlijke verantwoordelijkheid van UWV, SVB en VNG en rapporteert aan het zogenaamde Opdrachtgeversberaad, waarin bestuurders van de organisaties zitting hebben.

De eerste helft van 2015 stond vooral in het teken van uitwerking van oplossingen. In de tweede helft van dit jaar worden korte termijn-oplossingen gerealiseerd en geïmplementeerd. Het jaar 2016 staat vooral in het teken van realisatie van meer structurele oplossingen en de verdere implementatie.

Hieronder geven we per maatregel een korte beschrijving.

Maatregel 1: fijnmazige autorisatiestructuur
Het rapport Privacy Impact Assessment (opgesteld in opdracht van SZW in 2014) merkt over de huidige autorisatierollenstructuur op dat een fijnmazigere aanpak gewenst is, waarbij makkelijker deeloverzichten van de huidige gegevenssets gecreëerd kunnen worden die beter aansluiten bij de eigen rollen en functies van de gebruiker. Mede naar aanleiding hiervan is een structurele oplossing onderzocht, waarbij partijen in staat zijn zelf de autorisatiestructuur als maatwerk in te richten. Onderdeel van deze structurele oplossing is dat gemeenten zelf de te gebruiken pagina's voor de diverse rollen gaan samenstellen.

Deze structurele oplossing heeft de voorkeur, omdat hiermee een volledig sluitende autorisatiestructuur kan worden bewerkstelligd. De realisatie van deze structurele oplossing vraagt echter een forse investering en een lange doorlooptijd. Deze oplossing zal niet voor 2017 beschikbaar zijn.

Verbeterslagen op korte termijn
Om op korte termijn toch een aantal belangrijke verbeteringen te kunnen bewerkstelligen, worden stapsgewijs in de tweede helft van 2015 nieuwe (thema) pagina's met beperktere gegevenssets beschikbaar gesteld.

Het gaat hier om:
- Afzonderlijke kolompagina's van SVB, UWW Uitkeringen, UWV Inkomensverhoudingen en DUO
- Nieuwe overzichtspagina's voor rechtmatigheid en re-integratie

Aansluitend op de oplevering van nieuwe pagina's worden algemene pagina's die te brede gegevenssets bevatten, begin 2016 verwijderd.

Weliswaar kent deze korte termijn-maatregel haar beperkingen ten opzichte van de hiervoor genoemde structurele oplossing, maar met deze nieuwe pagina's kan al een belangrijk positief effect worden bereikt.

Van belang is dat gemeenten de nieuwe pagina's gaan gebruiken zodra deze beschikbaar komen (uiteraard wordt u hiervan tijdig op de hoogte gesteld). Op het moment dat de algemene pagina's worden uitgefaseerd, is het uiteraard cruciaal dat u de nieuwe pagina's in gebruik heeft genomen. Aanbevolen wordt om vooraf voor uw organisatie goed in beeld te hebben welke taken door welke medewerkers worden uitgevoerd, de rol die hierbij hoort en de hieraan gerelateerde pagina's (afhankelijk van de te raadplegen gegevens).

Maatregel 2: verbetering logging en gebruiksrapportages
De Suwi-partijen hebben hun rapportages in de afgelopen periode verbeterd en met elkaar afgestemd. In november 2014 verscheen voor gemeenten de eindversie van de vernieuwde GSD-gebruikersrapportages waarmee intern controleurs van de gemeente na kunnen gaan of het opvragen van gegevens conform voorschriften verliep. Voor optimaal en efficiënt gebruik van de rapportage heeft de VNG een handreiking gemaakt:
http://www.vng.nl/files/vng/20140612-gebruikersrapportages-suwinet.pdf
Deze maatregel spitst zich nu verder toe op het sneller kunnen leveren van opgevraagde (specifieke) loggingrapportages en het ontwikkelen van signaleringsrapportages om inzicht te verkrijgen in afwijkende patronen, om misbruik beter te kunnen opsporen.

Maatregel 3: ontwikkeling en vaststelling aansluit- en gebruiksvoorwaarden inlezen
Naast de online raadpleegfunctie van Suwinet (Inkijk) bestaat de mogelijkheid om via een interface gegevens uit te wisselen en geautomatiseerd gegevens via SUWINET in te lezen in een eigen applicatie (wordt Inlezen genoemd). Gemeenten moeten hiervoor aan voorwaarden te voldoen, vastgelegd en ondertekend door beide partijen.

Bij de uitwerking van deze maatregel is er voor gekozen om allereerst een visienota op te leveren, waarin de verantwoordelijkheden vanuit de Wet bescherming persoonsgegevens (Wbp) worden gedefinieerd. Een gedeelde visie over wie waarvoor verantwoordelijk in de zin van de Wbp, is onontbeerlijk voor het treffen van en sturen op de uitvoering van de verbetermaatregelen. De feitelijke Wbp-verantwoordelijkheid moet ook leidend zijn voor de uitwerking van aansluit- en gebruiksvoorwaarden.

Mede op basis van de visienota is geconcludeerd dat bestuurlijk niet kan worden volstaan met het sec stellen van aansluitvoorwaarden (voor de aansluiting op Suwinet). Doelbinding,

proportionaliteit en subsidiariteit behoeven bestuurlijke focus en sturing, zowel bij de bronhouder als bij de afnemer. Hiervan uitgaande wordt een benadering gekozen op drie niveaus.

Allereerst dient op bestuurlijk niveau een gedragscode Verstrekken en Gebruik Persoonsgegevens te worden vastgesteld. De gedragscode is een statement dat de WBP uitgangspunt is bij de uitvoering van hun taken. Daarnaast dient een protocol Verzoek en Verstrekken Persoonsgegevens te worden vastgesteld vast met bestuurlijke afspraken over de indiening van en besluitvorming over verzoeken gegevens te verstrekken.
Ten slotte worden – als sluitstuk – de afspraken tussen bronhouder (namens hem de beheerder) en de individuele afnemer (College van B&W) over de wijze van verstrekken (bijvoorbeeld de aansluiting op Inlezen) vastgelegd in de aansluitvoorwaarden. De aansluitvoorwaarden worden op lokaal bestuurlijk niveau ondertekend.

Maatregel 4: ketenbrede awareness
Er wordt een ketenbrede awareness- en voorlichtingscampagne opgezet, rekening houdend met de diverse doelgroepen (bestuurders, toezichthouders/raadsleden, leidinggevenden, medewerkers, beheerders, beveiligingsfunctionarissen, etc.), de voor hen relevante informatie en hierop aansluitende communicatiemethoden-/middelen.

Een van de onderdelen van het plan richt zich op e-learning en/of serious gaming. Hierbij worden bijvoorbeeld eindgebruikers geïnstrueerd over privacy- en beveiligingsaspecten bij het gebruik van Suwinet. De staatssecretaris heeft in haar brief aan de Tweede Kamer meegedeeld dat gebruikers met een hierop gebaseerde test moeten aantonen dat deze zich voldoende bewust zijn van eisen en regels op het gebied van privacy en beveiliging.

Maatregel 5: sanctiebeleid misbruik gegevens
De Suwi-partijen streven een uniform sanctiebeleid na. Het uitgangspunt is dat misbruik ernstige gevolgen kan hebben voor de privacy van burgers en soms ook de persoonlijke veiligheid van burgers kan raken. Op grond hiervan dient misbruik te leiden tot zware sancties (ontslag van de desbetreffende medewerker).

Maatregel 6: herijking normenkader en verantwoordingsrichtlijn
De huidige verantwoordingsrichtlijn sluit niet goed aan bij de wijze waarop gemeenten verantwoording willen nemen. Er wordt naar gestreefd om zoveel mogelijk langs generieke normenkaders te verantwoorden (zoals de Baseline Informatiebeveiliging Gemeenten, i.c. BIG). In verband hiermee wordt het bestaande wettelijk kader rondom Suwinet herijkt en moet deze meer in lijn worden gebracht met generieke normenkaders.

Maatregel 7: telewerken en doorlevering van gegevens
De Suwi-partijen streven ernaar om gezamenlijke afspraken te maken over voorwaarden en criteria met betrekking tot gegevensleveringen aan partijen die gegevens doorleveren, taken uitbesteden (inclusief samenwerkingsverbanden) en telewerken toestaan.

Maatregel 8: beperking van zoeksleutels
Uitgangspunt is nu reeds dat uitsluitend het BSN als zoeksleutel wordt gehanteerd. Voor andere zoeksleutels zijn er speciale zoekpagina's ontwikkeld, waarvoor gebruikers expliciet dienen te worden geautoriseerd. Het aantal medewerkers dat andere zoeksleutels dan BSN kan gebruiken, is hierdoor beperkt.

Afwijkingen van het BSN als zoeksleutel moeten worden gemeld. Er is al een rapportage beschikbaar, waarin bevragingen anders dan op BSN zijn opgenomen. Naast verfijning van de rapportage, moeten procedures met betrekking tot het autoriseren en gebruik van afwijkende zoeksleutels worden aangescherpt. Hierover wordt een handreiking voor gemeemten worden opgesteld.

Maatregel 9: beperken toegang tot relevante personen
Uitgangspunt is dat de toegang wordt beperkt tot de zogenaamde caseload, dat wil zeggen dat in principe alleen toegang kan worden verkregen tot gegevens van burgers waarmee een concrete dienstverleningsrelatie bestaat en waarvoor het derhalve relevant is gegevens te kunnen raadplegen. Voor de uitvoering van de werkzaamheden is het echter ook vaak nodig om gegevens te kunnen raadplegen van bijvoorbeeld de (ex-) partner en eventuele huisgenoten.

Om invulling te kunnen geven aan de gevraagde aansluiting op de caseload, is de zogenaamde 'White list-oplossing' beschikbaar. De White list bestaat uit de BSN nummers van personen waarvan gegevens mogen worden geraadpleegd door gebruikers binnen de desbetreffende gemeente. Een bijzonder aandachtspunt hierbij zijn de gemeentelijke samenwerkingsverbanden. Deze moeten bekend zijn om een goede werking van de White list te kunnen garanderen.
De basis hiervan is al beschikbaar binnen Suwinet, maar het blijkt dat deze functionaliteit nog nauwelijks wordt gebruikt door gemeenten. Enerzijds heeft dit te maken met onvoldoende bekendheid, maar het ontbreken van de mogelijkheid om (wanneer dat nodig is) ook gegevens van anderen te kunnen raadplegen, leidt ook tot het niet gebruiken van de White list.

Naar aanleiding hiervan zal de 'White list-functie' in Suwinet Inkijk op korte termijn worden aangepast en uitgebreid met een zogenaamde 'escape-functie', waarmee het mogelijk is de 'White list' incidenteel te omzeilen. Dit leidt wel tot een signalering bij de verantwoordelijke die moet vaststellen of deze raadpleging terecht heeft plaatsgevonden.

Daarnaast moet in 2016 de nieuwe functionaliteit worden gerealiseerd, waarmee het mogelijk is aanvullende voorwaarden te verbinden aan het opvragen van gegevens (bijvoorbeeld medewerker, postcodegebied of leeftijd). Een caseload moet hiermee ook aan individuele medewerkers van de gemeente kunnen worden gekoppeld.

Maatregel 10: analyse van gegevens van bepaalde risicoklassen
Onderzocht wordt welke gegevens binnen Suwinet behoren tot een risicoklasse met een hogere privacy-gevoeligheid en welke aanvullende beveiligingsmaatregelen hiervoor passend zijn.

Maatregelen ministerie van SZW

De hiervoor benoemde maatregelen worden onder gezamenlijke verantwoordelijkheid van de Suwi-partijen uitgewerkt. Deze maatregelen zijn echter niet afdoende om alle kwetsbaarheden weg te nemen en de benodigde vervolgacties te kunnen oppakken. Ook het ministerie van SZW zal in dit verband een aantal maatregelen oppakken. Deze maatregelen betreffen de herijking van wet- en regelgeving, levering van informatie in plaats van gegevens, transparantie richting de burger over het gebruik van zijn of haar gegevens en een te introduceren afsluitbeleid.

Onderlinge relatie maatregelen

Het programmaplan benoemt diverse afhankelijkheden tussen maatregelen. Maatregel 4 (communicatie/awareness) kent de grootste afhankelijkheid van andere maatregelen: uitwerkingen hiervan moeten immers worden meegenomen in een voorlichtings- en awareness campagne.

De uitwerking van maatregel 3 (aansluitvoorwaarden) kent ook veel raakvlakken met andere maatregelen. Er worden eisen gesteld aan de toegang tot gegevens (maatregelen 1, 8 en 9). En de indeling in risicoklassen leidt tot aanvullende eisen die in de desbetreffende aansluitvoorwaarden (maatregel 3) worden meegenomen.

Daarnaast kent maatregel 2 (logging en rapportages misbruik) veel afhankelijkheden met andere maatregelen, vooral waar het de toegang tot gegevens betreft. Naarmate de autorisatiestructuur fijnmaziger is (maatregel 1), kan het controleregime ook strakker worden ingericht. Als met behulp van rapportages misbruik kan worden aangetoond, kan het sanctiebeleid (maatregel 5) worden ingezet.

De herijking van het normenkader (maatregel 6) zal leiden tot de behoefte om wet- en regelgeving te herzien (maatregel SZW). Bij de herijking van het normenkader zal tevens telewerken en doorlevering van gegevens (maatregel 7) aan de orde komen. Ook moet rekening worden gehouden met toegang tot meer privacygevoelige- gegevens en de aanvullende eisen die hieraan worden gesteld (maatregel 10).

Meer informatie

Wanneer u vragen heeft over het programma, de aanpak of de maatregelen, dan kunt u terecht bij de VNG: tel.nr. 070 – 373 8393, e-mail informatiecentrum@vng.nl.