# Zienswijze inzake de toepassing van de Wet bescherming persoonsgegevens bij een overeenkomst met betrekking tot cloud computing diensten van een Amerikaanse leverancier

## Inleiding

Op 20 februari 2012 (gedateerd 25 januari 2012) ontving het College bescherming persoonsgegevens (CBP) een verzoek van SURFmarket (destijds nog SURFdiensten geheten) om een zienswijze.[1] Parallel aan de beantwoording van dit verzoek werkte het CBP samen met de andere Europese privacy-toezichthouders, verenigd in de Groep gegevensbescherming artikel 29 (WP29), aan een gezamenlijk standpunt over cloud computing in relatie tot de bescherming van persoonsgegevens. Deze laatste activiteit heeft geresulteerd in een advies dat op 1 juli 2012 door de plenaire vergadering van WP29 werd aangenomen.[2] Mede omdat het CBP in deze zienswijze aan wilde sluiten op het Europese standpunt heeft de beantwoording van het verzoek langer geduurd dan gebruikelijk is. Het CBP heeft hierover tussentijds contact gehad met SURFmarket.

In het verzoek geeft SURFmarket aan in bespreking te zijn met een Europese vestiging van een Amerikaanse leverancier over het gratis aanbieden van een aantal cloud-diensten,[3] en dat in deze besprekingen 'verschillen [zijn] gerezen over de interpretatie van de Europese Privacyrichtlijn 95/ 46/ EG' en de implementatie daarvan in de Wet bescherming persoonsgegevens (Wbp). SURFmarket geeft daarbij aan dat door de verschillen in interpretatie 'het gevaar kan ontstaan dat de beveiliging en bescherming van persoonsgegevens van zeer vele personen tekort schiet. SURFmarket kan met haar dienstverlening potentieel namelijk honderdduizenden medewerkers en studenten voorzien van de [cloud-diensten].' SURFmarket wijst er op dat er ook bijzondere persoonsgegevens worden verwerkt.

SURFmarket legt het CBP – kort samengevat – de volgende vragen voor:

1. Biedt de zelfcertificering door de Amerikaanse leverancier bij het *Safe Harbor Framework* voldoende waarborgen voor de doorgifte van persoonsgegevens aan de Verenigde Staten (VS)?
2. Biedt de standaard *Statement on Auditing Standards no.* 70 (SAS 70) voldoende zekerheid over de beveiliging van de verwerkte persoonsgegevens of zijn de standaarden *International Standard for Assurance Engagements* (ISAE) 3402 en *Statement on Standards for Attestation Engagements* (SSAE) 16 daartoe beter toegerust?
3. Volstaat de zelfcertificering van de Amerikaanse leverancier bij het *Safe Harbor Framework* om te waarborgen dat sub-bewerkers die door de leverancier worden ingeschakeld voldoen aan een vergelijkbaar passend beschermingsniveau?

---

[1] SURFmarket maakt deel uit van SURF, de samenwerkingsorganisatie voor het hoger onderwijs en onderzoek waarbinnen de Nederlandse universiteiten, hogescholen en onderzoeksinstellingen nationaal en internationaal gezamenlijk investeren in ICT-innovatie. SURF bestaat uit een aantal organisaties met een eigen werkterrein, te weten: SURF, SURFnet, SURFmarket, SURFshare en binnenkort SURFsara. SURFmarket sluit sinds 1991 overeenkomsten met aanbieders van software en wetenschappelijke informatiebronnen ten behoeve van medewerkers en studenten in het hoger onderwijs en wetenschappelijk onderzoek in Nederland.
Zie < http://www.surfmarket.nl/Over/Paginas/Samenwerking.aspx >.

[2] Bij het uitbrengen van deze zienswijze was dit advies uitsluitend nog beschikbaar in het Engels: *Opinion 05/2012 on Cloud Computing* van 1 juli 2012,
< http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf >.

[3] Bij de aangeboden cloud-diensten gaat het onder meer om e-mail, agendabeheer, groepsdiscussies en relatiebeheer.

Het vervolg van deze zienswijze geeft antwoord op de drie vragen die SURFmarket heeft voorgelegd aan het CBP. Met de beantwoording wil het CBP een zo groot mogelijke groep van aanbieders en afnemers duidelijkheid bieden over de kwesties die in de vragen van SURFmarket aan de orde komen. De vragen worden daarom in meer algemene zin beantwoord. De beantwoording gaat uit van een in Nederland gevestigde verantwoordelijke die, voor een verwerking van persoonsgegevens waarop de Wet bescherming persoonsgegevens (Wbp) van toepassing is, gebruik maakt van de cloud computing diensten van een leverancier die gevestigd is in de Verenigde Staten (VS).

## Juridisch kader

Relevant voor de beantwoording van de gestelde vragen zijn de artikelen 13 (beveiliging), 14 (het inschakelen van bewerkers), 15 (toezicht door de verantwoordelijke) en de artikelen 76 en 77 (internationale doorgifte) van de Wbp. Bij de beantwoording van de vragen in het vervolg van deze zienswijze worden deze artikelen nader besproken.

Het *Safe Harbor Framework*, dat in twee van de gestelde vragen wordt genoemd, heeft tot doel om de doorgifte van persoonsgegevens vanuit de Europese Unie (EU) / de Europese Economische Ruimte (EER) naar de VS te vergemakkelijken zonder daarbij afbreuk te doen aan de bescherming van de persoonsgegevens. Het gaat om een vorm van zelfcertificering, waarbij organisaties zich verplichten om een aantal principes op het gebied van de gegevensbescherming na te leven (de *Safe Harbor Principles* of Veilige Haven Beginselen). Bij de beantwoording van de betreffende vragen wordt nader ingegaan op de relevante inhoudelijke aspecten van het *Safe Harbor Framework*.

WP29, een samenwerkingsverband van Europese toezichthouders op de gegevensbescherming, heeft op 1 juli 2012 een advies aangenomen over cloud computing in relatie tot de bescherming van persoonsgegevens.[4] Deze zienswijze is mede gebaseerd op dit advies. Verder heeft het CBP bij het opstellen van deze zienswijze kennis genomen van de eerdere uitspraken van de Noorse[5] en de Deense[6] toezichthouders over cloud computing.

## Doorgifte van persoonsgegevens in de cloud

*Biedt de zelfcertificering door de Amerikaanse leverancier bij het Safe Harbor Framework voldoende waarborgen voor de doorgifte van persoonsgegevens aan de VS?*

Alvorens tot beantwoording van bovengenoemde vraag over te gaan worden onderstaand eerst de eisen weergegeven die de Wbp en de *Safe Harbor Principles* stellen aan doorgifte in het algemeen. Ook wordt daarbij ingegaan op wat het advies van WP 29 daarover overweegt.

De artikelen 76 en 77 Wbp regelen de doorgifte van persoonsgegevens naar landen buiten de EU/ EER. Doorgifte is een vorm van gegevensverwerking. Persoonsgegevens mogen in beginsel slechts naar landen buiten de EU/ EER worden doorgegeven indien dat land een 'passend beschermingsniveau' kent.
Indien een passend beschermingsniveau ontbreekt geldt in beginsel een doorgifteverbod en mogen persoonsgegevens alleen aan landen buiten de EU/ EER worden doorgegeven op grond van een van de in artikel 77 Wbp genoemde (wettelijke) uitzonderingen, zoals de uitdrukkelijke toestemming van een betrokkene, voor de noodzakelijke uitvoering van een overeenkomst of op grond van een vergunning van de minister van Veiligheid en Justitie. Steeds moet ook voldaan zijn aan de algemene vereisten van de Wbp.

---

[4] WP29, *Opinion 05/2012 on Cloud Computing* van 1 juli 2012.
[5] Uitspraak van de Noorse toezichthouder: *Will not let Norvegian enterprises use Google Apps,*
< http://www.datatilsynet.no/English/Publications/Will-not-let-Norwegian-enterprises-of-Google-Apps/ >
[6] Uitspraak van de Deense toezichthouder: *Processing of sensitive personal data in a cloud solution,*
< http://www.datatilsynet.dk/english/processing-of-sensitive-personal-data-in-a-cloud-solution/ >

De VS worden niet aangemerkt als een land met een 'passend beschermingsniveau' omdat er geen algemene wetgeving voor de bescherming van persoonsgegevens bestaat. Ter bevordering van de handelsrelaties tussen de VS en de EU en zonder afbreuk te willen doen aan het beschermingsniveau van persoonsgegevens, is daarom in 2000 het VS-EU *Safe Harbor Framework* tot stand gekomen, dat door de Europese Commissie bij beschikking is aangemerkt als 'passend beschermingsniveau'.[7]
Het *Safe Harbor Framework* is een vorm van zelfregulering door bedrijven. Voor zelfcertificering moet een organisatie die tot de Veilige Haven toe wil treden, zich aanmelden bij het ministerie van Handel van de VS en in het openbaar verklaren dat zij de Veilige Haven Beginselen zullen naleven. Aan de aanmelding worden overigens verschillende eisen gesteld in de beschikking, zoals de beschrijving en publicatie van een privacybeleid. Alleen voor die organisaties die zich verplicht hebben tot naleving van de zogenaamde Veilige Haven Beginselen (*Safe Harbor Principles*) geldt dat er sprake is van een passend beschermingsniveau.

De verklaring van naleving van de Veilige Haven Beginselen op zichzelf garandeert niet dat de bedrijven daaraan in de praktijk ook uitvoering geven. Het advies van WP29 merkt hierover het volgende op:

> *"The Working Party considers that companies exporting data should not merely rely on the statement of the data importer claiming that he has a Safe Harbor certification. On the contrary, the company exporting data should obtain evidence that the Safe Harbor selfcertifications exists and request evidence demonstrating that their principles are complied with. This is important especially with regard to the information provided to data subjects affected by the data processing."*[8]

Van de verantwoordelijke voor de doorgifte wordt in een cloud computing context aldus verwacht dat hij niet alleen verifieert of de zelfcertificering bestaat maar ook dat hij verzoekt om bewijs waaruit blijkt dat de Veilige Haven Beginselen door de importeur van de persoonsgegevens ook daadwerkelijk worden nageleefd.

De Veilige Haven Beginselen, op basis waarvan de zelfcertificering plaatsvindt, zijn geformuleerd op een hoog abstractieniveau.[9] Als handreiking bij de interpretatie heeft de Amerikaanse overheid een aantal *Frequently Asked Questions* (FAQ's) gepubliceerd.[10] Over de relatie tussen de Veilige Haven Beginselen en de bijbehorende FAQ's enerzijds, en de richtlijn 95/ 46/ EG anderzijds, bepaalt de Europese Commissie in artikel 2 van de eerder genoemde beschikking het volgende:

> *"Deze beschikking heeft alleen betrekking op de gepastheid van de bescherming die in de Verenigde Staten overeenkomstig de volgens de FAQ's ten uitvoer gelegde beginselen wordt geboden […] en laat de toepassing van andere bepalingen van die richtlijn de op de verwerking van persoonsgegevens in de lidstaten betrekking hebben […] onverlet."*

Naleving van de *Safe Harbor Principles* betekent dus uitsluitend dat doorgifte van persoonsgegevens naar de VS plaats kan vinden, en garandeert niet dat de verwerking van de persoonsgegevens in de VS voldoet aan alle eisen uit de richtlijn 95/ 46/ EG. Evenmin is

---

[7] 2000/520/EC Commission Decision of 26 July 2000, L 215, 25/08/2000, p. 0007-0047. Zie ook:
< http://export.gov/safeharbor/ >.
[8] WP 29, *Opinion 05/2012 on Cloud Computing* van 1 juli 2012, § 3.5.1, pagina 17.
[9] *Safe Harbor Privacy Principles, issued by the U.S. Department of Commerce on July 21, 2000,*
< http://export.gov/safeharbor/eu/eg_main_018475.asp >
[10] *U.S.-EU Safe Harbor Framework Documents: C. Frequently Asked Questions,*
< http://export.gov/safeharbor/eu/eg_main_018493.asp >

gegarandeerd dat de verwerking in de VS voldoet aan alle eisen uit de van toepassing zijnde nationale wet waarin de richtlijn 95/ 46/ EG is geïmplementeerd. De verantwoordelijke blijft ook bij verwerking door een bewerker, en ook bij verwerking in de cloud, verantwoordelijk voor de naleving van deze wet. Bij het sluiten van de overeenkomst zal de verantwoordelijke zich daarom ervan moeten vergewissen dat alle van toepassing zijnde wettelijke bepalingen zijn afgedekt, en zal hij eventueel aanvullende afspraken in de overeenkomst op moeten nemen.

Een onderwerp dat in dit verband specifiek om aandacht vraagt is de beveiliging van de verwerkte persoonsgegevens. WP29 stelt hierover het volgende:

> *"Finally, the Working Party considers that the Safe Harbor principles by themselves may also not guarantee the data exporter the necessary means to ensure that appropriate security measures have been applied by the cloud provider in the US, as may be required by national legislations based on the Directive 95/46/EC. In terms of data security cloud computing raises several cloud-specific security risks, such as loss of governance, insecure or incomplete data deletion, insufficient audit trails or isolation failures, which are not sufficiently addressed by the existing Safe Harbor principles on data security. Additional safeguards for data security may thus be deployed; such as by incorporating the expertise and resources of third parties that are capable of assessing the adequacy of cloud providers through different auditing, standardization and certification schemes. For these reasons it might be advisable to complement the commitment of the data importer to the Safe Harbor with additional safeguards taking into account the specific nature of the cloud."* [11]

Naleving van de *Safe Harbor Principles* biedt op zichzelf dus geen zekerheid dat de in de cloud verwerkte persoonsgegevens voldoende worden beveiligd, en het zal nodig zijn om daarover in de bewerkersovereenkomst aanvullende afspraken te maken.[12]

Resumerend kan het volgende worden gesteld over de waarborgen die zelfcertificering bij het *Safe Harbor Framework* biedt voor de doorgifte van persoonsgegevens aan de VS, en kunnen de volgende aandachtspunten worden aangereikt:

1. De verklaring van naleving van de *Safe Harbor Principles* garandeert op zichzelf niet dat de organisatie deze in de praktijk ook daadwerkelijk naleeft. De verantwoordelijke zal zich ervan moeten vergewissen dat de zelfcertificering bestaat en dat deze in de praktijk daadwerkelijk wordt nageleefd.
2. Ook als de *Safe Harbor Principles* aantoonbaar worden nageleefd, betekent dit uitsluitend dat de doorgifte van persoonsgegevens naar de VS plaats kan vinden en niet dat de verwerking in de VS voldoet aan alle eisen uit de richtlijn 95/46/EG. Evenmin is gegarandeerd dat de verwerking in de VS voldoet aan alle eisen uit de van toepassing zijnde nationale wet waarin de richtlijn 95/46/EG is geïmplementeerd. De verantwoordelijke blijft ook bij verwerking door een bewerker, en ook bij verwerking in de cloud, verantwoordelijk voor de naleving van deze wet. Bij het sluiten van de overeenkomst zal de verantwoordelijke zich daarom ervan moeten vergewissen dat alle van toepassing zijnde wettelijke bepalingen zijn afgedekt, en zal hij eventueel aanvullende afspraken in de overeenkomst op moeten nemen.
3. Een onderwerp dat in dit verband specifiek om aandacht vraagt is de beveiliging van de verwerkte persoonsgegevens. Naleving van de *Safe Harbor Principles* biedt op zichzelf geen

[11] WP 29, *Opinion 05/2012 on Cloud Computing* van 1 juli 2012, § 3.5.1, pagina 18.
[12] ENISA, een Europese organisatie die zich bezig houdt met informatiebeveiliging, heeft een handreiking over dit onderwerp gepubliceerd. ENISA, *Procure secure: A guide to monitoring of security service levels in cloud contracts*, < http://www.enisa.europa.eu/activities/application-security/cloud-computing/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts >

zekerheid dat de in de cloud verwerkte persoonsgegevens voldoende worden beveiligd, en het zal nodig zijn om daarover in de bewerkersovereenkomst aanvullende afspraken te maken.

## Beveiliging van persoonsgegevens in de cloud

*Biedt de standaard Statement on Auditing Standards no. 70 (SAS 70) voldoende zekerheid over de beveiliging van de verwerkte persoonsgegevens of zijn de standaarden International Standard for Assurance Engagements (ISAE) 3402 en Statement on Standards for Attestation Engagements (SSAE) 16 daartoe beter toegerust?*

De standaards die in de vraag worden genoemd bevatten richtlijnen voor het afgeven van een zogenaamde '*third party* mededeling' (TPM). Een TPM is een verklaring van een onafhankelijke externe deskundige, waarin deze een oordeel geeft over de maatregelen die een bewerker heeft getroffen. De TPM wordt opgesteld in opdracht van de bewerker, en wordt verstrekt aan de verantwoordelijken die gebruik maken van diens diensten. Het doel van het verstrekken van een TPM is om de verantwoordelijken inzicht te bieden in de getroffen maatregelen, zonder dat iedere verantwoordelijke daar zelf onderzoek naar hoeft te (laten) doen.
Voor het opstellen van TPM's bestaat een aantal breed geaccepteerde standaarden. De belangrijkste daarvan zijn de drie standaarden die in de vraag worden genoemd: SAS70, ISAE 3402 en SSAE 16. In Nederland wordt vooral ISAE 3402 toegepast. SSAE 16 is sterk gebaseerd op ISAE 3402, maar heeft op punten een uitwerking gekregen die past binnen de Amerikaanse regelgeving. Beide standaards vervangen de inmiddels vervallen SAS70.
Binnen zowel ISAE 3402 als SSAE 16 wordt de basis voor de TPM gevormd door een beschrijving door de bewerker van de maatregelen die voor de doelgroep van de TPM relevant zijn. De externe deskundige toetst deze beschrijving onder meer op volledigheid en stelt vervolgens vast of de bewerker de beschreven maatregelen daadwerkelijk heeft getroffen. Afhankelijk van het type TPM doet de externe deskundige een uitspraak over de aanwezigheid van de beschreven maatregelen op een bepaalde datum (type 1) of gedurende een bepaalde periode (type 2).

Alvorens over te gaan tot de beantwoording van de gestelde vraag, worden onderstaand eerst kort de eisen weergegeven die de Wbp stelt aan de beveiliging van persoonsgegevens bij verwerking door een bewerker. Deze eisen zijn van toepassing op iedere vorm van verwerking door een bewerker, ook als de verwerking plaatsvindt in de cloud. De kern van deze eisen is opgenomen in artikel 14 Wbp. Daarnaast zijn ook de artikelen 12 en 13 Wbp van toepassing op de verwerking door een bewerker.
Artikel 14 Wbp schrijft voor dat de verantwoordelijke, als hij persoonsgegevens laat verwerken door een bewerker, moet zorgen dat de bewerker voldoende technische en organisatorische beveiligingsmaatregelen treft. De verantwoordelijke moet toezien op naleving van die maatregelen.[13] De afspraken die de verantwoordelijke met de bewerker maakt over de bescherming en de beveiliging van persoonsgegevens moeten schriftelijk of in een andere, gelijkwaardige vorm worden vastgelegd.[14]
Artikel 13 Wbp schrijft voor dat de verantwoordelijke passende technische en organisatorische maatregelen moet treffen om de persoonsgegevens die hij verwerkt te beveiligen tegen verlies en onrechtmatige verwerking. Bij verwerking door een bewerker moet de verantwoordelijke zorgen dat de bewerker de verplichtingen nakomt die ingevolge artikel 13 op de verantwoordelijke rusten.[15]

---

[13] Artikel 14 lid 1 Wbp.
[14] Artikel 14 lid 2 Wbp: 'De uitvoering van verwerkingen door een bewerker wordt geregeld in een overeenkomst of krachtens een andere rechtshandeling waardoor een verbintenis ontstaat tussen de bewerker en de verantwoordelijke'. Artikel 14 lid 5 Wbp: 'Met het oog op het bewaren van het bewijs worden de onderdelen van de overeenkomst of de rechtshandeling die betrekking hebben op de bescherming van persoonsgegevens, alsmede de beveiligingsmaatregelen als bedoeld in artikel 13 schriftelijk of in een andere, gelijkwaardige vorm vastgelegd'.
[15] Artikel 14 lid 3 onderdeel b Wbp.

Artikel 12 Wbp schrijft voor dat de bewerker, diens personeel en anderen die onder zijn gezag vallen, persoonsgegevens uitsluitend mogen verwerken in opdracht van de verantwoordelijke. De verantwoordelijke moet toezien op naleving van deze verplichting.[16] Verder legt artikel 12 aan de bewerker, diens personeel en anderen die onder zijn gezag vallen, een geheimhoudingsplicht op met betrekking tot de persoonsgegevens die zij verwerken.

Een TPM kan voor de verantwoordelijke een middel zijn om vast te stellen of de bewerker de noodzakelijke organisatorische en technische beveiligingsmaatregelen daadwerkelijk getroffen heeft. Aandachtspunten daarbij zijn:

1. De standaard SAS 70 wordt niet meer gebruikt. De standaarden ISAE 3402 en SSAE 16, die SAS 70 vervangen, zijn onderling min of meer vergelijkbaar. Beide standaarden zien op de wijze waarop de onafhankelijke externe deskundige zijn onderzoek uitvoert en daarover rapporteert, en niet op de maatregelen die worden beoordeeld.
2. Voor de verantwoordelijke is het vooral van belang welke maatregelen in de TPM worden betrokken, en of een uitspraak wordt gedaan over de aanwezigheid van de beschreven maatregelen op een bepaalde datum (type 1) of gedurende een bepaalde periode (type 2). Hiaten in de TPM, bijvoorbeeld waar het gaat om technische beveiligingsmaatregelen die specifiek zijn voor verwerking in de cloud,[17] zullen via aanvullende rapportages moeten worden ingevuld.

## Verwerking door sub-bewerkers in de cloud

*Volstaat de zelfcertificering van de Amerikaanse leverancier bij het Safe Harbor Framework om te waarborgen dat sub-bewerkers die door de aanbieder worden ingeschakeld voldoen aan een vergelijkbaar passend beschermingsniveau?*

Bewerkers van persoonsgegevens kunnen bij de verwerking van persoonsgegevens sub-bewerkers inschakelen. Een cloud-dienstverlener die applicaties aan zijn afnemers ter beschikking stelt, kan bijvoorbeeld voor de fysieke opslag van de verwerkte persoonsgegevens gebruik maken van de diensten van een sub-bewerker.

Alvorens over te gaan tot de beantwoording van de gestelde vraag, wordt onderstaand eerst kort de eisen weergegeven uit de Wbp en uit de *Safe Harbor Principles* die betrekking hebben op het inschakelen van sub-bewerkers bij de verwerking van persoonsgegevens.

Bij de beantwoording van de voorgaande vraag zijn de eisen besproken die de artikelen 12, 13 en 14 van de Wbp stellen aan de beveiliging van persoonsgegevens bij verwerking door een bewerker. Deze eisen zijn integraal van toepassing als de bewerker de persoonsgegevens laat verwerken door een of meer sub-bewerkers.
Uitgangspunt blijft dat de verantwoordelijke verantwoordelijk is voor alles wat er met de persoonsgegevens gebeurt, en uit deze verantwoordelijkheid vloeit voort dat persoonsgegevens alleen maar door een sub-bewerker kunnen worden verwerkt als de verantwoordelijke daar uitdrukkelijk mee heeft ingestemd. Indien de verantwoordelijke daarvoor in de bewerkersovereenkomst uitdrukkelijk ruimte heeft gegeven mag de bewerker – met behoud van zijn volle aansprakelijkheid voor de naleving van zijn overeenkomst met de verantwoordelijke – delen van de verwerking uitbesteden aan sub-bewerkers. De bewerker dient dan wel contractueel verzekerd te hebben dat de sub-bewerker zich eveneens richt naar de instructies van

[16] Artikel 14 lid 3 onderdeel a Wbp.
[17] Zie voor meer informatie ENISA, *Procure secure: A guide to monitoring of security service levels in cloud contracts*, URL: http://www.enisa.europa.eu/activities/application-security/cloud-computing/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts

de verantwoordelijke, tot geheimhouding verplicht is en de nodige beveiligingsmaatregelen ten opzichte van de gegevensverwerking neemt.[18]

De *Safe Harbor Principles* stellen in het beginsel 'verdere doorgifte' de volgende eisen aan het inschakelen van (sub)bewerkers:

> *"Wanneer [een organisatie] informatie wil doorgeven aan een derde die als haar vertegenwoordiger optreedt[19], mag dit indien zij zich er eerst van vergewist dat deze derde de Veiligehavenbeginselen onderschrijft, dan wel de richtlijn of een andere vaststelling van gepastheid op hem van toepassing is, of indien zij een schriftelijke overeenkomst met deze derde aangaat waarin zij eist dat deze derde ten minste dezelfde bescherming van de persoonlijke levenssfeer biedt als de betreffende Veiligehavenbeginselen bieden. Indien de organisatie aan deze eisen voldoet, zal zij niet aansprakelijk worden gehouden (tenzij door de organisatie anders wordt overeengekomen) indien een derde partij waaraan de informatie is doorgegeven, deze verwerkt op een manier die strijdig is met eventuele restricties of verklaringen, tenzij de organisatie wist of had moeten weten dat de derde partij de informatie op een dergelijke manier zou verwerken, maar geen redelijke maatregelen heeft genomen om deze verwerking te voorkomen of stop te zetten."*

Over het inschakelen van sub-bewerkers bij de verwerking van persoonsgegevens in de cloud stelt WP29 het volgende:

> *"If processors subcontract services out to sub-processors, they are obliged to make this information available to the client, detailing the type of service subcontracted, the characteristics of current or potential subcontractors and guarantees that these entities offer to the provider of cloud computing services to comply with Directive 95/46/EC. All the relevant obligations must therefore apply also to the sub-processors through contracts between the cloud provider and subcontractor reflecting the stipulations of the contract between cloud client and cloud provider.* […] *In the view of the WP29, the processor can subcontract its activities only on the basis of the consent of the controller, which may be generally given at the beginning of the service with a clear duty for the processor to inform the controller of any intended changes concerning the addition or replacement of subcontractors with the controller retaining at all times the possibility to object to such changes or to terminate the contract. There should be a clear obligation of the cloud provider to name all the subcontractors commissioned. In addition, a contract should be signed between cloud provider and subcontractor reflecting the stipulations of the contract between cloud client and cloud provider."* [20]

WP29 benadrukt dat, ook in situaties met meerdere (sub)bewerkers, de verantwoordelijkheden met betrekking tot de naleving van de wettelijke voorschriften helder moeten worden belegd en dat de verantwoordelijke eindverantwoordelijk blijft:

> *"In such scenarios, the obligations and responsibilities deriving from data protection legislation should be set out clearly and not dispersed throughout the chain of outsourcing or subcontracting, in order to ensure effective control over and allocate clear responsibility for processing activities."* [21]

Resumerend kan worden gesteld dat zelfcertificering bij het *Safe Harbor Framework* om de volgende redenen niet volstaat om te waarborgen dat (sub-) bewerkers voldoen aan een

---

[18] Memorie van Toelichting Wbp bij artikel 1 onder e.
[19] In de *Safe Harbor Principles* wordt de rol van (sub)bewerker omschreven als 'een derde die optreedt als vertegenwoordiger van een organisatie om uit haar naam en in haar opdracht een of meer taken uit te voeren'.
[20] WP 29, *Opinion 05/2012 on Cloud Computing* van 1 juli 2012, § 3.3.2, pagina 9.
[21] WP 29, *Opinion 05/2012 on Cloud Computing* van 1 juli 2012, § 3.3.2, pagina 9.

vergelijkbaar passend beschermingsniveau, en kunnen de volgende aandachtspunten worden aangereikt:

1. Het beginsel 'verdere doorgifte' uit de Veilige Haven Beginselen staat verwerking door een (sub-) bewerker onder bepaalde voorwaarden toe: de (sub-) bewerker moet bijvoorbeeld zelf ook de Veilige Haven Beginselen onderschrijven.
2. De beperkingen van de waarborgen die de zelfcertificering biedt bij verwerking door een (sub-) bewerker zijn analoog aan wat eerder in deze zienswijze werd aangegeven. Een organisatie die de *Safe Harbor Principles* onderschrijft is niet verplicht om vast te stellen of een (sub-) bewerker de gestelde voorwaarden in de praktijk daadwerkelijk naleeft. Daarbij komt dat, ook als de (sub-) bewerker de gestelde voorwaarden daadwerkelijk naleeft, er nog geen garantie is dat de verwerking door de (sub-) bewerker daarmee eveneens voldoet aan alle eisen uit de Europese richtlijn 95/46/EG of uit de nationale wet waarin deze richtlijn is geïmplementeerd.
3. De eisen die de Wbp stelt aan de verwerking door sub-bewerkers gaan verder dan de eisen uit de *Safe Harbor Principles*. De Wbp staat de inzet van sub-bewerkers uitsluitend toe als de verantwoordelijke daar in de bewerkersovereenkomst uitdrukkelijk ruimte voor biedt, en de bewerker dient contractueel verzekerd te hebben dat de sub-bewerker zich eveneens richt naar de instructies van de verantwoordelijke, tot geheimhouding verplicht is en de nodige beveiligingsmaatregelen ten opzichte van de gegevensverwerking neemt.
4. Ook bij inzet van meerdere (sub-) bewerkers blijft de verantwoordelijke volledig verantwoordelijk voor de naleving van de Wbp.
5. In relatie met de voorgaande vraag kan nog worden opgemerkt dat TPM's kunnen worden afgegeven met medeneming of met uitsluiting van de maatregelen die door sub-bewerkers worden getroffen ('*inclusive*' of '*carve-out*'). Als gebruik wordt gemaakt van TPM's moet de verantwoordelijke in de bewerkersovereenkomst vastleggen of de maatregelen door sub-bewerkers wel of niet worden meegenomen.

## Slotbeschouwing

Het CBP heeft in deze zienswijze de voorgelegde vragen in algemene zin beantwoord. Daarbij is uitgegaan van een verwerking van persoonsgegevens waarop de Wbp van toepassing is, met een in Nederland gevestigde verantwoordelijke die cloud computing diensten afneemt van een in de VS gevestigde bewerker die de *Safe Harbor Principles* onderschrijft.

Kenmerkend voor cloud computing is echter dat de gegevensverwerking in potentie plaats kan vinden op servers die in de hele wereld kunnen staan. Het advies van WP 29 merkt daarover het volgende op:

> *"However, cloud computing is most frequently based on a complete lack of any stable location of data within the cloud provider's network. Data can be in one data centre at 2pm and on the other side of the world at 4pm. The cloud client is therefore rarely in a position to be able to know in real time where the data are located or stored or transferred. In this context, the traditional legal instruments providing a framework to regulate data transfers to non-EU third countries not providing adequate protection, have limitations."* [22]

[22] WP 29, *Opinion 05/2012 on Cloud Computing* van 1 juli 2012, § 3.5, pagina 17.

WP 29 voegt daaraan toe:

> *"Adequacy findings, including Safe Harbor, are limited in respect of the geographical scope, and therefore do not cover all transfers within the cloud."* [23]

Verder zal er binnen een cloud-context vaak sprake zijn van meerdere (sub-) bewerkers en zelfs van meerdere verantwoordelijken. Uitgangspunt blijft, zoals eerder aangegeven, dat de verantwoordelijke ook bij verwerking van persoonsgegevens in de cloud, eindverantwoordelijk is voor de naleving van de Wbp.

Om invulling te geven aan zijn verantwoordelijkheid voor naleving van de Wbp, zal de verantwoordelijke ten eerste een risicoanalyse uit moeten voeren om vast te stellen of, en onder welke voorwaarden, er in zijn specifieke situatie gebruik kan worden gemaakt van cloud computing. Dit was ook een belangrijke conclusie in het advies van WP 29:

> *"A key conclusion of this Opinion is that businesses and administrations wishing to use cloud computing should conduct, as a first step, a comprehensive and thorough risk analysis. All cloud providers offering services in the EEA should provide the cloud client with all the information necessary to rightly assess the pros and cons of adopting such a service. Security, transparency and legal certainty for the clients should be key drivers behind the offer of cloud computing services."* [24]

De risicoanalyse geeft niet alleen inzicht in de risico's, maar ook in de aanvullende maatregelen die moeten worden getroffen om te waarborgen dat de betreffende verwerking van persoonsgegevens in de cloud voldoet aan de Wbp.

Ten tweede zal de verantwoordelijke moeten kiezen voor een cloud-dienstverlener die voldoende waarborgen biedt, en zal hij de noodzakelijke afspraken moeten vastleggen in het bewerkerscontract. WP 29 doet hierover de volgende globale aanbevelingen:

> *"In terms of the recommendations contained in this Opinion, a cloud client's responsibilities as a controller is highlighted and it is thus recommended that the client should select a cloud provider that guarantees compliance with EU data protection legislation. […] any contract between the cloud client and cloud provider should afford sufficient guarantees in terms of technical and organizational measures. Also of significance is the recommendation that the cloud client should verify whether the cloud provider can guarantee the lawfulness of any cross-border international data transfers."* [25]

Een aandachtspunt is de aansprakelijkheid voor eventuele inbreuken op de bescherming van de persoonlijke levenssfeer. Artikel 49 Wbp stelt de verantwoordelijke aansprakelijk voor de schade of het nadeel dat voortvloeit uit niet-naleving van de Wbp, en stelt de bewerker aansprakelijk voor de schade of het nadeel voor zover ontstaan door zijn werkzaamheid. Het is noodzakelijk om deze aansprakelijkheid te concretiseren in het bewerkerscontract, en op voorhand duidelijk vast te stellen welke natuurlijke of rechtspersoon in welke gevallen en in welke mate aansprakelijk is.

Tot slot wijst het CBP op het voornemen van de regering om de zogenoemde 'brede meldplicht' voor datalekken in het leven te roepen. Voor aanbieders van openbare elektronische communicatiediensten is een dergelijke meldplicht nu al opgenomen in artikel 11.3a van de Telecommunicatiewet (de zogenoemde 'smalle meldplicht'). De brede meldplicht richt zich tot de

[23] WP 29, *Opinion 05/2012 on Cloud Computing* van 1 juli 2012, § 3.5.1, pagina 17.
[24] WP 29, *Opinion 05/2012 on Cloud Computing* van 1 juli 2012, *Executive summary*, pagina 2.
[25] WP 29, *Opinion 05/2012 on Cloud Computing* van 1 juli 2012, *Executive summary*, pagina 2.

verantwoordelijke. Bij verwerking door een bewerker draagt de verantwoordelijke zorg dat de bewerker 'de verplichtingen nakomt die op de verantwoordelijke rusten ten aanzien van de verplichting tot melding van [datalekken]'. De afspraken die de verantwoordelijke met de bewerker maakt over de nakoming met de meldplicht moeten schriftelijk of in een andere, gelijkwaardige vorm worden vastgelegd.[26] De eisen uit het wetsvoorstel zijn integraal van toepassing op verwerking van persoonsgegevens in de cloud en op verwerking door sub-bewerkers. Het verdient aanbeveling om hier bij het afsluiten van overeenkomsten met aanbieders van cloud-diensten nu reeds rekening mee te houden.

[26] Wijziging van de Wet bescherming persoonsgegevens voor verruiming gebruik camerabeelden en invoering van meldplicht bij datalekken
< http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2011/12/20/wijziging-van-de-wet-bescherming-persoonsgegevens-voor-verruiming-gebruik-camerabeelden-en-invoering-van-meldplicht-bij-datalekken.html >;
Memorie van Toelichting Wijziging van de Wet bescherming persoonsgegevens
< http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2011/12/20/memorie-van-toelichting-wijziging-van-de-wet-bescherming-persoonsgegevens.html >.