Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2016–2017

34 413 Wijziging van de Telecommunicatiewet, de Boeken 3 en 6 van het Burgerlijk Wetboek, de Algemene wet bestuursrecht alsmede daarmee samenhangende wijzigingen van andere wetten in verband met de uitvoering van EU-verordening elektronische identiteiten en vertrouwensdiensten (uitvoering EU-verordening elektronische identiteiten en vertrouwensdiensten)

Nr. 9 **BRIEF VAN DE MINISTER VAN ECONOMISCHE ZAKEN**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 22 december 2016

Hierbij stuur ik u, mede namens de Minister van Binnenlandse Zaken en Koninkrijksrelaties, het Privacy Impact Assessment (hierna te noemen: PIA)[1] die aanbevelingen doet over de Nederlandse uitvoering van de eIDAS-verordening[2] via de beoogde nationale stelsels voor elektronische identificatie[3]. Dit assessment is toegezegd in de nota naar aanleiding van het verslag[4] over de eIDAS-uitvoeringswet die op 28 april 2016 aan de Tweede Kamer is aangeboden. Bij de behandeling van de eIDAS-verordening in uw Kamer op 29 november jl. (Handelingen II 2016/17, nr. 28, item 37) heb ik vervolgens toegezegd het PIA nog in 2016 aan uw Kamer toe te sturen. Vervolgens ga ik in deze brief in op een tweetal toezeggingen die ik tijdens de plenaire behandeling van de uitvoeringswet aan uw Kamer heb gedaan. Mede namens de Minister van Veiligheid en Justitie ga ik in op de internationale samenwerking tussen cybersecurity-centra.

De eIDAS-verordening stelt lidstaten verplicht de bij de Europese Commissie aangemelde elektronische identificatiemiddelen uit andere

[1] Raadpleegbaar via www.tweedekamer.nl

[2] De verordening (EU Nr. 910/2014) van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG.

[3] Er is een technische architectuur voor de aansluiting van het eIDAS-knooppunt op het Afsprakenstelstel Elektronische Toegangsdiensten (eTD). Deze architectuur is onverkort ook van toepassing voor het inloggen binnen het BSN-domein, zoals deze in de Wet GDI is voorzien. Voor achtergronden over eTD verwijs ik naar het Besluit van de Minister van Economische Zaken van 15 april 2015, nr. WJZ/15023462, houdende instelling van de besturing van een afsprakenstelsel elektronische toegangsdiensten (Instellingsbesluit besturing elektronische toegangsdiensten). Voor achtergronden over het BSN-domein verwijs ik naar de Kamerbrief over het nationale eID beleid: Kamerstuk 26 643, nr. 419.

[4] Kamerstuk 34 413, nr. 6.

kst-34413-9
ISSN 0921 - 7371
's-Gravenhage 2016

lidstaten per 18 september 2018 te accepteren. Om grensoverschrijdend gebruik van elektronische identificatiemiddelen mogelijk te maken, heeft iedere lidstaat een digitaal knooppunt nodig. Dit eIDAS-knooppunt geleidt identificatiegegevens door van burgers en bedrijven die willen inloggen op een website van een publieke organisatie in een andere lidstaat. Het eIDAS-knooppunt wordt beveiligd in overeenstemming met de standaarden en afspraken die de eIDAS-verordening daaraan stelt. Overeenkomstig die verordening dient daarbij ook de Europese wet- en regelgeving op het gebied van privacy in acht te worden genomen.

Het eIDAS-knooppunt kan worden aangesloten op de toekomstige Nederlandse stelsels voor elektronische identificatie en authenticatie. Overheden kunnen op die manier gegevens van burgers en bedrijven uit het buitenland op eenzelfde manier verwerken als Nederlandse burgers en bedrijven. Het bijgevoegde PIA is gebaseerd op de technische architectuur en doet aanbevelingen over de wijze waarop het eIDAS knooppunt op de Nederlandse stelsels voor elektronische identificatie kan worden aangesloten. Hieronder wordt aangeven welke aanbevelingen dit zijn, alsmede hoe ik hieraan opvolging zal geven.

Aanbevelingen

1. De rollen en verantwoordelijkheden van de ministers van Binnenlandse Zaken en Koninkrijksrelaties en Economische Zaken ten aanzien van eIDAS en het eTD-stelsel moeten duidelijk zijn vastgelegd. De rol van bewerkers, inclusief eisen op het gebied van privacy en informatiebeveiliging, moet verankerd worden in de ministeriële regeling inzake elektronisch berichtenverkeer (Regeling EBV), de in voorbereiding zijnde Wet Generieke Digitale Infrastructuur (Wet GDI) en het Afsprakenstelstel Elektronische Toegangsdiensten. In aanvulling op de eIDAS-verordening en de uitvoeringswet eIDAS moeten de contouren van de implementatie van het Nederlandse eID-stelsel, zoals de componenten, rollen, taken, bevoegdheden en verantwoordelijkheden, in de toekomstige Wet GDI worden vastgelegd.
   De Minister van Economische Zaken is verantwoordelijk voor het eIDAS-knooppunt en voorlopig de beheerder van het knooppunt. Dit is in de memorie van toelichting op de uitvoeringswet eIDAS[5] vastgelegd. Wanneer het knooppunt wordt aangesloten op de Nederlands stelsels brengt dit een verantwoordelijkheid voor de vertaling van persoonsgegevens van inwoners en bedrijven uit andere lidstaten naar gangbare afspraken in Nederland met zich mee. De Minister van Binnenlandse Zaken en Koninkrijksrelaties is verantwoordelijk voor het inloggen in het BSN-domein, alsmede voor de voorziening waarmee de binnengekomen identificatiegegevens vergeleken worden met de gegevens die in de Basis Registratie Personen bekend zijn. Deze aanbeveling is immers ook van toepassing voor het inloggen in het BSN-domein.
   Bovendien zal er aandacht worden besteed aan de benodigde wettelijke kaders voor een gedegen aansluiting van de toekomstige eID-stelsels op het eIDAS-knooppunt.
2. Nagaan of er aanvullende maatregelen nodig zijn voor het mitigeren van risico's die kunnen optreden wanneer persoonsnummers niet uniek aan individuen gekoppeld blijken te zijn.
   Bij verdere uitwerking van aansluiting op de voorziene elektronische stelsels zal deze aanbeveling worden meegenomen. Het burgerservicenummer zal nooit aan buitenlandse overheden worden verstrekt.

[5] Kamerstuk 34 413, nr. 3.

3. Als private dienstverleners met buitenlandse gegevens gaan werken, moet dit aan dezelfde eisen als het stelsel voor elektronische identificatie voldoen.
   Vooralsnog is het aansluiten van private dienstverlener op het eIDAS-knooppunt niet voorzien. Indien hier op een later moment alsnog sprake van zal zijn, zal de aanbeveling worden opgevolgd.
4. Het PIA gaat ook in op privacy-risico's van het uitwisselen van andersoortige gegevens dan identiteitsgegevens, waarin de eIDAS-verordening voorziet. Aanbevolen wordt op het moment dat die situatie zich voordoet opnieuw de privacy-risico's hiervan te beoordelen.
   Vooralsnog zal van deze situatie geen sprake zijn. Het voornemen is alleen de persoons- of bedrijfsidentificatiegegevens door te geleiden waarin de eIDAS-verordening voorziet. Wanneer later alsnog voor doorgifte van andersoortige gegevens gekozen wordt, zal de aanbeveling worden opgevolgd.

Reality checks bij audits

Tijdens de plenaire behandeling van de uitvoeringswet eIDAS heb ik aan de heer Bosma (VVD) toegezegd mij erin te verdiepen of er in het publieke toezicht op de bedrijven die die audits uitvoeren, ook reality checks plaatsvinden. De audits die worden uitgevoerd bij publieke en private organisaties die gekwalificeerde vertrouwensdiensten uitgeven, bevatten reality checks. Er is echter geen publiek toezicht op de bedrijven die audits uitvoeren. Deze bedrijven worden in de verordening conformiteitbeoordelingsorganen genoemd. De verordening voorziet niet in publiek toezicht op deze organen en het nationaal stellen van eisen en organiseren van toezicht past niet bij een gelijk Europees speelveld voor deze conformiteitbeoordelingsorganen. Accreditatie is wel een vereiste uit de verordening. In de eIDAS-verordening, de audits en het toezicht staat aandacht voor de veiligheid van de verleende vertrouwensdiensten centraal. De auditsystematiek is zodanig ingericht dat er aandacht is voor de veiligheid van de gekwalificeerde vertrouwensdiensten zelf, naast die voor het managementsysteem van de vertrouwensdienstverlener. De bekwaamheid van de auditor wordt getoetst door de Raad van Accreditatie. Daarnaast is de rol van de toezichthouder aangepast en verstevigd. De aanpassing in het toezicht betekent dat de toezichthouder bepaalt of aan de eisen van de verordening is voldaan en niet de auditor (conformiteitsbeoordelingsorgaan). Het auditrapport is een belangrijk hulpmiddel bij het toezicht. De toezichthouder zal in de praktijk thematisch en steekproefsgewijs aanvullende controles uitvoeren.

Preventie Cybersecuritycentrum en Europese Samenwerking

Bij de plenaire behandeling van de uitvoeringswet eIDAS heb ik aan mevrouw Oosenbrug (PvdA) toegezegd terug te komen op de Europese samenwerking tussen Cyber Security Centra in de lidstaten en hoe zij gezamenlijk een goede bijdrage kunnen leveren aan het vooraf monitoren van het netwerk.
De vertrouwensdiensten behoren tot de vitale infrastructuur Telecom/ICT. Dit betekent dat het Nationaal Cyber Security Centrum vertrouwensdienstverleners onder andere kan informeren en adviseren over dreigingen en kwetsbaarheden met betrekking tot hun informatiesystemen. Daarbij wordt op Europees en internationaal niveau samengewerkt.
Als bijvoorbeeld het Spaanse Cybersecuritycentrum een nieuwe dreiging voor vertrouwensdiensten ontdekt, wordt deze informatie met de Cybersecuritycentra in andere lidstaten gedeeld. Het Nederlandse NCSC zal dit signaal doorgeven aan de Nederlandse vertrouwensdienstverleners. Op deze wijze kunnen vertrouwensdienstverleners zich voorbe-

reiden op de nieuwe dreiging. Wanneer het toch misgaat bij een vertrouwensdienstverlener kan deze een beroep doen op het Nationaal Cyber Security Centrum voor advies en hulp.
Het NCSC zal de lessen van incidenten (geanonimiseerd) delen met de Cybersecuritycentra in andere lidstaten. Op deze wijze wordt kennis gedeeld en samengewerkt.
De Cybersecurity Centra monitoren het internet als geheel op dreigingen maar niet de ICT-systemen van de vertrouwensdienstverleners afzonderlijk. De beveiliging van de systemen is een verantwoordelijkheid van elke aanbieder.
De veiligheid van de systemen van gekwalificeerde aanbieders wordt periodiek bij eerder genoemde audit door het conformiteitsbeoordelingsorgaan en steekproefsgewijs door de toezichthouder gecheckt.

De Minister van Economische Zaken,
H.G.J. Kamp