

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

2570

Vragen van het lid **El Fassed** (GroenLinks) aan de ministers van Veiligheid en Justitie en van Binnenlandse Zaken en Koninkrijksrelaties over *digitale onveiligheid van de site meermetminder.nl* (ingezonden 25 april 2012).

Antwoord van minister **Spies** (Binnenlandse Zaken en Koninkrijksrelaties) (ontvangen 22 mei 2012).

Vraag 1

Is het waar dat via de website meermetminder.nl informatie wordt gevraagd (waaronder het burgerservicenummer en bankgegevens) van degenen die in aanmerking willen komen voor een subsidie voor energiebesparende maatregelen?¹

Antwoord 1

Ja. Rechtmatigheid van de subsidieverstrekking is een absolute voorwaarde. Met behulp van het burgerservicenummer wordt eenduidig vastgesteld dat de subsidie aan de juiste en rechthebbende persoon wordt verstrekt. Het bankrekeningnummer is nodig om het rechtmatige subsidiebedrag over te maken.

Vraag 2

Bent u zich bewust van de consequenties van identiteitsfraude als deze gegevens in verkeerde handen vallen? Zo ja, kunt u aangeven welk beveiligingsniveau voor deze site is gekozen en of dit niveau volstaat?

Antwoord 2

Ja. Uit de door de Stichting Meer Met Minder verstrekte informatie blijkt dat er is gekozen voor het benodigde beveiligingsniveau dat wordt geborgd door de volgende systeemkeuzes:

- Voor de toegang tot de onderdelen van de website die betrekking hebben op de Rijkspremieregeling Meer Met Minder wordt gewerkt met een Single Sign On inlogsysteem. De uitgifte in dit proces en de wijze van authenticatie zijn vergelijkbaar met betrouwbaarheidsniveau 1 van eHerkenning. Via de website is het voor bezoekers niet mogelijk toegang tot de persoonsgegevens te krijgen. De administrator kan alleen via de achterkant van de webapplicatie inloggen op de database.

¹ www.meermetminder.nl

- De data met burgerservicenummers en bankgegevens worden opgeslagen in een gescheiden database die niet rechtstreeks benaderbaar is.
- De data met de persoonsgegevens worden ten behoeve van de vaststelling en het uitbetalen van de Rijkspremieregeling Meer Met Minder in gecodeerde vorm (.xml-format) rechtstreeks door Agentschap NL uit de database opgehaald.

Gezien het bovenstaande, ben ik van mening dat het beveiligingsniveau van het deel van de website www.meermetminder.nl dat wordt ingezet voor de Rijkspremieregeling Meer Met Minder proportioneel gekozen is en een «passend beschermingsniveau» en bijbehorende maatregelen omvat (zie ook het antwoord op vraag 5).

Vraag 3

Is tot nu toe al eens een poging tot ongeoorloofde toegang ondernomen? Zo ja, hoe vaak en had dit succes?

Antwoord 3

De Stichting Meer Met Minder heeft tot nu toe geen ongeoorloofde toegang of poging daartoe geconstateerd. Het deel van de website www.meermetminder.nl dat wordt ingezet voor de Rijkspremieregeling Meer Met Minder functioneert sinds april 2010, zonder enige melding dat persoonsgegevens ongeoorloofd van de website of uit de database zijn gehaald.

Vraag 4

Deelt u de mening dat kwetsbare, persoonsvertrouwelijke gegevens, zoals bijvoorbeeld het burgerservicenummer, met uiterste terughoudendheid gebruikt dient te worden? Zo nee, waarom niet?

Antwoord 4

Ja. Ik verwijs hierbij naar de Wet algemene bepalingen burgerservicenummer (Wabb) die de toekenning, het beheer en het gebruik van het burgerservicenummer bepaalt.

Vraag 5

Welke maatregelen stelt u zich voor om de veiligheid te garanderen bij het uitwisselen van vertrouwelijke informatie via internet?

Antwoord 5

Bij het verwerken van persoonsgegevens dient men te voldoen aan de geldende nationale privacy wet- en regelgeving, die op haar beurt moet voldoen aan de Europese Privacyrichtlijn. Daarin staat dat een «passend beschermingsniveau» moet worden gekozen. In de Wet bescherming persoonsgegevens (Wbp) is dit verder uitgewerkt in artikel 13. Artikel 13 Wbp luidt: *«De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.»*