Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2012–2013

33 331 EU-voorstel: Verordening betreffende elektronische identificatie en diensten voor elektronische transacties in de interne markt COM(2012) 238

D

BRIEF VAN DE VICEVOORZITTER VAN DE EUROPESE COMMISSIE

Aan de Voorzitter van de Eerste Kamer der Staten-Generaal

Brussel, 12 december 2012

De Commissie dankt de Eerste Kamer voor haar advies over het voorstel voor een verordening betreffende «elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt» {COM(2012) 238 final}.

De voorgestelde verordening heeft tot doel de ontwikkeling van elektronische transacties in de Europese Unie te ondersteunen door te zorgen voor wederzijdse erkenning en aanvaarding van elektronische identificatie en authenticatie in de EU, door de interoperabiliteit en bruikbaarheid van elektronische handtekeningen te verbeteren en door rechtsgevolgen te verlenen aan daarmee verband houdende vertrouwensdiensten betreffende elektronische zegels, elektronische tijdsstempels. elektronische documenten, elektronische bezorgingsdiensten en authenticatie van websites.

De voorgestelde verordening moet het mogelijk maken het potentieel aan te boren dat de internetrevolutie ons biedt. Zij moet zorgen voor een betrouwbare en veilige omgeving waarin mogelijkheden ontstaan voor veilige grensoverschrijdende diensten en bedrijfskansen die naar verwachting groei en banen zullen opleveren in een bloeiende interne markt.

De voorgestelde verordening bevat de basisbeginselen en -bepalingen die de rechtszekerheid moeten waarborgen die nodig is voor het verstrekken en het gebruiken van elektronische identificatie en vertrouwensdiensten.

In dit opzicht legt de voorgestelde verordening geen vereisten op waaraan slechts met een specifieke technologie kan worden voldaan. Er worden dan ook gedelegeerde handelingen en uitvoeringshandelingen in het vooruitzicht gesteld met daarin de nadere regels voor de toepassing van

kst-33331-D
ISSN 0921 - 7371
's-Gravenhage 2012

specifieke bepalingen van de voorgestelde verordening. Een dergelijke regeling moet zorgen voor technologische neutraliteit en flexibiliteit waardoor het voorgestelde rechtskader zich in de toekomst gemakkelijk kan aanpassen aan innovatie en de opkomst van nieuwe technologieën.

Burgers voorzien van nationale elektronische identificatiemiddelen is een aangelegenheid die tot de nationale soevereiniteit behoort. Het staat immers aan de lidstaten te beslissen of zij een dergelijke vorm van identificatie aannemen wanneer dit vereist is, en welke technologie zij daarvoor gebruiken.

In dit verband heeft de voorgestelde verordening al/een tot doel (artikelen 5 tot en met 8) door middel van wederzijdse erkenning ervoor te zorgen dat wanneer deze elektronische identificatiemiddelen bestaan om toegang tot overheidsdiensten te verkrijgen, deze grensoverschrijdend kunnen worden gebruikt. Wederzijdse erkenning Iran echter al/een maar worden gewaarborgd indien elke lidstaat verantwoordelijk is voor het nationale elektronische identificatiestelsel dat hij voor zijn burgers heeft vastgesteld Dit is een van de voorwaarden die moeten worden bepaald om de lidstaten te helpen «om het noodzakelijke vertrouwen in elkaars elektronische identificatieregelingen op te bouwen» (overweging 13). In dezelfde geest bepaalt de voorgestelde verordening in artikel 8 dat alle lidstaten «samen[werken] om de interoperabiliteit te waarborgen van middelen voor elektronische identificatie» en «om de veiligheid ervan te verhogen».

Wat het authenticatieproces betreft, wil de Commissie met «beschikbaarheid op ieder moment» aangeven dat de mogelijkheden voor authenticatie beschikbaar moeten zijn zonder ongerechtvaardigde onderbreking. terwijl technische onbeschikbaarheid wegens overmacht Iran worden aanvaard Voorts bepaalt de voorgestelde verordening dat grensoverschrijdende onlineauthenticatie gratis wordt verleend ten aanzien van een derde partij om te voorkomen dat er clandestiene markten kunnen ontstaan en derhalve ook om oneerlijke concurrentie te beletten.

Met betrekking tot de aansprakelijkheid in artikel 6 is het inderdaad de bedoeling de lidstaten ten aanzien van derde partijen aansprakelijk te stel/en voor «de ondubbelzinnige koppeling van de persoonsidentificatiegegevens» en voor de «authenticatiemogelijkheid». Wanneer de uitgifte van elektronische identificatiemiddelen «namens» of «onder de verantwoordelijkheid» van de lidstaat geschiedt, staat het de lidstaten echter vrij deze aansprakelijkheid In hun formele of informele overeenkomsten met uitgevende instanties te regelen en dus vrij te beslissen hoe de aansprakelijkheid wordt verdeeld in overeenstemming met de toepasselijke nationale wetten.

In artikel 13, lid 2, onder c), dat betrekking heeft op de verplichting voor een gekwalificeerde verlener van vertrouwensdiensten om ervoor te zorgen dat de gegevens toegankelijk blijven nadat hij zijn activiteiten heeft gestaakt, wordt terecht verwezen naar punt g) van artikel 19, lid 2, dat voorschrijft hoe een gekwalificeerde verlener van vertrouwensdiensten de informatie met betrekking tot de afgegeven en ontvangen gegevens moet vastleggen.

De verwijzing naar Richtlijn 95/46/EG inzake gegevensbescherming in artikel 11 van de voorgestelde verordening betreffende «elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt» moet worden uitgelegd als een verwijzing naar het voorstel voor een algemene verordening inzake gegevensbescherming zodra deze in werking zal treden.

Wat uw vraag over het toepassingsgebied van de in artikel 16, lid 1, bedoelde veiligheidsaudit betreft, heeft de Commissie voor ogen dat de audit betrekking moet hebben op alle veiligheidsaspecten die noodzakelijk zijn om te waarborgen dat de gekwalificeerde verlener van vertrouwensdiensten zijn activiteiten naar behoren zal uitvoeren met het oog op de technische, financiële en juridische zekerheid De veiligheidsaudit moet derhalve alle relevante informatie bevallen die de technische, financiële en juridische zekerheid van de gekwalificeerde verlener van vertrouwensdiensten kan waarborgen. Een dergelijke verslag kan ook nuttig zijn voor de gekwalificeerde verleners van vertrouwensdiensten om te voldoen aan de in artikel 19, lid 2, onder b), bedoelde verplichting, namelijk het «dragen [van] het risico van aansprakelijkheid voor schade door ervoor te zorgen dat zij voldoende financiële middelen tot hun beschikking hebben of door middel van een toereikende aansprakelijkheidsverzekering».

Wat uw vraag over artikel 19, lid 2, onder d), betreft, is er in de Nederlandse versie van de verordening jammer genoeg een fout ten opzichte van de door de Commissie aangenomen tekst. De Engelse versie luidt immers «Qualified trust service providers providing qualified trust services shall: .. «, hetgeen in de Nederlandse versie vertaald is door «Gekwalificeerde verleners van vertrouwensdiensten die gekwalificeerde vertrouwensdiensten verlenen: ... « in plaats van «Gekwalificeerde verleners van vertrouwensdiensten die gekwalificeerde vertrouwensdiensten verlenen, moeten: ... «. Gelet op de kritieke rol die verleners van vertrouwensdiensten vervullen voor de samenleving, zoals duidelijk aangetoond is door de zaak DigiNotar, zijn de in artikel 19, lid 2, onder d), bedoelde bepalingen ten slotte van belang en relevant en dat niet alleen voor gegevensbescherming.

De Commissie hoopt dat deze verduidelijkingen tegemoetkomen aan de bezorgdheid van de Eerste Kamer en wenst hiermee haar politieke dialoog over deze belangrijke onderwerpen voort te zetten.

Marcoš Šefčovič
Vicevoorzitter