Rapport
De wolk in het onderwijs

Privacy aspecten bij cloud computing services

TILT, Tilburg Institute for Law, Technology, and Society
Dr. Colette Cuijpers
Prof. Ronald Leenes
Sandra Olislaegers, LLM
Prof. Kees Stuurman

Het SURFnet/ Kennisnet Innovatieprogramma wordt financieel mogelijk gemaakt door het Ministerie van Onderwijs, Cultuur en Wetenschap.

Inhoudsopgave

Samenvatting **5**

Inleiding **6**

1 Wolkenkaart **8**

1.1 Cloud Computing 8

1.2 Cloud Service Provider 8

1.3 Verschillende modellen 9

2 Juridisch kader privacy en gegevensbescherming **11**

2.1 Inleiding 11

2.2 Privacy en gegevensbescherming 11

2.3 Het recht op privacy, Handvest en EVRM 12

2.4 Een gelaagd systeem van gegevensbescherming 14

3 Toepasselijkheid Wbp **16**

3.1 Introductie 16

3.2 Begrippen 16

3.3 Toepassing en reikwijdte 18

3.4 Toepasselijk recht 19

3.5 Begrip ´voor de verwerking verantwoordelijke´ 21

3.6 Conclusies 23

4 De Wet bescherming persoonsgegevens **25**

4.1 Laag 1: Algemene bepalingen 25

4.2 Laag 2: Bijzondere persoonsgegevens 27

4.3 Laag 3: Doorgifte naar derde landen 28

4.4 De Safe Harbor principles 33

5 Cloud Computing, contracten en privacy **35**

5.1 Inleiding 35

5.2 Een voorbeeld: de Google Apps Education Edition Agreement 35

5.3 Overeenkomsten en privacy 36

5.4 De Google Apps Education Edition Agreement en privacy 37

6 Aandachtspunten en kritische noten **39**

6.1 Complexiteit van de rolverdeling 41

6.2 Open vragen 42

Literatuur **43**

Samenvatting

Wat te doen bij Cloud Computing?

- Breng de rolverdeling en bevoegdheidsverdeling tussen de partijen betrokken bij Cloud Computing deugdelijk in kaart. Wie is voor welke verwerking verantwoordelijke en wie is/zijn bewerker(s)?
  - De onderwijsinstelling zal voor het merendeel van de verwerkingen verantwoordelijk zijn en daarbij gebonden zijn aan de Wbp, ongeacht de locatie van de gegevens.
- De relatie tussen verantwoordelijke en bewerker moet contractueel worden geregeld. Een van de belangrijkste punten betreft de bevoegdheden van de bewerker om gegevens voor door hem vastgestelde doeleinden te verwerken (en waarvoor de bewerker dus verantwoordelijke wordt).
- De verantwoordelijke moet er zorg voor dragen dat de Wbp ook door de ingeschakelde bewerkers wordt nageleefd.
- De doeleinden voor verwerking moeten gerechtvaardigd zijn en door de verantwoordelijke welbepaald en uitdrukkelijk worden omschreven. Dit moet schriftelijk worden vastgelegd, gecommuniceerd naar de betrokkenen en moet worden aangepast zodra zaken wijzigen.
- De onderwijsinstelling moet een gedragscode opstellen hoe studenten en medewerkers van de Clouddiensten gebruik mogen maken (hieruit moeten de gerechtvaardigde doeleinden voor verwerking van gegevens door studenten/medewerkers kunnen worden afgeleid, aangezien ook zijn onder omstandigheden verantwoordelijke kunnen zijn).
- In de gedragscode moeten uitdrukkelijk ook de consequenties op niet naleven van de gedragscode worden opgenomen. (zie rapport rechtmatig operationeel handelen uitgevoerd in opdracht van SURF)
- De keuze voor een Cloud Computing Service Provider vergt naast een kosten-baten-analyse een risico-analyse.
- Hoewel de locatie van de opgeslagen en verwerkte data niet bepalend is voor de toepasselijkheid van de Wbp speelt de locatie van de data een rol voor de toepasselijkheid van vreemd recht (bijv. USA Patriot Act) onderzoek daarom welke keuzes een beoogde Cloud Computing Service Provider biedt ten aanzien van de locatie van verwerking.

Inleiding

In het onderwijs wordt meer en meer online samengewerkt en gebruikt men veel online applicaties. Online applicaties aangeboden door derde partijen (waaronder Cloud Computing diensten) zorgen ervoor dat verantwoordelijkheden omtrent data en persoonsgegevens diffuser worden omdat ze mogelijk van de instelling verschuiven naar deze derde partijen, danwel gezamenlijke verantwoordelijkheden worden. Veel instellingen hebben nu vragen op dit gebied.

SURFnet heeft in samenwerking met SURFdirect, de digitale rechten expertise community van SURF, en Kennisnet, het Centrum voor Recht, Technologie en Samenleving (TILT) van de Universiteit van Tilburg gevraagd om antwoorden te formuleren op gesignaleerde vragen. Het resultaat is een whitepaper waarin aandacht wordt gegeven aan onderwerpen rond Cloud Computing waar basisscholen, middelbaar onderwijs en bij SURF aangesloten instellingen vragen over hebben. Met dit whitepaper kunnen de instellingen beter gefundeerd hun keuzes over het inzetten van online applicaties maken.

De vraagstelling die centraal staat in dit whitepaper is:

> *Welke privacy en data protectie vraagstukken leven onder basisscholen, middelbare scholen en de bij SURFnet aangesloten instellingen omtrent Cloud Computing services en hoe kunnen deze juridisch worden geduid?*

SURFnet
SURFnet, motor voor ICT-innovatie, maakt samenwerking in het hoger onderwijs en onderzoek mogelijk. Via een geavanceerde netwerkinfrastructuur, SURFnet6, zijn 160 instellingen in hoger onderwijs en onderzoek met elkaar verbonden. Om veilig en efficiënt toegang te hebben tot allerlei diensten op dat netwerk, ontwikkelt SURFnet authenticatie- en autorisatiediensten. Voor het samenwerken over de grenzen van instellingen heen, biedt SURFnet innovatieve omgevingen waarbinnen docenten, onderzoekers en studenten data uitwisselen, online overleggen en mediabestanden delen. Bij al deze activiteiten staat beveiliging hoog in het vaandel. Door de pioniersrol ontwikkelt SURFnet continu kennis over en ervaring met nieuwe technologieën. SURFnet vindt het belangrijk deze kennis te delen met de internationale netwerkgemeenschap en de SURFnet gebruikers.

Binnen het expertisedomein ‘Collaboration Infrastructure’ wil SURFnet stimulerend optreden op het gebied van online applicaties en unified communications. Daarnaast werkt SURFnet aan een actieve community van gebruikers van online applicaties.

SURFdirect
SURFdirect, de digitale rechten expertise community van SURF, identificeert de juridische aspecten die spelen bij diverse thema’s in e-learning en e-science. SURFdirect richt zich binnen de missie van SURF (innovatie, samenwerking en ICT) op het ondersteunen van het hoger onderwijs en onderzoek bij juridische kwesties rond toegang en hergebruik van tekst, beeld en geluid. Privacy is een van de gebieden waar SURFdirect haar kennis wil vergroten en wil publiceren ten behoeve van de doelgroep hoger onderwijs en onderzoek.

Kennisnet
Kennisnet is hét expertisecentrum als het gaat om ICT in het basis-, voortgezet, mbo en speciale onderwijs. Kennisnet ziet het als opdracht om scholen en onderwijsinstellingen onafhankelijke diensten aan te bieden bij het effectief inzetten van ICT. Zo kan de kwaliteit van het leren verder toenemen. De missie van Kennisnet is onderwijsinstellingen te ondersteunen en te inspireren met onafhankelijke expertise en diensten bij het effectief gebruik van ICT. De ontwikkelingen in het onderwijs zijn bepalend voor de focus van Kennisnet.

Centrum voor Recht, Technologie en Samenleving (TILT) van de Universiteit van Tilburg
Het onderzoek is uitgevoerd door onderzoekers van het Centrum voor Recht, Technologie en Samenleving (TILT) van de Universiteit van Tilburg in de periode november-december 2010. Het onderzoek is afgesloten op 15 december 2010.

Het onderzoek is vertrokken vanuit gesprekken met vertegenwoordigers van vijf instellingen, de UvT, de Universiteit Utrecht, Avans Hogeschool, de Open Universiteit en stichting Kennisnet. Het doel van deze gesprekken was een inventarisatie van onder instellingen van basis, middelbaar en hoger onderwijs levende behoeften en gesignaleerde vraagstukken ten aanzien van Cloud Computing services. Het gaat hierbij zowel om online applicaties zoals Google Apps en Microsoft's Live@edu, maar ook meer onderwijsinhoudelijke uitbesteding van software naar de Cloud zoals bijvoorbeeld Elektronische LeerOmgevingen (ELO's) of onderwijs informatie systemen. Een samenvatting van de gesprekken is te vinden in bijlage 1.
Op basis van de gesprekken heeft literatuuronderzoek en deskonderzoek plaatsgevonden om de gesignaleerde vragen te beantwoorden.

Inhoud
De opbouw van dit whitepaper is als volgt. Hoofdstuk 1 schetst kort het veld van studie, Cloud Computing services om een beeld te krijgen wat wel en niet binnen het blikveld van dit whitepaper valt. Hoofdstuk 2 zet het juridische kader rond privacy en de bescherming van persoonsgegevens in hoofdlijnen uiteen. Vervolgens wordt in hoofdstuk 3 ingegaan op een van de lastigste vragen rond Cloud Computing en privacy: het toepasselijke recht. Hoofdstuk 4 behandelt de kernonderdelen van de Wet bescherming persoonsgegevens in het licht van Cloud Computing. Daarbij wordt ook gekeken naar doorgifte van gegevens naar landen buiten de EU, hetgeen in veel Cloud scenario's het geval is. In hoofdstuk 5 gaan we in op de rol van overeenkomsten naast de Wbp in het regelen van de rechtsverhoudingen tussen de verschillende partijen. Hoofdstuk 6 sluit het document af met een aantal aandachtspunten en overwegingen voor nadere reflectie.

1 Wolkenkaart

1.1 Cloud Computing

Cloud Computing is een verzamelnaam voor verschillende soorten configuraties van apparatuur, diensten en voorzieningen. Om de juridische aspecten rond privacy en gegevensbescherming te kunnen bespreken, is het noodzakelijk de relevante onderscheiden en modellen helder te hebben.

Met betrekking tot diensten die worden aangeboden in de Cloud wordt doorgaans een onderscheid gemaakt in Software as a Service (SaaS), Platform as a Service (PaaS) en Infrastructure as a Service (IaaS). Bij SaaS gaat het om applicaties die via internet worden aangeboden door een Cloud Service Provider. Het kan hierbij gaan om diensten zoals e-mail (bijv. Hotmail) voorzieningen, office-achtige applicaties (bijv. Google docs), maar ook om online sociale netwerken. Eigenlijk iedere applicatie die in een browser kan worden gebruikt, kan als SaaS worden aangeboden. SaaS is in de context van SURFnet/Kennisnet de meest relevante vorm van Clouddienstverlening.

Bij Platform as a Service biedt de Cloud Service Provider een computer- en softwareplatform aan waarop de klant zelf diensten en voorzieningen kan ontwikkelen. Een voorbeeld hiervan is Amazon AWS.[1] Klanten kunnen binnen AWS zelf websites en webapplicaties bouwen die ze ter beschikking kunnen stellen aan hun gebruikers en/of klanten.[2]

IaaS gaat een stap verder. De Cloud Service Provider levert hier in wezen hardware die via het internet kan worden benaderd. De klant kan hierop iedere gewenste software installeren, van besturingssysteem (Windows, Linux, Mac OS) tot daarop draaiende applicaties. IaaS maakt het daarmee mogelijk om lokaal met eenvoudige hard- en software te volstaan (bijv. een iPad of een thin client[3]) en krachtige hardware en software van elders te gebruiken.

Aangezien de onderwijsinstellingen betrokken in de interviews aan hebben gegeven momenteel met name te focussen op mogelijkheden van SaaS, zal dit rapport zich hierop richten.[4]

1.2 Cloud Service Provider

Naast verschillende soorten diensten zijn er ook verschillende configuraties van diensten mogelijk waarbij meerdere partijen betrokken kunnen zijn. Er is in alle gevallen sprake van een Cloud Service Provider (CCSP[5]). Dit is de juridische entiteit die de dienst(en) aanbiedt. De feitelijke levering van diensten vindt plaats vanaf servers die al dan niet aan de CCSP toebehoren en die zich al dan niet op dezelfde fysieke plaats bevinden als de CCSP. Ze kunnen zelfs geheel of gedeeltelijk in verschillende landen staan. Om die reden benoemen we de servers apart. We kunnen op het vlak van de servers onderscheid maken tussen Applicatie Servers (AS) en Storage Servers (SS).

---

1 Zie http://AWS.amazon.com/

2 Het in december 2010 in opspraak geraakte WikiLeaks draaide bijvoorbeeld op Amazon AWS. Zie bijvoorbeeld http://AWS.amazon.com/message/65348/

3 Een 'thin client' is een apparaat dat beschikt over beperkte eigen opslag en verwerkingscapaciteit en die derhalve alleen dient als 'terminal' voor een krachtiger computer. Een thin client is bijvorbeeld een internet TV die alleen beschikt over een web browser.

4 Zie bijlage I voor een samenvatting van de interviews.

5 Afgekort als CCSP, Cloud Computing Service Provider, dit om verwarring met Certification Service Provider (CSP) te voorkomen.

Vaak zullen deze fysiek op één enkele server draaien, maar het is mogelijk dat de applicatie (webservice) op een andere server draait dan die waarop de data van de gebruikers worden opgeslagen. Ook hier geldt dat de AS en SS mogelijk in verschillende landen staan en onder verschillende jurisdicties vallen.

Aan de andere kant van de dienstverlening staat de gebruiker. Dit is de natuurlijke persoon die feitelijk van de Cloud Service gebruik maakt. Dit is voor onderhavig rapport dus doorgaans een student, docent of medewerker van een (hogere) onderwijsinstelling. De gebruiker zal zich doorgaans binnen Nederland bevinden, maar dat hoeft niet; Cloud Services zijn bij uitstek geschikt om waar dan ook ter wereld afgenomen te worden. De gebruiker kan klant zijn van een CCSP. Dat is bijvoorbeeld het geval voor een student die een Hotmail account heeft bij Microsoft of Google Docs gebruikt buiten de onderwijsinstelling om. In dit rapport richten we ons echter vooral op het geval waarin ook de onderwijsinstelling is betrokken in de relatie met de CCSP. In dat geval is de (eind-)gebruiker geen klant van de CCSP, maar is de instelling dat.

1.3 Verschillende modellen

Tussen de gebruiker en de CCSP kunnen zich zoals aangeduid allerlei partijen bevinden. In de context van dit rapport zijn dat in ieder geval een onderwijsinstelling die als klant van de CCSP opereert. De klant sluit een contract af met de CCSP waarin afspraken worden gemaakt over het gebruik van de dienst en de voorwaarden waaraan dit gebruik is gebonden.[6]

Verder staan tussen de gebruiker en de CCSP in de context van het onderwijs partijen zoals SURFnet en Kennisnet. Deze partijen faciliteren het identiteitsmanagement en spelen een rol in eventuele mantelovereenkomsten.

De juridische positie van de verschillende partijen is afhankelijk van de feitelijke en juridische configuratie van een concrete Cloud Service. Hieronder worden drie bestaande basismodellen weergegeven die behulpzaam zijn om de juridische positie van de verschillende partijen te duiden en aandachtspunten te benoemen.

Basismodel
In het basismodel gaat de gebruiker (student) een overeenkomst aan met een CCSP. Dit betekent in de praktijk dat de student een account aanmaakt op de website van de CCSP en middels de bekende click overeenkomst aangeeft akkoord te gaan met de voorwaarden van de dienstverlener.[7] De gebruiker bepaalt in deze configuratie zelfstanding wat zij wel en niet doet binnen de Clouddienst, binnen de grenzen van de overeenkomst van de CCSP.

Instellingsmodel
Binnen de context van dit model sluit een onderwijsinstelling een overeenkomst met een CCSP waarin zaken aan bod komen zoals de diensten, kosten en het service level (onder meer bepalingen over de beschikbaarheid van de dienst in de tijd). De onderwijsinstelling biedt de dienst vervolgens aan haar studenten en medewerkers aan, maar is feitelijk zelf niet of nauwelijks bij de operationele dienstverlening betrokken. De gebruikers werken direct op de servers van de Cloud Service. De Cloud Service kan in het instellingsmodel worden gepersonaliseerd naar zowel gebruiker als instelling. Zo zal de student in dit geval niet als e-mail adres hebben guppie24@hotmail.com, maar g.pieters@Luus.college.nl.
De gebruiker is in deze configuratie niet de enige die bepaalt welke handelingen worden verricht binnen de Cloud Service en welke gegevens daarbij heen en weer stromen.

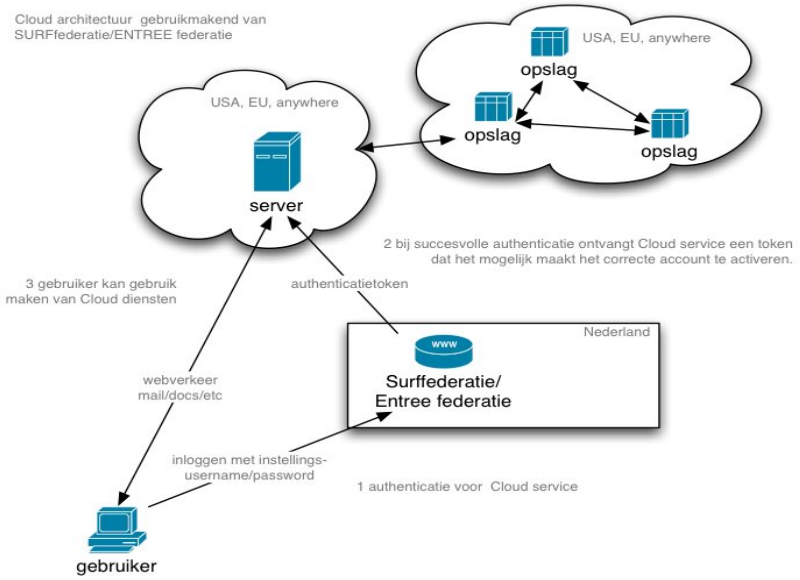
---

6 Naast het contract zijn er uiteraard allerhande wetten en regelingen van toepassing op het gebruik van de Clouddienst. Een deel daarvan komt in dit whitepaper aan bod.

7 Doorgaans zal de gebruiker de voorwaarden waarmee zij akkoord gaat niet hebben gelezen. Dat staat de rechtskracht van die voorwaarden niet in de weg. Door middel van het aanvinken van het 'akkoord' vakje verklaart de gebruiker de voorwaarden te accepteren.

De onderwijsinstelling bepaalt alleen of gedeeltelijk wat onder de dienstverlening valt, wederom binnen de grenzen van de overeenkomst met de CCSP. Binnen het instellingsmodel zal de onderwijsinstelling of de eindgebruiker zorg moeten dragen voor het identiteitsmanagement. Wanneer de instelling de gebruikers de mogelijkheid wil bieden om met een enkele set credentials (gebruikersnaam en wachtwoord) gebruik te maken van verschillende diensten, dan zal de instelling of de credentials aan de CCSP moeten verstrekken of het eigen identiteitsmanagementsysteem moeten koppelen met dat van de CCSP.

Federatiemodel
In het federatiemodel wordt gebruik gemaakt van de reeds bestaande federated identity infrastructuur binnen SURFnet en Kennisnet.[8] In dit model loopt de identificatie en authenticatie van de gebruiker via de SURFfederatie/Entree, die vervolgens de relevante informatie doorsluist naar de CCSP om deze het juiste user-account te laten selecteren. SURFfederatie en Entree zijn verder niet bij de dienstverlening betrokken.



Figuur 2: Cloud architectuur met authenticatie

[8] SURFfederatie is een dienst van SURFnet, De SURFfederatie is de authenticatie- en autorisatiedienst voor het hoger onderwijs en de research instellingen in Nederland. Leden van de SURFnet-doelgroep kunnen met hun instellingsaccount authenticeren bij diensten- en contentleveranciers op het internet. Zie: http://www.SURFnet.nl/nl/Thema/SURFfederatie/Pages/Default.aspx Meer informatie over de Kennisnet Federatie, de aanbieder van de dienst Entree, vindt u op http://www.kennisnetfederatie.nl. Het voordeel van Entree en SURFfederatie is dat een oplossing geboden wordt voor het probleem dat een gebruiker voor elke afgeschermde website een account nodig heeft. Dat leidt tot verschillende sets van gebruikersnamen en wachtwoorden, met alle problemen die daarbij horen. Identiteitsfederaties bieden single sign-on, met een gebruikersnaam/wachtwoord in kunnen loggen op alle websites binnen de federatie.

2 Juridisch kader privacy en gegevensbescherming

2.1 Inleiding

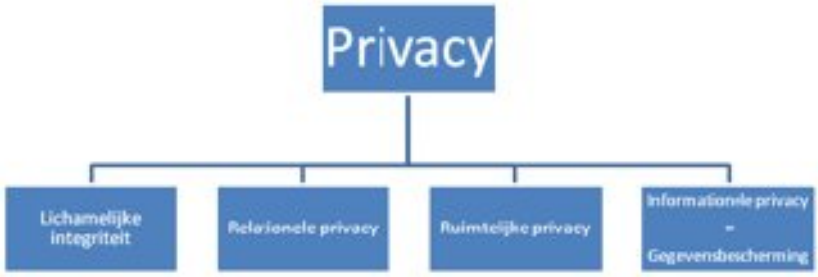
De in het vorige hoofdstuk beschreven Cloud Services roepen vragen op vanuit het perspectief van privacy en gegevensbescherming. Afhankelijk van de gekozen CCSP en het gekozen model, kunnen verschillende entiteiten (mede) verantwoordelijk zijn voor de verwerking van persoonsgegevens. De verwerking van gegevens kan op verschillende plaatsen in de wereld plaatsvinden. Gegevens kunnen op verschillende plaatsen in de wereld worden opgeslagen. Dit alles betekent dat de verwerking en de gegevens dus mogelijk onderworpen zijn aan verschillende juridische regimes. In dit hoofdstuk wordt de geldende wetgeving op het gebied van privacy en gegevensbescherming in kaart gebracht en toegelicht. Het Europese reguleringskader geldt als uitgangspunt, omdat alle 27 lidstaten van de EU verplicht zijn dit kader om te zetten in hun eigen nationale rechtsorde. Door deze omzetting in nationaal recht kunnen er (geringe) verschillen bestaan tussen de wetgeving van de individuele lidstaten op het gebied van privacy en gegevensbescherming. Op de hoofdlijnen komen de nationale regimes overeen. Omdat dit rapport zich toespitst op de Nederlandse situatie, zal de inhoudelijke uitleg van het recht op gegevensverwerking plaatsvinden aan de hand van de Nederlandse implementatie van de privacy richtlijn[9], de Wet bescherming persoonsgegevens. Naast EU-wetgeving kan ook wetgeving uit andere landen, zoals bijvoorbeeld de Verenigde Staten, van toepassing zijn omdat gebruik wordt gemaakt van diensten van aanbieders van buiten de EU en van apparatuur die zich buiten het grondgebied van de EU bevindt. De vraag welk recht van toepassing is op een concrete Cloud configuratie komt aan de orde in hoofdstuk 3.

2.2 Privacy en gegevensbescherming

In de eerste plaats is het belangrijk de concepten privacy en gegevensbescherming te begrijpen. Privacy en gegevensbescherming zijn gerelateerde begrippen maar vallen niet samen. Privacy is een overkoepelend begrip, een fundamenteel recht dat nauw verbonden is met persoonlijke vrijheid. Onder het overkoepelende begrip privacy kunnen verschillende dimensies worden onderscheiden. Zo is er een recht op lichamelijke integriteit, het recht om zelf te bepalen met wie men al dan niet relaties aan wil gaan en de bescherming van de ruimte waarin men zich bevindt, zoals het huisrecht. Als een vierde dimensie kan gewezen worden op de zogenaamde informationele privacy, ofwel het recht op gegevensbescherming. Figuur 3 geeft een goed beeld hoe de begrippen privacy en gegevensbescherming zich ten opzichte van elkaar verhouden. Door de enorme toename in de (geautomatiseerde) verwerking van persoonsgegevens, en de grote aandacht die de informationele privacy dimensie daardoor is gaan genieten, wordt privacy soms ten onrechte vereenzelvigd met gegevensbescherming. Bescherming van persoonsgegevens maakt deel uit van het ruimere begrip privacy, maar heeft ook een zelfstandige betekenis en een deel van gegevensbescherming heeft weinig met privacy te maken.
Het belang in het maken van onderscheid tussen privacy en gegevensbescherming, is gelegen in het feit dat beide rechten een eigen wettelijk regime kennen.

[9] Richtlijn 95/46/EG.

Wanneer vast staat dat de privacy van een individu is geschonden, hoeft dit niet te betekenen dat dit komt doordat onrechtmatig met persoonsgegevens is gehandeld, de schending kan verband houden met een van de drie andere privacy dimensies.



Figuur 3: De verschillende dimensies van het privacy begrip

2.3 Het recht op privacy, Handvest en EVRM

Voor Europa is tot op heden de meest belangrijke bepaling betreffende het recht op privacy artikel 8 van het Europees Verdrag voor de Rechten van de Mens en de Fundamentele Vrijheden (EVRM).[10] We schrijven hier bewust ´tot op heden´, aangezien op 1 december 2009 het Verdrag van Lissabon in werking is getreden.[11] Met dit Verdrag zijn de vrijheden en beginselen die in het Handvest van de Grondrechten van de Europese Unie zijn opgenomen bindend voor de Unie en de lidstaten.[12] In het Handvest zijn het recht op privacy en het recht op gegevensverwerking vastgelegd.

Artikel 7, Eerbiediging van het privé-leven en het familie- en gezinsleven, luidt:

> *"Eenieder heeft recht op eerbiediging van zijn privé-leven, zijn familie- en gezinsleven, zijn woning en zijn communicatie."*

Artikel 8, Bescherming van persoonsgegevens, luidt:

> *"1. Eenieder heeft recht op bescherming van de hem betreffende persoonsgegevens.*
> *2. Deze gegevens moeten eerlijk worden verwerkt, voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet.*
> *Eenieder heeft recht op toegang tot de over hem verzamelde gegevens en op rectificatie daarvan.*
> *3. Een onafhankelijke autoriteit ziet toe op de naleving van deze regels."*

Ondanks de verankering van privacy en bescherming van persoonsgegevens in het Handvest, zal artikel 8 EVRM van groot belang blijven voor de EU.

---

10 Zie voor het EVRM: http://www.echr.coe.int/NR/rdonlyres/655FDBCF-1D46-4B36-9DAB-99F4CB59863C/0/NLD_CONV.pdf

11 Zie voor het Verdrag van Lissabon: http://europa.eu/lisbon_treaty/full_text/index_nl.htm

12 Zie voor het Handvest: http://www.europarl.europa.eu/charter/pdf/text_nl.pdf

Dit komt in de eerste plaats doordat het Handvest beoogt de grondrechten van personen te beschermen tegen regelgeving van de instellingen van de Unie en van de lidstaten wanneer zij de Verdragen van de Unie toepassen.[13] Artikel 8 EVRM is vooral bedoeld om burgers te beschermen tegen de overheid. Voor artikel 8 EVRM is algemeen aanvaard dat dit recht ook gelding heeft in private relaties (bijvoorbeeld tussen bedrijven en consumenten). Een tweede reden voor een blijvend belang van artikel 8 EVRM is dat de EU bezig is toe te treden tot het EVRM.[14] Met het Verdrag van Lissabon is hiertoe de mogelijkheid gecreëerd. Door deze toetreding, maar ook reeds gegeven het feit dat de lidstaten van de EU alle partij zijn bij het EVRM, zal de uitleg van het recht op privacy zoals deze gegeven wordt door het Europees Hof van de Rechten van de Mens leidend zijn, en blijven, in de EU.

Artikel 8 van het EVRM betreffende het Recht op eerbiediging van privé-, familie- en gezinsleven, luidt:

> *"1. Een ieder heeft recht op respect voor zijn privé leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.*
>
> *2. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen."*

Uit deze bepaling is een gelaagde privacytoets af te leiden, die uiteenvalt in de volgende vragen: Is er een privacyschending? Zo ja, is deze gerechtvaardigd? Hiertoe moet eerst bekeken worden of de inmenging op het recht op privacy voorzien is bij de wet (met betrekking tot Cloud Computing kan hier bijvoorbeeld gewezen worden op wettelijke bewaarplichten en zorgplichten die de verwerking van persoonsgegevens noodzakelijk maken). Vervolgens moet gekeken worden of een van de in artikel 8 genoemde belangen met de schending gediend wordt. Zoals blijkt uit de laatste regel van artikel 8 kan hier sprake zijn van een belangenafweging tussen het recht op privacy van het individu en de rechten en vrijheden van anderen, zoals bijvoorbeeld die van de Cloud Service Provider. Tot slot moet getoetst worden of de schending ´noodzakelijk is in een democratische samenleving´. Dit criterium wordt uitgelegd aan de hand van het beginsel van proportionaliteit en subsidiariteit. Proportionaliteit betekent dat de privacyschendende maatregel in verhouding moet staan tot het doel dat men wil bereiken. Subsidiariteit houdt in dat bij een keuze uit verschillende middelen, het minst ingrijpende middel ingezet moet worden.

Indien geen specifieke wetgeving ter bescherming van de persoonlijke levenssfeer voorhanden is, kan bij privacy inbreuken altijd worden teruggevallen op het fundamentele recht op privacy zoals verankerd in artikel 8 EVRM. Echter, aangezien bij Cloud Computing een eventuele schending van privacy veelal gebaseerd zal zijn op de verwerking van persoonsgegevens, ligt een beroep op het meer specifieke recht op gegevensbescherming doorgaans meer voor de hand.

---

[13] Zie: http://www.europarl.europa.eu/parliament/public/staticDisplay.do?id=137&pageRank=2&language=NL

[14] Op deze pagina is te zien dat de EU al wel genoemd wordt, maar dat nog geen sprake is van ratificatie en ondertekening: http://conventions.coe.int/Treaty/Commun/ListeTableauCourt.asp?MA=3&CM=16&CL=ENG. De EU lidstaten zijn elk afzonderlijk al verdragspartij in het EVRM.

2.4 Een gelaagd systeem van gegevensbescherming

De omschrijving van het recht op gegevensbescherming in artikel 7 van het Handvest van de Grondrechten van de EU betreft een vrij algemene omschrijving, die nader is uitgewerkt in verschillende Richtlijnen.
Deze richtlijnen zijn Richtlijn 95/46/EG welke de algemene richtlijn betreffende gegevensverwerking is (kortweg de Dataprotectierichtlijn), Richtlijn 2002/58 EG betreffende de verwerking van persoonsgegevens in de elektronische communicatie sector, en Richtlijn 2006/24/EG betreffende dataretentie.[15] Deze richtlijnen zullen hieronder, als onderdeel van het gelaagde systeem van gegevensbescherming in de EU, nader worden besproken.

In de Europese Unie is vanaf begin jaren negentig een gelaagd systeem van gegevensverwerking ontwikkeld. Het systeem bestaat uit vijf lagen:

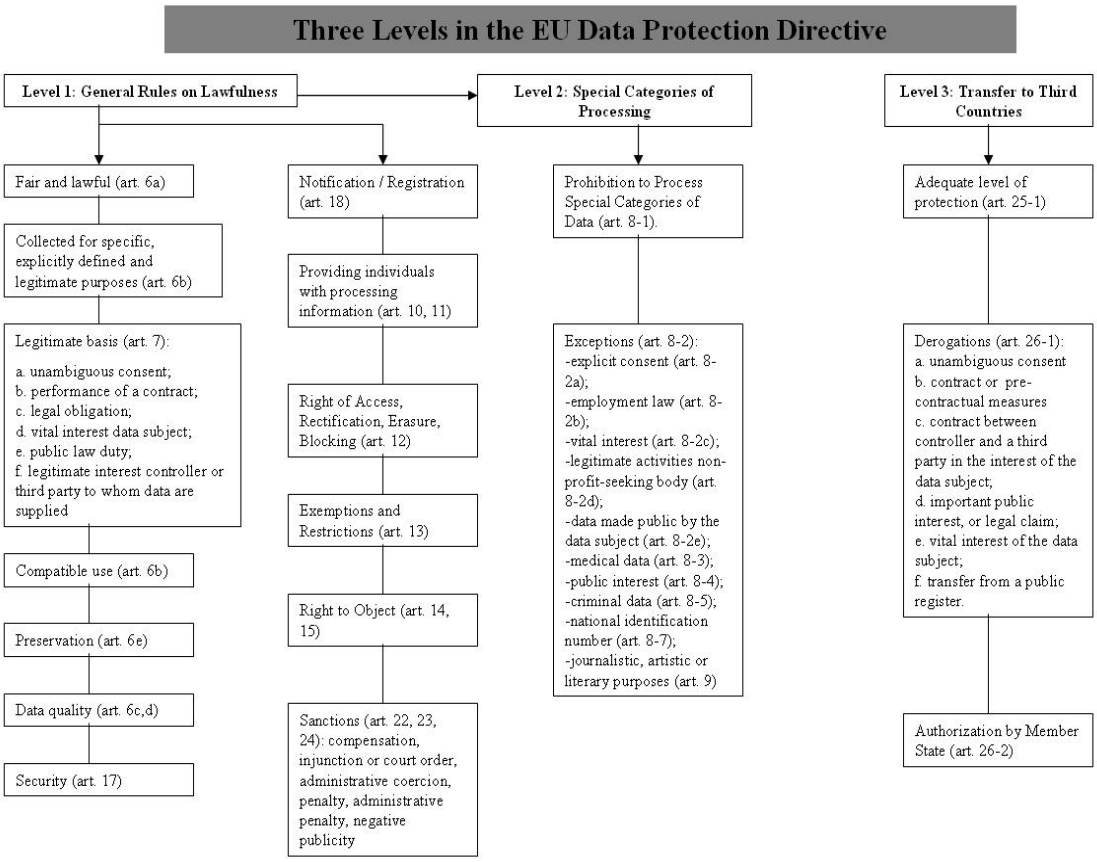
1. Algemene regels voor de rechtmatigheid van de verwerking van persoonsgegevens
2. Regels voor de verwerking van bijzondere (gevoelige) gegevens
3. Regels betreffende de doorgifte van gegevens naar derde landen (landen buiten de EU)
4. Sectorspecifieke wet- en regelgeving
5. Onderliggende (contractuele) rechtsverhoudingen

Van belang is dat deze lagen elkaar aanvullen. Indien bijzondere persoonsgegevens (zoals gegevens over etnische afkomst of lidmaatschap van een vakbond) verwerkt worden, dan zijn zowel de bepalingen uit de eerste laag, als die uit de tweede laag van toepassing. Als deze bijzondere gegevens vervolgens ook nog doorgegeven worden aan een derde land, dan is bovendien ook nog laag 3 van toepassing. Bovendien moet per geval altijd bekeken worden of er sprake is van toepasselijke sectorspecifieke wetgeving, en of er wellicht binnen de rechtsverhouding contractuele afspraken zijn gemaakt die van invloed zijn op de wijze waarop gegevens al dan niet rechtmatig verwerkt mogen worden.
De eerste drie lagen van het systeem van gegevensbescherming zijn opgenomen in de dataprotectie Richtlijn 95/46/EG.[16] Figuur 4 geeft een mooi overzicht van deze drie lagen. Zoals uit deze figuur blijkt, is het eerste artikel dat in de figuur genoemd wordt artikel 6.
Artikel 5 van de richtlijn bepaalt: *De Lid-Staten bepalen binnen de grenzen van de bepalingen van dit hoofdstuk nader de voorwaarden waaronder de verwerking van persoonsgegevens rechtmatig is.* Dit artikel vormt dus de verplichting aan de lidstaten de onderhavige richtlijn om te zetten in nationaal recht. In Nederland is de richtlijn omgezet in de Wet bescherming persoonsgegevens (Wbp), die als uitgangspunt dient voor de inhoudelijke bespreking van het gegevensbeschermingsregime. Nederland heeft de Richtlijn zeer nauwgezet omgezet waardoor de Wbp dus slechts marginaal afwijkt van de Richtlijn.

---

[15] Zowel Richtlijn 95/46/EG als Richtlijn 2002/58 EG worden momenteel herzien. De consultatieronde over de herziening staat open tot 15 januari 2011, zie http://ec.europa.eu/justice/policies/privacy/review/index_en.htm en http://ec.europa.eu/justice/news/consulting_public/news_consulting_0006_en.htm

[16] Voluit Richtlijn 95/46/EG betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens. Zie Publicatieblad Nr. L 281 van 23/11/1995 blz. 0031 – 0050, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:nl:HTML



Figuur 4: De drie lagen in de Dataprotectierichtlijn

Alvorens de inhoud van het regime van gegevensverwerking aan de hand van de Wbp nader uit te leggen, is het van belang om vast te stellen in welke gevallen de Wbp van toepassing is. De toepasselijkheid van de Wbp moet worden bepaald aan de hand van de eerste vier artikelen van de Richtlijn. Deze vormen als het ware een ´vóórlaag´, om vast te stellen of de eerste drie lagen van het gegevensbeschermingsregime überhaupt van toepassing zijn. Het vraagstuk van toepasselijk recht is het onderwerp van het volgende (derde) hoofdstuk.

3 Toepasselijkheid Wbp

3.1 Introductie

De eerste vier artikelen van de Wbp betreffen de toepasselijkheid en reikwijdte van de Wbp. Om deze vast te stellen is allereerst inzicht noodzakelijk in de kernconcepten waarop de Wbp is gebaseerd. Deze zijn grotendeels beschreven in artikel 1 van de Wbp. In de volgende paragraaf zal worden ingegaan op de termen ´verwerking´ en ´persoonsgegeven´, omdat deze nauw samenhangen met de werkingssfeer van de Wbp. Het vraagstuk van ´toepasselijk recht´ wordt geregeld in artikel 4 van de Wbp. Na behandeling van de belangrijkste begrippen zal paragraaf 3.3 de reikwijdte van de Wbp behandelen en zal in paragraaf 3.4 worden ingegaan op de toepasselijkheidsvoorwaarden van de Wbp. Belangrijk voor het bepalen van het toepasselijke recht zijn de concepten ´verantwoordelijke´ en ´bewerker´[17]. Deze worden behandeld in paragraaf 3.5.

3.2 Begrippen

Centraal in de Wbp staan de begrippen persoonsgegeven en verwerking. De Wbp regelt immers onder welke voorwaarden persoonsgegevens mogen worden verwerkt en wat daarbij de regels zijn. De definitie van 'persoonsgegeven' en 'verwerking van persoonsgegevens' is te vinden in artikel1 sub a en b van de Wbp:

> *"a. persoonsgegeven: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon;*
> *b. verwerking van persoonsgegevens: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens".*

Het begrip 'verwerking' zal hier slechts zeer summier worden besproken, omdat er tot op heden relatief weinig onduidelijkheid heeft bestaan over de reikwijdte en invulling van dit begrip. Het omvat alles van creatie tot en met de vernietiging van gegevens.
Rond het begrip 'persoonsgegeven' bestaat meer onduidelijkheid en over dit begrip is dan ook veel geschreven. Wij zullen ons hier beperken tot hetgeen de artikel 29 Werkgroep[18] heeft geschreven over de interpretatie van het begrip 'persoonsgegeven'. Er is door de artikel 29 Werkgroep een 28 pagina's tellend document dat alleen over het begrip 'persoonsgegeven' gaat gepubliceerd.[19] Dit laat zien dat het niet evident is in welke gevallen een gegeven is aan te merken als 'een gegeven dat een natuurlijk persoon identificeert of mogelijk kan identificeren'.

---

[17] Richtlijn 95/46/EG hanteert, in de Nederlandse vertaling ervan, het begrip "verwerker", terwijl in de Wbp dit begrip vertaalt wordt als "bewerker" (in het Engels: processor). Hier zal het begrip "bewerker" gebruikt worden, tenzij er verwezen wordt naar stukken van de Artikel 29 werkgroep, die het begrip "verwerker" hanteren.

[18] De artikel 29 Werkgroep is in het leven geroepen door artikel 29 van de Dataprotectie Richtlijn, en heeft met name als taak het adviseren van de Europese Commissie over de uniforme toepassing (tevens interpretatie) en uitvoering van de Richtlijn, en in het algemeen over het niveau van databescherming binnen de Europese Unie. Zie ook artikel 30 Databescherming richtlijn.

[19] Groep gegevensbescherming artikel 29 (2007) Advies 4/2007 over het begrip persoonsgegeven. 01248/07/NL, WP 136. Toegankelijk via: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_nl.pdf. Laatst geraadpleegd op 13 december 2010.

Het belangrijkste om hier te vermelden is dat de definitie van 'persoonsgegeven' bestaat uit vier elementen, te weten:

- "iedere informatie" (of, zoals opgenomen in de Wbp, 'elk gegeven')
- "betreffende"
- "geïdentificeerd of identificeerbaar"
- "natuurlijke persoon".

Het eerste element, "iedere informatie", dient ruim geïnterpreteerd te worden, zowel als het gaat om vorm als om inhoud. In het algemeen valt onder dit element zowel objectieve (feitelijke) informatie als subjectieve informatie (meningen en oordelen). Wat betreft de inhoud wordt door de artikel 29 Werkgroep aangegeven dat het hierbij gaat om

> *"informatie die betrekking heeft op iemands privéleven of familie- en gezinsleven in strikte zin, maar ook informatie over allerlei activiteiten die iemand onderneemt, bijvoorbeeld over iemands beroepsrelaties of economisch of sociaal gedrag."*[20]

Het volgende element van de definitie van persoonsgegeven is het woord "betreffende". De artikel 29 Werkgroep stelt dat "[i]n algemene termen kan informatie worden geacht een persoon te "betreffen" wanneer het om informatie over die persoon gaat."[21] Dit lijkt eenvoudig te bepalen, maar niet in elke situatie is dat het geval, denk bijvoorbeeld aan onderhoudsregisters van auto's, telefoonregisters, of de waarde van een woning.[22] In elk van deze gevallen gaat het niet over een bepaald persoon, maar is uit de gegevens wel informatie te herleiden die gaat over een specifiek persoon. Met betrekking tot het derde element, "geïdentificeerd of identificeerbaar", stelt de Werkgroep het volgende:

> *" In algemene termen kan een natuurlijke persoon als "geïdentificeerd" worden beschouwd als hij of zij binnen een groep personen wordt "onderscheiden" van alle andere leden van de groep. Analoog is een natuurlijke persoon "identificeerbaar" als die persoon weliswaar nog niet is geïdentificeerd, maar wel geïdentificeerd kan worden (…)."*[23]

Zowel directe, als indirecte identificatie valt onder het begrip persoonsgegeven. Directe identificatie is bijvoorbeeld identificatie door naam. Indirecte identificatie houdt in identificatie door middel van identificatienummers, een unieke combinatie van gegevens zoals adres, leeftijd, beroep, etc.[24] Enkele specifieke voorbeelden van gegevens die indirect kunnen leiden tot identificatie zijn IP-adressen en video-opnamen van een bewakingscamera. Echter, of deze gegevens vallen onder gegevens die (mogelijk) leiden tot identificatie is steeds sterk afhankelijk van de context. Zo kunnen bijvoorbeeld IP-adressen die zijn toegewezen aan computers in een internetcafé waar geen legitimatie wordt verlangd niet leiden tot identificatie.[25] IP-adressen van consumenten die via een reguliere ISP worden verstrekt zullen in veel gevallen wel persoonsgegevens zijn. Aan de hand van de door de ISP bijgehouden verkeersgegevens is immers vast te stellen wie gebruik heeft gemaakt van het betreffende IP-adres op een bepaald tijdstip. Over het vierde en laatste element kan kort gezegd worden dat het begrip "natuurlijke personen", rechtspersonen uitsluit en dat het moet gaan om levende personen.[26]
Uit deze korte beschouwing zal duidelijk zijn dat veel gegevens persoonsgegevens zijn. E-mail adressen zijn persoonsgegevens en daarmee vallen e-mail berichten ook al snel onder persoonsgegevens. Ook berichten of teksten waarin namen van individuen voorkomen zijn persoonsgegevens of bevatten persoonsgegevens.

---

20 Ibid., p. 7.
21 Ibid., p. 9.
22 Ibid.
23 Ibid., p. 13.
24 Ibid., p. 14.
25 Of de betreffende gegevens ook daadwerkelijk leiden tot identificatie is niet van belang; het criterium is dat de gegevens mogelijk kunnen leiden tot identificatie.
26 Ibid., p. 23-25.

Dan rest nog een korte uitleg over het begrip 'verwerking'. Ook dit begrip dient ruim te worden uitgelegd. In de Wbp wordt een niet limitatieve opsomming gegeven van handelingen met betrekking tot persoonsgegevens die vallen onder het begrip verwerking. Echter, met de steeds nieuwere technologische mogelijkheden duiken steeds nieuwe situaties op die niet voorkomen op de lijst handelingen in de definitie van verwerking. Datamining wordt bijvoorbeeld niet concreet genoemd. Dergelijke nieuwe gevallen zullen steeds specifiek geanalyseerd moeten worden om te bezien of ze vallen onder het begrip verwerken.[27] In veel gevallen zal dat zo zijn omdat de kerndefinitie van verwerking erg open is en in beginsel iedere handeling omvat die op gegevens kan worden uitgevoerd. In het geval van Cloud Computing worden er echter geen bijzonder nieuwe middelen van gegevensverwerking toegepast, en zullen er in die context weinig vragen rijzen met betrekking tot het begrip 'verwerking'.

3.3 Toepassing en reikwijdte

Artikel 2 Wbp bepaalt op hoofdlijnen wanneer de Wbp van toepassing is:

> *"1. Deze wet is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede de niet geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen."*

Grofweg gaat het dus om geautomatiseerde verwerking van persoonsgegevens. Dat is wat er in ieder geval gebeurt in Cloud Computing, waardoor aan een eerste toepasselijkheidsvoorwaarde van de Wbp is voldaan.

Artikel 2 Wbp noemt tevens een aantal uitzonderingen, waarvan de volgende in de context van het gebruik van Clouddiensten door onderwijsinstellingen het belangrijkste is :

> *"2. Deze wet is niet van toepassing op verwerking van persoonsgegevens:*
> *a. ten behoeve van activiteiten met uitsluitend persoonlijke of huishoudelijke doeleinden".*

Deze uitzondering vergt enige uitleg. Het artikel zegt dat wanneer een verwerking van persoonsgegevens valt onder deze uitzondering, de Wet bescherming persoonsgegevens niet van toepassing is. Dat betekent vervolgens dat de verplichtingen in de Wbp niet gelden voor dergelijke situaties.
In de context van cloud computing binnen het onderwijs, kan deze uitzondering met name van belang zijn in het geval van het verwerken van gegevens door studenten. De vraag is of (en wanneer) het schrijven van e-mails en het produceren van documenten binnen "de Cloud" valt binnen die uitzondering. Een absoluut antwoord valt niet te geven, maar duidelijk is wel dat deze "huishoudelijke aard uitzondering" beperkt dient te worden uitgelegd.[28] Mogelijk is het zo, dat wanneer de persoonsgegevens worden verwerkt binnen het kader van onderwijs, geen beroep meer kan worden gedaan op deze uitzondering omdat het verwerken van de gegevens niet meer binnen een puur huishoudelijke setting plaats vindt. Het Europese Hof van Justitie heeft in de Lindqvist zaak bepaald dat wanneer persoonsgegevens op een publieke persoonlijke website worden geplaatst, geen beroep kan worden gedaan op de uitzondering van "puur huishoudelijke aard".

---

[27] Zo is bijvoorbeeld onlangs een document gepubliceerd door de artikel 29 Werkgroep over hoe het gebruik van cookies bij gerichte online marketing valt onder het begrip verwerking. Zie opinie 2/2010 van die Werkgroep.

[28] ARREST VAN HET HOF van 6 november 2003 in zaak C-101/01 (verzoek van het Göta hovrätt om een prejudiciële beslissing): Bodil Lindqvist ("Richtlijn 95/46/EG (Werkingssfeer (Openbaarmaking van persoonsgegevens op internet (Plaats van openbaarmaking (Begrip doorgifte van persoonsgegevens naar derde landen (Vrijheid van meningsuiting (Verenigbaarheid met richtlijn 95/46 van verdergaande bescherming van persoonsgegevens door wettelijke regeling van lidstaat") Lindqvist.

Wanneer de webpagina is afgeschermd (zoals bij een afgeschermde profielpagina op een online sociaal netwerk, zoals Hyves) en alleen toegankelijk is voor bij de gebruiker bekende personen, kan mogelijk wel een beroep gedaan worden op verwerking voor “puur huishoudelijke aard”, waarmee de Wbp niet van toepassing is op dergelijke verwerking van persoonsgegevens.[29] In het licht van Cloud Computing geldt dan dus de vraag of er wel of geen openbare toegang is tot de persoonsgegevens. Mogelijk kan toch een beroep worden gedaan op de uitzondering indien de gegevens versleuteld zijn en door de CCSP alleen bewerkt worden in opdracht van de verantwoordelijke. Indien de gegevens door de CCSP voor additionele doeleinden verwerkt worden, dan is de kans dat op deze uitzondering een beroep kan worden gedaan ons inziens erg klein.

Tot slot is er nog artikel 3 van de Wbp, dat mede de reikwijdte van de Wbp bepaalt. Het artikel stelt dat de Wbp niet van toepassing is op de ”verwerking van persoonsgegevens voor uitsluitend journalistieke, artistieke of literaire doeleinden”. Hiervan zal bij uitbesteding van diensten aan de Cloud door onderwijsinstellingen niet snel sprake zijn. Bovendien, een groot deel van de verplichtingen voor de voor verwerking verantwoordelijke valt buiten deze uitzondering, en moeten dus gewoon worden nageleefd. Dit zijn onder meer de algemene bepalingen uit laag 1, die besproken wordt in paragraaf 4.1 van dit rapport.

3.4 Toepasselijk recht

Het Europese juridische raamwerk rond de bescherming van persoonsgegevens tracht twee doelen te bereiken: het vrij verkeer van (persoons)gegevens en het bieden van voldoende bescherming voor de persoonlijke levenssfeer bij dergelijk verkeer. Het raamwerk is er dus niet alleen ter bescherming van Europese burgers, maar ook voor de verwerkers van gegevens. Het is dan ook begrijpelijk dat (Europese) entiteiten, die met de verwerking van persoonsgegevens te maken krijgen, willen dat deze verwerking valt onder de relevante Europese regelgeving. Vanuit die gedachte is het bij de overweging om daadwerkelijk over te gaan tot het afnemen van een Cloud Service, voor EU-entiteiten vaak van belang dat gegevens binnen de EU blijven. Het is echter een misvatting dat de locatie van de gegevens bepalend is voor het antwoord op de vraag of Europese dataprotectie regelgeving van toepassing is. Op basis van Richtlijn 95/46/EG bepaalt artikel 4 van de Wbp namelijk dat de locatie van de vestiging(en) van de verantwoordelijke in dit opzicht doorslaggevend is.[30]

Om te bepalen welk recht van toepassing is, moet worden gekeken naar artikel 4 van de Wbp:

“1. Deze wet is van toepassing op de verwerking van persoonsgegevens in het kader van activiteiten van een vestiging van een verantwoordelijke in Nederland.

2. *Deze wet is van toepassing op de verwerking van persoonsgegevens door of ten behoeve van een verantwoordelijke die geen vestiging heeft in de Europese Unie, waarbij gebruik wordt gemaakt van al dan niet geautomatiseerde middelen die zich in Nederland bevinden, tenzij deze middelen slechts worden gebruikt voor de doorvoer van persoonsgegevens.*
3. *Het is een verantwoordelijke als bedoeld in het tweede lid, verboden persoonsgegevens te verwerken, tenzij hij in Nederland een persoon of instantie aanwijst die namens hem handelt overeenkomstig de bepalingen van deze wet. Voor de toepassing van deze wet en de daarop berustende bepalingen, wordt hij aangemerkt als de verantwoordelijke”*

---

[29] Zie hierover Artikel 29 WG, Opinion 5/2009 on online social networking, 01189/09/EN WP 163.

[30] Vgl. Leenes, R.E. (2010) Who controls the cloud? To be published in IDP. REVISTA DE INTERNET, DERECHO Y POLÍTICA, nr. 11 2010, toegankelijk via: http://idp.uoc.edu/ojs/index.php/idp/. Laatst geraadpleegd op: 1 december 2010. Zie ook Balboni, P. (2010) Data Protection and Data Security Issues Related to Cloud Computing in the EU. ISSE 2010 Securing Electronic Business Processes - Highlights of the Information Security Solutions Europe Conference 2010: Tilburg Law School Research Paper No. 022/2010, p. 5-7. Te raadplegen via: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1661437. Laatst geraadpleegd op 1 december 2010.

Artikel 4 lid 1 spreekt over de *vestiging* van de verantwoordelijke. Wanneer een verantwoordelijke een vestiging heeft in Nederland die zich bezig houdt met de verwerking van persoonsgegevens, deze vestiging zich voor de verwerking van die gegevens moet houden aan de Wbp.[31] Met vestiging wordt bedoeld de zetel van de rechtspersoon en niet de locatie van de IT-faciliteiten die voor de verwerking van persoonsgegevens worden gebruikt. Met andere woorden, niet relevant is waar de gegevens feitelijk worden verwerkt en opgeslagen, maar waar de vestigingsplaats is van de verantwoordelijke. Wanneer deze zich in een EU-lidstaat bevindt, dan is de richtlijn van toepassing, ook al bevinden de IT-activiteiten en faciliteiten zich buiten het grondgebied van de EU-lidstaten. Het maakt vanuit dit perspectief dus niet uit of gegevens worden opgeslagen in Ierland of in de VS wanneer gebruik wordt gemaakt van de diensten van een provider met een vestiging in Nederland die zeggenschap heeft over de gegevensverwerking (dat maakt deze entiteit verantwoordelijke).[32] Het maakt in die zin niet uit of Google Docs gegevens in de EU opslaat, dan wel buiten de EU voor bijvoorbeeld de Open Universiteit. De Richtlijn biedt bescherming ongeacht de locatie van de gegevensopslag. De locatie van de gegevensopslag is echter wel vanuit een ander perspectief van belang. Wanneer gegevens zijn opgeslagen op Amerikaans grondgebied, is bijvoorbeeld de USA PATRIOT Act van toepassing die verstrekkende privacy consequenties kan hebben. We komen op dit aspect terug in hoofdstuk 6.

Ook wanneer de aanbieder van Cloud Services buiten Nederlands grondgebied is gevestigd, kan de Wbp van toepassing zijn. Artikel 4 lid 2 bepaalt immers dat de Wbp ook van toepassing is indien de verantwoordelijke niet in Nederland gevestigd is, maar voor de verwerking van persoonsgegevens wèl gebruik maakt van al dan niet geautomatiseerde middelen welke zich op Nederlands grondgebied bevinden. Richtlijn 95/46/EG bepaalt in dit verband dat de nationale wetgeving van de plaats waar de al dan niet geautomatiseerde middelen zich bevinden, van toepassing is.
Het begrip geautomatiseerde middelen roept wellicht de gedachte op dat het hier gaat om apparatuur, zoals PC's. Dat is het geval, maar de reikwijdte gaat veel verder. Ook cookies vallen onder het begrip geautomatiseerde middelen.[33] Wanneer een Cloud Service Provider één of meer cookies plaatst op de terminal van de gebruiker (lees de webbrowser), dan is er volgens de uitleg die gegeven wordt aan Richtlijn 95/46/EG, en daarmee ook aan de Wbp, sprake van een geautomatiseerd middel. Aangezien diensten die via de webbrowser worden benaderd bijna ondenkbaar zijn zonder cookies, valt vrijwel iedere buiten de EU gevestigde Cloud Service Provider op basis van art 4 lid 1 onder c derhalve onder de Richtlijn. Dat wil zeggen dat een aanbieder, zoals Google, die voor het leveren van diensten (zoals Google Docs) gebruik maakt van Cookies voor wat betreft die dienst (Google Docs) moet voldoen aan de voorwaarden die de Wbp stelt.

Met andere woorden, de locatie van de Cloud Service Provider doet er vrijwel niet toe, de Wbp, of een met de Wbp vergelijkbare nationale uitwerking van Richtlijn 95/46/EG, is hoe dan ook van toepassing.

---

31 Uit artikel 4 (en de Richtlijn 95/46/EG) volgt verder dat wanneer een verantwoordelijke meerdere ondernemingen binnen de EU heeft, elk van die ondernemingen zich moet houden aan de wetgeving betreffende de verwerking van persoonsgegevens van het land waar ze gevestigd is.

32 Dat is anders wanneer het gaat om een vestiging die bijvoorbeeld alleen reclames inkoopt voor een Amerikaanse Cloud Service provider.

33 Dit volgt uit de opinies van de Art. 29 werkgroep, in het bijzonder WP56, Article 29 Data Protection Working Party (2002) Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites (wp56), WP148 over search engines (Article 29 Data Protection Working Party, 2008) en 5/2009 over Social Network Sites (Article 29 Data Protection Working Party, 2009).

3.5 Begrip ´voor de verwerking verantwoordelijke´

Cruciaal om te bepalen welk recht van toepassing is, is het begrip 'verantwoordelijke'. Immers, de vestigingslocatie van de verantwoordelijke is bepalend voor het beantwoorden van die vraag. Artikel 1 d van de Wbp definieert 'voor de verwerking verantwoordelijke´ als volgt:

> *"de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of te zamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt;"*

In het geval van Cloud Computing is het lastig te bepalen welke partij(en) voor de verwerking verantwoordelijk zijn, en welke partijen slechts de gegevens ´bewerken´.[34] Artikel 1 e van de Wbp definieert ´bewerker´ als:

> *"degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen."*

Het grote verschil bestaat erin dat de bewerker niet de doelen en middelen voor de verwerking van persoonsgegevens bepaalt, maar slechts in opdracht van de verantwoordelijke persoonsgegevens verwerkt. Degene op wie een persoonsgegeven betrekking heeft, wordt ´betrokkene´ genoemd.

In de Wbp is de relatie tussen verantwoordelijke, bewerker en derden[35] nader toegelicht in artikel 12 dat bepaalt:

> *"Een ieder die handelt onder het gezag van de verantwoordelijke of van de bewerker, alsmede de bewerker zelf, voor zover deze toegang hebben tot persoonsgegevens, verwerkt deze slechts in opdracht van de verantwoordelijke, behoudens afwijkende wettelijke verplichtingen."*

Voor deze personen geldt een plicht tot geheimhouding van de gegevens waarvan zij kennis nemen, behoudens voor zover enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit.

Artikel 14 van de Wbp betreft de plicht om de uitvoering van verwerkingen door een bewerker te regelen in een overeenkomst. De onderdelen van de overeenkomst die betrekking hebben op de bescherming van persoonsgegevens, alsmede de beveiligingsmaatregelen worden schriftelijk vastgelegd. Voorts bepaalt dit artikel dat de verantwoordelijke zorg draagt dat de bewerker persoonsgegevens verwerkt in overeenstemming met artikel 12, eerste lid en de verplichtingen nakomt die op de verantwoordelijke rusten ingevolge artikel 13 (beveiligingsplicht, zie verder hoofdstuk 4). Is de bewerker gevestigd in een ander land van de Europese Unie, dan draagt de verantwoordelijke zorg dat de bewerker het recht van dat andere land nakomt. Op grond van artikel 15 Wbp moet de verantwoordelijke bovendien zorg dragen dat de bewerker de verplichtingen uit de artikelen 6 tot en met 12 en 14 van de Wbp naleeft.

Niet in alle gevallen is duidelijk welke partij welke rol(len) vervult in de verwerking van persoonsgegevens. Wat die rollen zijn, kan per situatie verschillen. Dit is te illustreren aan de hand van de verschillende typen Cloud Services zoals die reeds in hoofdstuk 1 zijn onderscheiden; Software as a Service (SaaS), Infrastructure as a Service (IaaS) en Platform as a Service (PaaS).[36] Zoals aangegeven in hoofdstuk 1, richt deze studie zich vooral op SaaS.

---

[34] Supra noot 22. Zie ook Thole, E. (2010) Privacy en cloud computing: beveiliging van persoonsgegevens in de cloud. Informatie juli/augustus 2010, Legale kaders in cyberspace, p. 29. Te raadplegen via: http://www.van-doorne.com/Global/Publicaties/Privacy%20en%20cloud%20computing_Thole_Informatie%202010.pdf. Laatst geraadpleegd op 1 december 2010.

[35] In artikel 1 g Wbp gedefinieerd als: "ieder, niet zijnde de betrokkene, de verantwoordelijke, de bewerker, of enig persoon die onder rechtstreeks gezag van de verantwoordelijke of de bewerker gemachtigd is om persoonsgegevens te verwerken."

[36] Supra noot 22.

Bij het gebruik van SaaS wordt een applicatie gebruikt die wordt ontwikkeld en aangeboden door de CCSP. De Cloud Service gebruiker zal hier nauwelijks vorm geven aan de applicatie. In dit geval kunnen zowel de gebruiker van de Cloud Service als de CCSP als verantwoordelijke beschouwd worden. Bij de gebruiker is dit evident; zij bepaalt immers het doel en de middelen voor de verwerking van persoonsgegevens. Het doel van de gebruikers bij het gebruik van bijvoorbeeld Hotmail[37], Facebook[38] of Flickr[39] is respectievelijk communicatie en het opslaan van bestanden, het onderhouden van/informatie delen met contacten en het opslaan en delen van foto's. Zij kiezen hier tevens zelf de middelen om die doelen uit te voeren. De doelen van CCSPs worden bepaald door middel van de gebruiksrechten overeenkomsten, ofwel algemene voorwaarden. In alle drie de genoemde voorbeelden zijn de voornaamste doelen het verlenen van de dienst en gerichte marketing. Ook kiezen CCSPs de middelen voor het verwerken van persoonsgegevens, namelijk hun eigen services en eventueel die van derden. Wanneer een CCSP gebruik maakt van diensten van derden zal er een subcontract moeten zijn, dat bepaalt hoe de persoonsgegevens verwerkt moeten worden. Denk hierbij aan het verzenden van data naar datacenters die niet onder eigen beheer vallen, maar ook aan de verwerking van persoonsgegevens voor de eigen doelen van de CCSPs, zoals gerichte marketing. Bij de zojuist genoemde voorbeelden zullen de CCSPs beschouwd kunnen worden als (mede) verantwoordelijken. Immers, zij formuleren in hun gebruiksrechtovereenkomsten bepaalde (eigen) doelen voor het verwerken van de persoonsgegevens die de gebruikers van die service aanleveren.

Bij PaaS en IaaS ligt dit mogelijk anders. In het geval van PaaS voorziet de CCSP in een platform, waarbinnen Cloud Service gebruikers zelf applicaties kunnen ontwikkelen; bij IaaS biedt de CCSP de IT-infrastructuur aan om software, inclusief besturingssystemen en complete virtuele omgevingen, op te laten draaien.[40] Wanneer dergelijke CCSPs enkel en alleen een platform of infrastructuur aanbieden, en verder niets doen met de gegevens die de gebruikers van die services aanleveren, dan zijn zij geen verantwoordelijke. Met andere woorden: de CCSP werkt in dit geval enkel en alleen in opdracht van de Cloud Service gebruiker en stelt geen, eigen doelen (zoals marketing) voor de verwerking van persoonsgegevens anders dan die zijn overeengekomen met de gebruiker. Of dit het geval is, is afhankelijk van de individuele situatie.[41] Maar let op; zodra een CCSP andere doelen stelt voor de verwerking van persoonsgegevens dan zijn overeengekomen met de gebruiker, is zij een verantwoordelijke in de zin van de Wbp, en is dientengevolge aan de verplichtingen van die wet gebonden.[42]

---

37 Microsoft (2010) Gebruiksrechtovereenkomst van Microsoft. Zie clausule 5 en 6. Toegankelijk via: http://explore.live.com/microsoft-service-agreement?ref=none. Voor het laatst geraadpleegd op 1 december 2010. Zie ook Microsoft (2010) Belangrijkste punten Microsoft Online Privacyverklaring. Te raadplegen via: http://privacy.microsoft.com/nl-nl/default.mspx. Laatst geraadpleegd op 1 december 2010.

38 Facebook (2010) Statement of Rights and Responsibilities (Terms). Zie clausule 10. Te raadplegen via: http://www.facebook.com/terms.php?ref=pf. Laatst geraadpleegd op 1 december 2010.

39 Yahoo! (2008) Yahoo! Terms of Service, clausules 2 en 4. Toegankelijk via: http://info.yahoo.com/legal/us/yahoo/utos/utos-173.html. Laatst geraadpleegd op 1 december 2010, en Yahoo! (2006) Yahoo! Privacy Policy, INFORMATION COLLECTION AND USE. Toegankelijk via: http://info.yahoo.com/privacy/us/yahoo/. Laatst geraadpleegd op 1 december 2010.

40 Ibid.

41 Artikel 29 Werkgroep (2010) WP169: Advies 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker". Te raadplegen via: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_nl.pdf. Nota bene: de Databescherming Richtlijn hanteert, in de Nederlandse vertaling ervan, het begrip "verwerker", terwijl in de Wbp dit begrip vertaalt wordt als "bewerker" (in het Engels: processor).

42 Thole, E. (2010) Privacy en cloud computing: beveiliging van persoonsgegevens in de cloud. Informatie juli/augustus 2010, Legale kaders in cyberspace, p. 29. Te raadplegen via: http://www.van-doorne.com/Global/Publicaties/Privacy%20en%20cloud%20computing_Thole_Informatie%202010.pdf. Laatst geraadpleegd op 1 december 2010.

3.6 Conclusies

Aan de hand van de individuele situatie moet bekeken worden welke partij welke rol speelt bij de verwerking van persoonsgegevens in de Cloud; hetzij die van verantwoordelijke, hetzij die van bewerker hetzij die van eindgebruiker. De locatie van de verantwoordelijke is bepalend voor het antwoord op de vraag of de Wbp, of enig ander nationaal EU-gevensbeschermingsrecht van toepassing is. Een Nederlandse entiteit die gebruik wil maken van een Cloud Service is doorgaans een verantwoordelijke in de zin van de Wbp. Wil een Nederlandse entiteit, zijnde een verantwoordelijke, gebruik maken van een Cloud Service, dan is die entiteit gebonden aan de Wbp, ongeacht de locatie van de gegevens. Wanneer de Nederlandse entiteit persoonsgegevens doorgeeft aan een CCSP blijft zij, ongeacht de locatie van die CCSP, verantwoordelijk voor de verwerking van die persoonsgegevens en moet zij ervoor zorg dragen dat de relevante regelgeving met betrekking tot die gegevensverwerking wordt nageleefd.

CCSPs gevestigd binnen de EU zijn volgens Richtlijn 95/46/EG verantwoordelijke wanneer zij eigen doelen stellen en middelen kiezen voor de verwerking van persoonsgegevens; denk bijvoorbeeld aan marketing doeleinden en het kiezen voor een bepaalde IT-infrastructuur, zoals datacenters. Wanneer zij enkel en alleen werken in opdracht van de Cloud Service gebruiker, dan vallen zij binnen het begrip bewerker.
Is de CCSP gevestigd buiten de EU en maakt zij gebruik van al dan niet geautomatiseerde middelen binnen de EU, dan is zij, op voorwaarde dat zij beschouwd kan worden als verantwoordelijke, tevens gebonden aan het Europese gegevensbeschermingsrecht. Maakt zij geen gebruik van dergelijke middelen, dan is zij dat niet. Indien een verantwoordelijke gebruik maakt van middelen die zich op het Nederlandse grondgebied bevinden, dan is de Wbp van toepassing.

Tot slot zijn nog enkele aanvullende opmerkingen op zijn plaats. Zoals gezegd maakt het voor de toepassing van het Europees gegevensbeschermingsrecht niet uit waar gegevens zich daadwerkelijk bevinden. Echter, de locatie van gegevens is wel van belang voor de toepassing van andere, lokale regelgeving. Bedenk dat CCSPs gebruik kunnen maken van datacenters in privacy-onvriendelijke landen zoals China, Rusland en de VS.[43] Als een datacenter of een CCSP zich bijvoorbeeld in de VS bevindt, dan kan de Amerikaanse overheid op basis van federale antiterrorisme wetgeving toegang krijgen tot die data, zonder dat de gebruiker van de Cloud Service of de betrokkene hierover wordt ingelicht. Voor deze verwerking is waarschijnlijk de CCSP verantwoordelijke. Op basis van wetgeving en/of gedragscode zal de CCSP het doel en de middelen (voldoen aan verplichtingen voortvloeiend uit antiterrorisme wetgeving en het verlenen van toegang tot de data aan de Amerikaanse overheid) vast stellen. Als de CCSP een vestigingsplaats in Nederland is, is deze ook voor de genoemde verwerking gebonden aan de Wbp. Op grond van artikel 8 c) mogen persoonsgegevens worden verwerkt indien de gegevensverwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is. De Wbp biedt dus een verwerkingsgrond voor de genoemde verwerking. Zolang de CCSP verder alle rechten en plichten die voortvloeien uit de Wbp naleeft, is er dus geen sprake van een schending van de Wbp. Het is niet waarschijnlijk dat onderwijsinstellingen dit soort verwerkingen van persoonsgegevens door een CCSP contractueel uit kunnen sluiten, het gaat immers om wettelijke plichten waaraan de CCSP onderworpen is. Voor niet verplichte verwerkingen, zoals marketing, kan de onderwijsinstelling wel contractueel trachten te bedingen dat een CCSP de persoonsgegevens verkregen van de onderwijsinstelling hier niet voor gebruikt. Als de CCSP dat dan toch doet, dan is sprake van schending van de Wbp (geen legitieme verwerkingsgrond aanwezig) en van contractbreuk.

---

[43] Vgl. Computable (2010) Vraagtekens bij eigenaarschap clouddata. Te raadplegen via: http://www.computable.nl/artikel/ict_topics/cloud_computing/3448041/2333364/vraagtekens-bij-eigenaarschap-clouddata.html. Laatst geraadpleegd op 1 december 2010.

Een laatste punt waaraan gedacht moet worden als het gaat om de bescherming van ´onze´ gegevens door Europese regelgeving, is de mogelijkheid dat op basis van onze gegevens nieuwe, geaggregeerde gegevens worden gemaakt. Denk hierbij aan individuele- of groepsprofielen die gemaakt worden op basis van persoonsgegevens, en die bijvoorbeeld vervolgens worden gebruikt voor gerichte marketing.[44] Dit soort gegevens zijn niet langer gegevens van de initiële betrokkenen of de initiële Cloud Service gebruiker, maar van degene die deze nieuwe gegevens heeft gecreëerd, in dit geval de CCSP of eventuele derden. De CCSP is dan verantwoordelijk voor die nieuwe geaggregeerde gegevens. Wanneer de CCSP niet gebonden is aan het Europese gegevensbeschermingsrecht, is die geaggregeerde data in het geheel niet beschermd door dat recht. Dit is wel het geval bij de gegevens die in eerste instantie door de Cloud Service gebruiker naar de CCSP gezonden is. Immers, de Cloud Service gebruiker is dan, als verantwoordelijke binnen de EU, verantwoordelijk voor bescherming van die gegevens op basis van het Europese gegevensbeschermingsrecht, ook wanneer die gegevens zich bij de CCSP bevinden. Er moet dus op worden gelet of de CCSP, in de specifieke situatie, ook eigen doelen stelt voor de verwerking van persoonsgegevens. In principe is de verantwoordelijke (de onderwijsinstelling) voor de verwerking van persoonsgegevens met het oog op deze eigen doelen van de CCSP niet verantwoordelijk. Het kan evenwel zo zijn dat als de onderwijsinstelling de betrokkenen onvoldoende inlicht over het feit dat gegevens ook verwerkt kunnen worden voor andere doeleinden, vastgesteld door de CCSP, hij op dit punt wel de Wbp schendt en hiervoor verantwoordelijk is. Nieuwe gegevens die de CCSP in het kader van haar eigen doelen creëert, op basis van de door de Cloud Service gebruikers aangeleverde persoonsgegevens, valt, wanneer de CCSP niet gebonden is aan het Europese recht, buiten de bescherming van dat recht. Vaak zijn CCSPs commerciële bedrijven, denk aan Google en Microsoft, en bieden zij de Cloud Service niet voor niets voordelig aan. Binnen onze huidige informatiemaatschappij zijn gegevens immers van ongekende waarde.

[44] Of deze geaggregeerde gegevens persoonsgegevens zijn in de zin van de Wbp is in zijn algemeenheid lastig te beantwoorden, maar als de gegevens herleidbaar zijn naar een identificeerbaar individu, ook als dat erg moeilijk is, zal in het algemeen sprake zijn van persoonsgegevens.

4 De Wet bescherming persoonsgegevens

Nu is vastgesteld dat de Wbp, of in ieder geval een met de Wbp vergelijkbaar regime van gegevensverwerking, veelal van toepassing is wanneer Nederlandse onderwijsinstellingen Clouddiensten afnemen, wordt in dit hoofdstuk nader ingegaan op de vraag wat dit inhoudelijk betekent op basis van de Wbp. Zoals beschreven in hoofdstuk 2, bestaat het juridische raamwerk uit vijf lagen, waarvan de eerste drie zijn terug te vinden in de Wbp: algemene bepalingen, bijzondere gegevens en doorgifte van gegevens naar derde landen.

4.1 Laag 1: Algemene bepalingen

Artikel 6 van de Wbp bepaalt dat *persoonsgegevens worden verwerkt in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze*. Wat precies een ´behoorlijke en zorgvuldige wijze´ is, wordt vervolgens uitgelegd in de artikelen die volgen op artikel 6. In de eerste plaats mogen gegevens alleen verzameld worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden (Art. 7). Zowel de instelling als de CCSP zullen voor de verwerking van persoonsgegevens waarvoor zij doel en middelen vaststellen, deze doelen dus expliciet, compleet en duidelijk moeten beschrijven. Voor zover de verwerking van persoonsgegevens wordt uitbesteed aan een bewerker, zal de doelomschrijving in de overeenkomst tussen verantwoordelijke en bewerker opgenomen moeten worden. De verantwoordelijke moet niet alleen zorg dragen voor een deugdelijke vaststelling van het doel, maar zal tevens moeten garanderen dat gegevens niet worden verwerkt op een wijze die onverenigbaar is met de vastgestelde doeleinden (Art. 9). Verdere verwerking van de gegevens voor historische, statistische of wetenschappelijke doeleinden is toegestaan (want wordt niet als onverenigbaar beschouwd), mits de verantwoordelijke passende voorzieningen treft om te waarborgen dat de verdere verwerking beperkt zal blijven tot deze doeleinden. Artikel 9 bepaalt voorts dat verwerking van persoonsgegevens niet is toegestaan wanneer sprake is van een geheimhoudingsplicht op basis van ambt, beroep (bijv. arts) of wettelijk voorschrift. In het licht van onderwijsinstellingen kan deze bepaling relevant zijn omdat er bij bepaalde functies binnen het onderwijs sprake kan zijn van een geheimhoudingsplicht (bijvoorbeeld vertrouwenspersonen, schoolartsen of schoolpsychologen).

Een tweede belangrijke voorwaarde voor de verwerking van persoonsgegevens betreft de aanwezigheid van een legitieme verwerkingsgrond. De rechtmatige verwerkingsgronden zijn limitatief opgesomd in artikel 8.
De eerste rechtmatige verwerkingsgrond om gegevens te mogen verwerken (artikel 8 a Wbp) is 'toestemming van betrokkenen'. De Wbp definieert het begrip 'toestemming' in artikel 1 sub i als volgt: *´elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem betreffende persoonsgegevens worden verwerkt'.* Deze verwerkingsgrond is in Cloud context niet erg voor de hand liggend. Niet alleen is het bij verwerkingen van gegevens van vele verschillende personen omslachtig om toestemming van elk van hen te verkrijgen, hiervan zal ook een registratie aangelegd moeten worden. Deze registratie is noodzakelijk omdat de verwerker moet kunnen aantonen dat hij toestemming heeft en de toestemming te allen tijde ingetrokken mag worden. Dit betekent voor de verantwoordelijke een administratieve last. Bovendien, is de verwerkingsgrond toestemming in de parlementaire geschiedenis uitgelegd als betekenend dat wanneer toestemming eenmaal geweigerd of ingetrokken is, gegevens niet meer op een van de andere verwerkingsgronden, zoals het gerechtvaardigd belang, gestoeld mogen worden.[45]

[45] Kamerstukken II 1997-1998, 25 892, nr. 3 p. 81-82. Behoorlijk en zorgvuldig betreft de terminologie uit artikel 6 Wbp.

Voor het uitbesteden van diensten aan de Cloud, ligt daarom verwerkingsgrond b) meer voor de hand:

> *“de gegevensverwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die noodzakelijk zijn voor het sluiten van een overeenkomst.*

Andere mogelijke verwerkingsgronden zijn de nakoming van een wettelijke verplichting, het vitaal belang van de betrokkene (levensbedreigende situaties) en de vervulling van een publiekrechtelijke taak door een bestuursorgaan. Als restgrond wordt artikel 8 f beschouwd, dat bepaalt dat gegevens verwerkt mogen worden indien de gegevensverwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde, tenzij het recht van de betrokkene prevaleert.

Naast het doel en de verwerkingsgrond, worden vervolgens eisen gesteld aan de kwaliteit van de gegevens. Zo moeten gegevens toereikend, ter zake dienend, niet bovenmatig, juist en nauwkeurig zijn met het oog op de doeleinden waarvoor zij worden verzameld of waarvoor zij vervolgens worden verwerkt. Gegevens mogen in identificerende vorm niet langer worden bewaard dan nodig is voor het doel (Art. 10). Voor gegevens die voor historische, statistische of wetenschappelijke doeleinden worden bewaard mogen langer worden bewaard, mits verantwoordelijke de nodige waarborgen treft om te garanderen dat de persoonsgegevens alleen voor die doelen worden gebruikt.

Een andere belangrijke verplichting, zeker met het oog op Cloud Computing, betreft de in artikel 13 Wbp verankerde beveiligingsverplichting:

> *"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."*

Indien een bewerker wordt ingeschakeld, moet de verantwoordelijke zorg dragen dat deze voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerkingen. Naast de beveiligingsplicht geldt voor verantwoordelijken een informatieplicht welke is neergelegd in de artikelen 33 en 34 Wbp. De verantwoordelijke moet de betrokkene informeren over zijn identiteit en de doeleinden van de verwerking waarvoor de gegevens zijn bestemd, alsmede nadere informatie verstrekken voor zover dat gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen. Hoofdstuk 4 van de Wbp geeft aan in welke gevallen de verantwoordelijke bovendien de plicht heeft om de verwerking van persoonsgegevens te melden bij de bevoegde nationale toezichthoudende autoriteit, in Nederland het College Bescherming Persoonsgegevens (CBP).[46]

Naast plichten voor verantwoordelijken, bevat de Wbp enkele rechten van betrokkenen (eindgebruikers van de Cloud Services, maar mogelijk ook anderen, zoals personen wiens gegevens worden verwerkt in Cloud Services), zoals een recht op toegang tot de eigen gegevens, een recht om gegevens te rectificeren, te wissen, af te schermen en het recht zich te verzetten tegen de verwerking van persoonsgegevens.

---

[46] Hoofdstuk 4 van de Wbp betreft melding en voorafgaand onderzoek en hoofdstuk 9 betreffende toezicht gaat nader in op het CBP en de functionaris voor de gegevensverwerking.

Op grond van artikel 13 van de Richtlijn hebben de lidstaten de vrijheid om, op basis van zwaarwegende belangen, de reikwijdte van enkele rechten en plichten te beperken.
Tot slot moet nog gewezen worden op de artikelen 22-24 die een plicht opleggen aan de lidstaten om passende sancties vast te stellen voor schendingen van de met de Richtlijn ingestelde rechten.

Tot slot is het met het oog op onderwijsinstellingen van belang te wijzen op artikel 5 van de Wbp betreffende minderjarigheid. Wanneer persoonsgegevens verwerkt worden van betrokkenen beneden de zestien jaar, is daarvoor steeds in plaats van toestemming van de betrokkene, toestemming van de wettelijk vertegenwoordiger (ouder of voogd) vereist (Art. 5 Wbp). Daar waar toestemming nodig is voor bijvoorbeeld het verwerken van persoonsgegevens buiten de Europese Unie in landen zonder voldoende beschermingsniveau, dient deze toestemming bij minderjarigen verkregen te worden van hun wettelijk vertegenwoordigers. Dit geldt ook indien de betrokkene onder curatele is gesteld of ten behoeve van de betrokkene een mentorschap is ingesteld. Daarbij kan toestemming door de betrokkene of zijn wettelijk vertegenwoordiger te allen tijde worden ingetrokken.

4.2 Laag 2: Bijzondere persoonsgegevens

Bijzondere persoonsgegevens, ook wel gevoelige gegevens genoemd, zijn persoonlijke gegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven en betreffende het lidmaatschap van een vakvereniging. Merk op dat (portret)foto's dergelijke persoonsgegevens kunnen bevatten: een portretfoto van een studente met haardoek verstrekt immers informatie over godsdienst en mogelijk ras. Op grond van artikel 16 van de Wbp is verwerking van deze gegevens verboden tenzij een van de uitzonderingen in de artikelen 17 -23 Wbp van toepassing is. Hetzelfde geldt voor strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag (Art. 16 Wbp). Eerst wordt in de artikelen 17 tot en met 22 per specifieke categorie bepaald welke uitzonderingen gelden met betrekking tot het verwerkingsverbod. Artikel 18 betreffende ras bepaalt bijvoorbeeld dat het verbod om persoonsgegevens betreffende iemands ras te verwerken niet van toepassing is indien de verwerking geschiedt met het oog op de identificatie van de betrokkene en slechts voor zover dit voor dit doel onvermijdelijk is. In artikel 23 zijn een aantal uitzonderingen op het verbod om bijzondere persoonsgegevens te verwerken neergelegd die gelden voor alle categorieën bijzondere persoonsgegevens. Op grond van dit artikel is het verwerkingsverbod niet van toepassing voor zover de verwerking geschiedt met uitdrukkelijke toestemming van de betrokkene; de gegevens door de betrokkene duidelijk openbaar zijn gemaakt; dit noodzakelijk is voor de vaststelling, de uitoefening of de verdediging van een recht in rechte; dit noodzakelijk is ter voldoening aan een volkenrechtelijke verplichting of dit noodzakelijk is met het oog op een zwaarwegend algemeen belang, passende waarborgen worden geboden ter bescherming van de persoonlijke levenssfeer en dit bij wet wordt bepaald dan wel het College bescherming persoonsgegevens ontheffing heeft verleend. Het College kan bij de verlening van ontheffing beperkingen en voorschriften opleggen.[47] Bovendien geeft artikel 23 uitzonderingen voor de verwerking van bijzondere persoonsgegevens ten behoeve van wetenschappelijk onderzoek of statistiek wanneer het onderzoek een algemeen belang dient; de verwerking voor het betreffende onderzoek of de betreffende statistiek noodzakelijk is; het vragen van uitdrukkelijke toestemming onmogelijk blijkt of een onevenredige inspanning kost en bij de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad.

[47] Op grond van lid 3 moeten de verwerkingen op grond van art. 23 lid 1 gemeld worden bij de Europese Commissie. Onze Minister wie het aangaat verricht de melding indien de verwerking bij wet is voorzien. Het College verricht de melding indien het voor de verwerking ontheffing heeft verleend.

Doorgaans zal een onderwijsinstelling slechts in beperkte mate te maken krijgen met de verwerking van bijzondere persoonsgegevens. Gegevens die betrekking hebben op zaken als godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid en seksuele leven zullen in het kader van Clouddiensten door onderwijsinstellingen nauwelijks worden verwerkt. Zoals hierboven beschreven zijn gegevens over ras, hetgeen zou kunnen blijken uit een achternaam, uitgesloten van het verwerkingsverbod wanneer de verwerking geschiedt voor identificatie. Een ander voorbeeld waar een onderwijsinstelling bijzondere gegevens verwerkt, betreft de verwerking van persoonsgegevens door een instelling voor bijzonder onderwijs. Uit het gegeven dat leerlingen bijzonder onderwijs volgen, kan iets worden afgeleid over de medische toestand van die leerlingen. Voor de verwerking van dergelijke gegevens, geldt in principe een verwerkingsverbod. Ook hier zal een beroep moeten worden gedaan op een van de uitzonderingen. Artikel 21 lid 1 sub c van de Wbp stelt dat onderwijsinstellingen gegevens betreffende iemands gezondheid mogen verwerken als dat “met het oog op de speciale begeleiding van leerlingen of het treffen van bijzondere voorzieningen in verband met hun gezondheidstoestand noodzakelijk is”. Deze uitzondering zal niet opgaan in het geval van het gebruik van Cloud Computing diensten, aangezien het verwerken van persoonsgegevens voor het gebruik van die diensten niet noodzakelijk is in verband met de gezondheidstoestand van de leerlingen. Daarom zal een van de algemene uitzonderingen uit artikel 23 uitkomst moeten bieden. Artikel 23 lid 1 sub a bepaalt dat het verbod om bijzondere persoonsgegevens te verwerken niet van toepassing is waar uitdrukkelijke toestemming door de betrokkene is gegeven voor het verwerken van die bijzondere gegevens. Het begrip ‘toestemming’ is reeds uitgelegd in paragraaf 4.1. Cruciaal bij toestemming is dat deze vrij is en expliciet betrekking heeft op hetgeen waarvoor toestemming is gegeven. Bovendien moet de beslissing om tot toestemming te komen een geïnformeerde beslissing zijn. Punt van aandacht is dat toestemming ten alle tijden door de betrokkene of, wanneer deze beneden de zestien is, de wettelijk vertegenwoordiger, kan worden ingetrokken (Art. 5 lid 2 Wbp). Toestemming is in het voorbeeld van de gezondheidsgegevens wellicht niet nodig, aangezien artikel 23 lid 1 sub b de verwerking van bijzondere persoonsgegevens toestaat wanneer de betrokkene de gegevens duidelijk openbaar heeft gemaakt. Zoals gezegd zullen onderwijsinstellingen bij het gebruik van Clouddiensten nauwelijks bijzondere gegevens verwerken. Punt van aandacht is nog wel dat eindgebruikers, zoals studenten, mogelijk wel bijzondere gegevens verwerken, bijvoorbeeld in e-mails. Voor zover de inhoud van de e-mail uitsluitend persoonlijke of huishoudelijke doeleinden dient, is de Wbp niet van toepassing (art. 2 lid 2). Echter, deze uitzondering wordt beperkt uitgelegd.48 Hierdoor vallen e-mails die betrekking hebben op de onderwijssituatie, waarschijnlijk binnen de werkingssfeer van de Wbp. In dit geval zijn de studenten op grond van de Wbp verantwoordelijke en dus gebonden aan de in de Wbp neergelegde bepalingen. In hoofdstuk 5 zullen we zien dat de CCSP de aansprakelijkheid voor de inhoud van wat eindgebruikers op de Cloud servers plaatsen contractueel zal beleggen bij de onderwijsinstellingen. Dit betekent dat de onderwijsinstellingen beleid op moeten stellen hoe eindgebruikers met de aangeboden Cloud faciliteiten om mogen gaan. Dit beleid zal in ieder geval uitleg over de verwerking van persoonsgegevens moeten omvatten.

4.3 Laag 3: Doorgifte naar derde landen

De derde laag van het gegevensbeschermingsregime betreft de doorgifte van persoonsgegevens naar derde landen, landen buiten de EU. Aangezien een van de kenmerken van Clouddiensten het verwerken en bewaren van gegevens op niet lokale en vaak zelfs wisselende servers op wisselende locaties betreft, is deze laag zeer relevant. De artikelen 76 en 77 van de Wbp bepalen onder welke voorwaarden de doorgifte van persoonsgegevens naar derde landen is toegestaan.

---

[48] ARREST VAN HET HOF van 6 november 2003 in zaak C-101/01 (verzoek van het Göta hovrätt om een prejudiciële beslissing): Bodil Lindqvist ("Richtlijn 95/46/EG (Werkingssfeer (Openbaarmaking van persoonsgegevens op internet (Plaats van openbaarmaking (Begrip doorgifte van persoonsgegevens naar derde landen (Vrijheid van meningsuiting (Verenigbaarheid met richtlijn 95/46 van verdergaande bescherming van persoonsgegevens door wettelijke regeling van lidstaat") Lindqvist.

Op grond van artikel 76 mogen persoonsgegevens slechts aan landen buiten de EU worden doorgegeven indien deze landen een *'passend beschermingsniveau waarborgen'.* Het passend beschermingsniveau moet worden beoordeeld aan de hand van de specifieke omstandigheden die op de doorgifte van invloed zijn. In het bijzonder wordt rekening gehouden met de aard van de gegevens, met doeleinden en de duur van de voorgenomen verwerking, het land van herkomst en het land van eindbestemming, de algemene en sector specifieke rechtsregels die in het betrokken derde land gelden, alsmede de regels van het beroepsleven en de veiligheidsmaatregelen die in die landen worden nageleefd. Of sprake is van een passend beschermingsniveau wordt formeel bepaald door de Europese Commissie.[49] Op een zogenaamde witte lijst zijn de landen opgenomen die door Europa worden aangemerkt als land met een passend beschermingsniveau.[50] Op deze lijst staan landen zoals Australië, Canada en voor wat betreft de Verenigde Staten staan de zowel de *Safe Harbor* overeenkomst als de *Transfer of Air Passenger Name Record (PNR) Data* overeenkomst op de witte lijst. Of dit ook de juiste waarborgen biedt is momenteel echter onderwerp van hevige discussie. In paragraaf 4.4 komen we hier op terug.

Indien geen passend beschermingsniveau aanwezig is, is doorgifte naar derde landen alleen toegestaan op een van de gronden genoemd in artikel 77. Kort weergegeven betreft het de volgende verwerkingsgronden:

a) de betrokkene heeft zijn ondubbelzinnige toestemming gegeven;
b) de doorgifte is noodzakelijk voor de uitvoering van een overeenkomst tussen de betrokkene en de verantwoordelijke;
c) de doorgifte is noodzakelijk voor de sluiting of uitvoering van een in het belang van de betrokkene tussen de verantwoordelijke en een derde gesloten of te sluiten overeenkomst;
d) de doorgifte noodzakelijk is vanwege een zwaarwegend algemeen belang, de vaststelling, de uitvoering of de verdediging van enig recht;
e) de doorgifte noodzakelijk is ter vrijwaring van een vitaal belang van de betrokkene, of;
f) de doorgifte geschiedt vanuit een openbaar register dat bij wettelijk voorschrift is.

Indien geen van de genoemde gronden uitkomst biedt, kan op grond van het tweede lid van artikel 77 een vergunning gevraagd worden aan de Minister. Deze dient het College hierover te horen en nadere voorschriften worden aan de vergunning verbonden die nodig zijn om de bescherming van de persoonlijke levenssfeer en de fundamentele rechten en vrijheden van personen, alsmede de uitoefening van de daarmee verband houdende rechten te waarborgen.

Gezien de voorgaande bepalingen, zijn de volgende vragen van belang wanneer diensten worden uitbesteed aan de Cloud:

- *Worden persoonsgegevens doorgegeven aan een land buiten de EU?*
- *Zijn de specifieke regels betreffende de doorgifte van gegevens naar derde landen van toepassing?*
- *Mogen persoonsgegevens worden doorgegeven naar of verwerkt worden in een land buiten de EU?*
- *Indien persoonsgegevens buiten de EU worden verwerkt, in hoeverre worden die gegevens dan in de praktijk daadwerkelijk beschermd door het Europese recht?*

---

[49] Zie artikel 25 lid 4 en 6 Databescherming Richtlijn, en artikel 78 lid 2 Wet bescherming persoonsgegevens.

[50] Zie voor de witte lijst: http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm (sic), laatst geraadpleegd op 13-12-2010.

De vraag of persoonsgegevens afkomstig uit de EU, die worden verwerkt in een land buiten de EU, vallen onder het Europese recht op gegevensbescherming, bijvoorbeeld door het gebruik van al dan niet geautomatiseerde middelen in de EU, is reeds aan de orde geweest in hoofdstuk 3. Deze vraag zal hier dan ook niet worden behandeld.

Voor het beantwoorden van de eerste vraag is het van belang vast te stellen hoe het gegevensverkeer feitelijk verloopt. Als voorbeeld gaan we uit van de situatie dat de CCSP gevestigd is buiten de EU, althans dat de ontvangen gegevens door de CCSP verwerkt worden buiten de EU. We bespreken hier alleen de verhoudingen van verschillende partijen met de CCSP, omdat alleen binnen deze relaties het waarschijnlijk is dat persoonsgegevens naar een land buiten de EU doorgegeven worden. De kans dat een dergelijke situatie zich voordoet bij bijvoorbeeld de relatie onderwijsinstelling <-> SURFfederatie/ENTREE is erg beperkt.
We beginnen met de relatie onderwijsinstelling <-> CCSP. De onderwijsinstelling heeft de beschikking over persoonsgegevens van haar studenten. De vraag is in hoeverre zij die persoonsgegevens uitwisselt met de CCSP. Er zijn twee situaties denkbaar: de onderwijsinstelling, of de daaraan verbonden docenten, maken zelf geen gebruik van de Clouddiensten, of zij doen dat juist wel. Wanneer de onderwijsinstelling geen gebruik maakt van deze diensten, dan zal zij doorgaans geen persoonsgegevens met de CCSP uitwisselen. De onderwijsinstelling heeft weliswaar een contract gesloten met de CCSP voor het gebruik van de diensten, maar het feitelijk gegevensverkeer gaat in dit geval niet tussen deze twee partijen maar tussen de eindgebruikers (studenten) en de CCSP. Gebruiken onderwijsinstellingen de Clouddiensten wèl en worden persoonsgegevens op de Clouddienst geplaatst, bijvoorbeeld wanneer docenten namen en e-mailadressen van studenten plaatsen op een applicatie zoals Blackboard, dan geven zij deze gegevens door aan de CCSP en daarmee mogelijk ook aan een land buiten de EU. Indien persoonsgegevens daadwerkelijk worden doorgegeven aan een land buiten de EU, dan zijn de specifieke regels betreffende de doorgifte van gegevens naar derde landen van toepassing.

Een andere relatie is die tussen SURFfederatie/ENTREE <-> CCSPs. SURFfederatie/ENTREE zal moeten verifiëren dat een bepaalde persoon toegang heeft tot de Clouddiensten door middel van identificatie en authenticatie. Het zal die verificatie vervolgens kenbaar moeten maken aan de CCSP, zodat toegang tot de diensten mogelijk wordt. De vraag hier is of een dergelijke verificatie, die gecommuniceerd wordt van SURFfederatie/ENTREE naar de CCSP, ook persoonsgegevens bevat. Indien dit het geval is en deze persoonsgegevens daadwerkelijk worden doorgegeven aan een land buiten de EU, dan zijn de specifieke regels betreffende de doorgifte van gegevens naar derde landen wederom van toepassing.

De volgende en laatste verhouding waarbij we stil staan is de verhouding tussen eindgebruikers (studenten) <-> CCSP. De studenten zijn degenen die, eventueel naast de onderwijsinstelling, voornamelijk gebruik zullen gaan maken van de Clouddiensten. Deze situatie moet worden ontleed voor twee gevallen: die waarin de student zelf verantwoordelijke is voor persoonsgegevens van anderen en die waarin dat wel niet het geval is.
Ook studenten kunnen persoonsgegevens verwerken, bijvoorbeeld door in een e-mail te schrijven over een ander persoon. Een dergelijke e-mail kan persoonsgegevens zoals naam, locatie, e-mail, leeftijd, en/of een verzameling van karakteristieken (zoals interesses), bevatten. Wanneer de personenkring die kennis kan nemen van deze informatie voldoende groot is (memoreer de Lindqvist zaak), dan zijn zij zelf verantwoordelijke.[51] Wanneer zij dergelijke persoonsgegevens op de Clouddienst plaatsen en deze gegevens uiteindelijk terecht komen of worden verwerkt in een land buiten de EU, is sprake van doorgifte van persoonsgegevens.

[51] Mogelijk zouden studenten zich kunnen beroepen op de “van huishoudelijke aard” uitzondering, hetgeen inhoudt dat als de persoonsgegevens worden verwerkt puur in een huishoudelijke, persoonlijke context databeschermingsregelgeving niet van toepassing is. Zie artikel 3 lid 2 Databescherming Richtlijn en artikel 2 lid 2 sub a Wet bescherming persoonsgegevens. Deze uitzondering wordt echter beperkt uitgelegd, hetgeen betekent dat deze uitzondering niet stel van toepassing zal zijn.

De student is daarmee gebonden aan de regels betreffende de doorgifte van gegevens naar derde landen. Zij zullen bijvoorbeeld een verwerkingsgrond moeten kunnen aanduiden binnen de kaders van artikel 77 Wbp (de betrokkene kan bijvoorbeeld ondubbelzinnig toestemming hebben gegeven voor de verwerking).
Wanneer geen sprake is van verwerking van persoonsgegevens van derden door de student, maar de studente direct werkt op een server van een verwerker in een land buiten de EU (een server van Google in de VS, bijvoorbeeld), dan is er geen sprake van doorgifte. Er is in dat geval immers geen intermediaire verantwoordelijke tussen student en verwerker (Google).[52]

Het antwoord op de tweede vraag is wederom afhankelijk van het feitelijke dataverkeer, en uitdrukkelijk niet van de rollen van partijen, te weten die van verantwoordelijke, bewerker en betrokkene. Zoals hierboven beschreven verbieden de Wet bescherming persoonsgegevens en Richtlijn 95/46/EG in principe de doorgifte van persoonsgegevens naar derde landen, tenzij een uitzonderingsgrond van toepassing is. Welke rol degene heeft die de persoonsgegevens doorgeeft doet niet ter zake. Naast verantwoordelijken kunnen ook bewerkers persoonsgegevens doorgeven naar een land buiten de EU. Echter, het laten verwerken van persoonsgegevens buiten de EU zal enkel in opdracht van een verantwoordelijke kunnen gebeuren, welke ook de doelen voor die verwerking zal bepalen. Indien de bewerker gegevens op eigen initiatief doorgeeft naar landen buiten de EU zal dit in strijd zijn met zijn met de Wbp en de met de contractuele verplichtingen jegens de verantwoordelijke. Dit is anders wanneer deze doorgifte door de bewerker contractueel is vastgelegd, echter, dan betreft het een verwerking waarvoor de bewerker verantwoordelijke is, aangezien deze dan doel en middelen vaststelt. Het betreft dus een andere verwerking dan die waartoe hij van de verantwoordelijke opdracht gekregen heeft.

Bij Cloud Computing zijn met name de uitzonderingsgronden *'ondubbelzinnige toestemming', 'overeenkomst'* en *'Vergunning van de minister'* relevant.
Indien onderwijsinstellingen persoonsgegevens willen doorgeven naar een land buiten de EU dat geen passend beschermingsniveau biedt, dan zou een van deze uitzonderingsgronden uitkomst kunnen bieden om dit verkeer toch mogelijk te maken. Ingeval van toestemming moet deze specifiek betrekking hebben op het doorgeven en laten verwerken van persoonsgegevens in een land, of landen buiten de EU. Ditzelfde geldt voor SURFfederatie/ENTREE en de gebruikers van de Cloud Services, indien zij persoonsgegevens doorgeven aan de CCSP die zich buiten de EU bevindt en/of persoonsgegevens laten verwerken buiten de EU in een land dat geen passend beschermingsniveau biedt. Nota bene, het is bij toestemming niet van belang welke rol degene die de persoonsgegevens doorgeeft naar derde landen vervult. In principe zal de verantwoordelijke toestemming moeten verkrijgen, en kan de bewerker contractueel bepalen dat verantwoordelijkheid voor het verkrijgen van de benodigde toestemming ook een taak van de verantwoordelijke is. Vervolgens zal de bewerker zich uiteraard wel aan alle geldende regels moeten houden, hetgeen voortvloeit uit zowel de Wbp als de contractuele relatie tussen verantwoordelijke en bewerker. Ook hier geldt weer dat toestemming een 'dynamische' verwerkingsgrond is aangezien toestemming te allen tijde kan worden ingetrokken. In Nederland wordt 'toestemming' zodanig uitgelegd dat wanneer toestemming niet wordt gegeven, of later wordt ingetrokken, het niet als behoorlijk en zorgvuldig wordt beschouwd de verwerking alsnog op een andere grond te baseren.[53] Intrekking van de toestemming betekent daarmee dat de verwerking niet langer rechtmatig is.

Om te bepalen of een overeenkomst uitkomst kan bieden voor de doorgifte van persoonsgegevens naar derde landen zonder passend beschermingsniveau, moeten de rollen van partijen duidelijk worden bepaald.

---

[52] Zie ook Kuczerawy (2010) die dit punt illustreert aan de hand van Facebook.
[53] Kamerstukken II 1997-1998, 25 892, nr. 3 p. 81-82. Behoorlijk en zorgvuldig betreft de terminologie uit artikel 6 Wbp.

De in artikel 77 lid 1 onder b genoemde uitzondering betreft een verwerking die noodzakelijk is voor het uitvoeren van de overeenkomst tussen de betrokkene en de verantwoordelijke. In het geval van Cloud Computing kan het zo zijn dat onderwijsinstellingen en/of SURFfederatie/ENTREE een beroep kunnen doen op deze uitzondering. Zij sluiten een overeenkomst met de CCSP voor het gebruik van Clouddiensten, en voor de uitvoering van die overeenkomst is het mogelijk noodzakelijk dat persoonsgegevens buiten de EU, in een land zonder passend beschermingsniveau verwerkt worden, bijvoorbeeld indien de CCSP niet kan garanderen dat de data binnen de EU blijft vanwege technische, organisatorische of andere redenen. Het is belangrijk goed voor ogen te houden wat de contractuele relaties zijn, en om de vraag te stellen of het met betrekking tot die specifieke relatie noodzakelijk is de data buiten de EU, in een land dat geen passend beschermingsniveau heeft, te laten verwerken.

Ten slotte is de vraag naar de uitwerking in de praktijk van belang. Deze vraag valt uiteen in een aantal subvragen, waarbij de vraag of de Wbp van toepassing is op de verwerking van persoonsgegevens door entiteiten die gevestigd zijn buiten Nederland hier buiten beschouwing blijft. In hoofdstuk 3 is aangegeven dat in deze situatie bepalend is of gebruik gemaakt wordt van geautomatiseerde middelen, niet slechts dienend voor doorvoer, op Nederlands grondgebied. De relevante praktijkgerichte vragen zijn:

- *Wat betekent het in de praktijk wanneer de Wbp van toepassing is op de verwerking van persoonsgegevens door buitenlandse entiteiten?*
- *Is de Wbp in het buitenland juridisch afdwingbaar?*
- *Wat betekent het in de praktijk dat persoonsgegevens worden doorgegeven aan derde landen die wel een passend beschermingsniveau waarborgen?*
- *In hoeverre worden persoonsgegevens in dit geval ook daadwerkelijk volgens de Wbp verwerkt?*
- *Wat betekent het in de praktijk dat persoonsgegevens worden doorgegeven aan derde landen die geen passend beschermingsniveau waarborgen?*
- *Welke privacyrisico's brengt een doorgifte van data naar dergelijke landen met zich mee?*

Zoals de vragen al suggereren, is er een onderscheid tussen de situatie dat de Wbp direct van toepassing is op buitenlandse entiteiten die persoonsgegevens verwerken in derde landen, en de situatie dat, ongeacht of de Wbp direct van toepassing is, persoonsgegevens worden doorgegeven aan een derde land dat al dan niet een passend beschermingsniveau waarborgt. Beide situaties brengen andere issues met zich mee.
In hoofdstuk 3 is uitgelegd dat bij het afnemen van diensten van CCSPs buiten de Wbp, of een vergelijkbaar EU gegevensbeschermingsregime toch van toepassing is vanwege het gebruik van cookies door CCSPs. Maar, het is maar de vraag hoe betekenisvol dit gegeven in de praktijk is, omdat het recht waarschijnlijk moeilijk af te dwingen is in een derde land. Buiten de kosten en de tijd die afdwingen met zich meebrengt, is het überhaupt maar de vraag in hoeverre buitenlandse overheden, private partijen en gerechten zich gebonden zullen achten aan het Europese recht. Handhaving van dit recht ter plaatse zal dan ook niet verwacht moeten worden, en handhaving vanuit Europa zal, zoals aangegeven, problematisch zijn. Wat wel mogelijk is, is het opnemen van gegevensbeschermingsregels in een contract. Een contract is juridisch bindend tussen partijen; wanneer het contract niet wordt nageleefd kan nakoming alsnog juridisch gevorderd worden. De conclusie is dat wanneer een Europese entiteit te maken heeft met een buitenlandse CCSPs die persoonsgegevens zal (laten) verwerken in derde landen, het verstandig is om essentiële gegevensbeschermingsregels in het contract op te nemen zodat deze via de contractuele weg ook in het buitenland juridisch afdwingbaar zijn.

De vraag in hoeverre doorgifte naar een land met een passend beschermingsniveau waarborgen biedt, zal beantwoord worden aan de hand van een concreet voorbeeld: namelijk de Safe Harbor principles.[54]

4.4 De Safe Harbor principles

Zoals eerder aangegeven, de Europese Commissie heeft de Safe Harbor op de witte lijst geplaatst en dus aangemerkt als een passend beschermingsniveau. Dat een derde land op deze lijst staat, wil echter niet zeggen dat het betreffende land precies dezelfde regelgeving kent als Europa. Het wil zeggen dat er, onder de specifieke omstandigheden, voldoende waarborgen zijn voor een passend beschermingsniveau. Of die waarborgen aanwezig zijn wordt door de Commissie beoordeeld "op grond van (...) nationale wetgeving of (…) internationale verbintenissen (…) met het oog op de bescherming van de persoonlijke levenssfeer en de fundamentele vrijheden en rechten van personen."[55] Echter, het voorbeeld van de Safe Harbor principles laat zien dat plaatsing op de witte lijst niet garandeert dat privacystandaarden in de praktijk naar behoren worden nageleefd. Europese bedrijven die persoonsgegevens willen doorgeven aan Amerikaanse bedrijven mogen dat alleen doen indien het betreffende bedrijf een Safe Harbor certificaat heeft verkregen.[56] Dit certificaat zou moeten betekenen dat het bedrijf zich houdt aan de tussen de EU en VS ruim tien jaar geleden gemaakte afspraken, die moeten waarborgen dat persoonsgegevens op een passende wijze beschermd worden. Het Safe Harbor systeem is recentelijk echter bestempeld als onbetrouwbaar en frauduleus.[57] De belangrijkste kwesties zijn de volgende:
De Amerikaanse overheid kan op basis van federale anti-terrorismewetgeving, te weten de USA PATRIOT-act[58] gegevens opvorderen zonder gerechtelijk bevel, althans met beperkte gerechtelijke toetsing[59], zonder toestemming of wetenschap van betrokkene, en in bepaalde gevallen zelfs zonder geconcretiseerd doel.[60]

---

54 Expert.gov (2010) Welcome to the U.S.-EU & Swiss Safe Harbor Frameworks. Toegankelijk via: http://www.export.gov/safeharbor/. Laatst geraadpleegd op 8 december 2010.

55 Artikel 25 lid 6 Richtlijn 95/46/EG. Hoe het begrip "passend beschermingsniveau" moet worden uitgelegd wordt door de artikel 29 Werkgroep toegelicht in: Groep voor de bescherming van personen in verband met de verwerking van persoonsgegevens (1998) WP 12: Doorgifte van persoonsgegevens naar derde landen: toepassing van de artikelen 25 en 26 van de EU-richtlijn betreffende gegevensbescherming, Hoofdstuk 1. Toegankelijk via: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_nl.pdf. Laatst geraadpleegd op 10 december 2010. De artikel 29 Werkgroep geeft aan dat bij de analyse in elk geval rekening moet worden gehouden met "twee fundamentele elementen (...): de inhoud van de toepasselijke voorschriften en de middelen om de handhaving ervan te garanderen." (p. 5) Verder is er in het voorgenoemde een lijst gemaakt van principes die in elk geval, zowel wat betreft de inhoud als de handhaving, gewaarborgd moeten worden; zie p. 6-8.

56 http://www.export.gov/safeharbor/

57 De Haes, A.U. (2010) Grootschalige privacyfraude tussen EU en VS. Webwereld. Toegankelijk via: http://mobile.webwereld.nl/nieuws/67936/grootschalige-privacyfraude-tussen-eu-en-vs.html. Laatst geraadpleegd op 10 december 2010. Zie ook Van Blommestein, M. (2010) Data mag niet zomaar het land uit. Webwereld. Toegankelijk via: http://webwereld.nl/nieuws/66348/data-mag-niet-zomaar-het-land-uit.html. Laatst geraadpleegd op 10 december 2010.

58 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001.

59 Electronic Privacy Information Center. Zie onder 'Pen Registers, the Internet and Carnivore'. Toegankelijk via: http://epic.org/privacy/terrorism/usapatriot/. Laatst geraadpleegd op 10 december 2010.

60 Electronic Privacy Information Center. Zie onder 'Liberalized Use of Pen Register/Trap and Trace Devices under FISA' en 'Multi-Point ("Roving Wiretap") Authority' Toegankelijk via: http://epic.org/privacy/terrorism/usapatriot/. Laatst geraadpleegd op 10 december 2010.

De USA PATRIOT-act gaat met name over het opvorderen van verkeersdata, maar in bepaalde gevallen kan ook de inhoud van communicaties worden gescreend.[61] Echter, bedacht moet worden dat ook verkeersgegevens persoonlijke gegevens kunnen bevatten, zoals e-mailadres, surfgedrag, IP-adres, etc.[62]
Hoe ver reiken nu de bevoegdheden die voortkomen uit de USA PATRIOT-act? Kan de Amerikaanse overheid bijvoorbeeld ook gegevens opvragen wanneer een CCSP in de VS gevestigd is, en toegang heeft tot datacenters in andere landen? In principe is de USA PATRIOT-Act alleen geldig in de VS, en heeft de Act geen betrekking op Europa. Desalniettemin kan het zo zijn dat wanneer in de VS data- en communicatieverkeer gescand of gesurveilleerd wordt, ook "Europese data" in die surveillance wordt betrokken omdat die data op Amerikaanse servers staat. De vraag is vervolgens of je als Europese entiteit een Cloud Service wil afnemen van een Amerikaanse CCSP die Europese persoonsgegevens op zal slaan op Amerikaanse datacentra, met als risico dat die data ook gescand worden. Zelfs als een Amerikaanse CCSP gegevens buiten de VS zou opslaan kan het zijn dat, omdat zij lokale wetten moeten naleven, ook die gegevens opgevorderd worden door de lokale overheid.

Vastgesteld is dat door Amerikaanse bedrijven al jarenlang fraude wordt gepleegd met het Safe Harbor-keurmerk.[63] Bedrijven die niet of beperkt aan de Safe Harbor principles voldoen krijgen toch het certificaat. Of het certificaat wordt gebruikt terwijl het betreffende bedrijf niet eens is aangesloten bij Safe Harbor. Dit komt doordat er vanuit de US Departement of Commerce, de instantie die gaat over Safe Harbor, geen controle bij de toegang tot Safe Harbor en later bij de naleving van de beginselen is.[64] De reden hiervoor is dat het Safe Harbor systeem louter een vorm van zelfregulering is, hetgeen betekent dat de beginselen juridisch niet bindend zijn en dat het aan de bedrijven zelf is om te zorgen voor naleving. Het gaat dus in feite om "self certification"[65] en niet om overheidscertificering.

Hoewel dus de locatie van gegevens in beginsel niet bepalend is voor de toepasselijkheid van de Wbp, is het toch noodzakelijk dat onderwijsinstellingen rekening houden met de locatie waarnaar persoonsgegevens doorgegeven en verwerkt worden in het kader van Cloud Computing. Dit met het oog op de risico's die beperktere handhavingsmogelijkheden en toepasselijke lokale wetgeving betreffende vorderings en monitoringsrechten, met zich meebrengen.

---

61 Electronic Privacy Information Center. Zie onder 'Pen Registers, the Internet and Carnivore', 'Surveillance and Privacy Laws Affected', en 'Interception of "Computer Trespasser" Communications'. Toegankelijk via: http://epic.org/privacy/terrorism/usapatriot/. Laatst geraadpleegd op 10 december 2010.

62 Electronic Privacy Information Center. Zie onder 'Pen Registers, the Internet and Carnivore'. Toegankelijk via: http://epic.org/privacy/terrorism/usapatriot/. Laatst geraadpleegd op 10 december 2010.

63 De Haes, A.U. (2010) Grootschalige privacyfraude tussen EU en VS. Webwereld. Toegankelijk via: http://mobile.webwereld.nl/nieuws/67936/grootschalige-privacyfraude-tussen-eu-en-vs.html. Laatst geraadpleegd op 10 december 2010.

64 Export.gov. Safe Harbor List. Toegankelijk via: https://safeharbor.export.gov/list.aspx. Laatst geraadpleegd op 10 december 2010.

65 Ibid.

5 Cloud Computing, contracten en privacy

5.1 Inleiding

Aan het gebruik van Cloud Computing door onderwijsinstellingen ligt een groot aantal contractuele relaties ten grondslag.
In het kader van het onderzoek dat aan dit rapport ten grondslag ligt hebben de onderzoekers kennis kunnen nemen van zowel de overeenkomst welke door Google met de Open Universiteit[66] is afgesloten alsmede van een verkorte versie van een modelovereenkomst op basis waarvan andere instellingen een overeenkomst met Google zijn aangegaan. Naast Google is ook Microsoft op deze markt als leverancier actief; andere aanbieders zullen wellicht volgen.
In dit hoofdstuk behandelen we de inhoud van de overeenkomst tussen Google en de Open Universiteit in het kort. Het doel daarvan is uitsluitend om te illustreren op welke wijze de betreffende partijen met het onderwerp “privacy” zijn omgegaan. Er heeft geen beoordeling van die overeenkomst plaatsgevonden.

In het model zoals weergegeven in figuur 2 zijn onder meer overeenkomsten tussen de volgende partijen van belang:

eindgebruiker – onderwijsinstelling;
onderwijsinstelling – authenticatie- en autorisatiedienstleverancier (SURFnet, Kennisnet);
SURFnet/Kennisnet – Google;
onderwijsinstelling – Google;
eindgebruiker – Google.

5.2 Een voorbeeld: de Google Apps Education Edition Agreement

De "Google Apps Education Edition Agreement" is een voorbeeld van een overeenkomst tussen een CCSP en een onderwijsinstelling op basis waarvan Cloud Computing diensten worden aangeboden aan Nederlandse onderwijsinstellingen.

De "Google Apps Education Edition Agreement" is afgesloten tussen Google Inc. en (onder meer) een aantal Nederlandse onderwijsinstellingen. Hieronder wordt kort nader ingegaan op de versie van de overeenkomst die in 2008 is afgesloten door de Open Universiteit met Google.[67]

De Open Universiteit heeft op 21 februari 2008 een “Google Apps Education Edition Agreement" afgesloten met Google Inc. De overeenkomst is aangegaan voor een initiële periode van een kalenderjaar, met automatische verlenging voor een periode van driemaal één kalenderjaar. Op de overeenkomst is Amerikaans recht (de staat Californië en toepasselijke federale wetgeving) van toepassing. Dit betekent ondermeer dat de Open Universiteit is gebonden aan Amerikaanse exportwetgeving.

De overeenkomst beschrijft de voorwaarden waaronder Google de zogenaamde “Services” ter beschikking stelt aan de Open Universiteit. Dit betreft in het bijzonder de "Google Apps Education Edition", kortweg "Google Apps".

---

[66] We gebruiken in de tekst Open Universiteit omdat de OU zich zo momenteel afficheert in communicatie uitingen. De juridische entiteit die feitelijk met Google Inc. contracteert is Open Universiteit Nederland.

[67] De inhoud van deze overeenkomst lijkt tenminste op hoofdlijnen representatief voor de overeenkomsten die nadien door andere instellingen met Google zijn gesloten. Er heeft echter geen gedetailleerde vergelijking plaatsgevonden.

De kern van de dienstverlening bestaat uit de mogelijkheid voor de onderwijsinstelling om “End User accounts” (mailboxaccounts) aan eindgebruikers aan te bieden en deze accounts te administreren. Uitgangspunt van de overeenkomst is dat Google hiervoor geen vergoeding ontvangt. De Open Universiteit verbindt zich de “Services” alleen te gebruiken voor doeleinden die "legal, proper and in accordance with this Agreement and all applicable policies or guidelines" zijn (artikel 3.4).
De overeenkomst omvat overigens aanzienlijk meer voorwaarden dan in de ondertekende versie op papier zijn gezet. In de tekst van de overeenkomst zijn namelijk talrijke voorwaarden of verwijzingen opgenomen naar aanvullende voorwaarden welke van toepassing zijn. Dit betreft onder meer een “Service Level Agreement”, de “Google Privacy Policy”, de “Administrative Policy”, “Google’s Technical Support Services Guidelines” en de “Google Apps Education Edition API Terms” alsmede onder meer nadere regels voor het gebruik van de Google trademarks (merken).

Google behoudt zich voorts het recht voor om aanvullende policies of guidelines aan customers op te leggen. Google heeft het recht de van toepassing zijnde “policies” van tijd tot tijd aan te passen. De Open Universiteit heeft het recht om de overeenkomst op te zeggen indien een dergelijke wijziging een substantieel nadelig effect voor haar heeft (artikel 17).

5.3 Overeenkomsten en privacy

Zoals opgemerkt is de bescherming van persoonsgegevens in Nederland primair gebaseerd op de Wbp. De bepalingen van deze wet zijn in beginsel van dwingend recht (zie onder). De Wbp laat als gevolg daarvan voor wat althans de kern van de privacybescherming betreft weinig vrijheid aan partijen.

De rol van overeenkomsten in de Wbp
Dit betekent niet dat overeenkomsten (in essentie: afspraken tussen partijen) geen rol spelen in dit wettelijk systeem. Integendeel; overeenkomsten spelen op diverse wijzen een rol bij het invullen of onderbouwen van de normstelling van de Wbp en vormen dan een zeer relevant instrument bij het concretiseren van de beoogde wettelijke privacybescherming.

Enkele voorbeelden. In sommige gevallen is het afsluiten van een overeenkomst verplicht ter uitvoering van de Wbp. Dit betreft onder andere de verplichting tot het sluiten van een bewerkersovereenkomst uit hoofde van de Wbp in geval een verantwoordelijke gegevens laat verwerken door een derde (de bewerker) (art. 14 lid 2 Wbp).[68] Ook kan bij de export van gegevens het afsluiten van een (Europese model)overeenkomst verplicht zijn. Overeenkomsten kunnen echter ook een geheel andere rol vervullen en bijvoorbeeld mede bepalen of een verwerking van persoonsgegevens rechtmatig is. Zo is de uitvoering van een overeenkomst een mogelijke verwerkingsgrondslag onder de Wbp (artikel 8 sub b). In die zin levert de overeenkomst tussen Google en de Open Universiteit een grondslag voor de verwerking van persoonsgegevens van de studenten van de Open Universiteit die via deze weg gebruik maken van de diensten van Google.

Door middel van overeenkomsten kunnen ook open normen uit de Wbp verder worden ingevuld. Zo is voor wat de beveiliging van persoonsgegevens betreft bepaald dat indien een bewerker wordt ingeschakeld de verantwoordelijke er op toeziet dat de bewerker voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen (artikel 14 lid 1 Wbp). In de (wettelijk verplichte) bewerkersovereenkomst kunnen partijen over de concrete

[68] Strikt genomen kunnen de afspraken ook in een andere juridische vorm worden neergelegd (art. 14 lid 2 Wbp). In de praktijk is het afsluiten van een bewerkersovereenkomst de regel.

invulling daarvan nadere afspraken maken.

Ook kunnen door middel van overeenkomsten (praktische) afspraken worden gemaakt over de wijze waarop bepaalde wettelijke rechten van de betrokkene kunnen worden uitgeoefend. Voorbeelden zijn de uitoefening van het recht van inzage (art. 35 Wbp) en het recht op correctie (art. 36). Ook ten aanzien van beveiligingsmaatregelen ter vervulling van de verplichtingen uit artikel 13 kunnen afspraken worden gemaakt.

Bovenstaande voorbeelden zijn overigens geen limitatieve opsomming van de wijze waarop contracten een rol kunnen spelen in relatie tot de Wbp.

Kan de Wbp door middel van een overeenkomst opzij worden gezet?
Een belangrijke vraag inzake de relatie tussen de Wbp en overeenkomsten is of de Wbp door middel van een overeenkomst opzij kan worden gezet. Kan bijvoorbeeld de Wbp worden ontweken door te kiezen voor toepasselijkheid van buitenlands recht, zoals het recht van de Verenigde Staten (waar een ander privacy regime heerst). Of zou de partij zelfs de Wbp of bepaalde delen daarvan buiten werking kunnen verklaren?

Het antwoord op deze vraag luidt ontkennend. De voorschriften van de Wbp gelden als dwingend recht[69] hetgeen betekent dat partijen daar in principe niet door middel van een overeenkomst van kunnen afwijken.

Privacybescherming wordt gezien als een recht dat onlosmakelijk met de persoonlijkheid van het individu is verbonden en derhalve in beginsel niet overdraagbaar en (daarmee) ook niet voor contractuele afstand vatbaar is. Als gevolg hiervan is bijvoorbeeld een overeenkomst waarbij afstand wordt gedaan van door de Wbp toegekende rechten in beginsel nietig wegens strijd met de openbare orde (art. 3:40 Burgerlijk Wetboek).

Contractuele afwijkingen van de voorschriften uit de Wbp zijn derhalve niet toelaatbaar tenzij die mogelijkheid in de Wbp zelf uitdrukkelijk wordt geboden. In de memorie van toelichting wordt als voorbeeld gewezen op artikel 8 sub a Wbp waarin wordt bepaald dat gegevensverwerking geoorloofd is als de betrokkene daarvoor zijn ondubbelzinnige toestemming heeft verleend. Zoals eerder reeds opgemerkt worden aan deze toestemmingverlening wel zware eisen gesteld.

Een ander voorbeeld wordt gevormd door artikel 8 sub b Wbp waarin is bepaald dat verwerking van gegevens is toegestaan voor zover dat noodzakelijk is voor de uitvoering van een overeenkomst. In dat geval wordt gedoeld op een overeenkomst die niet primair is gericht op de verwerking van persoonsgegevens, maar voor de uitvoering waarvan wel persoonsgegevens moeten worden verwerkt. Een voorbeeld is een overeenkomst welke wordt gesloten bij de online aankoop van vliegtickets. De websiteaanbieder zal de gegevens van de passagiers moeten doorgeven aan de vliegmaatschappij voor het daadwerkelijk aanmaken van de tickets.

5.4 De Google Apps Education Edition Agreement en privacy

De terminologie die wordt gehanteerd in de door de Open Universiteit met Google afgesloten Google Apps Education Edition Agreement is niet toegespitst op toepasselijkheid van de Wbp. In de overeenkomst wordt namelijk niet verwezen naar de begrippen ‘verantwoordelijke’ (data controller) en ‘bewerker’ (data processor). Ook staat niet vermeld dat de Wbp van toepassing is. Een dergelijke verwijzing dan wel bepaling is overigens ook geen voorwaarde voor toepasselijkheid van de Wbp.

[69] Kamerstukken II, 25892, nr. 3 p. 10.

In de Google Apps Education Edition Agreement is slechts in algemene zin bepaald (artikel 2.2) dat binnen de toepasselijke wettelijke kaders, Google het recht verkrijgt om gegevens op te slaan en te verwerken in de Verenigde Staten dan wel enige andere jurisdictie waar Google faciliteiten heeft of gebruikt. Dit op voorwaarde dat deze faciliteiten voldoen aan de beveiligings- en privacynormen die niet minder bescherming bieden dan de betreffende normen welke worden toegepast op de eigen informatie van Google (art. 2.2). Door gebruik te maken van de `Services` stemt de Open Universiteit in met de hiervoor bedoelde overdracht, opslag en verwerking van gegevens.

Op de dienstverlening aan de Open Universiteit is de Google Privacy Policy van toepassing. In dat document is onder meer nader omschreven welke informatie door Google wordt verzameld, voor welke doeleinden dit gebeurt, en met welke derden (en onder welke voorwaarden) persoonsgegevens worden gedeeld. Voorts bevat de Google Privacy Policy bepalingen over onder andere informatiebeveiliging en de voorwaarden voor het corrigeren en verwijderen van persoonsgegevens.

Op grond van de overeenkomst is de Open Universiteit verplicht de privacy van de eindgebruikers te beschermen door middel van een privacybeleid dat aan alle toepasselijke wet- en regelgeving voldoet en aan de eindgebruikers wordt gecommuniceerd (art. 3.1). Het is voorts de taak van de onderwijsinstelling om een aantal verplichtingen uit de overeenkomst door te geven aan de eindgebruikers (onder andere de ‘Acceptable Use Policy’) en voor zover vereist de instemming van de eindgebruikers met de toepasselijke wet- en regelgeving te verkrijgen.

Ten opzichte van studenten hanteert de Open Universiteit als beleid dat zij vooraf worden geïnformeerd over het feit dat de mail van de Open Universiteit wordt afgehandeld door Google. Daarbij wordt ook hun ondubbelzinnige toestemming gevraagd (opt-in). Indien een student bezwaren heeft kan hij ook een eigen (privé dan wel zakelijk) e-mailaccount blijven gebruiken. Door de Open Universiteit worden aan Google alleen de voorletters en achternaam van de studenten verstrekt.

In hoeverre de inhoud en uitvoering van door de Open Universiteit met Google gesloten overeenkomst volledig voldoet aan de toepasselijke regelgeving kan in het kader van dit onderzoek niet worden vastgesteld. Daarvoor is onder andere een nadere analyse nodig van de informatiestromen, de rollen van partijen, en de overige toepasselijke afspraken (waaronder het privacybeleid van Google en van de Open Universiteit). Zoals opgemerkt valt een dergelijke analyse buiten de scope van dit onderzoek.

6 Aandachtspunten en kritische noten

In dit laatste hoofdstuk vatten we de voorgaande hoofdstukken samen in een aantal aandachtspunten, gevolgd door wat kritische noten en punten voor nadere reflectie en onderzoek.

Aandachtspunten die van belang zijn bij het afnemen van Clouddiensten:

- Het in kaart brengen van de rolverdeling tussen de partijen betrokken bij Cloud Computing is van groot belang. Verantwoordelijke is degene die doel en middelen van verwerking vaststelt. Bewerkers verwerken persoonsgegevens in opdracht van de verantwoordelijke.
- Van belang is derhalve om te bepalen door wie, op gezag van wie, met welk doel en met welke middelen door wie bepaald, gegevens worden verwerkt? Zowel de rollen als de doelen en middelen zullen uitdrukkelijk en duidelijk vastgelegd moeten worden.
- De complexiteit van de rolverdeling en belegging van verantwoordelijkheden in Cloud Computing is een heikel punt door de complexiteit van de arrangementen.
- Rechten en plichten die voortvloeien uit de Wbp gelden voor verantwoordelijken die tevens moeten garanderen dat de door hen ingeschakelde bewerkers deze wet naleven. Wie met betrekking tot welke verwerking verantwoordelijke, bewerker of derde is, is dus van groot belang.
- Uit de Wbp vloeit voort dat de doeleinden voor verwerking welbepaald, uitdrukkelijk omschreven en gerechtvaardigd moeten zijn. De bij Cloud Computing betrokken partijen zullen de doeleinden voor verwerking dus gedetailleerd schriftelijk vast moeten leggen.
- Een Nederlandse entiteit die gebruik wil maken van een Cloud Service is doorgaans een verantwoordelijke in de zin van de Wbp. Voor zover een Cloud Computing Service Provider zelf doel en middelen voor een verwerking vaststelt (bijv. marketing) is de CCSP met betrekking tot deze verwerking verantwoordelijke.
- De vestigingslocatie van de verantwoordelijke is bepalend voor het antwoord op de vraag of de Wbp, of enig ander nationaal EU-gevensbeschermingsrecht van toepassing is.
- Voor zover een Nederlandse entiteit, zijnde een verantwoordelijke, gebruik maakt van een Cloud Service, dan is deze entiteit gebonden aan de Wbp, ongeacht de locatie van de gegevens.
- De lokatie waar gegevens worden verwerkt of opgeslagen is niet bepalend voor het toepasselijke gegevensbeschermingsrecht, maar de vestigingsplaats van de verantwoordelijke of gebruik van middelen (waaronder cookies) op NL/EU-grondgebied ter verwerking van persoonsgegevens wel.
- Een verantwoordelijke die gevestigd is buiten de EU en die, niet slechts voor doorvoer, gebruik maakt van al dan niet geautomatiseerde middelen binnen de EU is op grond van artikel 4 lid 2 Wbp gebonden aan deze wet. ´Geautomatiseerde middelen´ wordt dusdanig breed uitgelegd dat hieronder bijvoorbeeld ook cookies vallen. Diensten die via de webbrowser worden benaderd zijn bijna ondenkbaar zonder cookies waardoor de Wbp veelal van toepassing zal zijn op CCSP´s voor wat betreft de diensten die zij verlenen aan Nederlandse onderwijsinstellingen. Derhalve vallen vrijwel alle Cloud services aangeboden door partijen buiten de EU onder de EU dataprotectieregelgeving.
- De locatie van opgeslagen gegevens kan ook een rol spelen in het kader van toepasselijke vorderingsrechten van buitenlandse autoriteiten.
- De USA PATRIOT-Act is alleen geldig in de VS, en heeft geen betrekking op Europa.
- Echter, wanneer in de VS data- en communicatieverkeer gescand of gesurveilleerd wordt, kan ook “Europese data” in die surveillance wordt betrokken omdat die data op Amerikaanse servers staat.

- Als een CCSP data opslaat in een niet EU land bestaat het risico dat lokale wetgeving lokale autoriteiten een recht tot toegang tot die data geven. Alleen al vanuit een oogpunt van handhaving en toezicht zal het lastig zijn dit tegen te gaan.
- Vraag is echter hoe groot dit risico is, hoe groot de gevolgen zijn als het risico zich manifesteert en in hoeverre de risico´s en gevolgen zwaarder moeten wegen dan de voordelen om te kiezen voor een CCSP die data buiten Europa opslaat. De risico´s bij het uitbesteden van studenten mail en data opslagvoorzieningen zullen geringer zijn dan bij het uitbesteden van medewerkers mail en opslagvoorzieningen, bijvoorbeeld met het oog op (geheime) onderzoeksresultaten en bedrijfsgeheimen.
- De Safe Harbor principles liggen momenteel zwaar onder vuur: het lijkt een dode letter en biedt derhalve geen bescherming voor EU burgers.
- Wanneer de Nederlandse entiteit persoonsgegevens doorgeeft aan een CCSP blijft zij, ongeacht de locatie van die CCSP, verantwoordelijk voor de verwerking van persoonsgegevens waarvoor zij doel en middelen heeft vastgesteld en moet zij ervoor zorg dragen dat de relevante regelgeving met betrekking tot die gegevensverwerking wordt nageleefd, ook door de CCSP die als bewerker is aan te merken.
- Wanneer een Europese entiteit te maken heeft met een buitenlandse CCSPs die persoonsgegevens zal (laten) verwerken in derde landen zonder passend beschermingsniveau is het verstandig om essentiële gegevensbeschermingsregels in het contract op te nemen zodat deze via de contractuele weg ook in het buitenland juridisch afdwingbaar zijn.
- Contracten spelen daarmee in Cloud Computing configuraties een zeer belangrijke rol.
- In hoeverre een CCSP met betrekking tot persoonsgegevens van de onderwijsinstelling ´eigen´ verwerkingen uit mag voeren (bijvoorbeeld het omwerken van deze gegevens tot groepsprofielen voor marketing), hangt af van de contractuele relatie tussen onderwijsinstelling en de CCSP. De relatie tussen en bevoegdheden van onderwijsinstelling en CCSP moeten dus gedetailleerd contractueel geregeld worden.
- Aangezien CCSPs over het algemeen grote en machtige partijen zijn, kan verenigen van onderwijsinstellingen mogelijk de positie van de (gezamenlijke) onderwijsinstellingen ten opzichte van CCSPs versterken waardoor betere privacy bescherming kan worden onderhandeld.
- Onderwijsinstellingen zullen veelal als verantwoordelijke aangemerkt kunnen worden, en daarmee gebonden zijn aan de rechten en plichten die voortvloeien uit de Wbp.
- De CCSP zal zoveel mogelijk verantwoordelijkheden uitsluiten, of deze beleggen bij de onderwijsinstelling, met name plichten die volgen uit de relatie onderwijsinstelling-eindgebruiker: bijvoorbeeld toestemming van student (ouder) verkrijgen voor bepaalde verwerkingen.
- Contracten kunnen echter de rechten en plichten uit de Wbp niet terzijde schuiven.
- Ook de verantwoordelijkheid voor het gebruik van Clouddiensten door eindgebruikers (studenten) kan door CCSPs contractueel worden ´neergelegd´ bij de onderwijsinstellingen: scholing en richtlijnen over hoe studenten de Clouddiensten al dan niet mogen gebruiken zijn dus van wezenlijk belang.
- Verantwoordelijken moeten bedacht zijn op de bijkomende regels die gelden wanneer bijzondere gegevens verwerkt worden, of wanneer gegevens doorgegeven worden naar derde landen.
- Voor eindgebruikers, zoals studenten en medewerkers, geldt dat ook zij onder omstandigheden verantwoordelijke kunnen zijn voor de verwerking van persoonsgegevens (bijv. voor zover de inhoud van hun e-mails persoonsgegevens betreffen). Voor hen zal uit een door de onderwijsinstelling opgestelde gedragscode moeten blijken hoe zij van de Clouddiensten gebruik mogen maken (hieruit moeten de gerechtvaardigde doeleinden voor verwerking van gegevens door studenten/medewerkers kunnen worden afgeleid).

- Het is verstandig in dergelijke gedragscodes uitdrukkelijk ook de consequenties op niet naleven van deze gedragscode op te nemen (zie rapport rechtmatig operationeel handelen uitgevoerd in opdracht van SURF)

6.1 Complexiteit van de rolverdeling

Allereerst ligt de complexiteit van Cloud Computing, in verhouding tot het recht op gegevensbescherming, in het feit dat de exacte rolverdeling tussen entiteiten zoals de eindgebruiker, de instelling, de CCSP en SURFfederatie/Entree lastig vast te stellen is. Wie in een bepaald scenario respectievelijk betrokkene, bewerker en verantwoordelijke is, is steeds afhankelijk van de contractuele verhoudingen en het feitelijke dataverkeer. In een contract kan worden afgesproken wie welke functie vervult. Daarin kan worden gespecificeerd welke partij de doelen en middelen voor de verwerking van persoonsgegevens vaststelt, en welke partij gegevens slechts verwerkt in opdracht van de verantwoordelijke.
Echter, de feitelijke situatie is altijd leidend en bepalend met betrekking tot de vraag wie welke rol in Cloud Computing vervult. Bijvoorbeeld, als in een contract tussen een onderwijsinstelling en Google, wordt afgesproken dat Google slechts bewerker is, maar Google vervolgens wel zelf bepaalde handelingen met de verkregen persoonsgegevens (verwerken) uitvoert waarvoor Google doel en middelen vaststelt, bijvoorbeeld voor marketing, is Google hiervoor, ongeacht het contract met de onderwijsinstelling waarin Google als bewerker bestempeld wordt, voor deze ´eigen´ verwerking de verantwoordelijke.
Dat de rolverdeling alras complex wordt, laat zich eenvoudig illustreren aan de hand van het gebruik van onderwijsapplicaties van Google[70] door studenten. Voor zover in het contract niets anders is bepaald, zal de onderwijsinstelling doorgaans de verantwoordelijke zijn voor de verwerking van persoonsgegevens met betrekking tot de studenten. De student zelf is verantwoordelijke ten aanzien van de inhoud van hetgeen hij of zij op de Clouddienst plaatst. Google is slechts bewerker, voor zover zij zelf niets anders met de data doet dan waartoe opdracht is gegeven door de verantwoordelijken. Google geeft immers slechts de data weer, maar bepaalt niet het doel en de middelen van de verwerking van persoonsgegevens. Waar door onderwijsinstellingen gebruik wordt gemaakt van SURFfederatie/Entree, zal de instelling ten aanzien van de persoonsgegevens van studenten verantwoordelijke zijn, en SURFfederatie/Entree de bewerker. SURFfederatie bewerkt die gegevens namelijk alleen in opdracht van de onderwijsinstelling en zorgt voor authenticatie en toegang tot de aangesloten Clouddiensten. Het hiervoor geschetste voorbeeld is een mogelijke rolverdeling, maar welke partij welke rol vervult zal steeds afhangen van de concrete situatie. Kleine wijzigingen binnen de feitelijke situatie, kunnen mogelijk grote gevolgen hebben voor de rolverdeling en de verantwoordelijkheden betreffende de verwerking van persoonsgegevens. Wanneer bijvoorbeeld de dienstverlening van SURFfederatie/Entree in de toekomst uitgebreider zal worden dan enkel authenticatie en identificatie, zal mogelijk naast de rol van bewerker, tevens een rol als verantwoordelijke ontstaan. Om deze rolverdeling helder te krijgen zal dus per specifiek geval bekeken moeten worden naar de contractuele verhoudingen, de feitelijke situatie en de in het geding zijnde gegevensverwerkingen.

[70] Voor Google mag ook Microsoft worden gelezen, dat doet aan het voorbeeld weinig af.

6.2 Open vragen

Eerder hebben we gewezen op de mogelijkheden die buitenlandse overheden hebben om gegevens te vorderen, met als voorbeeld de Amerikaanse overheid die op basis van de USA PATRIOT-act[71] gegevens kan opvorderen zonder gerechtelijk bevel, althans met beperkte gerechtelijke toetsing[72], zonder toestemming of wetenschap van betrokkene, en in bepaalde gevallen zelfs zonder geconcretiseerd doel.[73] De USA PATRIOT-act gaat weliswaar over het opvorderen van verkeersdata, maar in bepaalde gevallen kan ook de inhoud van communicaties worden gescreend en bovendien moet worden aangetekend dat verkeersgegevens ook persoonsgegevens kunnen zijn of bevatten, denk aan IP-adres en e-mail adres.

Betoogd is dat de USA PATRIOT-Act alleen geldig is in de VS, en geen betrekking heeft op Europa. Desalniettemin kan het zo zijn dat wanneer in de VS data- en communicatieverkeer volgt, ook data van Europese burgers in die surveillance wordt betrokken omdat die data op Amerikaanse servers staat of middels dergelijke servers wordt verwerkt.

De vraag is vervolgens of een Europese entiteit die een Cloud Service wil afnemen van een Amerikaanse CCSP die Europese persoonsgegevens op zal slaan op Amerikaanse datacentra, het risico loopt dat die data ook gescand worden op basis van de USA PATRIOT Act. Zelfs als een Amerikaanse CCSP gegevens buiten de VS zou opslaan kan het zijn dat, omdat zij lokale wetten moeten naleven, ook die gegevens opgevorderd worden door de lokale overheid.

Voor verschillende klanten van Cloud Services zijn dergelijke overwegingen belangrijk. Een vraag die bijvoorbeeld door de Universiteit Utrecht is geopperd of de Amerikaanse overheid ook inzage kan krijgen in gegevens die in Europa staan op servers van Amerikaanse bedrijven. Als dat zo is maakt het weinig uit of wordt gekozen voor Microsoft die garandeert dat de gegevens van hun Europese Cloud klanten in de EU worden opgeslagen of Google die dit nadrukkelijk niet kan garanderen. Het valt buiten het blikveld van deze studie om hier een gedegen antwoord op te geven. Het lijkt de auteurs van dit whitepaper wenselijk om nader onderzoek te verrichten op dit thema.

Een oplossing voor deze jurisdictievraagstukken ligt mogelijk in het ontwikkelen danwel inzetten van een private Cloud voor het Nederlands onderwijs (leerlingen/studenten/docenten).

---

71 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001. Zie over de reikwijdte van de USA PATRIOT Act bijvoorbeeld Kollar (2004).

72 Electronic Privacy Information Center. Zie onder 'Pen Registers, the Internet and Carnivore'. Toegankelijk via: http://epic.org/privacy/terrorism/usapatriot/. Laatst geraadpleegd op 10 december 2010.

73 Electronic Privacy Information Center. Zie onder 'Liberalized Use of Pen Register/Trap and Trace Devices under FISA' en 'Multi-Point ("Roving Wiretap") Authority' Toegankelijk via: http://epic.org/privacy/terrorism/usapatriot/. Laatst geraadpleegd op 10 december 2010.

Literatuur

Article 29 Data Protection Working Party (2002) Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites (wp56), Adopted on 30 May 2002.

Article 29 Data Protection Working Party (2007) Advies 4/2007 over het begrip persoonsgegeven. 01248/07/NL, WP 136. Toegankelijk via: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_nl.pdf. Laatst geraadpleegd op 13 december 2010.

Article 29 Data Protection Working Party (2008) Opinion 1/2008 on data protection issues related to search engines (WP 148).

Article 29 Data Protection Working Party (2009) Opinion 5/2009 on online social networking, adopted on June 12, 2009, Brussels, Article 29 Data Protection Working Party

Artikel 29 Werkgroep (2010) WP169: Advies 1/2010 over de begrippen “voor de verwerking verantwoordelijke” en “verwerker”. Toegankelijk via: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_nl.pdf.

Balboni, P. (2010) Data Protection and Data Security Issues Related to Cloud Computing in the EU. ISSE 2010 Securing Electronic Business Processes - Highlights of the Information Security Solutions Europe Conference 2010: Tilburg Law School Research Paper No. 022/2010, p. 5-7. Toegankelijk via via: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1661437. Laatst geraadpleegd op 1 december 2010.

Catteddu, Daniele and Giles (eds.) Hogben (2009) Cloud computing – Benefits, risks and recommendations for information security, Heraklion: ENISA.

De Haes, A.U. (2010) Grootschalige privacyfraude tussen EU en VS. Webwereld.

Kollar, Justin L., USA PATRIOT Act, the Fourth Amendment, and Paranoia: Can They Read this While I’m Typing?, in: 3 J. High Tech. L. 67 (2004)

Kuczerawy, Aleksandra (2010) Facebook and its EU users - applicability of the EU data protection law to US based SNS. in: M. Bezzi, P. Duquenoy, S. Fischer-Hübner, M. Hansen and G. Zhang (eds.), Privacy and Identity Management for Life. 5th IFIP WG 9.2, 9.6/11.4, 11.6, 11.7/PrimeLife International Summer School, Nice, France, September 7-11, 2009, Revised Selected Papers: Springer, 75-85.

Leenes, R.E. (2010) Who controls the cloud? Verschijnt in IDP. REVISTA DE INTERNET, DERECHO Y POLÍTICA, nr. 11 2010, toegankelijk via: http://idp.uoc.edu/ojs/index.php/idp/.

Thole, E. (2010) Privacy en cloud computing: beveiliging van persoonsgegevens in de cloud. Informatie juli/augustus 2010, Legale kaders in cyberspace, p. 29. Te raadplegen via: http://www.van-doorne.com/Global/Publicaties/Privacy%20en%20cloud%20computing_Thole_Informatie%202010.pdf. Laatst geraadpleegd op 1 december 2010.