DE EUROPESE TOEZICHTHOUDER VOOR GEGEVENSBESCHERMING

Samenvatting van het Advies van de Europese Toezichthouder voor gegevensbescherming inzake de mededeling van de Commissie over „Het aanboren van het potentieel van cloud computing in Europa"

(De volledige tekst van dit advies is beschikbaar in de Engelse, Franse en Duitse taal op de website van de Europese Toezichthouder voor gegevensbescherming (EDPS): http://www.edps.europa.eu)

(2013/C 253/03)

I. **Inleiding**

I.1. *Doel van het advies*

1. Gezien het belang van cloud computing in de zich ontwikkelende informatiemaatschappij en van het lopende beleidsdebat over cloud computing in de EU heeft de EDPS besloten op eigen initiatief dit advies uit te brengen.

2. Dit advies is een reactie op de Mededeling van de Commissie van 27 september 2012 getiteld „Het aanboren van het potentieel van cloud computing in Europa" (hierna te noemen: „de mededeling") ([1]), waarin kernacties en beleidsmaatregelen worden besproken die moeten worden ingezet om het gebruik van cloud-diensten sneller ingang te laten vinden in Europa. De EDPS is, voordat de mededeling werd aangenomen, informeel geraadpleegd en heeft informele opmerkingen geplaatst. Het doet hem deugd dat een aantal van zijn opmerkingen in de mededeling is verwerkt.

3. Gezien de omvang en het belang van het lopende debat over het verband tussen cloud computing en het rechtskader voor gegevensbescherming beslaat dit advies echter een breder terrein dan alleen de onderwerpen die in de mededeling worden behandeld.

4. Het advies besteedt met name aandacht aan de uitdagingen die cloud computing opwerpt op het gebied van gegevensbescherming, en de aanpak daarvan in de voorgestelde algemene verordening gegevensbescherming (hierna te noemen: „de voorgestelde verordening") ([2]). Daarnaast wordt ingegaan op de gebieden waarop volgens de mededeling verdere actie zou moeten worden ondernomen.

I.2. *Achtergrond*

5. In de context van het algemene beleidsdebat over cloud computing in de EU zijn de volgende activiteiten en documenten van speciaal belang:

— Aansluitend op haar mededeling uit 2010 over de digitale agenda voor Europa ([3]) heeft de Commissie tussen 16 mei en 31 augustus 2011 een openbare raadpleging gehouden over cloud computing in Europa, en de resultaten daarvan gepubliceerd op 5 december 2011 ([4]);

— Op 1 juli 2012 heeft de werkgroep artikel 29 ([5]) een advies inzake cloud computing aangenomen (hierna te noemen: „het advies van de werkgroep artikel 29") ([6]) waarin de toepassing van de vigerende gegevensbeschermingsregels zoals vervat in Richtlijn 95/46/EG op verleners van cloud-diensten die actief zijn in de Europese Economische Ruimte (EER) en hun klanten wordt geanalyseerd ([7]);

— Op 26 oktober 2012 hebben de commissarissen voor de bescherming van persoonsgegevens en de privacy tijdens hun 34ste internationale conferentie een resolutie over cloud computing aangenomen ([8]).

([1]) COM(2012) 529 final.
([2]) COM(2012) 11 final.
([3]) COM(2010) 245 definitief.
([4]) http://ec.europa.eu/energy/gas_electricity/smartgrids/taskforce_en.htm
([5]) De werkgroep artikel 29 is een adviesorgaan dat is ingesteld uit hoofde van artikel 29 van Richtlijn 95/46/EG. Het bestaat uit vertegenwoordigers van nationale toezichthoudende instanties en de EDPS, en een vertegenwoordiger van de Commissie.
([6]) Advies 05/2012 inzake cloud computing van werkgroep artikel 29, beschikbaar op http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_nl.pdf
([7]) Daarnaast hebben nationale gegevensbeschermingsautoriteiten in diverse lidstaten hun eigen richtsnoeren betreffende cloud computing uitgebracht, bijvoorbeeld in Italië, Zweden, Denemarken, Duitsland, Frankrijk en het Verenigd Koninkrijk.
([8]) Resolutie over cloud computing, aangenomen tijdens de 34ste internationale conferentie van de commissarissen voor de bescherming van persoonsgegevens en de privacy, Uruguay, 26 oktober 2012.

I.3. *Mededeling over cloud computing*

6. De EDPS is ingenomen met de mededeling. Hierin worden drie specifieke kernacties genoemd die op EU-niveau moeten worden ingezet om het gebruik van cloud computing in Europa te begeleiden en te bevorderen, namelijk:

— Kernactie 1: De wirwar van normen ontwarren

— Kernactie 2: Veilige en billijke contractvoorwaarden

— Kernactie 3: Een Europees cloud-partnerschap oprichten om innovatie en groei vanuit de overheidssector aan te moedigen.

7. Daarnaast worden nog aanvullende beleidsmaatregelen genoemd, zoals acties om het gebruik van cloud computing te stimuleren via onderzoek en ontwikkeling of bewustmakingsacties, en het aan de orde stellen van kernthema's met betrekking tot cloud computing — waaronder gegevensbescherming, toegankelijkheid voor ordehandhavingsdiensten, beveiliging en aansprakelijkheid van tussenpersonen bij de dienstverlening — in een versterkte internationale dialoog.

8. Gegevensbescherming wordt in de mededeling genoemd als een essentiële voorwaarde voor een succesvolle invoering van cloud computing in Europa. In dit verband wordt aangegeven [1] dat in de voorgestelde verordening veel van de zorgen die verleners van cloud-diensten en cloud-klanten hebben geuit, aan bod komen [2].

I.4. *Focus en structuur van het advies*

9. Dit advies heeft drie doelen.

10. Het eerste doel is het benadrukken van de relevantie van privacy en gegevensbescherming in de huidige discussies over cloud computing. Meer specifiek wordt in het advies onderstreept dat het niveau van gegevensbescherming in een cloud-omgeving niet lager mag zijn dan het niveau dat vereist is in om het even welke andere context waarbinnen gegevens worden verwerkt. Cloud computing-praktijken kunnen alleen legaal worden ontwikkeld en toegepast als dit niveau van gegevensbescherming gegarandeerd wordt (zie hoofdstuk III.3). Het advies volgt de richting die in het advies van de werkgroep artikel 29 is aangegeven.

11. Het tweede doel is het verder analyseren van de belangrijkste problemen die cloud computing opwerpt voor de gegevensbescherming tegen de achtergrond van de voorgestelde algemene verordening gegevensbescherming, en met name de problematiek van het eenduidig definiëren van de verantwoordelijkheden van de verschillende actoren en de begrippen „voor de verwerking verantwoordelijke" en „verwerker". In het advies (hoofdzakelijk hoofdstuk IV) wordt geanalyseerd hoe de voorgestelde verordening in de huidige vorm [3] voor cloud-diensten een hoog niveau van gegevensbescherming zou helpen waarborgen. Het advies gaat daarom uit van de door de EDPS uitgewerkte standpunten in zijn advies inzake het hervormingspakket gegevensbescherming (hierna te noemen „het advies van de EDPS inzake het hervormingspakket gegevensbescherming") [4] en vult dit aan door zich specifiek te concentreren op de cloud-omgeving. De EDPS beklemtoont dat zijn advies inzake het hervormingspakket gegevensbescherming volledig van toepassing is op cloud-diensten en moet worden beschouwd als een basis voor het onderhavige advies. Bovendien zijn bepaalde punten die daarin worden genoemd — zoals zijn analyse van de nieuwe bepalingen betreffende de rechten van datasubjecten [5] — al duidelijk genoeg. Deze zullen in dit advies dan ook niet verder worden uitgewerkt.

12. Het derde doel is het aanwijzen van gebieden waarop op Europees niveau vanuit het oogpunt van gegevensbescherming en privacy verdere actie moet worden ondernomen gezien de door de Commissie voorgestelde cloud-strategie in de mededeling. Hierbij moet onder meer worden gedacht aan het verstrekken van aanvullende richtsnoeren, inspanningen op het gebied van standaardisering, het uitvoeren van aanvullende risicobeoordelingen voor specifieke sectoren, het voeren van een internationale dialoog over kwesties met betrekking tot cloud computing, en zorgdragen voor een effectieve vorm van internationale samenwerking (uit te werken in hoofdstuk V).

[1] Zie pagina 8 van de mededeling, paragraaf over „Acties van de digitale agenda voor het opbouwen van het digitale vertrouwen".

[2] De term „cloud-klanten" wordt in dit advies over het algemeen gebruikt om te verwijzen naar klanten optredend in de hoedanigheid van een bedrijf, en naar consumenten optredend als individuele eindgebruikers.

[3] Er zij op gewezen dat het voorstel voor een verordening momenteel wordt behandeld door de Raad en het Europees Parlement als onderdeel van de gewone wetgevingsprocedure.

[4] Het advies is beschikbaar op http://www.edps.europa.eu

[5] Zie het advies van de EDPS, in het bijzonder paragrafen 140 tot en met 158.

13. Het advies is als volgt opgebouwd: In hoofdstuk II wordt een overzicht gegeven van de belangrijkste kenmerken van cloud computing en de problemen op het gebied van gegevensbescherming die daarmee verband houden. In hoofdstuk III worden de meest relevante elementen van het bestaande Europese rechtskader en van de voorgestelde verordening besproken. In hoofdstuk IV wordt geanalyseerd hoe de voorgestelde verordening zou helpen de problemen op het gebied van gegevensbescherming die het gebruik van cloud-diensten met zich meebrengt, aan te pakken. In hoofdstuk V worden de suggesties van de Commissie voor verdere beleidsontwikkeling geanalyseerd en de gebieden aangewezen waarop verdere actie mogelijk noodzakelijk is. Hoofdstuk VI bevat de conclusies.

14. Hoewel veel van de overwegingen in dit advies van toepassing zijn op alle omgevingen waarin gebruik wordt gemaakt van cloud computing, wordt in dit advies niet ingegaan op het gebruik van cloud-diensten specifiek door EU-instellingen en -organen onder supervisie van de EDPS uit hoofde van Verordening (EG) nr. 45/2001. De EDPS zal deze instellingen en organen afzonderlijk richtlijnen verstrekken.

VI. **Conclusies**

121. Zoals beschreven in de mededeling biedt cloud computing bedrijven, consumenten en de overheidssector veel nieuwe kansen voor het beheer van gegevens met gebruikmaking van externe IT-hulpmiddelen op een andere locatie. Tegelijkertijd werpt cloud computing veel uitdagingen op, met name ten aanzien van het juiste niveau van gegevensbescherming voor in de cloud verwerkte gegevens.

122. Aan het gebruik van cloud-diensten kleeft een aanzienlijk risico dat verantwoordelijkheden in verband met de verwerking van gegevens door verleners van cloud-diensten in rook opgaan als de criteria voor de toepasselijkheid van de Europese gegevensbeschermingswetgeving onvoldoende duidelijk zijn en de rol en de verantwoordelijkheden van verleners van cloud-diensten te beperkt worden gedefinieerd of opgevat, of niet effectief worden geïmplementeerd. De EDPS benadrukt dat het gebruik van cloud-diensten geen rechtvaardiging mag zijn voor een versoepeling van de gegevensbeschermingsnormen vergeleken met de normen voor conventionele gegevensverwerking.

123. In dit verband zou de voorgestelde algemene verordening gegevensbescherming, zoals die nu voorligt, veel verduidelijkingen en hulpmiddelen bieden die zouden helpen waarborgen dat met name verleners van cloud-diensten die hun diensten aanbieden aan klanten in Europa, zorgen voor een adequaat niveau van gegevensbescherming, waaronder in het bijzonder:

— Artikel 3 zou het geografische toepassingsgebied van de Europese gegevensbeschermingsregels verduidelijken en het toepassingsbereik verbreden zodat ook cloud-diensten eronder zouden vallen;

— Artikel 4, lid 5 zou een nieuw element toevoegen aan de rol van de voor de verwerking verantwoordelijke, en wel „voorwaarden". Dit zou aansluiten op de opkomende trend waarbij het, gezien de technische IT-complexiteit die aan cloud-diensten ten grondslag ligt, noodzakelijk is de omstandigheden uit te breiden waarin een verlener van cloud-diensten mag worden aangemerkt als voor de verwerking verantwoordelijke. Dit zou de mate waarin er invloed wordt uitgeoefend op de gegevensverwerking beter weerspiegelen;

— De voorgestelde verordening zou de verantwoordelijkheid en verantwoordingsplicht van voor de verwerking verantwoordelijken en verwerkers vergroten door specifieke verplichtingen in te voeren, zoals privacy by design en by default (artikel 23), het melden van gegevensinbreuken (artikelen 31 en 32) en privacyeffectbeoordelingen (artikel 33). Verder zou de verordening voor de verwerking verantwoordelijken en verwerkers verplichten mechanismen in te voeren om de effectiviteit van de geïmplementeerde gegevensbeschermingsmechanismen aan te tonen (artikel 22);

— Artikelen 42 en 43 van de voorgestelde verordening zouden voorzien in een flexibeler gebruik van mechanismen voor internationale gegevensoverdracht, zodat cloud-klanten en verleners van cloud-diensten verzekerd zijn van passende waarborgen met betrekking tot gegevensbescherming wanneer zij persoonsgegevens overdragen aan datacenters of servers in derde landen;

— Artikelen 30, 31 en 32 van de voorgestelde verordening zouden de verplichtingen van voor de verwerking verantwoordelijken en verwerkers verduidelijken als het gaat om de beveiliging van de verwerking en de verplichting gegevensinbreuken te melden, en leggen daarmee de basis voor een uitgebreide, coöperatieve benadering van beveiligingsbeheer door de verschillende actoren in een cloud-omgeving;

— Artikelen 55 tot en met 63 van de voorgestelde verordening zouden de samenwerking tussen toezichthoudende autoriteiten en hun gezamenlijke toezicht op grensoverschrijdende gegevensverwerking versterken, wat zeker in een cloud computing-omgeving van groot belang is.

124. Desalniettemin stelt de EDPS voor om, na kennis te hebben genomen van de bijzonderheden van cloud-diensten, in de voorgestelde verordening verdere verduidelijkingen aan te brengen op de volgende punten:

— om, ten aanzien van het geografisch toepassingsgebied van de voorgestelde verordening, artikel 3, lid 2, letter a) als volgt te wijzigen: „het aanbieden van goederen of diensten *waarbij persoonsgegevens worden verwerkt van* deze betrokkenen in de Unie", of, als alternatief, een nieuwe overweging in te voegen waarin wordt aangegeven dat de verwerking van persoonsgegevens van datasubjecten in de Unie door niet in de EU gevestigde voor de verwerking verantwoordelijken die diensten aanbieden aan in de EU gevestigde rechtspersonen, ook binnen het geografisch toepassingsgebied van de voorgestelde verordening valt;

— om een duidelijke definitie van het begrip „overdracht" toe te voegen, zoals uiteengezet in zijn advies inzake het hervormingspakket gegevensbescherming;

— om een specifieke bepaling in te voegen ter verduidelijking van de voorwaarden waaronder rechtshandhavingsinstanties uit niet EER-landen toegang kunnen krijgen tot in de cloud opgeslagen gegevens. Een dergelijke bepaling zou ook de ontvanger van het verzoek kunnen verplichten om in specifieke gevallen de bevoegde toezichthoudende instantie in de EU te informeren en te raadplegen.

125. De EDPS onderstreept ook dat verdere sturing van de Commissie en/of van toezichthoudende instanties (in het bijzonder via het toekomstige Europees Comité voor gegevensbescherming) noodzakelijk zal zijn op de volgende gebieden:

— om te verduidelijken welke mechanismen moeten worden ingesteld om te waarborgen dat de effectiviteit van de gegevensbeschermingsmaatregelen in de praktijk wordt gecontroleerd;

— om verwerkers te ondersteunen bij het gebruik van bindende bedrijfsvoorschriften en ze te helpen voldoen aan de toepasselijke vereisten;

— om beste praktijken te verstrekken voor zaken als de verantwoordelijkheid van de voor de verwerking verantwoordelijke/de verwerker, het op de juiste wijze bewaren van gegevens in de cloud, de overdraagbaarheid van gegevens en de uitoefening van de rechten van datasubjecten.

126. De EDPS erkent voorts dat gedragscodes die door de branche worden opgesteld en die door de relevante toezichthoudende instanties worden goedgekeurd, een nuttig hulpmiddel kunnen zijn om de naleving door en het vertrouwen onder de verschillende actoren te bevorderen.

127. De EDPS ondersteunt de ontwikkeling door de Commissie, in overleg met toezichthoudende instanties, van standaardcontractvoorwaarden voor de levering van cloud-diensten die voldoen aan de gegevensbeschermingsvereisten, waarvan in het bijzonder:

— modelcontractvoorwaarden die moeten worden opgenomen in de commerciële voorwaarden van aanbiedingen voor het leveren van cloud-diensten;

— algemene aankoopvoorwaarden voor de overheidssector, rekening houdend met de gevoeligheid van de verwerkte gegevens;

— het verder afstemmen van mechanismen voor internationale gegevensoverdracht op de cloud computing-omgeving, in het bijzonder door de huidige standaardcontractbepalingen te actualiseren en door standaardcontractbepalingen aan te leveren voor de overdracht van gegevens van in de EU gevestigde verwerkers aan buiten de EU gevestigde verwerkers.

128. De EDPS beklemtoont dat er passende aandacht moet worden besteed aan gegevensbeschermingsvereisten bij de ontwikkeling van normen en certificeringsmechanismen, waarbij in het bijzonder moet worden gedacht aan:

— het toepassen van de beginselen privacy by design en privacy by default bij de ontwikkeling van de normen;

— het integreren van gegevensbeschermingsvereisten, zoals doelbegrenzing en opslagbeperking, in het ontwerp van de normen;

— de verplichtingen van providers om hun klanten te voorzien van de informatie die nodig is om een geldige risicobeoordeling uit te voeren en hen te informeren over de getroffen veiligheidsmaatregelen, en tevens melding te maken van eventuele beveiligingsincidenten.

129. Tot slot onderstreept de EDPS dat het noodzakelijk is de problemen die cloud computing met zich meebrengt op internationaal niveau aan te pakken. Hij spoort de Commissie aan een internationale dialoog te starten over de problemen die cloud computing met zich meebrengt, met inbegrip van jurisdictie en toegang voor rechtshandhavingsinstanties, en suggereert dat veel van deze problemen in verschillende internationale of bilaterale overeenkomsten kunnen worden afgedekt, zoals overeenkomsten voor wederzijdse bijstand en ook handelsovereenkomsten. Mondiale normen moeten op international niveau worden ontwikkeld om te komen tot minimale voorwaarden en beginselen ten aanzien van de toegankelijkheid van gegevens voor rechtshandhavingsinstanties. Hij ondersteunt ook de ontwikkeling door de toezichthoudende instanties van effectieve mechanismen voor internationale samenwerking, in het bijzonder op het gebied van kwesties omtrent cloud computing.

Gedaan te Brussel, 16 november 2012.

Peter HUSTINX

Europese Toezichthouder voor gegevensbescherming