HoGent

Gegevensverkeer in de Cloud: mogen mijn persoonsgegevens worden opgeslagen in landen buiten Europa?

Femke Vanden Buverie

1 Inleiding

"*We want technology to advance, but timeless values should endure. And privacy is a timeless value that deserves to endure.*" [1] – Microsoft CEO Satya Vadella

Bovenstaande quote omsluit op bondige wijze de problematiek die geanalyseerd wordt in deze bachelorproef. Een wereld zonder technologie is ondenkbaar geworden. Voor de grote meerderheid onder ons vormt technologie een soort zesde zintuig gedurende het dagdagelijkse leven. Niet alleen op privégebied, maar ook professioneel is er het laatste decennium een enorme toevloed aan nieuwe technologieën merkbaar.

Bij toepassing van nieuwe technologieën, wordt er vaak gebruik gemaakt van persoonsgegevens om een gepersonaliseerde en optimale service ter beschikking te stellen. De insteek van deze bachelorproef ligt voornamelijk op het gebruik van Cloudservices. Door het gebruik van deze nieuwe toepassing bevinden zich een overvloed aan data 'in the Cloud'. Denk maar aan uw Gmail-account, gegevens op Dropbox, Google drive… Deze data moeten ergens worden opgeslagen. Bij deze opslag moet echter rekening worden gehouden dat kennis over data een vorm van macht uitmaakt. Gezien macht vaak misbruikt wordt, is controle noodzakelijk. Hoe wordt deze controle op een juridische manier benaderd?

Cloudservices dringen steeds meer door in het professionele leven. Deze bachelorproef werd dan ook geïnspireerd op het model van dé start-up van het jaar: *Teamleader*.[2] Dit softwarebedrijf richt zich op het ontwikkelen van een online applicatie voor CRM[3], projectmanagement en facturatie. Alle klantengegevens, bedrijfsgegevens, offertes en facturen bevinden zich in de Cloud. De efficiëntie waarmee een bedrijf op deze manier aan de slag kan gaan, stijgt op exponentiele wijze. Alle informatie over klanten, leveranciers en partners kunnen namelijk altijd, overal en vanop elk toestel geraadpleegd worden. *Teamleader* verleende een bron aan informatie over Cloudservices. Hun aanpak in de Cloudservice-sector wat betreft gegevensverkeer in de Cloud, vormde dan ook mijn uitgangspunt bij de opmaak van deze bachelorproef.

Ook de MKB Cloud Barometer toont een positieve trend aan bij implementatie van Cloudservices in de bedrijfswereld. MKB Cloud Barometer[4] is een jaarlijks onderzoek uitgevoerd door KPN en Exact bij wereldwijde KMO's over het gebruik van Cloudservices. Cijfers van deze peiling tonen in 2015 een vrij positieve houding van ondernemingen tegenover Cloud-oplossingen: 46 % van de onderzochte bedrijven maakt er gebruik van. Onder andere voor boekhouding, CRM, productie, voorraadbeheer & logistiek,

[1] B. SMITH, "The collapse of the US-EU safe harbour solving the new privacy rubiks cube", 20 oktober 2015, http://blogs.microsoft.com/on-the-issues/2015/10/20/the-collapse-of-the-us-eu-safe-harbor-solving-the-new-privacy-rubiks-cube/#sm.00000m5kprxfqgdqyrm04o3furzkd (geconsulteerd op 10 april 2016).
[2] Teamleader werd verkozen in februari 2016 tot dé start-up van het jaar op de Tech Startup Day.
[3] Customer Relationship Management. Dit is klantrelatiebeheer waarbij het optimaliseren van het contact met de klant centraal staat. Alle interacties met de klant worden hierbij geregistreerd en geoptimaliseerd.
[4] Factsheet MKB Barometer 2015, http://static.exact.com/nl/pdf/Factsheet%20MKB%20Cloud%20Barometer%202015.pdf (geconsulteerd op 15 maart 2016).

orderverwerking & facturatie, salarisadministratie en projectmanagement zijn Cloud-toepassingen in de bedrijfswereld een nieuwe mogelijkheid. Tevens blijkt uit de MKB Cloud Barometer dat er een sterke correlatie op te merken is tussen Cloud-implementatie en het groeicijfer. KMO's die drie of meer Cloud-toepassingen gebruiken, genereren gemiddeld 20% meer groei dan bedrijven die kiezen voor de klassieke offline programma's.

En toch… Sommige bedrijven zijn nog steeds niet overtuigd van het gebruik van Cloudservices. Bij navraag naar de aanleiding van deze weigerachtige mening, komen een aantal mythes over het Cloudgebruik naar de voorgrond: de Cloud is onbetrouwbaar, de Cloud is onveilig, de Cloud is in strijd met privacywetgeving.

Mijn opzet is om in deze bachelorproef bovenstaande mythes te ontkrachten door Cloudservices op een juridisch gefundeerde wijze te benaderen. De specifieke rechtsvraag die het onderwerp vormt van deze bachelorproef kan als volgt worden omschreven: **"*Gegevensverkeer in de Cloud: mogen mijn persoonsgegevens worden opgeslagen in landen buiten Europa?*".**

Privacy wordt namelijk wereldwijd op een verschillende wijze benaderd. In de Europese Unie geldt er een streng beschermingsniveau. De onthullingen van Snowden en het PRISM-afluisterschandaal zijn slechts voorbeelden waaruit bijvoorbeeld blijkt dat Amerika anders omgaat met privacy van persoonsgegevens. Kan het dat Europese gegevens opgeslagen worden in Amerika, zonder garantie op een (hoog) beschermingsniveau op vlak van privacy? Is de oversteek van een landsgrens een factor van verlies aan privacy wat betreft dataverkeer?

Deze vraagstelling was gedurende de opmaak van deze bachelorproef op Europees niveau een 'hot topic'. Onderhandelingen lagen op tafel en wijzigingen werden doorgevoerd. Dit zorgde ervoor dat dit onderwerp een tastbaar gegeven vormde voor mij. De stand van zaken in de media werd steeds verwerkt en deze bachelorproef is dan ook een poging om een up-to-date weergave te bieden over dit thema.

Het eerste luik van deze bachelorproef bestaat uit de omschrijving van Cloudcomputing. Dit is een term die iedereen wel reeds heeft gehoord, maar een strikte omschrijving is noodzakelijk voor een correct beeld over Cloudservices. Daarnaast wordt ook het wettelijk kader waarbinnen Cloudservices kunnen omgaan met persoonsgegevens gestructureerd weergegeven.

Het tweede luik bespreekt de effectieve doorgifte van persoonsgegevens. Zowel doorgifte van persoonsgegevens naar landen binnen de Europese Unie, als doorgifte van deze gegevens naar landen buiten de Europese Unie worden besproken. De verschillende mogelijke manieren om deze doorgifte op een juridisch correcte manier te laten verlopen, worden steeds getailleerd weergegeven.

Ten slotte ligt de klemtoon van deze bachelorproef op de doorgifte van persoonsgegevens naar de Verenigde Staten. Deze doorgifte kreeg mijn persoonlijke voorkeur, aangezien er de laatste maanden veel op til is over deze doorgifte. De Verenigde Staten hebben een andere visie op privacy en persoonsgegevens dan binnen de Europese Unie. De laatste maanden

werd er op Europees niveau dan ook sterk onderhandeld met de Verenigde Staten over een EU-VS Privacy Shield die de doorgifte van persoonsgegevens tussen beide zal reguleren. Deze recente insteek wordt verwerkt in het laatste deel van deze bachelorproef.

Dankzij de samenwerking met mijn stagebedrijf deJuristen is de opmaak van deze bachelorproef positief geëvolueerd. DeJuristen heeft een grote expertise in ICT-recht, waaronder de privacybescherming van verwerking van persoonsgegevens. De opmaak van privacy policies behoort voor hen dan ook tot één van hun kerntaken.

Ook het bijwonen van het seminarie '*Legal update: overzicht van nieuwe en toekomstige regels inzake privacy en consumentenbescherming bij e-commerce*', gebracht door Dhr. Van den Brande (advocaat – partner Sirius Legal)[5] op de Shopping Innovation Expo 2016, werd als uitgangsbasis genomen voor de uitwerking van dit thema.

Ik hoop dat ik bij u, als lezer, eenzelfde interesse kan opwekken als degene die ik voor dit onderwerp voel. Het is een thema dat niet meteen tijdens de opleiding Rechtspraktijk aan bod kwam, maar op basis van de aangeleerde competenties van de voorbije jaren probeerde ik mijn eigen weg te vinden in de wetgeving, rechtsleer en rechtspraak over Cloudservices en meer in het bijzonder doorgifte van persoonsgegevens. Deze bachelorproef vormt dan ook een mooi sluitstuk van mijn opleiding Rechtspraktijk.

[5] Meester Van den Brande heeft een uitgebreide expertise opgebouwd in media- en reclamerecht, marktpraktijken en consumentenbescherming, intellectuele eigendomsrecht, internet en e-commerce, privacy- en databescherming, IT, softwareontwikkeling en kansspelenwetgeving.

2 Organisatie op wolkjes[6]

2.1 Wat is Cloudcomputing?

Cloudcomputing is een computermodel waarbij de gebruiker een toegangsrecht verkrijgt tot toepassingen (bv. CRM, applicaties, data,…) en gegevens die opgeslagen zijn door de Cloud-leverancier in zwaarbeveiligde datacentra. De gegevens worden aldus niet op traditionele wijze bij de gebruiker op zijn server bewaard, maar bevinden zich ergens in de *internetwolk*. Een specifiek aanwijsbare server kan aldus niet aangeduid worden. De gegevens kunnen namelijk in diverse datacenters van de leverancier over de wereld verwerkt worden.

Er bestaan over het algemeen drie modellen voor Cloudservices. Vooreerst geeft het model ***Infrastructure as a Service*** (IaaS) de leverancier louter toegang tot servers. De gebruiker kan dan zijn eigen software daarop installeren. Bekende IaaS-providers zijn bijvoorbeeld Rackspace en Amazon Web Services. Het tweede mogelijke model ***Platform as a Service*** (PaaS) verleent de Cloudserviceleverancier toegang tot een ontwikkelingsomgeving waardoor de gebruiker op een snelle en efficiënte manier eigen applicaties kan ontwikkelen. Google App Engine is een voorbeeld van het tweede type. Ten slotte geeft het model ***Software as a Service*** (SaaS) de gebruiker toegang tot enkele reeds ontwikkelde applicaties of programma's. Een dure softwarelicentie is dus overbodig geworden. Dit is dan ook de meest gebruikte vorm van Cloudcomputing. Hieronder valt bijvoorbeeld ook Gmail. Deze bachelorproef werd overigens opgesteld met ondersteuning van *Teamleader,* die gebruik maakt van dit laatste model om een CRM-programma ter beschikking te stellen aan hun klanten.[7]

2.2 Het succes van Cloudcomputing

Waarom is Cloudcomputing, een nieuwe vorm van organisatie, nu zo begeerd in de moderne bedrijfswereld? Vooral de ruime beschikbaarheid van de applicatie en de gegevens kan aanzien worden als het grootste voordeel. Aangezien de diensten via internet verleend worden, zijn de toepassingen en data overal beschikbaar. Een loutere internetverbinding op uw personal computer, smartphone of tablet volstaat om aan de slag te gaan. Verder is ook het gebruiksgemak een belangrijke factor om overtuigd te geraken van de voordelen van Cloudcomputing. Updates, upgrades en beveiliging van de systemen en gegevens behoren namelijk volledig tot de taak van de Cloudservice-verlener.[8] Bovendien biedt een

[6] B. DOCQUIR, "Cloud computing of "virtuele informatica": gegevensbescherming staat centraal in de contractuele relatie", *Cah. Jur.* 4/2011, 105-117.

[7] Teamleader verleende een bron aan informatie over Cloudservices. Hun aanpak in de Cloudservice-sector vormde het uitgangspunt bij de opmaak van deze bachelorproef.

[8] E. VALGAEREN en S. COSTERMANS, *Grenzeloze advocatuur: obstakels worden uitdagingen*, Brugge, 2012, Die Keure, 188.

Cloudservice verregaande mogelijkheden om online samen te werken aan documenten. Iedereen kan op ieder moment documenten of data opvragen. Dit is voor een bedrijf vaak een grote efficiëntiewinst.

In contrast met de traditionele opslag van persoonsgegevens op je eigen server, gebeurt de opslag in de Cloud vaak simultaan op verschillende servers over de ganse wereld. Het is dan niet ondenkbaar dat persoonsgegevens ook bewaard en verwerkt worden op servers die de landsgrenzen overschrijden. Dit is nu net het knelpunt dat in deze bachelorproef besproken zal worden. Wat is de privacybescherming van persoonsgegevens bij doorgifte van gegevens naar derde landen?

3 Wettelijk kader

Het is van belang om een ruim juridisch kader te schetsen rond de bescherming van persoonsgegevens. Zowel nationaal als binnen de Europese Unie zijn er waarborgen rond de doorgifte van persoonsgegevens. Deze wetgevende initiatieven vormen de basis voor de grenzen die gesteld worden aan de overdracht van deze gegevens aan landen buiten Europa.

3.1 Bescherming van persoonlijke levenssfeer - Grondwettelijke bescherming

De bescherming van persoonsgegevens wordt niet expliciet opgenomen als grondrecht in de Belgische Grondwet. Eventuele grenzen die gesteld moeten worden aan de verwerking van deze gegevens kunnen aldus niet op letterlijke wijze in de Grondwet gelezen worden. Dit betekent evenwel niet dat er een juridisch vacuüm is op grondwettelijk vlak. De grenzen aan de verwerking van persoonsgegevens kaderen namelijk in het recht op eerbiediging van privéleven.[9] Elk individu moet beschermd worden in zijn privésfeer om zijn ontwikkeling en ontplooiing mogelijk te maken.[10] De verwerking van persoonsgegevens moet voldoen aan deze eerbiediging. Een grondwettelijke basis lijkt op het eerste zicht afwezig, maar kan onrechtstreeks in artikel 22 van de Grondwet teruggevonden worden.

3.2 Bescherming van persoonlijke levenssfeer - Europese rechtsorde

I. Artikel 8 EVRM

Op Europees niveau wordt in het Europees Verdrag voor de Rechten van de Mens niet expliciet in een artikel voorzien over de verwerking van persoonsgegevens. Toch kan hier eveneens verwezen worden naar de eerbiediging van het privéleven, opgenomen in artikel 8 EVRM. Uit de lezing van dit artikel kan besloten worden dat dit recht bedoeld is voor de bescherming van privéleven van de burgers ten aanzien van de overheid. Toch wordt algemeen aanvaard dat deze bescherming ook geldt in private relaties onderling.[11] Verder is de toetreding van de Europese Unie tot het EVRM door het Verdrag van Lissabon[12] niet van gering belang. Hierdoor zal de uitlegging van artikel 8 EVRM door het Europees Hof van de Rechten van de Mens binnen de Europese Unie een cruciale rol spelen. De Europese Unie is

[9] Artikel 22 Gw.
[10] Arbitragehof 21 december 2004, nr. 202/2004, *BS* 6 januari 2005.
[11] F. SCHRAM, *Verwerking van persoonsgegevens*, Brussel, Politea, 2013, 22.
[12] Artikel 6, tweede lid verdrag van Lissabon van 13 december 2001, *Pb.L.* 17 december 2007, C306.

op vlak van privacybescherming van data een voortrekker en wil voor de Europese burgers op basis van een juridisch kader dan ook strenge waarborgen verlenen.

3.3 Bescherming van persoonsgegevens – Dataprotectierichtlijn

De bescherming van de persoonlijke levenssfeer uit artikel 8 EVRM vormt wel een wetgevend kader voor de bescherming van persoonsgegevens, maar dit artikel laat ruimte voor het verplaatsen van persoonsgegevens naar *datahavens* waar geen of een minder verregaande bescherming geldt dan de nationale bescherming. Zowel de Europese Raad[13] als de OESO[14] namen initiatief om dit hiaat in de wetgeving op te vullen en liggen dus aan de basis van Europese en internationale regelgeving over de verwerking van persoonsgegevens.

De dataprotectierichtlijn 95/46/EG is het uiteindelijke resultaat voor de bescherming van persoonsgegevens op Europees niveau.[15] Deze richtlijn had als doel harmonisatie door te voeren van de verschillende nationale wetgevende initiatieven met betrekking tot de verwerking van persoonsgegevens. België voldeed aan deze omzetting door de verder vermelde wet van 8 december 1992 grondig te hervormen en in overeenstemming te brengen met de dataprotectierichtlijn.[16]

Recht is echter een steeds evoluerend gegeven. Midden december 2015 werd er consensus bereikt over een nieuwe Europese Privacyverordening.[17] Deze verordening zal bovenvermelde dataprotectierichtlijn vervangen. De dataprotectierichtlijn werd opgemaakt in een periode waar Cloudcomputing, sociale netwerksites en locatie gebaseerde diensten nog in hun kinderschoenen stonden. Een modernisering was dan ook een noodzakelijkheid. Opmerkelijk is dat op Europees niveau niet geopteerd wordt voor een nieuwe richtlijn, maar voor een verordening. Hiermee stuurt de Europese Unie het signaal dat de verschillende omzettingen op nationaal niveau geen geharmoniseerd geheel vormen. De nieuwe verordening zal daarentegen rechtsreeks toepasselijk zijn in alle Europese lidstaten, dit zonder een omzetting in nationaal recht. De voornaamste wijzigingen zijn het recht op vergetelheid, 'data portability'[18], ondubbelzinnige toestemming voor verwerking persoonsgegevens, verdergaande verplichtingen voor ondernemingen, werkwijze bij datalekken,…

[13] Verdrag van de Raad van Europa van 28 januari 1981 tot bescherming van personen ter zake van de geautomatiseerde verwerking van persoonsgegevens, *Intern. Legal Mater*., 1981, 317, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37 (geconsulteerd op 3 maart 2016).
[14] OESO, *Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data*, OESO, 1980, http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf (geconsulteerd op 3 maart 2016).
[15] Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de verwerking van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, *Pb.L.* 23 november 1995, afl. 281, 31-50.
[16] Wet van 11 december 1998, *BS* 3 februari 1999.
[17] R. SCHOEFS, "Witte rook voor nieuwe privacyverordening", *Juristenkrant*, nr. 321, 2016, 16.
[18] Data portability verwijst naar de mogelijkheid om data te verplaatsen of te kopiëren naar andere databases of opslagplaatsen.

Verder is het ook opmerkelijk dat alle bedrijven, die binnen de Europese Unie diensten verlenen, onder het toepassingsgebied van de verordening vallen. Dit in tegenstelling tot de huidige richtlijn waar het vestigingscriterium van belang was voor de toepassing binnen de Europese Unie. Door de uitbreiding van het toepassingsgebied zal de verordening minder snel ontlopen kunnen worden door bedrijven die buiten de Europese Unie gevestigd zijn, maar binnen de Europese Unie operationeel zijn. De mate van rechtsafdwinging van dit ruim toepassingsgebied is evenwel nog een groot vraagteken.[19]

De nieuwe verordening werd op 14 april 2016 goedgekeurd door het Europees Parlement en zal over twee jaar in werking treden. Cloudservice verleners zullen tegen 2018 de nodige maatregelen moeten nemen om in overeenstemming te zijn met deze nieuwe regelgeving. Het niet-respecteren van deze verordening kan aanleiding geven tot geldboetes tot 20 miljoen euro of 4 procent van de jaarlijkse wereldwijde omzet. Deze nieuwe evolutie in het wetgevend kader rond privacy en dataverkeer is zeker de vermelding waard, maar verder ga ik hier niet op in aangezien dit op huidig moment nog niet van kracht is.

3.4 Wet 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens[20]

Zoals reeds eerder aangegeven, zette België de Dataprotectierichtlijn om in nationaal recht door middel van de Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (Verder: Wet Verwerking Persoonsgegevens). Aangezien deze op heden nog van toepassing is tot dat de nieuwe dataprotectieverordening in werking treedt, is het van belang om hieruit enkele belangrijke elementen te kaderen voor een goed begrip van de onderzoeksvraag van deze Bachelorproef.

Wat wordt er bedoeld met persoonsgegevens? Wanneer is er sprake van doorgifte van deze gegevens? Welke rechten hebben de betrokkenen met betrekking tot hun persoonsgegevens?

I. Persoonsgegevens

Het is van belang om de term 'persoonsgegevens' duidelijk te omschrijven. Op die manier is het duidelijk welke data aan eventuele transferbeperkingen onderworpen zijn. Uit de lezing van artikel 1,§ 1 Wet Verwerking Persoonsgegevens kan afgeleid worden dat dit een ruim

[19] Seminarie "Legal update: overzicht van nieuwe en toekomstige regels inzake privacy en consumentenbescherming bij e-commerce" Shopping Innovation Expo 2016 door B. VAN DEN BRANDE oprichtend vennoot Sirius Legal.

[20] Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, *BS* 18 maart 1993.

begrip is. Zowel teksten, beelden als geluiden vallen onder het toepassingsgebied. De belangrijkste voorwaarde is dat de gegevens kunnen leiden tot de identificatie van een **natuurlijk persoon** (criterium van identificeerbaarheid). Gegevens die louter betrekking hebben op vennootschappen of verenigingen zijn aldus niet onderworpen aan de Wet Verwerking Persoonsgegevens.

Het criterium van identificeerbaarheid is niet steeds een zwart-wit redenering. Wanneer er een uitgebreid aanbod aan persoonsgegevens beschikbaar is, staat de term niet ter discussie. Bijvoorbeeld: naam, adres, geboortedatum. Hier is dan duidelijk sprake van persoonsgegevens. In tegenstelling tot dit voorbeeld is er bij geanonimiseerde gegevens geen sprake van verwerking van persoonsgegevens, aangezien niemand geïdentificeerd kan worden. Tussen deze twee extreme gevallen, ligt er een waaier aan gevallen waar het niet altijd even duidelijk is of er sprake is van persoonsgegevens in de strikt zin van de wet. Hierbij zal steeds een praktische afweging gemaakt moeten worden. De beoordeling in de rechtspraak gebeurt vaak aan de hand van het criterium dat *iemand* nog in staat is om, met welk redelijkerwijs inzetbaar middel ook, te achterhalen op welk individu de informatie betrekking heeft.[21]

Een mooi voorbeeld hiervan is het IP-adres die verbonden is met een Belgische computer. Dit IP-adres laat over het algemeen niet toe om de persoonsgegevens van een internetgebruiker te bepalen door een doorsnee persoon. De internet service provider die het IP-adres heeft verleend, is met redelijke middelen echter wel in staat om de gebruiker te identificeren. Dit is voldoende om een IP-adres als een persoonsgegeven te kunnen beschouwen.

Verder spreekt de Commissie voor de bescherming van de persoonlijke levenssfeer (verder: Privacy Commissie)[22] zich geregeld uit over specifieke gevallen waarbij al dan niet gesproken kan worden over persoonsgegevens. Zo werd bijvoorbeeld onlangs, in het kader van de opmaak van wetgeving omtrent drones, beslist dat gegevens die opgenomen worden door een drone als persoonsgegevens kunnen worden beschouwd.[23]

II. Verwerking en doorgifte van persoonsgegevens

Naast de definiëring van de term persoonsgegevens, moet ook de draagwijdte van de bewerkingen van deze persoonsgegevens onderzocht worden.

[21] Memorie van Toelichting bij het wetsontwerp tot omzetting van de richtlijn 95/46/EG van 24 oktober 1995 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrij verkeer van die gegevens, *Parl.St.* Kamer 1997-98, nr. 1566/1, 12.
[22] Artikel 23ev. Wet Verwerking Persoonsgegevens.
[23] Commissie voor de Bescherming van de Persoonlijke Levenssfeer, Advies nr 32/2015 van 22 juli 2015 https://www.privacycommission.be/sites/privacycommission/files/documents/advies_32_2015.pdf (geconsulteerd op 4 april 2016).

Onder het toepassingsgebied van de Wet Verwerking Persoonsgegevens valt:

"Elke bewerking of elk geheel van bewerkingen met betrekking tot persoonsgegevens, al dan niet uitgevoerd met behulp van geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, ***bewaren****, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van* ***doorzending****, verspreiden of op enigerlei andere wijze ter beschikking stellen, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van persoonsgegevens."*[24]

Het louter opslaan of doorgeven van persoonsgegevens in het geval van Cloudservices, valt aldus onder dit toepassingsgebied.

In het *arrest Bodil Lindqvist t. Koninkrijk Zweden*[25] blijkt dat het Europees Hof van Justitie de term 'doorzenden' van persoonsgegevens vrij eng interpreteert.[26] Hierbij werd geoordeeld dat het plaatsen van persoonsgegevens op een website niet kan worden gekwalificeerd als een doorgifte van persoonsgegevens naar eventuele derde landen.

De argumenten van het Hof kunnen samengevat worden in drie hoofdelementen. (1) Indien het plaatsen van persoonsgegevens op een website als een doorgifte zou worden beschouwd, dan zou dit de werking van het internet volledig ondermijnen. (2) Om toegang te krijgen tot de gegevens op de desbetreffende website, moet een internetgebruiker niet alleen een internetverbinding hebben, maar is voor de raadpleging van de gegevens ook een handeling nodig van de internetgebruiker om de gegevens effectief op te vragen. Er is dus enkel sprake van een eventuele onrechtstreekse doorgifte. (3) teleologisch argument: bij de opmaak van de dataprotectierichtlijn heeft de wetgever niet stilgestaan bij de mogelijkheden die het internet bieden. Doorgifte heeft dus geen betrekking op persoonsgegevens op een website en kan probleemloos doorgevoerd worden.

III. Rechten van de betrokkene

Om een goed beeld te krijgen van het beschermingsniveau en de rechten die vanuit Europees niveau in het Belgisch recht geïmplementeerd zijn, wordt hieronder een kort overzicht gegeven van de rechten die de betrokkene bij de verwerking van zijn persoonsgegevens heeft. De nadruk van deze bachelorproef ligt evenwel op de doorgifte van persoonsgegevens naar landen buiten Europa. Met de kennis van het Europees beschermingsniveau voor verwerking van persoonsgegevens in het achterhoofd, kan evenwel een genuanceerder beeld geschetst worden bij het hoofdstuk over de doorgifte van persoonsgegevens naar landen met een minder verregaand beschermingsniveau dan dit binnen de Europese Unie. Het doel van de Europese Unie tijdens onderhandelingen over doorgifte van persoonsgegevens naar landen buiten Europa is vaak om een gelijkaardig

[24] Artikel 1, § 2 Wet Verwerking Persoonsgegevens.
[25] HvJ 6 november 2001, C101/01, Bodil Lindqvist/Koninkrijk Zweden.
[26] P. DE HERT en W. SCHREURS, "*De bescherming van persoonsgegevens op het internet: nuttige verduidelijking door de rechtspraak*", *AM* 2004/2, 127-137.

beschermingsniveau te implementeren van de Europese persoonsgegevens die verwerkt of opgeslagen worden in deze derde landen. Onderstaande drie rechten van de betrokkene zijn dé grote pijlers waarop het Europese systeem is gebaseerd.

(1) Recht op informatie

De verantwoordelijke voor de verwerking is verplicht om de betrokkene bepaalde informatie te verstrekken over de verwerking van zijn persoonsgegevens.[27]

Indien de gegevens rechtsreeks bij de betrokkene verkregen worden, moeten volgende gegevens ten laatste op het moment van de verwerking verschaft kunnen worden:[28]

- De naam en het adres van de verantwoordelijke voor de verwerking en, in voorkomend geval, diens vertegenwoordiger;
- De doeleinden van de verwerking
- Het bestaan van een recht om zich op verzoek en kosteloos tegen de voorgenomen verwerking van hem betreffende persoonsgegevens te verzetten, indien de verwerking verricht wordt met het oog op directe marketing;
- Bepaalde bijkomende informatie, tenzij dit niet nodig is om tegenover de betrokkene een eerlijke verwerking te waarborgen, met name: de ontvangers van de gegevens, het bestaan van een recht op toegang en op verbetering van de persoonsgegevens die op hem betrekking hebben.

Indien de persoonsgegevens verkregen worden van derden, dan geldt dezelfde informatieplicht, maar dan ten laatste te bezorgen op het moment van de registratie van de gegevens of uiterlijk op het moment van de eerste mededeling van de gegevens.[29] Dit is bijvoorbeeld het geval indien persoonsgegevens bekomen worden door het invullen van een enquête, waarbij de invuller de toestemming heeft gegeven om zijn gegevens door te geven aan ondernemingen die gelijkaardige producten of diensten aanbieden.

(2) Recht op inzage, verbetering en verhaal

De betrokkene heeft het recht om inzage te krijgen in de gegevens die een verantwoordelijke verwerkt.[30] Deze bepaling waarborgt een mededelingsrecht die ten allen tijde door de verwerker moet kunnen worden beantwoord. Naast dit mededelingsrecht heeft de betrokkene bovendien het recht om onjuiste persoonsgegevens, die betrekking op hem hebben, kosteloos te mogen verbeteren.[31] Tevens beschikt de betrokkene over een

[27] Artikel 9 Wet Verwerking Persoonsgegevens.
[28] Artikel 9, § 1 Wet Verwerking Persoonsgegevens.
[29] Artikel 9, § 2 Wet Verwerking Persoonsgegevens.
[30] Artikel 10 Wet Verwerking Persoonsgegevens.
[31] Artikel 12, eerste lid Wet Verwerking Persoonsgegevens.

verzetsrecht.[32] Dit houdt in dat de betrokkene zich kosteloos en zonder enige motivering tegen de voorgenomen verwerking van zijn persoonsgegevens kan verzetten. Naast deze grond, kan er ook verzet worden aangetekend op basis van zwaarwegende en gerechtvaardigde redenen.

(3) Bescherming tegen geautomatiseerde beslissingsvorming

Bij geautomatiseerde beslissingsvorming met betrekking tot persoonsgegevens had de wetgever zijn bedenkingen en werd gevreesd voor een *Big Brother-maatschappij* waarbij elke persoonlijke tussenkomst vermeden zou worden. Artikel 12*bis* Wet Verwerking Persoonsgegevens is een veruitwendiging van deze vrees: "*Een besluit waaraan voor een persoon rechtsgevolgen verbonden zijn of dat hem in aanzienlijke mate treft, niet louter mag worden genomen op grond van een geautomatiseerde gegevensverwerking die bestemd is om bepaalde aspecten van zijn persoonlijkheid te evalueren*."

Om dit artikel te kaderen kan gedacht worden aan de berekening van belastingen. Dit gebeurt op basis van een geautomatiseerd systeem van verwerking van persoonsgegevens, maar een menselijke tussenkomst is steeds vereist. Dit kan dan bijvoorbeeld onder de vorm van een *a posteriori* menselijke controle waarbij de juistheid van de uitkomst wordt nagezien.

[32] Artikel 12, tweede lid Wet Verwerking Persoonsgegevens.

4 Beschermingsniveau bij doorgifte persoonsgegevens

4.1 Article 29 Working Party

Vooraleer bestudeerd kan worden welke beperkingen of mogelijkheden er zijn voor transnationaal dataverkeer, is het niet onbelangrijk om de werkingsorganen die zich toespitsen op deze probleemstelling te kaderen. Binnen de Europese Unie is de voornaamste actor *The Article 29 Working Party* (verder Groep 29).[33] Deze groep bestaat uit vertegenwoordigers van Privacy Commissies uit de 28 Europese lidstaten, samen met de Europese Commissie. De kerntaak van dit orgaan is de onderhandeling en toepassing van regelgeving over transnationaal dataverkeer. Gegeven dat de Europese Unie een hoge standaard nastreeft op vlak van privacy, heeft deze groep een grote impact op de globale privacywetgeving zowel binnen als buiten de Europese Unie.

4.2 Doorgifte van persoonsgegevens naar landen binnen de Europese Unie

Binnen de Europese Unie is grensoverschrijdende overdracht van persoonsgegevens niet aan bijzondere beperkingen onderworpen. Aangezien de nationale wetten over de verwerking van persoonsgegevens een omzetting zijn van de dataprotectierichtlijn, beschikken landen van de Europese Unie over een geharmoniseerde en gelijkaardige (hoogwaardige) bescherming. Deze regeling is bij uitbreiding van toepassing ten aanzien van de EER-Lidstaten Noorwegen, Liechtenstein en IJsland.

Enkele praktische voorbeelden kunnen deze regelgeving kaderen: een bank kan gegevens van haar cliënteel overzenden om in Frankrijk een betaling door te voeren, een Italiaans ziekenhuis kan aan een Belgische instelling van de sociale zekerheid de gegevens over de hospitalisatiekosten meedelen, een Belgisch reisbureau kan aan de Portugese luchtvaartmaatschappij en het Spaans hotel gegevens over haar klant doorzenden…

Persoonsgegevens die in de Cloud zijn opgeslagen, kunnen dus probleemloos opgeslagen of verwerkt worden op servers gelegen binnen de Europese Unie. *Teamleader* maakt dan ook enkel gebruik van servers die zich binnen de Europese Unie bevinden. In hun algemene voorwaarden wordt hier expliciet naar verwezen. Deze clausule biedt voor de gebruikers van *Teamleader* een garantie dat hun persoonsgegevens binnen de Europese Unie worden opgeslagen en op die manier conform de EU-wetgeving behandeld worden.

[33] Artikel 29 Dataprotectierichtlijn.

"Teamleader beheert haar gebruikersdata in samenwerking met Amazon Web Services (AWS). Er wordt automatisch een back-up aangemaakt van alle gegevens, die bovendien redundant worden opgeslagen. Dankzij onze server- en netwerkstructuur blijft Teamleader steeds toegankelijk – zelfs wanneer er hardwareproblemen optreden. We handhaven een uptime van 99,9%, waardoor we een continue kwaliteitsvolle dienstverlening kunnen garanderen.

Data-privacy is van cruciaal belang. Daarom worden al onze data bewaard ***binnen de grenzen van de EU****. De datacenters van AWS zijn in clusters verdeeld over landen in de hele wereld, maar de gegevens van Teamleader (inclusief back-ups) worden enkel bewaard in Ierland. AWS handelt volledig in overeenstemming met de EU-wetgeving voor gegevensbescherming."*[34]

4.3 Doorgifte van persoonsgegevens naar landen buiten de Europese Unie

I. Een passend beschermingsniveau

Voor landen buiten de Europese Unie voorziet artikel 21 van de Wet Verwerking Persoonsgegevens en artikel 25,lid 1 van de Dataprotectierichtlijn wel in specifieke regels. Persoonsgegevens mogen maar worden overgedragen "*naar een land indien dat land een* ***passend*** *beschermingsniveau waarborgt en de andere bepalingen van deze wet en de uitvoeringsbesluiten ervan worden nageleefd.*"

De Europese wetgever wou met deze regeling enerzijds de internationale handel stimuleren door grensoverschrijdend dataverkeer mogelijk te maken en anderzijds, een uitholling van het verregaande beschermingsniveau binnen de Europese Unie vermijden. Doorgifte van persoonsgegevens buiten de Europese Unie is dus principieel verboden, tenzij een passend beschermingsniveau kan worden gegarandeerd.

Een wettelijke definitie van dit passend beschermingsniveau wordt noch in de wet, noch in de richtlijn voorzien. Een identiek beschermingsniveau als in de Europese Unie is echter niet noodzakelijk, het moet gaan om een **beschermingsniveau equivalent aan dit binnen de Europese Unie**.[35]

[34] http://public.teamleader.be/nl/beveiliging (geconsulteerd op 25 maart 2016).
[35] HvJ 6 oktober 2015, nr. C-362/14, Maximillian Schrems/Data Protection Commissioner.

Zowel de Wet Verwerking Persoonsgegevens als de Richtlijn stipuleren echter wel een aantal niet-limitatieve criteria om het door een derde land aangeboden beschermingsniveau te evalueren: [36]

- ***De aard van de gegevens***; Dit betekent dat het beschermingsniveau kan afhangen van gegevens die al dan niet een gevoelig karakter (zoals medische gegevens) vertonen. Louter administratieve gegevens (zoals naam en adres) vereisen een minder groot beschermingsniveau.
- ***Het doeleinde en de duur van de voorgenomen verwerking***; Het doeleinde van de overdracht van de gegevens moet gekend zijn. Ongerechtvaardigde doeleinden in het buitenland zullen niet getolereerd kunnen worden.
- ***Het land van herkomst en het land van eindbestemming***; Het land van herkomst biedt weinig problemen. Het totale beschermingsniveau van het land van eindbestemming moet echter wel in acht genomen worden.
- ***De algemene en sectorale rechtsregels;*** Het volledige beschermingsniveau op basis van regelgeving moet in rekening worden gebracht. Eventuele specifieke sectorale rechtsregels (bv. Medisch beroep of telecommunicatie) worden tevens onderzocht.
- ***De beroepscodes***; deze codes kunnen betrekking hebben op één onderneming of op een totale industrie.
- ***Veiligheidsmaatregelen die in de derde landen worden nageleefd***; Bv. Encryptie, PIN-codes enz.

De effectieve beoordeling of er al dan niet sprake is van een voldoende hoog beschermingsniveau, wordt in grote mate door de Europese Commissie, in samenwerking met Comité 31[37] en Groep 29, verleend.

Uit een samenvatting van de werkdocumenten van Groep 29, wordt bij de beoordeling vooral rekening gehouden wordt met (1) de inhoud van de toepasselijke voorschriften en (2) de middelen om de handhaving ervan te waarborgen.

Er is een positieve beslissing terug te vinden voor de landen Zwitserland[38], Argentinië[39], Canada[40], Israël[41], Andorra[42], de Faraö Eilanden[43], het Eiland Man[44], Guernsey[45], Jersey[46] en

[36] Artikel 21 § 1 Wet Verwerking Persoonsgegevens; D. DE BOT, *Verwerking van persoonsgegevens*, Antwerpen, Kluwer,2001, 307-308.
[37] Artikel 31 Dataprotectierichtlijn.
[38] *PB. L* 215/1 van 25 augustus 2000.
[39] *PB. L* 168/19 van 5 juli 2003.
[40] *PB. L* 2/13 van 4 januari 2002.
[41] *PB. L* 27/39 van 1 februari 2011.
[42] *PB. L* 277/27 van 21 oktober 2010.
[43] *PB. L* 58/17 van 9 maart 2010.
[44] *PB. L* 151/48 van 30 april 2004.
[45] *PB. L* 308/27 van 25 november 2003.
[46] Ibid.

Uruguay[47]. Europese persoonsgegevens in de Cloud kunnen in deze landen probleemloos verwerkt of opgeslagen worden.

II. Uitzonderingsgronden

Artikel 22 van de Wet op de Verwerking Persoonsgegevens voorziet zes uitzonderingsgronden, waarbij de doorgifte van persoonsgegevens buiten landen van de Europese Unie toch mogelijk is, ook al is er geen passend beschermingsniveau voor handen. Aangezien het hier gaat om uitzonderingen op een algemeen principe, moeten deze op restrictieve wijze worden geïnterpreteerd.

- ***Ondubbelzinnige toestemming****;* Indien er een ondubbelzinnige toestemming aanwezig is van de persoon waarvan de persoonsgegevens afkomstig zijn, is de doorgifte van deze persoonsgegevens steeds mogelijk.[48] Een passend beschermingsniveau hoeft hiervoor niet aanwezig te zijn bij de desbetreffende onderneming die de gegevens opslaat of verwerkt.[49] Toestemming voor de verwerking *sensu stricto* is hier echter niet voldoende, er moet een effectieve toestemming zijn voor de doorgifte van de persoonsgegevens.[50] Verder is ook noodzakelijk dat er een *Informed consent* verleend wordt. Dit betekent dat de betrokkene alle informatie ter beschikking moet hebben om de risico's en/of voordelen van deze doorgifte goed te kunnen inschatten.

Bovenstaande uitzonderingsgrond is in de praktijk vaak problematisch om toe te passen. Bij Cloud services is er vaak overdracht van een groot aantal persoonsgegevens van een grote groep personen. Naast data van klanten, moet er ook rekening gehouden worden met data van leveranciers of medewerkers. Een ondubbelzinnige en rechtstreekse toestemming van alle betrokken personen is vaak een onhaalbare kaart. Verder lijkt me een opsplitsing tussen personen die hun toestemming hebben gegeven en personen die dit niet gedaan hebben, praktisch onmogelijk voor de Cloud service verlener die hun data buiten de Europese Unie willen opslaan of overdragen. Modelovereenkomsten of Binding Corporate Rules kunnen hier een alternatieve oplossing bieden. Deze mogelijkheden worden later in deze Bachelorproef besproken.

- ***Noodzakelijk voor de uitvoering van de overeenkomst of precontractuele maatregelen of noodzakelijk voor de sluiting of uitvoering van een overeenkomst****;* In dit geval kan de instemming met de overeenkomst als een impliciete toestemming aanzien worden voor de verwerking van de persoonsgegevens in casu. Dit is bijvoorbeeld het geval bij het boeken van een reis, waarbij de persoonsgegevens worden doorgegeven aan de hotelbestemming.

[47] *PB. L* 227/11 van 23 augustus 2012.
[48] Artikel 22, 1° Wet Verwerking Persoonsgegevens.
[49] J. DUMORTIER, H. GRAUX en F. DEBUSSERÉ, *ICT-recht*, Leuven, Acco, 2013, 293.
[50] D. DEBOT, o.c., 317.

- ***Noodzakelijk vanwege algemeen belang;*** Dit is voornamelijk van toepassing bij taken toevertrouwd aan administratieve overheden of internationale samenwerking tussen inlichtingen- en veiligheidsdiensten.
- ***Vrijwaring vitale belangen;*** Dit is bijvoorbeeld het geval wanneer iemand dringende medische hulp nodig heeft en geen toestemming kan geven wegens zijn ziektetoestand voor de verwerking van zijn persoonsgegevens.
- ***Openbaar register***
- ***Voldoende waarborgen***

III. Passend beschermingsniveau in de praktijk

Naast de bovenvermelde uitzonderingsgronden, moet in elk ander geval een passend beschermingsniveau kunnen worden geboden bij de doorgifte van persoonsgegevens naar landen buiten de Europese Unie. Cloudserviceproviders hebben verschillende mogelijkheden om te voldoen aan dit beschermingsniveau: (1) Gebruik van modelcontractbepalingen van de Europese Commissie, (2) Binding Corporate Rules of (3) Aanvraag van een individuele machtiging.

(1) Modelcontractbepalingen Europese Commissie[51]

De Europese Commissie, in samenwerking met Groep 29, stelde modelcontractbepalingen op en publiceerde deze op hun website.[52] Doordat deze modelovereenkomsten uitgaan van de Europese Commissie, beschikken deze over een zekere legitimiteit.[53] Ondernemingen die conform deze modelbepalingen een transfer van data organiseren, zullen volledig legitiem te werk gaan. Onder "conform", dient te worden verstaan:[54]

- Bepalingen die **identiek** zijn aan de door de Europese Commissie goedgekeurde modelcontractbepalingen en vervolledigd werden op de specifiek hiertoe bestemde plaatsen (zoals de bijlagen of de namen van de partijen);
- Bepalingen die slechts **zeer beperkt** werden **gewijzigd** (bv. Leestekens of vertalingen) waarbij deze aanpassingen noch de betekenis noch de draagwijdte van de

[51] P. VERPLANCKE, "De Europese Commissie keurt nieuwe standaardclausules voor de doorgifte van persoonsgegevens naar derde landen goed", *R.D.C* 2005/5, 558-561.
[52] http://ec.europa.eu/justice (geconsulteerd op 13 april 2016).
[53] Besch. Comm. 2001/497/EG, 15 juni 2001 betreffende modelcontractbepalingen voor de doorgifte van persoonsgegeven naar derde landen krachtens Richtlijn 95/46/EG, *Pb.L* 4 juli 2001, 181; zoals aangevuld door Besch. Comm. 2004/5271/EG , 27 december 2004 tot wijziging van Beschikking 2001/497/EG betreffende de invoering van alternatieve modelcontractbepalingen voor de doorgifte van persoonsgegevens naar derde landen, *Pb.L* 29 december 2004, 74.
[54] Artikel 8 Protocolakkoord betreffende contractuele bepalingen 25 juli 2013, https://www.privacycommission.be/sites/privacycommission/files/documents/protocol-contracten-FOD-Justitie-CBPL_0.pdf (geconsulteerd op 13 april 2016).

modelcontractbepalingen wijzigen, noch een aantasting vormen van de fundamentele rechten en vrijheden van de betrokkene;

- Modelcontractbepalingen die opgenomen zijn in een ruimere overeenkomst alsook de invoeging van andere bepalingen, met name commerciële, op voorwaarde dat zij **noch rechtstreeks, noch onrechtstreeks in tegenspraak** zijn met de **modelcontractbepalingen** en geen afbreuk doen aan de fundamentele rechten en vrijheden van de betrokkenen.

De Belgische Privacy Commissie is evenwel steeds bevoegd om elke modelovereenkomst, voor de ingebruikname door een onderneming, te evalueren en controleren op eventuele afwijkingen in verband met het uitwisselen van persoonsgegevens. In principe is het zelfs verplicht om elke modelovereenkomst voor te leggen aan deze commissie en toestemming moet steeds afgewacht worden.[55] Indien besloten wordt dat de voorgelegde contractuele bepalingen in overeenstemming zijn met de modelcontractbepalingen, dan betekent dit *ipso facto* dat de bepalingen voldoende waarborgen bieden ten aanzien van de bescherming van de persoonlijke levenssfeer en de fundamentele rechten en vrijheden van personen. Een Koninklijk Besluit is in dit geval niet noodzakelijk. In het geval dat de Privacy Commissie echter besluit dat er geen overeenstemming is met de modelcontractbepalingen van de Europese Commissie, dan is een machtiging bij Koninklijk Besluit (zoals bij een individuele machtiging) vereist om alsnog de datatransfer te kunnen laten doorgaan (Zie punt 4, p.23).

Verschillende beschikkingen van de Europese Commissie bieden tot op heden drie modelcontractbepalingen aan die een passende waarborg bieden.[56] In bijlage is ter illustratie het meest recente modelcontract, opgesteld door de Europese Commissie, opgenomen (Zie bijlage 1 p.44). Wanneer een Cloudservice-verlener beroep doet op deze modelcontractbepalingen, dan is datatransfer naar derde landen onder deze voorwaarden toegelaten.

Enkele verplichte op te nemen bepalingen in een modelcontract omvatten onder meer (1) De **specifieke verplichtingen** van de gegevensexporteur en gegevensimporteur (technische en organisatorische beveiligingsmaatregelen, toestemming voor gegevensoverdracht…) (2) De **afdwingbaarheid** door de betrokkenen: er is een derdenbeding opgenomen in het modelcontract op grond waarvan de betrokkene die geen partij is bij de overeenkomst de naleving van een aantal contractuele bepalingen kan vorderen. (3) De **aansprakelijkheid** van de contractspartijen. (4) De **samenwerking** met **toezichthoudende autoriteiten**.

Een mooi praktisch voorbeeld die de toepassing van deze modelcontracten illustreert, is Microsoft. Na een grondige studie, heeft Groep 29 verklaard dat Microsoft Cloud Services (Microsoft Azure, Office 365, Microsoft Dynamics CRM en Windows Intune) in overeenstemming zijn met de hoge standaarden, opgenomen in de

[55] Artikel 10 Protocolakkoord betreffende contractuele bepalingen 25 juli 2013.

[56] Besch. Comm. 2001/497/EG, 15 juni 2001 betreffende modelcontractbepalingen voor de doorgifte van persoonsgegevens naar derde landen krachtens Richtlijn 95/46/EG, *Pb.L* 4 juli 2001, 181; Besch. Comm. 2004/915/EG, 27 december 2004 tot wijziging van Besch. 2001/497/EG betreffende de invoering van alternatieve modelcontractbepalingen voor de doorgifte van persoonsgegevens naar derde landen, *Pb.L* 29 december 2004, 74; Besch. Comm. 2010/87/EU, 5 februari 2010 betreffende modelcontractbepalingen voor de doorgifte van persoonsgegevens aan in derde landen gevestigde verwerkers krachtens Richtlijn 95/46/EG van het Europees Parlement en de Raad, *Pb. L* 12 februari 2010, 39.

modelcontractbepalingen.[57] Microsoft is de eerste en enige CloudService die deze erkenning van Groep 29 heeft verkregen. Persoonlijke data opgeslagen door Microsoft, hebben hierdoor een zeker hoogwaardig statuut. Dataverkeer binnen en buiten de EU-grenzen door Microsoft vormt dus geen probleem.

(2) Binding Corporate Rules[58]

Naast bovenstaande modelovereenkomsten van de Europese Commissie, bestaat er nog een tweede alternatief om transfer van persoonsgegevens buiten de Europese Unie te laten verlopen. Binding Corporate Rules worden vaak gebruikt bij (Cloudservice)ondernemingen die verschillende vestigingen hebben in verschillende landen met een ander (minder verregaand) beschermingsniveau. Om datatransfer tussen de verschillende landen mogelijk te maken, bieden Binding Corporate Rules soelaas. Deze Rules kunnen aanzien worden als een soort gebundelde exportlicentie.[59]

Groep 29 heeft reeds verschillende werkdocumenten opgesteld waarin de verplichte elementen voor een Binding Corporate Rule worden omschreven.[60] Voor een gedetailleerd overzicht van de noodzakelijke elementen stelde Groep 29 ook een tabel op waarin deze verplichte elementen opgelijst staan.[61] Ter illustratie moeten onder andere deze verplichte vermeldingen opgenomen worden:

- Een toelichting over de **werkwijze** die gevolgd zal worden om de Coporate Rules bindend te maken ten aanzien van de leden van de groep en de werknemers.
- Er moet een clausule voorzien zijn die een **schadevergoeding** begroot in geval van niet naleving van de Corporate Rules.
- De **bewijslast** van eventuele schendingen van ligt bij het bedrijf zelf, niet bij het individu die in zijn rechten geschaad is.
- Een gedetailleerde omschrijving van de datatransfer en zijn **doeleinden** moet opgenomen worden.
- …

[57] Article 29 Data Protection Working Party, 2 april 2014, Ref. Ares(2014)1033670, http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140402_microsoft.pdf (geconsulteerd op 13 maart 2016).
[58] Werkdocument WP 74, "Doorgifte van persoonsgegevens naar derde landen: toepassing van artikel 26 (2) van de EU-richtlijn betreffende gegevensbescherming op bindende ondernemingsregels voor internationale doorgiften van gegevens", goedgekeurd op 3 juni 2003 door de Groep 29.
[59] DUMORTIER, J., GRAUX, H en DEBUSSERÉ, F., *oc*, 294.
[60] GROEP 29, *Working Document relating to the Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers*, 3 juni 2003, http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2003_en.htm (geconsulteerd op 19 maart 2016); GROEP 29, *Working Document of 14/4/2005 Establishing a Model Checklist Application for Approval of Binding Corporate Rules*, http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2005_en.htm (geconsulteerd op 19 maart 2016).
[61] GROEP 29, *Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules*, 24 juni 2008, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm (geconsulteerd op 19 maart 2016).

In bijlage 2 is een voorbeeld opgenomen van Binding Coporate Rules, opgemaakt door *Siemens*. Dit document illustreert op een passende wijze bovenstaande theoretische uiteenzetting.

Groep 29 heeft tevens een geharmoniseerd Europees formulier opgemaakt voor de aanvraag van goedkeuring van de Binding Coporate Rules.[62] Het grote verschil met modelovereenkomsten bestaat erin dat deze ondernemingsregels niet door de Europese Commissie zijn gecontroleerd, opgesteld of geharmoniseerd. Door gebrek aan deze revisie op Europees niveau, moeten deze ondernemingsregels in eerste instantie worden voorgelegd aan de Privacy Commissie van de betrokken landen bij de doorgifte van persoonsgegevens.[63]

De Belgische Privacy Commissie zal in dit geval tevens advies vragen aan andere nationale Privacy Commissies. Op die manier kan er in alle betrokken landen goedkeuring verleend worden voor de Binding Corporate Rules. Om de samenwerking tussen de verschillende nationale instanties vlot te laten verlopen, heeft Groep 29 een samenwerkingsprocedure opgesteld. Hierbij werken de verschillende schakels in de procedure tot goedkeuring van de Binding Corporate Rules samen.[64] Deze samenwerking heeft tot voordeel dat bijvoorbeeld een multinational zijn aanvraag slechts bij één nationale autoriteit moet indienen, die vervolgens met de andere betrokken Europese instanties de zaak onderzoekt. Op deze manier ontstaat er een coherente beslissing tot goed- of afkeuring van de Binding Corporate Rules. Om de goedkeuringsprocedure op een efficiënte manier te laten verlopen, zijn een aantal autoriteiten, waaronder België, gehouden tot een wederzijdse erkenning wanneer de Corporate Binding Rules door drie nationale autoriteiten reeds is onderzocht en goedgekeurd. In tweede instantie moeten deze corporate Rules bij Koninklijk Besluit worden bekrachtigd.

(3) Binding Corporate rules of een contract ?

Wanneer wordt er nu geopteerd voor Binding Corporate Rules en wanneer voor een contract (Privacy Policy, modelcontract)? De Belgische Privacy Commissie gaf op deze vraag aan dat de verantwoordelijke voor de verwerking hierbij een volledig vrije keuze heeft. Om beide systemen te vergelijken, biedt onderstaande tabel, opgemaakt door de Privacy Commissie een overzicht.[65]

---

[62] GROEP 29, *Recommendation 1/2007 of 14/4/2005 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data*, 10 januari 2007, https://www.privacycommission.be/sites/privacycommission/files/documents/01.01.01.32-wp133.pdf.

[63] Zie bij wijze van voorbeeld het Advies nr 40/2014 van 30 april 2014 van de Privacycommissie met betrekking tot de Binding Corporate Rules voor de internationale overdracht van persoonsgegevens door de onderneming Linklaters https://www.privacycommission.be/nl/search/site/binding%20corporate%20rules?page=1 (geconsulteerd op 19 maart 2016).

[64] GROEP 29, *Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From "Binding Corporate Rules*, 14 april 2005, https://ico.org.uk/media/1042454/binding_corporate_rules_cooperation_procedure.pdf (geconsulteerd op 19 maart 2016).

[65] https://www.privacycommission.be/nl/faq-page/373#t373n4596 (geconsulteerd op 19 maart 2016).

Binding Corporate Rules (BCR)	(Model)contract
Doel: voldoende waarborgen bieden als kader voor gegevensdoorgifte naar derde landen	**Doel**: idem
Verplichte gedragscode **binnen een bedrijvengroep**	Contract tussen **twee juridische entiteiten** die al dan niet tot dezelfde bedrijvengroep behoren
Creëert enkel een kader voor gegevensdoorgifte **binnen de bedrijvengroep**	Creëert kader voor gegevensdoorgifte **binnen en buiten de bedrijvengroep**
Op maat	**Op maat of modelcontract** van de Europese Unie
Creëert per definitie een kader voor een **groot aantal gegevensdoorgiften** met verschillende doeleinden	Creëert per definitie een kader voor **specifieke gegevensdoorgiften**
Naast juridische verbintenissen rond privacy principes impliceren BCR ook **concrete maatregelen** die effectieve uitvoering van de regels garanderen (opleiding werknemers, privacy-audits, intern klachtenbehandeling systeem)	Eerder **beperkt tot juridische verbintenissen** rond privacy principes

(4) Individuele machtiging

Naast modelcontracten en Binding Corporate Rules, kan ook een individuele machtiging door de Koning verleend worden voor doorgifte van persoonsgegevens naar een derde land dat geen passend beschermingsniveau biedt. Dit gebeurt steeds na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer.[66] De verantwoordelijke voor de verwerking moet evenwel voldoende waarborgen bieden over de bescherming van de persoonlijke levenssfeer, de fundamentele rechten en vrijheden van personen, alsmede ten aanzien van de uitoefening van de daaraan verbonden rechten.

Er wordt opnieuw geen definiëring gegeven van de term 'voldoende waarborgen'. De wetgever geeft wel aan dat deze waarborgen kunnen voortvloeien uit passende contractuele bepalingen. In de praktijk zullen deze waarborgen gelijkwaardig moeten zijn als het niveau van bescherming die voor handen is door artikel 22 Wet Verwerking Persoonsgegevens. Indien niet, zou het de weg openen om de vereiste van passende bescherming te omzeilen via contractuele bepalingen.

Het is aldus voor een Cloudservice verlener perfect mogelijk om een overeenkomst te sluiten met een importeur van gegevens en door een individuele machtiging in een land met geen passend beschermingsniveau, een doorgifte van persoonsgegevens mogelijk te maken.

[66] Artikel 22, § 1, *in fine* Wet Verwerking Persoonsgegevens.

Deze individuele machtiging wordt in de praktijk echter weinig gebruikt, aangezien dit een vrij lange en logge procedure is. Het is efficiënter om beroep te doen op modelcontractbepalingen of Binding Corporate Rules. Gezien dit gering toepassingsgebied in de praktijk, wordt de individuele machtiging niet verder besproken in deze bachelorproef.

IV. Rol Privacy Policy

Privacy Policies van bedrijven die persoonlijke data verwerken, refereren vaak naar de waarborgen die zij bieden, indien gegevens overgedragen worden naar derde partijen. Privacy Policies zijn dan ook een belangrijk instrument voor een transparante communicatie met de betrokkenen over de verwerking en doorgifte van zijn persoonsgegevens.

In bijlage 3 vindt u een voorbeelddocument van een Privacy Policy opgemaakt door deJuristen. Voornamelijk onderstaand citaat, geeft weer dat transnationaal gegevensverkeer mogelijk is:

"(…) NAAM ONDERNEMING is een Belgische onderneming. Niettemin kan er gegevensverwerking en/of –overdracht zijn naar landen buiten de Europese Unie. Ingevolge artikel 21 van de privacywet mogen persoonsgegevens alleen worden doorgegeven aan ***landen die eenzelfde passend beschermingsniveau waarborgen****, en waar dezelfde of gelijkaardige bepalingen van de privacywet worden nageleefd. Het land, duur van de overdracht en opslag, aard van de gegevens en precieze doeleinden zijn criteria die per geval onderzocht moeten worden.*

NAAM ONDERNEMING garandeert dat er geen overdracht naar derde landen voor gegevensverwerking of –opslag plaats heeft zonder dat de nodige maatregelen genomen zijn om te voldoen aan de beschermingsvereisten uit de Belgische Privacywet. *Deze overdracht zal slechts plaats vinden op basis van één van de gronden zoals vermeld in artikel 2. (…)"*

5 De Amerikaanse Cloud: Safe Harbour-beschikking

5.1 The Safe Harbour Principles

Wat als een Cloud service verlener persoonsgegevens wil opslaan op een server in de Verenigde Staten (verder VS)?

De VS nemen een bijzondere positie in bij de beoordeling over de mogelijkheid van overdracht van persoonsgegevens. Binnen de VS is de regelgeving over privacy veel flexibeler dan in de Europese Unie, waar privacy gezien wordt als een fundamenteel recht. Enkel beperktere sectorale wetten zijn in de VS van toepassing. Een algemeen wetgevend kader rond privacy ontbreekt, waardoor een passend beschermingsniveau niet kan worden gegarandeerd.[67]

De Europese Commissie en het US Department of Commerce hebben een internationale overeenkomst opgesteld, waardoor gegevensoverdracht tussen de VS en de Europese Unie toch mogelijk werd. De Safe Harbour Principles zijn in 2000 hiervan het resultaat.[68] Deze principes sommen de voorwaarden op waaraan Amerikaanse bedrijven moeten voldoen om Europese persoonsgegevens te mogen verwerken of opslaan. De Safe Harbour Principles worden frequent gebruikt door internationale organisaties om bijvoorbeeld een Amerikaanse moederonderneming toe te staan om de activiteiten van haar Europese dochters te beheren. Ook Amerikaanse Clouddienstverleners maakten vaak toepassing van deze Principles.[69]

Enkele Safe Harbour Principles:

- *"(…)Verplichte voorafgaande kennisgeving over de **doeleinden** van de gegevensverzameling (…)";*
- *"(…) Een organisatie moet personen de mogelijkheid geven te kiezen of (zich ertegen te verzetten dat (**opt-out**)) hun persoonlijke informatie a) aan derden bekend zal worden gemaakt of b) zal worden gebruikt voor een doel dat onverenigbaar is met het (de) doel(en) waarvoor deze informatie oorspronkelijk is verzameld of waarvoor de betrokkene achteraf zijn toestemming heeft gegeven. Aan de betrokkene moeten duidelijke en opvallende, direct beschikbare en betaalbare mechanismen worden geboden om deze keuze te maken.(…)"*
- *"(…) Organisaties die persoonlijke informatie verzamelen, bijhouden, gebruiken of verspreiden, moeten **redelijke voorzorgsmaatregelen** nemen om deze te beschermen*

[67] Y., "Hoe veilig zijn onze gegevens in de cloud?", 4 januari 2016, http://www.synergics.be/blog/beveiliging-van-gegevens-safe-harbor (geconsulteerd op 4 april 2016).
[68] Besch. Comm. van 26 juli 2000 overeenkomstig Richtlijn 95/46/EG van het Europees Parlement en de Raad, betreffende de gepastheid van de bescherming geboden door de Veiligehavenbeginselen voor de bescherming van de persoonlijke levenssfeer en de daarmee verband houdende vaak gestelde vragen, die door het ministerie van Handel van de Verenigde Staten zijn gepubliceerd, *PB. L* 215/7 25 augustus 2000, 7-47.
[69] R. SCHOEFS, "Doorsturen van persoonsgegevens naar VS in het gedrang", *DeJuristenkrant* 2015, nr. 315, 3.

> *tegen verlies, misbruik en ongeoorloofde toegang, bekendmaking, wijziging en vernietiging. (…)"*

Het is van belang om op te merken dat deze principes geen bindend karakter hebben. Amerikaanse bedrijven kunnen zelf beslissen of ze de opgegeven waarborgen implementeren in hun handelingswijze. De naleving van de Safe Harbour Principles kan wel geregistreerd worden bij het Department of Commerce in de VS.[70] De publicatie van de onderneming als onderneming die een passend beschermingsniveau biedt, zorgt er dus voor dat Europese persoonsgegevens opgeslagen en verwerkt mogen worden in de desbetreffende Amerikaanse ondernemingen. Onder andere de giganten Amazon, Google en Rackspace namen de Safe Harbour Principles in acht en mogen dus persoonsgegevens van Europese burgers verwerken.[71]

5.2 Het einde van de veilige haven

I. Europees Hof van Justitie 6 oktober 2015

Op 6 oktober 2015 werd de Safe Harbour-beschikking ongeldig verklaard door het Hof van Justitie van de Europese Unie.[72] Dit mijlpaalarrest had een schokkend effect in de ICT-wereld. Nochtans hadden voorgaande schandalen reeds aangetoond dat er, ondanks de Safe Harbour Principles, onvoldoende bescherming geboden werd aan Europese persoonsgegevens. Onder andere het Snowden en het PRISM-afluisterschandaal zijn hier mooie voorbeelden van. Ook de USA Patriot Act (2001), opgemaakt in nasleep van de terreuraanslagen van 11 september 2001, zette de privacy van persoonsgegevens op losse schroeven.[73] De Patriot Act maakt namelijk mogelijk dat NSA en FBI zonder juridische procedures informatie bij Amerikaanse bedrijven kunnen opeisen. De Patriot Act werd in 2015 niet hernieuwd en de Freedom Act werd de nieuwe wettelijke basis. Er werden hierbij beperkingen gelegd op het massaal afluisteren en bijhouden van telefoongegevens. Ondanks veel positieve reacties, verandert er in wezen weinig aan het algemeen veiligheidsbeleid in de VS. *Mass surveillance* was en is in Amerika dus nog steeds toegelaten in kader van nationale veiligheid.

In tegenstelling tot het Amerikaanse beleid, is het binnen de Europese Unie niet toegelaten om op algemene wijze toezicht te houden op data. Bij een inmenging in het recht op privacy moet er steeds met drie principes worden rekening gehouden.[74] (1) **Legaliteitsbeginsel**: er moet steeds een wettelijke basis zijn die de inmenging expliciet voorziet. (2) **Finaliteitsbeginsel**: een wettelijk doel moet nagestreefd worden.

[70] http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list (geconsulteerd op 15 april 2016).
[71] A. ENGELFRIET, M. VAN BERGEN en I. OVERING, *Cloud – Deskundig en praktisch juridisch advies*, Eindhoven, Ius Mentis, 2012, 65.
[72] HvJ 6 oktober 2015, nr. C-362/14, Maximillian Schrems/Data Protection Commissioner.
[73] Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA Patriot Act), 2001.
[74] F. SCHRAM, *o.c.*, 70-72.

(3) **Proportionaliteitsbeginsel**: de inmenging in het recht op privacy mag niet verder gaan dan noodzakelijk ter realisatie van het nagestreefde doel. Deze beperkingen staan in schril contrast met de mogelijkheid van *Mass surveillance* in Amerika.

Verder zijn ook de inspanningen van Mr. Schrems een vermelding waard. Deze jonge Oostenrijkse privacy-activist is in feite de rechtstreekse aanleiding van de uitspraak van het Hof. Hij klaagde namelijk de overdacht van zijn Facebookgegevens naar Amerikaanse servers aan. Facebook Ierland (verantwoordelijk voor de exploitatie van Facebook in Europa) gaf persoonsgegevens van Europese Facebookgebruikers door aan servers van het Amerikaanse Facebook Inc. Deze laatste was weliswaar Safe-Harbourgecertificeerd. Volgens Mr. Schrems was er een te lage waarborg van een adequaat veiligheidsniveau van data voorhanden, dit onder andere in nasleep van de onthullingen van klokkenluider Edward Snowden. Onder verwijzing naar de Safe-Harbourbeschikking, werd de klacht afgewezen bij de Ierse privacytoezichthouder. Schrems tekende hoger beroep aan en het Ierse Hooggerechtshof verwees de zaak door naar het Hof van Justitie. Het Hof volgde de redenering van Schrems in het feit dat Safe Harbour-beschikking niet belet om een eigen onderzoek bij een nationale toezichthouder in te stellen over onvoldoende waarborgen voor gegevensbescherming in de VS.[75] De Safe Harbour-beschikking is aldus niet onaantastbaar en kan op zijn praktische geldigheid getoetst worden. Uiteindelijk volgde het Hof Schrems' volledige redenering en werden de Safe Harbour Principles ongeldig verklaard.

Na grondige studie kunnen onderstaande citaten uit het arrest een goed beeld vormen van de redenering van het Europees Hof van Justitie. De Safe Harbour Principles laten te veel ruimte om af te wijken van het beschermingsniveau voor persoonsgegevens naar Europese normen. [76]

"(…)The continuing transfer would create an ***imminent risk of grave harm*** *to data subjects.(…)"*

"(…)The ***right to respect for private life****, guaranteed by Article 7 of the Charter and by the core values common to the traditions of the Member States,* ***would be rendered meaningless*** *if the State authorities were authorised to access electronic communications on a casual and generalised basis without any objective justification based on considerations of national security or the prevention of crime that are specific to the individual concerned and without those practices being accompanied by appropriate and verifiable safeguards.(…)"*

"(…)The Safe Harbour Principles are applicable solely to self-certified United States organisations receiving personal data from the European Union, and United States public authorities are not required to comply with them. (…) ***National security, public interest, or law enforcement requirements have primacy over the safe harbour principles*** *(…)"*

[75] V. SAGAERT en D. SCHEERS, "VS niet langer een veilige haven voor uw persoonsgegevens", *RW* 5 december 2015, nr. 14, 522.

[76] HvJ, Press Release 6 October 2015 No 117/15, The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid, http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf (geconsulteerd op 10 maart 2016).

Samenvattend kan gesteld worden dat de Safe-Harbourbeschikking ongeldig wordt verklaard om volgende redenen.[77] Vooreerst werpt het Hof op dat de Europese Commissie in 2000 niet overging tot een onderzoek naar een passend beschermingsniveau in de Amerikaanse wetgeving zelf. Enkel een onderzoek naar Safe-Harbourregeling stond op de agenda. Voorts legt het Hof de nadruk op het feit dat de Principles niet van toepassing zijn op Amerikaanse overheidsinstanties. Nationale veiligheid, openbaar belang en rechtshandhaving in de VS hebben steeds voorrang op de Safe-Harbourregeling. Het Hof merkt op dat de werkwijze van de Amerikaanse autoriteiten een aantasting vormt van het grondrecht op de eerbiediging van het privéleven. Amerikaanse autoriteiten hebben namelijk een algemene toegang tot de doorgegeven persoonsgegevens. Deze regeling is niet beperkt tot wat strikt noodzakelijk en proportioneel is voor de bescherming van de nationale veiligheid. Ten slotte benadrukt het Hof dat er geen enkele beroepsmogelijkheid voorzien is voor individuen om toegang te krijgen tot de verwerkte persoonsgegevens. Dit is in strijd met het grondrecht op een effectieve voorziening in rechte.

II. Gevolgen voor de Cloud service-sector[78]

Meer dan 4.000 bedrijven vertrouwden op de Safe Harbour Principles.[79] Dit niet alleen om datatransfer naar Amerika mogelijk te maken, maar ook om overzeese handelsrelaties te stimuleren.

Kort na de nietigverklaring van Safe Harbour, verduidelijkte Groep 29 dat elke transfer van data op basis van de Safe Harbour principles naar de VS na 6 oktober 2015 onwettig is.[80] Is een stopzetting van dataverkeer over de grenzen heen dan een pertinente oplossing? Absoluut niet. Dit zou een terugkeer betekenen naar de 'digitale middeleeuwen'. Het is noodzakelijk dat data opgeslagen en verwerkt moet kunnen worden over de ganse wereld. De wereldwijde verwerking en opslag van persoonlijke data is van essentieel belang om de wereldeconomie niet te laten stagneren. Denk bijvoorbeeld aan persoonlijke data in kader van een vliegtuigticket naar Amerika die verwerkt moet kunnen worden door Amerikaanse maatschappijen. Dit internationaal dataverkeer is zowel noodzakelijk voor particulieren, als voor professionelen en zelfs voor landen in zijn geheel.

Verdere juridische stappen drongen zich bijgevolg op om rechtszekerheid te bieden aan Cloudservice verleners. Op Europees niveau werd er snel gewerkt aan een nieuw

[77] R. SCHOEFS, "Doorsturen van persoonsgegevens naar VS in het gedrang", *DeJuristenkrant* 2015, nr. 315, 3.
[78] S. CARRERA en E. GUILD, "The end of Safe Harbor: What future for EU-US data transfer?", *Maastricht Journal of European and Comparative Law* 2015, nr. 5, 651.
[79] B. SMITH, "The collapse of the US-EU Safe Harbor: Solving the new privacy Rubik's Cube", 20 oktober 2015, http://blogs.microsoft.com/on-the-issues/2015/10/20/the-collapse-of-the-us-eu-safe-harbor-solving-the-new-privacy-rubiks-cube/ (geconsulteerd op 9 maart 2016).
[80] GROEP 29, *Statement of the Article 29 Working Party,* 16 oktober 2015, http://ec.europa.eu/justice/data-protection/article-29/press-material/press release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf (geconsulteerd op 28 maart 2016).

aansluitsysteem. Deze onderhandelingen liggen momenteel nog op tafel en kunnen van lange duur zijn.

In tussentijd moeten vele bedrijven die data van hun Europese gebruikers in de VS bewaren, andere alternatieven zoeken. Zoals hierboven reeds besproken zijn dit de mogelijke tijdelijke oplossingen: uitdrukkelijke instemming van de betrokkene, implementatie van Binding Corporate Rules of het gebruik van EU-modelcontracten en –clausules. Uiteindelijk zijn dit niet de meest efficiënte oplossingen die kunnen worden aangereikt.

Vooreerst is de betrouwbaarheid van EU-modelcontracten en –clausules niet waterdicht. Vaak is hierin een beperking opgenomen van bevoegdheden van nationale Privacy Commissies. Onder andere verschillende Privacy Commissies in Duitsland beschouwen het gebruik van deze modelcontracten niet als een passend alternatief zonder bijkomende garanties.[81] Ook de toestemming is in de praktijk vaak onwerkbaar voor Cloudservice verleners. Verder valt op te merken dat veel toezichthouders, met inbegrip van onze Belgische Privacycommissie, de toestemming slechts uitzonderlijk als basis aanzien voor een internationale doorgifte van persoonsgegevens naar landen zonder een passend beschermingsniveau.[82] Verder is de implementatie van Binding Corporate Rules een tijdrovende activiteit. Een eventueel standaard model is nog niet ter beschikking gesteld.

Belgische en Europese ondernemingen verkrijgen door deze uitspraak een bevoorrechte positie bij de verwerking van Europese persoonsdata.[83] Europese servers verkrijgen zo een extra 'vertrouwelijke stempel'.

Als reactie op het einde van de 'veilige haven', sloot Microsoft als eerste een aanvullende overeenkomst af met Groep 29 over hun overeenstemming met de Europese modelcontractbepalingen. Microsoft kan gezien worden als een grote speler op de Cloudservice markt waardoor onmiddellijke maatregelen voor dit bedrijf dan ook van essentieel belang waren.[84]

[81] X, "More German regulators oppose model clauses for EU-US data transfers", 15 oktober 2015, http://www.out-law.com/en/articles/2015/october/more-german-regulators-oppose-model-clauses-for-eu-us-data-transfers/ (geconsulteerd op 7 maart 2016).
[82] https://www.privacycommission.be/nl/doorgifte-buiten-de-eu-zonder-passende-bescherming-uitzonderingen (geconsulteerd op 7 maart 2016).
[83] DOBBELAERE-WELVAERT, M., "Waarom uw privacy nu veiliger is", 7 oktober 2015, http://deredactie.be/cm/vrtnieuws/opinieblog/opinie/1.2462812 (geconsulteerd op 10 maart 2016).
[84] Y., "Hoe veilig zijn onze gegevens in de cloud?", 4 januari 2016, http://www.synergics.be/blog/beveiliging-van-gegevens-safe-harbor (geconsulteerd op 10 maart 2016).

5.3 EU-VS Privacy Shield

"Now we start turning the EU-US Privacy Shield into reality. Both sides of the Atlantic work to ensure that the personal data of citizens will be fully protected and that we are fit for the opportunities of the digital age. (…) We will continue our efforts, within the EU and on the global stage, to strengthen confidence in the online world. ***Trust is a must, it is what will drive our digital future****."* [85]– Vice President European Commission Ansip.

Op 2 februari 2016 werd er een nieuw akkoord bekend gemaakt tussen de VS en de Europese Unie onder de naam ***A new framework for transatlantic exchanges of personal data for commercial purposes: the EU-U.S. Privacy Shield*** (hierna 'EU-US Privacy Shield' of 'Privacy Shield'). Dit akkoord moet een oplossing bieden aan het wettelijk hiaat ontstaan na de vernietiging van de Safe Harbour Principles. De juridische omkadering van *EU-US Privacy Shield* werd door de Europese Commissie gepubliceerd op 29 februari 2016.[86] Dit resultaat kwam tot stand door de actieve medewerking van twee partijen. Aan de ene zijde vertegenwoordigde een grote lobbygroep de financiële en wereldwijde economische belangen (waaronder ook de Amerikaanse overheid en inlichtingendiensten). Aan de andere zijde participeerde een steeds groter wordende groep privacy-activisten.[87]

Concreet zal er zoals bij de *Safe Harbour Principles* gewerkt worden met een lijst van Amerikaanse bedrijven die jaarlijks geregistreerd zijn als bedrijven die de privacy regeling respecteren. The US Department of Commerce heeft als taak om deze lijst grondig te controleren en eventueel op te treden bij inbreuken.

[85] COMM., *Restoring trust in transatlantic data flows through strong safeguards: European Commission presents EU-US privacy shield*, 29 februari 2016, http://europa.eu/rapid/press-release_IP-16-433_en.htm (geconsulteerd op 10 april 2016).
[86] COMM., *Commission implementing decision,* 29 februari 2016, http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf (geconsulteerd op 12 april 2016).
[87] Dobbelaere-Welvaert, M., "Het EU-VS Privacyschild. Meer dan een mooi logo?", 3 maart 2016, Knack, http://datanews.knack.be/ict/nieuws/het-eu-vs-privacyschild-meer-dan-een-mooi-logo/article-opinion-673433.html (geconsulteerd op 10 maart 2016).

I. Privacy principles

Globaal genomen is de belangrijkste wijziging ten opzichte van de *Safe Harbour Principles* dat datatuitwisseling tussen de Europese Unie en de VS onder dezelfde (strikte) waarborgen moeten vallen als het intern dataverkeer binnen de Europese Unie.[88] Hierbij wordt volledig tegemoetgekomen aan de vereiste dat het Europees Hof van Justitie had opgenomen in haar uitspraak over de vernietiging van de *Safe Harbour Principles*. Uit een studie van de *Privacy Shield* probeert men dit te realiseren op basis van onderstaande principes:

(1) Notice Principle

Organisaties zijn verplicht om informatie te verschaffen over de persoonsgegevens met betrekking tot de verwerking van hun persoonsgegevens. Enkele voorbeelden hiervan zijn: de doelstelling van verwerking, het recht van toegang en verbetering, type van data verwerking,… Deze organisaties moeten verder ook hun privacy policy publiek maken met een verwijzing naar de Privacy Principles, de website van de Department of Commerce en de website van een alternatieve geschillenbeslechtingsmechanisme.

(2) Choice Principle

Personen waarvan hun persoonsgegevens verwerkt worden, moeten steeds de mogelijkheid hebben om deze verwerking stop te zetten indien de verwerking met een ander doel wordt gebruikt dan oorspronkelijk aangegeven (opt-out systeem).

(3) Security Principle

Er moeten redelijke en geschikte beveiligingsmaatregelen genomen worden om de persoonsgegevens te beschermen tegen eventuele hackers. Hierbij kan gedacht worden aan het inzetten van encryptie. Dit is het coderen en decoderen van gegevens, waardoor ze niet meer hun oorspronkelijke vorm hebben en dus niet gelezen kunnen worden.

[88] COMM., *Press release: EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield*, 2 februari 2016, http://europa.eu/rapid/press-release_IP-16-216_en.htm (geconsulteerd op 12 april 2016).

(4) Data Integrity and Purpose Limitation Principle

Persoonsgegevens mogen enkel verwerkt worden om het oorspronkelijke doel te verwezenlijken. Andere doeleinden zijn niet mogelijk zonder expliciete toestemming van de betrokkene. Indien gegevensverzameling aldus oorspronkelijk tot doel had omwille van facturatiegegevens, zullen deze gegevens niet gebruikt mogen worden voor commerciële doeleinden.

(5) Access Principle

Persoonsgegevens moeten steeds gecorrigeerd of aangevuld kunnen worden. Verwijdering door een niet-naleving van de privacy principles, moet ten allen tijde kunnen plaatsvinden op vraag van de betrokken partij. Privacy Policies moeten ook steeds voor het publiek beschikbaar zijn, waardoor dit *Access Principle* ook daadwerkelijk kan uitgeoefend worden met kennis van zaken.

(6) Accountability for Onward Transfer Principle

Doorgifte van persoonsgegevens is enkel mogelijk (1) voor gelimiteerde en specifieke doeleinden (welomlijnd doel, voorbeeld facturatie), (2) op basis van een contract, (3) enkel op voorwaarde dat het contract het zelfde beschermingsniveau biedt als de privacy principles.

(7) Recourse, Enforcement and Liability Principle

Geregistreerde organisaties die zich aansluiten bij de privacy principles moeten alles in het werk stellen om in overeenstemming met deze principes te handelen. Jaarlijks is er een herregistratie noodzakelijk. Ook is het onontbeerlijk dat er op regelmatige basis een interne controle gebeurt over de conformiteit met de privacy principles.

II. Massasurveillance

Een zeer belangrijke vermelding in de *Privacy Shield* is dat nationale veiligheidsdiensten zich in de toekomst moeten **onthouden van willekeurig of grootschalig toezicht op data**. Massasurveillance door de Amerikaanse veiligheidsdiensten zal enkel nog mogelijk zijn op

basis van terrorisme, wapenhandel, transnationale criminaliteit, spionage of bedreigingen voor het legercontingent. Deze nieuwe vereisten kunnen begrepen worden door te stellen dat enkel individueel toezicht door een Amerikaanse veiligheidsdienst nog mogelijk zal zijn, op voorwaarde dat er motivatie en afdoende redenen voor handen zijn.

Naar mijn mening zijn de uitzonderingsgronden waar massasurveillance nog steeds mogelijk is, te ruim gedefinieerd. Op deze wijze zal de Amerikaanse overheid steeds een grondslag vinden om over te gaan tot massasurveillance. Dit was net het punt waar het Europees Hof kritiek op had bij de vernietiging van *Safe Harbour*. Ik stel me de vraag of dit punt bij een eventuele latere toetsing van de *EU-US Privacy Shield* door het Europees Hof stand zal kunnen blijven houden.

III. Afdwingmechanisme

Verder wordt een beter afdwingingsmechanisme van deze nieuwe regelgeving voorzien. Vooreerst is er de mogelijkheid voor burgers om rechtsreeks contact te kunnen opnemen met de inbreukmakende Amerikaanse onderneming. Op deze onderneming rust dan de verplichting om binnen de 45 dagen het geschil te behandelen. De privacy policies van deze ondernemingen moeten dan ook melding maken van de mogelijkheid tot contactopneming bij eventuele inbreuken. Ook zal er beroep kunnen gedaan worden op een kosteloze alternatieve geschillenbeslechtingmechanisme. Indien de onderneming verzaakt aan de behandeling van de klacht, dan kan de EU-burger zich richten tot de nationale gegevensbeschermingsautoriteit (Privacycommissie), die samen met de US Department of Commerce en Federal Trade Commission de zaak behandelt. In laatste instantie kan beroep gedaan worden op *'an independent dispute resolution body'*. De concrete invulling van dit orgaan is evenwel nog niet voorhanden.

The Department of Commerce zal een belangrijke rol verkrijgen in de opvolging van bedrijven in kader van privacy garanties bij dataverkeer. Specifieke onderzoeken zullen verricht worden wanneer The Department of Commerce specifieke klachten ontvangt of wanneer er eventuele vermoedens zijn dat een bedrijf geen rekening houdt met de *Privacy Shield Principles*. Wanneer bedrijven niet in overeenstemming handelen met deze principes, kunnen er sancties volgen en is er een mogelijkheid om deze bedrijven te verwijderen van de lijst. Dataverkeer vanuit de Europese Unie zal dan niet meer mogelijk zijn voor hen.

Voor klachten die betrekking hebben op de toegang tot persoonlijke data van Amerikaanse overheden zal er tevens een ombudsman[89] ingesteld worden. Deze ombudsman zou onafhankelijk functioneren van de Amerikaanse inlichtingsdiensten. Het is nog wachten op

[89] De functie zal uitgeoefend worden door Undersecretary of State C. Novelli.

een concrete juridische uitwerking vooraleer dit afdwingingsmechanisme kan onderzocht worden op zijn doeltreffendheid.[90]

Ook een jaarlijkse evaluatie van de *EU-US Privacy Shield* is onder deze nieuwe regeling voorzien. Hierbij zal de werking, het toezicht en de wederzijdse verbintenissen op tafel gelegd worden en een stand van zaken wijst dan uit of er nog concrete stappen moeten worden ondernomen. Op basis van dit jaarlijks rapport zal de Europese Commissie verdere maatregelen stimuleren bij het Europees Parlement en de Europese Raad. Op deze wijze zal er steeds gewerkt worden aan een *up-to-date* versie van de *EU-US Privacy Shield*. Naast deze jaarlijkse evaluatie, wordt er ook een jaarlijkse 'privacy top' georganiseerd door de Europese Commissie. Samen met geïnteresseerde NGO's zal er onderhandeld worden over de verdere ontwikkelingen op vlak van privacy bij dataverkeer.

IV. Evaluatie Privacy Shield door Groep 29

(1) Algemeen

Kort na de publicatie van het ontwerp van de *EU-US Privacy Shield* maakte Mr. Schrems zijn mening reeds bekend:

"***The Court has required*** *the European Commission and the US government* ***to go an extra kilometer – the Privacy Shield is an aggregation of a couple extra inches****. There are obviously some minor improvements, but this is far from what the Court required for an 'adequacy decision'. Even if they try to cover this in a major PR exercise, this does unfortunately not seem like a stable solution."* [91]

Uit bovenstaand citaat is het duidelijk dat Mr. Schrems niet overtuigd is van de doeltreffendheid en de redactie van de *EU-US Privacy Shield*. De garanties, opgenomen in dit nieuw verdrag, bieden onvoldoende waarborgen tegen de bezwaren die het Europees Hof eerder had tegen *Safe Harbour*.

Naast de opinie van Mr. Schrems, maakte Groep 29 hun standpunt recent bekend over de voorlopige versie van de *Privacy Shield*.[92] Ook zij hebben hun bedenkingen over de doeltreffendheid van de nieuwe regelgeving over de doorgifte van persoonsgegevens. Over het algemeen is Groep 29 van mening dat de *Privacy Shield* een grote stap vooruit is, maar

[90] DANON, S., "EU-US Privacy Shield… the devil is in the details", 4 februari 2016, Knack, http://datanews.knack.be/ict/nieuws/eu-us-privacy-shield-the-devil-is-in-the-details/article-opinion-655317.html (geconsulteerd op 15 april 2016).
[91] GILBERT, D., "Safe Harbor 2.0: Max Schrems calls 'Privacy Shield' national security loopholes 'lipstick on a pig'", 29 februari 2016, http://www.ibtimes.com/safe-harbor-20-max-schrems-calls-privacy-shield-national-security-loopholes-lipstick-2327277 (geconsulteerd op 1 maart 2016).
[92] GROEP 29*, Opinion on the EU-US Privacy Shield draft adequacy decision*, 13 april 2016 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf (geconsulteerd op 14 april 2016).

toch zijn er enkele kritiekpunten. Voornamelijk komt er reactie op het gebrek aan beperkingen op dataretentie, de mogelijkheden die nog steeds bestaan om over te gaan tot mass surveillance, de ombudsfunctie, de complexiteit en inconsistentie van de tekst.

Zij hebben dan ook aan de Europese Commissie gevraagd om met hun standpunt rekening te houden en hun opmerkingen te verwerken in de definitieve versie van de *Privacy Shield,* die in juni 2016 wordt verwacht. Het advies van Groep 29 heeft evenwel geen bindende werking en de Europese Commissie is niet verplicht om hun opmerkingen in rekening te nemen.[93] Indien de Europese Commissie opteert om geen aangepaste definitieve versie te maken, kan echter een eventuele nieuwe gerechtelijke procedure voor het Europees Hof van Justitie door de Privacy Commissies de kop opsteken. Om de rechtszekerheid te bevorderen, is dit een route die ten allen tijde vermeden moet worden.

Een kort overzicht van de voornaamste kritiekpunten wordt hieronder weergegeven.

(2) Dataretentie beperking

Data retention limitation is een fundamenteel principe binnen de Europese Unie. Dit principe impliceert dat persoonsgegevens enkel bewaard kunnen worden voor de periode die noodzakelijk is om het vooraf opgestelde doel te bereiken.[94] In de tekst van de *Privacy Shield* kan echter geen enkele verwijzing gevonden worden naar deze beperking in de tijd van de opslag van persoonsgegevens. Groep 29 beklemtoont dat dit gebrek in de *Privacy Shield* er toe kan leiden dat Amerikaanse organisaties persoonsgegevens langer kunnen bewaren dan in de Europese Unie, ook al is het doel van de opslag reeds bereikt.

Verder merkt Groep 29 op dat er geen bescherming tegen geautomatiseerde beslissingvorming voorhanden is (Zie punt 3, p. 14).

(3) Wisselwerking 'Choice Principle' en 'Purpose Limitation Principle'

Groep 29 is van oordeel dat de *Choice Prinicple* niet gebruikt kan worden om de *Purpose Limitation Principle* te omzeilen. Het is niet omdat de betrokkene ten allen tijde ervoor kan kiezen om de verwerking van zijn persoonsgegevens stop te zetten, dat de verwerker de gegevens met een ander doel kan verwerken totdat de betrokkene zich verzet heeft tegen deze verwerking met een nieuw doel. In andere woorden, de *Choice Principle* vormt geen uitzondering op de *Purpose Limitation Principle*.

[93] Artikel 29 Dataprotectierichtlijn.
[94] Artikel 6(1) Dataprotectierichtlijn.

(4) Mass-surveillance

*"(…)The WP29 recalls its long-standing position that **massive and indiscriminate surveillance** of individuals **can never be considered as proportionate** and strictly necessary in a democratic society, as is required under the protection offered by the applicable fundamental rights. (…)"*[95]

Zoals reeds eerder aangegeven is massasurveillance door de Amerikaanse veiligheidsdiensten enkel nog mogelijk op basis van terrorisme, wapenhandel, transnationale criminaliteit, spionage of bedreigingen voor het legercontingent. Deze uitzonderingsgronden vloeien voort uit het intern wettelijk kader (PPD-28[96], FISA[97], USA FREEDOM ACT) binnen de Verenigde Staten.

Binnen de Europese Unie is deze tussenkomst enkel mogelijk indien dit in overeenstemming is met de wetgeving en indien deze procedures voldoende duidelijk en toegankelijk zijn voor de burgers. De omstandigheden waarin dit kan en de voorwaarden waaraan veiligheidsdiensten verbonden zijn, moeten op een transparante wijze toegankelijk zijn.

Groep 29 besluit dat het onduidelijk is welke implicaties het Amerikaanse intern wettelijk kader heeft. Het wetgevend kader is onvoldoende doorzichtig en de mogelijkheid tot mass-surveillance blijft behouden door een ruim begrip van de uitzonderingsgronden. In het rapport kan volgende zinssnede duidelijk weergeven wat het standpunt van Groep 29 is:

*"(…) There are **indications** that the **U.S. continue to collect massive and indiscriminate data**, or at least do not exclude that they may still do so in the future. The WP29 has consistently held that such data collection is not in conformity with EU law and is therefore not acceptable (…)"*[98]

(5) Ombudsfunctie

Groep 29 verwelkomt de nieuwe ombudsfunctie om de rechtstoegang voor betrokkenen te vergemakkelijken in geval van klachten bij doorgifte over verwerking van zijn persoonsgegevens. In haar opinie geeft Groep 29 echter aan dat er nog enkele werkpunten zijn bij de totstandbrenging van deze ombudsfunctie.

---

[95] GROEP 29*, Opinion on the EU-US Privacy Shield draft adequacy decision*, 13 april 2016 , 4, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf (geconsulteerd op 14 april 2016).
[96] Presidential Policy Directive 28.
[97] Foreign Intelligence Surveillance Act.
[98] GROEP 29*, Opinion on the EU-US Privacy Shield draft adequacy decision*, 13 april 2016 , 40, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf (geconsulteerd op 14 april 2016).

Vooreerst vraagt Groep 29 zich af of er wel aan de vereiste waarborgen uit het eerder vermelde arrest van 6 oktober 2015 van het Europees Hof van Justitie voldaan wordt door middel van de implementatie van een ombudsfunctie. In dit arrest wordt namelijk verwezen naar artikel 47 van het Handvest van de grondrechten van de Europese Unie, dat het recht op een doeltreffende voorziening in rechte en op een onpartijdig gerecht stipuleert. Groep 29 is van oordeel dat een ombudsfunctie geen effectieve voorziening in rechte uitmaakt, maar dat een ombudsfunctie kan fungeren zoals een effectieve voorziening in rechte, indien deze functie volledig onafhankelijk uitgeoefend wordt en indien de ombudsman over voldoende bevoegdheden beschikt.[99] Bij deze twee vereisten knelt nochtans het schoentje.

De onafhankelijkheid van de ombudsman wordt in vraag gesteld. Groep 29 is van oordeel dat de ombudsman geen volledig onafhankelijke positie kan innemen gezien zijn functie bij de Department of State. De *Privacy Shield* reikt verder geen specifieke criteria aan over het ontslag van de Ombudsman. Hierdoor is het mogelijk dat de ombudsman ontslagen kan worden in zijn ombudsfunctie op dezelfde wijze als hij ontslagen kan worden in zijn functie als Undersecretary in de Department of State. Dit kan het onafhankelijk karakter van de ombudsfunctie volgens Groep 29 (potentieel) ondermijnen.

Ook de aangereikte bevoegdheden van de ombudsman worden door Groep 29 bekritiseerd. Uit de *Privacy Shield* is het onduidelijk over welke bevoegdheden de ombudsman zal beschikken. Volgens Groep 29 zou de ombudsman de directe toegang moeten hebben tot de persoonsgegevens die ter discussie staan. Deze toegang wordt echter niet gespecifieerd in de *Privacy Shield*. Een ruime omschrijving van de bevoegdheden is in de definitieve versie van de *Privacy Shield* wenselijk.

(6) Complexiteit en inconsistentie van de tekst

Over het algemeen is Groep 29 van oordeel dat de Privacy Shield te complex is opgesteld en geen coherent geheel vormt. Door gebruik van annexes/bijlages wordt de transparantie naar de rechtszoekende toe niet bevorderd. Ook is er inconsistentie in het gebruik van begrippen (bijvoorbeeld 'persoonsgegevens') en is een inleidende verklarende woordenlijst aangeraden.

[99] EHRM 6 september 1978, Klass and others/Germany, § 56.

5.4 Judicial Redress Act

"The United States must guarantee that all EU citizens have the right to enforce data protection rights in US courts, whether or not the reside on US soil. Removing such discrimination will be essential for restoring trust in transatlantic relations." [100]– President Juncker

Dit nieuw wetgevend initiatief kan gezien worden als een rechtsreeks gevolg van de vernietiging van de Safe Harbour Principles en de nieuwe onderhandelingen die erna zijn ontstaan.

De Judicial Redress Act[101] werd ondertekend door president Obama op 24 februari 2016. Eenmaal deze acte in werking treedt, zal dit de basis vormen voor een gelijke behandeling tussen EU-burgers en Amerikaanse burgers wat betreft de toegang tot de Amerikaanse rechtbanken voor geschillen met betrekking tot privacy en dataverkeer. Door deze wet kunnen Europeanen voortaan gerechtelijke acties ondernemen in Amerikaanse rechtbanken als hun privacy in de VS geschonden wordt. Bijvoorbeeld wanneer de Amerikaanse overheid persoonlijke gegevens onrechtmatig zou verspreiden.

[100] NEOLINE/ GK, "The European Union (EU) and the United States (US) reached an agreement on the EU-US data protection Umbrella agreement", 9 september 2015, https://neurope.eu/article/eu-citizens-will-have-the-right-to-sue-us-in-case-of-privacy-breaches/ (geconsulteerd op 10 april 2016).
[101] Judicial Redress Act of 2015, *Public Law* 24 februari 2016.

6 Besluit

Het recente succes van Cloudcomputing vraagt een aangepast wettelijk kader met betrekking tot de verwerking van persoonsgegevens. Dit wettelijk kader kan zowel op nationaal als op Europees niveau gesitueerd worden. Aangezien de Europese Unie een voortrekkersrol aanneemt bij de bescherming van verwerking van persoonsgegevens en privacy in het algemeen, mag deze reglementering op wereldwijd niveau niet onderschat worden. Europese persoonsgegevens mogen enkel opgeslagen of verwerkt worden conform dit beschermingsniveau.

Concreet werd in deze Bachelorproef volgende rechtsvraag naar voor geschoven:

"Gegevensverkeer in de Cloud: mogen mijn persoonsgegevens worden opgeslagen in landen buiten Europa?"

Bij de beantwoording van deze vraag dient er een onderscheid gemaakt te worden tussen (1) de doorgifte van persoonsgegevens naar landen binnen de Europese Unie en (2) doorgifte van persoonsgegevens naar landen buiten de Europese Unie. Enerzijds vormt transnationaal verkeer van persoonsgegevens binnen de grenzen van de Europese Unie geen probleem, aangezien een geharmoniseerde regelgeving voor een gelijkwaardig beschermingsniveau zorgt binnen deze verschillende lidstaten. Anderzijds is voor de doorgifte van persoonsgegevens naar landen buiten de Europese Unie een passend beschermingsniveau noodzakelijk in het land waar de persoonsgegevens worden verwerkt of opgeslagen. Op basis van modelcontractbepalingen van de Europese Commissie of Binding Corporate Rules kan dit passend beschermingsniveau in de praktijk zijn uitwerking krijgen.

De doorgifte van persoonsgegevens naar de VS neemt een aparte positie in. In deze situatie waren de *Safe Harbour Principles* in het verleden een wettelijke grondslag om deze doorgifte juridisch correct te laten verlopen. Na de nietigverklaring van de *Safe Harbour* verordening door het Europees Hof van Justitie in oktober 2015, stond deze doorgifte op losse schroeven. Op Europees niveau ging men snel in onderhandeling met de VS om een nieuwe wettelijke basis te voorzien voor deze doorgifte. Tot op vandaag is deze wettelijke basis nog niet in werking getreden, maar een voorlopige versie van de *Privacy Shield* is reeds voor handen. Groep 29 evalueerde dit document recent en enkele kritiekpunten liggen terug op tafel. Eind juni 2016 wordt de definitieve versie verwacht, waarbij de opmerkingen van groep 29 waarschijnlijk geïmplementeerd zullen worden.

Deze Bachelorproef bevestigt de regel dat recht een evoluerend begrip is, die de maatschappelijke realiteit en nieuwe ontwikkelingen volgt en reguleert.

7 Bibliografie

7.1 Wetgeving

INTERNATIONALE NORMEN

Presidential Policy Directive 28.

Foreign Intelligence Surveillance Act.

Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA Patriot Act), 2001

Judicial Redress Act of 2015, *Public Law* 24 februari 2016.

Verdrag van de Raad van Europa van 28 januari 1981 tot bescherming van personen ter zake van de geautomatiseerde verwerking van persoonsgegevens, *Intern. Legal Mater*., 1981, 317.

Artikel 6, tweede lid verdrag van Lissabon van 13 december 2001, *Pb.L.* 17 december 2007, C306.

Artikel 6(1) Dataprotectierichtlijn.

Artikel 29 Dataprotectierichtlijn.

Besch. Comm. van 26 juli 2000 overeenkomstig Richtlijn 95/46/EG van het Europees Parlement en de Raad, betreffende de gepastheid van de bescherming geboden door de Veiligehavenbeginselen voor de bescherming van de persoonlijke levenssfeer en de daarmee verband houdende vaak gestelde vragen, die door het ministerie van Handel van de Verenigde Staten zijn gepubliceerd, *PB. L* 215/7 25 augustus 2000, 7-47

Besch. Comm. 2001/497/EG, 15 juni 2001 betreffende modelcontractbepalingen voor de doorgifte van persoonsgegeven naar derde landen krachtens Richtlijn 95/46/EG, *Pb.L* 4 juli 2001, 181; zoals aangevuld door Besch. Comm. 2004/5271/EG , 27 december 2004 tot wijziging van Beschikking 2001/497/EG betreffende de invoering van alternatieve modelcontractbepalingen voor de doorgifte van persoonsgegevens naar derde landen, *Pb.L* 29 december 2004, 74.

OESO, *Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data*, OESO, 1980, http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf (geconsulteerd op 3 maart 2016).

GROEP 29, *Working Document relating to the Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers*, 3 juni 2003, http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2003_en.htm (geconsulteerd op 19 maart 2016).

GROEP 29*, Working Document of 14/4/2005 Establishing a Model Checklist Application for Approval of Binding Corporate Rules*,

http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2005_en.htm (geconsulteerd op 19 maart 2016).

GROEP 29, *Recommendation 1/2007 of 14/4/2005 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data*, 10 januari 2007, https://www.privacycommission.be/sites/privacycommission/files/documents/01.01.01.32-wp133.pdf.

GROEP 29, *Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules*, 24 juni 2008, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm (geconsulteerd op 19 maart 2016).

NATIONALE NORMEN

Artikel 22 Gw.

Artikel 23ev. Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, *BS* 18 maart 1993 (verder Wet Verwerking Persoonsgegevens).

Artikel 1, § 2 Wet Verwerking Persoonsgegevens.

Artikel 9, § 1 Wet Verwerking Persoonsgegevens.

Artikel 9, § 2 Wet Verwerking Persoonsgegevens.

Artikel 10 Wet Verwerking Persoonsgegevens.

Artikel 12, eerste lid Wet Verwerking Persoonsgegevens.

Artikel 12, tweede lid Wet Verwerking Persoonsgegevens.

Artikel 21 § 1 Wet Verwerking Persoonsgegevens

Artikel 22, 1° Wet Verwerking Persoonsgegevens

Artikel 22, § 1, *in fine* Wet Verwerking Persoonsgegevens.

Wet van 11 december 1998, *BS* 3 februari 1999.

Artikel 8 Protocolakkoord betreffende contractuele bepalingen 25 juli 2013.

Artikel 10 Protocolakkoord betreffende contractuele bepalingen 25 juli 2013.

Memorie van Toelichting bij het wetsontwerp tot omzetting van de richtlijn 95/46/EG van 24 oktober 1995 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrij verkeer van die gegevens, *Parl.St.* Kamer 1997-98, nr. 1566/1, 12.

Commissie voor de Bescherming van de Persoonlijke Levenssfeer, Advies nr 40/2014 van 30 april 2014 van de Privacycommissie met betrekking tot de Binding Corporate Rules voor de internationale overdracht van persoonsgegevens door de onderneming Linklaters https://www.privacycommission.be/nl/search/site/binding%20corporate%20rules?page=1 (geconsulteerd op 19 maart 2016).

Commissie voor de Bescherming van de Persoonlijke Levenssfeer, Advies nr 32/2015 van 22 juli 2015 https://www.privacycommission.be/sites/privacycommission/files/documents/advies_32_2015.pdf (geconsulteerd op 4 april 2016).

7.2 Rechtsleer

BOEKEN

SCHRAM, F., *Verwerking van persoonsgegevens*, Brussel, Politeia, 2013, 158 p.

DUMORTIER, J., GRAUX, H. EN F. DEBUSSERÉ, *ICT-recht*, Leuven, Acco, 2013, 367 p.

ENGELFRIET, A., VAN BERGEN, M. EN OVERING, I, *Cloud – Deskundig en praktisch juridisch advies*, Eindhoven, Ius Mentis, 2012, 103 p.

VALGAEREN, E. EN COSTERMANS, S., Grenzeloze advocatuur: obstakels worden uitdagingen, 2012, Brugge, Die Keure, 234 p.

DE BOT, D., Verwerking van persoonsgegevens, 2001, Antwerpen, Kluwer, 403 p.

TIJDSCHRIFTARTIKELEN

CARRERA S. en GUILD E., "The end of Safe Harbor: What future for EU-US data transfer?", *Maastricht Journal of European and Comparative Law* 2015, nr. 5, 651.

DANON, S., "EU-US Privacy Shield… the devil is in the details", 4 februari 2016, Knack, http://datanews.knack.be/ict/nieuws/eu-us-privacy-shield-the-devil-is-in-the-details/article-opinion-655317.html (geconsulteerd op 15 april 2016).

DE HERT P. en SCHREURS W., "De bescherming van persoonsgegevens op het internet: nuttige verduidelijking door de rechtspraak", *AM* 2004/2, 127-137.

DOBBELAERE-WELVAERT, M., "Waarom uw privacy nu veiliger is", 7 oktober 2015, http://deredactie.be/cm/vrtnieuws/opinieblog/opinie/1.2462812 (geconsulteerd op 10 maart 2016).

DOBBELAERE-WELVAERT, M., "Het EU-VS Privacyschild. Meer dan een mooi logo?", 3 maart 2016, Knack, http://datanews.knack.be/ict/nieuws/het-eu-vs-privacyschild-meer-dan-een-mooi-logo/article-opinion-673433.html (geconsulteerd op 10 maart 2016).

DOCQUIR, B., "Cloud computing of "virtuele informatica": gegevensbescherming staat centraal in de contractuele relatie", *Cah. Jur.* 4/2011, 105-117.

GILBERT, D., "Safe Harbor 2.0: Max Schrems calls 'Privacy Shield' national security loopholes 'lipstick on a pig'", 29 februari 2016, http://www.ibtimes.com/safe-harbor-20-max-schrems-calls-privacy-shield-national-security-loopholes-lipstick-2327277 (geconsulteerd op 1 maart 2016).

NEOLINE/ GK, "The European Union (EU) and the United States (US) reached an agreement on the EU-US data protection Umbrella agreement", 9 september 2015, https://neurope.eu/article/eu-citizens-will-have-the-right-to-sue-us-in-case-of-privacy-breaches/ (geconsulteerd op 10 april 2016).

SAGAERT V. en SCHEERS D., "VS niet langer een veilige haven voor uw persoonsgegevens", *RW* 5 december 2015, nr. 14, 522.

SCHOEFS, R., "Doorsturen van persoonsgegevens naar VS in het gedrang", *DeJuristenkrant* 2015, nr. 315, 3.

SCHOEFS, R., "Witte rook voor nieuwe privacyverordening", *Juristenkrant*, nr. 321, 2016, 16.

SMITH, B., "The collapse of the US-EU safe harbour solving the new privacy rubiks cube", 20 oktober 2015, http://blogs.microsoft.com/on-the-issues/2015/10/20/the-collapse-of-the-us-eu-safe-harbor-solving-the-new-privacy-rubiks-cube/#sm.00000m5kprxfqgdqyrm04o3furzkd (geconsulteerd op 10 april 2016).

VERPLANCKE P., "De Europese Commissie keurt nieuwe standaardclausules voor de doorgifte van persoonsgegevens naar derde landen goed", *R.D.C* 2005/5, 558-561.

Y., "Hoe veilig zijn onze gegevens in de cloud?", 4 januari 2016, http://www.synergics.be/blog/beveiliging-van-gegevens-safe-harbor (geconsulteerd op 4 april 2016).

X, "More German regulators oppose model clauses for EU-US data transfers", 15 oktober 2015, http://www.out-law.com/en/articles/2015/october/more-german-regulators-oppose-model-clauses-for-eu-us-data-transfers/ (geconsulteerd op 7 maart 2016).

7.3 Rechtspraak

EHRM 6 september 1978, Klass and others/Germany, § 56.

HvJ 6 november 2001, C101/01, Bodil Lindqvist/Koninkrijk Zweden.

HvJ 6 oktober 2015, nr. C-362/14, Maximillian Schrems/Data Protection Commissioner.

Arbitragehof 21 december 2004, nr. 202/2004.

8 Bijlage

8.1 BIJLAGE 1: Modelcontractbepaling Europese Commissie

MODELCONTRACTBEPALINGEN („VERWERKERS")

Voor de toepassing van artikel 26, lid 2, van Richtlijn 95/46/EG, voor de doorgifte van persoonsgegevens aan verwerkers die gevestigd zijn in derde landen die geen passend beschermingsniveau waarborgen

Naam van de organisatie die de gegevens uitvoert: …

Adres: …

Tel. …; fax …; e-mail: …

Andere gegevens ter identificatie van de organisatie:

…

(de gegevens**exporteur**)

en

Naam van de organisatie die de gegevens invoert: …

Adres: …

Tel. …; fax …; e-mail: …

Andere gegevens ter identificatie van de organisatie:

…

(de gegevens**importeur**)

elk afzonderlijk „partij" en gezamenlijk „de partijen" genoemd,

ZIJN OVEREENGEKOMEN de volgende contractbepalingen, hierna „de bepalingen" genoemd, vast te stellen teneinde voldoende waarborgen te bieden ten aanzien van de bescherming van de persoonlijke levenssfeer en de fundamentele rechten en vrijheden van personen, bij de doorgifte van de in aanhangsel 1 vermelde persoonsgegevens door de gegevensexporteur aan de gegevensimporteur.

Bepaling 1

Definities

Voor de toepassing van de bepalingen:

a) gelden voor „persoonsgegevens", „bijzondere categorieën gegevens", „verwerken/verwerking", „voor de verwerking verantwoordelijke", „verwerker", „betrokkene" en „toezichthoudende autoriteit" dezelfde definities als in Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (1);

b) wordt onder „gegevensexporteur" verstaan: de voor de verwerking verantwoordelijke die de

persoonsgegevens doorgeeft;

c)wordt onder „gegevensimporteur" verstaan: de verwerker die overeenkomt van de gegevensexporteur persoonsgegevens te ontvangen om deze na doorgifte namens de gegevensexporteur te verwerken in overeenstemming met zijn instructies en de voorwaarden van de bepalingen, en die niet onderworpen is aan een regeling van een derde land die passende bescherming biedt in de zin van artikel 25, lid 1, van Richtlijn 95/46/EG;

d)wordt onder „subverwerker" verstaan: een verwerker die door de gegevensimporteur of een andere voor de gegevensimporteur werkende subverwerker is gecontracteerd en die overeenkomt van de gegevensimporteur of van een andere voor de gegevensimporteur werkende subverwerker persoonsgegevens te ontvangen, uitsluitend ten behoeve van de verwerkingsactiviteiten die namens de gegevensexporteur worden verricht na de doorgifte, overeenkomstig de instructies van de gegevensexporteur, de voorwaarden van de bepalingen en de voorwaarden van het schriftelijke contract inzake subverwerking;

e)wordt onder „toepasselijk recht inzake gegevensbescherming" verstaan: de wettelijke bepalingen ter bescherming van de fundamentele rechten en vrijheden van personen, en met name hun recht op bescherming van de persoonlijke levenssfeer in verband met de verwerking van persoonsgegevens, die in de lidstaat van vestiging van de gegevensexporteur van toepassing zijn op een voor de verwerking verantwoordelijke;

f)wordt onder „technische en organisatorische beveiligingsmaatregelen" verstaan: maatregelen die tot doel hebben persoonsgegevens te beveiligen tegen vernietiging, hetzij per ongeluk, hetzij onrechtmatig, tegen verlies, vervalsing, niet-toegelaten verspreiding of toegang, met name wanneer de verwerking de doorzending van gegevens in een netwerk omvat, dan wel tegen enige andere vorm van onwettige verwerking.

Bepaling 2

Bijzonderheden betreffende de doorgifte

De bijzonderheden betreffende de doorgifte, met name, in voorkomend geval, de bijzondere categorieën persoonsgegevens, worden nader omschreven in aanhangsel 1, dat een integrerend deel van de bepalingen vormt.

Bepaling 3

Derdenbeding

1.De betrokkenen kunnen deze bepaling en bepaling 4, onder b) tot en met i), bepaling 5, onder a) tot en met e) en g) tot en met j), bepaling 6, leden 1 en 2, bepaling 7, bepaling 8, lid 2, en de bepalingen 9 tot en met 12 als derde begunstigden tegenover de gegevensexporteur afdwingen.

2.De betrokkenen kunnen deze bepaling, bepaling 5, onder a) tot en met e) en onder g), bepaling 6, bepaling 7, bepaling 8, lid 2, en de bepalingen 9 tot en met 12 tegenover de gegevensimporteur afdwingen in gevallen waarin de gegevensexporteur feitelijk is verdwenen of heeft opgehouden rechtens te bestaan, tenzij een rechtsopvolger contractueel of rechtens alle wettelijke verplichtingen van de gegevensexporteur heeft overgenomen en daardoor de rechten en verplichtingen van de gegevensexporteur op zich neemt; in dit geval kunnen betrokkenen de genoemde bepalingen tegenover deze rechtsopvolger afdwingen.

3.De betrokkenen kunnen deze bepaling, bepaling 5, onder a) tot en met e) en onder g), bepaling 6, bepaling 7, bepaling 8, lid 2, en de bepalingen 9 tot en met 12 tegenover de

subverwerker afdwingen in die gevallen waarin zowel de gegevensexporteur als de gegevensimporteur feitelijk is verdwenen, heeft opgehouden rechtens te bestaan of insolvent is geworden, tenzij een rechtsopvolger contractueel of rechtens alle wettelijke verplichtingen van de gegevensexporteur heeft overgenomen en daardoor de rechten en verplichtingen van de gegevensexporteur op zich neemt; in dat geval kunnen betrokkenen de genoemde bepalingen tegenover deze rechtsopvolger afdwingen. Deze aansprakelijkheid van de subverwerker jegens derden blijft beperkt tot de verwerkingswerkzaamheden die deze zelf heeft uitgevoerd krachtens de bepalingen.

4. De partijen verzetten zich er niet tegen dat de betrokkenen door een vereniging of andere instelling worden vertegenwoordigd, indien de betrokkenen dit uitdrukkelijk wensen en dit in het nationale recht is toegestaan.

Bepaling 4

Verplichtingen van de gegevensexporteur

De gegevensexporteur stemt ermee in en garandeert dat:

a) de verwerking van de persoonsgegevens, met inbegrip van de doorgifte zelf, is geschied en zal blijven geschieden in overeenstemming met alle relevante bepalingen van het toepasselijke recht inzake gegevensbescherming (en, waar van toepassing, is gemeld aan de betrokken autoriteiten van de lidstaat waar de gegevensexporteur is gevestigd), en dat zij niet in strijd is met de toepasselijke bepalingen van die staat;

b) hij de gegevensimporteur instructie heeft gegeven, en gedurende de verwerking van de persoonsgegevens zal geven, de persoonsgegevens uitsluitend namens de gegevensexporteur en in overeenstemming met het toepasselijke recht inzake gegevensbescherming en de bepalingen te verwerken;

c) de gegevensimporteur voldoende waarborgen zal bieden ten aanzien van de technische en organisatorische beveiligingsmaatregelen die in aanhangsel 2 bij dit contract worden omschreven;

d) deze beveiligingsmaatregelen, na een beoordeling van de vereisten van het toepasselijke recht inzake gegevensbescherming, geschikt zijn bevonden om persoonsgegevens te beschermen tegen vernietiging, hetzij bij ongeluk, hetzij onrechtmatig, tegen verlies, vervalsing, niet-toegelaten verspreiding of toegang, met name wanneer de verwerking doorzending van gegevens via een netwerk omvat, dan wel tegen enige andere vorm van onwettige verwerking, en deze maatregelen gezien de aan de verwerking en de aard van de te beschermen gegevens verbonden risico's een passend beveiligingsniveau waarborgen, gelet op de stand van de techniek en de kosten van de tenuitvoerlegging;

e) hij op de naleving van deze beveiligingsmaatregelen zal toezien;

f) wanneer de doorgifte bijzondere categorieën gegevens betreft, de betrokkene ervan in kennis is gesteld, of vóór of zo spoedig mogelijk na de doorgifte ervan in kennis zal worden gesteld, dat zijn gegevens kunnen worden doorgegeven naar een derde land dat geen passende bescherming biedt als bedoeld in Richtlijn 95/46/EG;

g) hij overeenkomstig bepaling 5, onder b), en bepaling 8, lid 3, ontvangen kennisgevingen van de gegevensimporteur of een subverwerker aan de toezichthoudende autoriteit zal doorzenden, wanneer hij (dat wil zeggen de gegevensexporteur) besluit de doorgifte voort te zetten of de opschorting op te heffen;

h) hij op verzoek een afschrift van de bepalingen ter beschikking van de betrokkene zal stellen,

met uitzondering van aanhangsel 2, alsmede een beknopte beschrijving van de beveiligingsmaatregelen en een afschrift van elk contract voor subverwerkingsdiensten dat overeenkomstig de bepalingen dient te worden opgesteld; indien de bepalingen of het contract commerciële informatie bevatten, mag de gegevensexporteur deze commerciële informatie verwijderen;

i) in geval van subverwerking de verwerkingsactiviteiten worden uitgevoerd overeenkomstig bepaling 11 door een subverwerker die ten minste hetzelfde beschermingsniveau voor de persoonsgegevens en de rechten van de betrokkenen waarborgt als de gegevensimporteur overeenkomstig deze bepalingen; en

j) hij zal toezien op de naleving van bepaling 4, onder a) tot en met i).

Bepaling 5

Verplichtingen van de gegevensimporteur (2)

De gegevensimporteur stemt ermee in en garandeert dat:

a) hij de persoonsgegevens uitsluitend namens de gegevensexporteur en in overeenstemming met diens instructies en met de bepalingen verwerkt; indien hij om welke reden dan ook daartoe niet in staat is, stemt hij ermee in de gegevensexporteur onverwijld daarvan in kennis te stellen, in welk geval de gegevensexporteur de gegevensdoorgifte mag opschorten en/of het contract mag beëindigen;

b) hij geen reden heeft aan te nemen dat de op hem toepasselijke wetgeving hem belet de van de gegevensexporteur ontvangen instructies en zijn verplichtingen krachtens het contract na te komen, en dat hij in geval van een wijziging in deze wetgeving die in aanzienlijke mate afbreuk dreigt te doen aan de in de bepalingen opgenomen waarborgen en verplichtingen, de gegevensexporteur, zodra hij de wijziging kent, onverwijld daarvan in kennis stelt, in welk geval de gegevensexporteur de gegevensdoorgifte mag opschorten en/of het contract mag beëindigen;

c) hij de in aanhangsel 2 omschreven technische en organisatorische beveiligingsmaatregelen vóór de verwerking van de doorgegeven persoonsgegevens heeft getroffen;

d) hij de gegevensexporteur onverwijld ervan in kennis stelt wanneer:

   i) een wetshandhavingsinstantie een juridisch bindend verzoek om verstrekking van persoonsgegevens heeft gedaan, tenzij deze kennisgeving anderszins is verboden, zoals een strafrechtelijk verbod dat ten doel heeft de vertrouwelijkheid van een wetshandhavingsonderzoek te bewaren;

   ii) iemand per ongeluk of op ongeoorloofde wijze toegang tot de gegevens heeft gehad;

   iii) hij van de betrokkenen rechtstreeks een verzoek heeft ontvangen, waarop hij niet ingaat, tenzij hem dit anderszins is toegestaan;

e) hij alle vragen van de gegevensexporteur betreffende de door hem uitgevoerde verwerking van de doorgegeven persoonsgegevens zo spoedig mogelijk naar behoren beantwoordt en het advies van de toezichthoudende autoriteit volgt bij de verwerking van de doorgegeven gegevens;

f) hij op verzoek van de gegevensexporteur zijn verwerkingsvoorzieningen beschikbaar stelt voor controle van de onder deze bepalingen vallende verwerkingsactiviteiten, welke wordt uitgevoerd door de gegevensexporteur of door een controleorgaan waarvan de leden onafhankelijk zijn, over de vereiste beroepskwalificaties beschikken, tot geheimhouding

verplicht zijn en door de gegevensexporteur worden aangewezen, waar van toepassing in overleg met de toezichthoudende autoriteit;

g)hij, wanneer de betrokkene geen afschrift van de gegevensexporteur kan verkrijgen, hem op verzoek een afschrift van de bepalingen alsmede eventuele subverwerkingscontracten ter beschikking stelt, met uitzondering van aanhangsel 2 dat door een beknopte beschrijving van de beveiligingsmaatregelen wordt vervangen; indien de bepalingen of contracten commerciële informatie bevatten, mag de gegevensimporteur deze commerciële informatie verwijderen;

h)hij, wanneer subverwerking plaatsvindt, de gegevensexporteur tevoren heeft ingelicht en diens schriftelijke toestemming heeft verkregen;

i)de verwerkingsdiensten van de subverwerker overeenkomstig bepaling 11 zullen worden uitgevoerd;

j)hij van elk subverwerkingscontract dat hij in het kader van de bepalingen aangaat, onverwijld een afschrift doet toekomen aan de gegevensexporteur.

Bepaling 6

Aansprakelijkheid

1.De partijen komen overeen dat elke betrokkene die ten gevolge van een schending van de verplichtingen bedoeld in bepaling 3 of bepaling 11 door een partij of een subverwerker schade heeft geleden, het recht heeft van de gegevensexporteur vergoeding voor de geleden schade te ontvangen.

2.Wanneer de betrokkene geen vordering tot schadevergoeding wegens niet-nakoming door de gegevensimporteur of diens subverwerker van een van de in bepaling 3 of bepaling 11 bedoelde verplichtingen, als bedoeld in lid 1, tegen de gegevensexporteur kan instellen doordat de gegevensexporteur feitelijk is verdwenen, heeft opgehouden rechtens te bestaan of insolvent is geworden, stemt de gegevensimporteur ermee in dat de betrokkene een vordering kan instellen tegen de gegevensimporteur alsof hij de gegevensexporteur was, tenzij een rechtsopvolger contractueel of rechtens alle wettelijke verplichtingen van de gegevensexporteur heeft overgenomen, in welk geval de betrokkene zijn rechten tegenover die rechtsopvolger kan doen gelden.

De gegevensimporteur kan zich niet aan zijn aansprakelijkheid onttrekken door zich te beroepen op niet-nakoming van verplichtingen door de subverwerker.

3.Wanneer de betrokkene de in lid 1 of 2 bedoelde vordering wegens niet-nakoming door de subverwerker van een van de in bepaling 3 of bepaling 11 bedoelde verplichtingen niet tegen de gegevensexporteur of de gegevensimporteur kan instellen doordat zowel de gegevensexporteur als de gegevensimporteur feitelijk is verdwenen, heeft opgehouden rechtens te bestaan of insolvent is geworden, stemt de subverwerker ermee in dat de betrokkene een vordering kan instellen tegen de subverwerker, met betrekking tot diens eigen verwerkingsactiviteiten krachtens de bepalingen, alsof deze de gegevensexporteur of de gegevensimporteur was, tenzij een rechtsopvolger contractueel of rechtens alle wettelijke verplichtingen van de gegevensexporteur of de gegevensimporteur heeft overgenomen, in welk geval de betrokkene zijn rechten tegenover die rechtsopvolger kan doen gelden. De aansprakelijkheid van de subverwerker blijft beperkt tot de verwerkingsactiviteiten die deze zelf heeft uitgevoerd krachtens de bepalingen.

Bepaling 7

Bemiddeling en rechtsmacht

1. De gegevensimporteur stemt ermee in dat, indien de betrokkene tegen hem rechten ten behoeve van derden en/of vorderingen tot schadevergoeding krachtens de bepalingen inroept, de gegevensimporteur de beslissing van de betrokkene aanvaardt:
   a) om het geschil te onderwerpen aan bemiddeling door een onafhankelijke persoon of, waar van toepassing, door de toezichthoudende autoriteit;
   b) om het geschil voor te leggen aan een rechterlijke instantie in de lidstaat waar de gegevensexporteur is gevestigd.
2. De partijen komen overeen dat de door de betrokkene gemaakte keuze geen afbreuk doet aan diens materiële of formele rechten om op grond van andere bepalingen van nationaal of internationaal recht verhaal te zoeken.

Bepaling 8

Samenwerking met de toezichthoudende autoriteiten

1. De gegevensexporteur stemt ermee in een afschrift van dit contract bij de toezichthoudende autoriteit neer te leggen, indien deze daarom verzoekt of indien dit krachtens het toepasselijke recht inzake gegevensbescherming vereist is.
2. De partijen komen overeen dat de toezichthoudende autoriteit bevoegd is bij de gegevensimporteur en eventuele subverwerkers een controle te verrichten die dezelfde reikwijdte heeft en aan dezelfde voorwaarden is onderworpen als die welke krachtens het toepasselijke recht inzake gegevensbescherming voor haar controle van de gegevensexporteur zouden gelden.
3. Indien er wetgeving bestaat die op de gegevensimporteur of een subverwerker van toepassing is en die de uitvoering van controles als in lid 2 bedoeld op de gegevensimporteur of een subverwerker verbiedt, stelt de gegevensimporteur de gegevensexporteur daarvan onverwijld in kennis. In een dergelijk geval mag de gegevensexporteur de in bepaling 5, onder b), bedoelde maatregelen nemen.

Bepaling 9

Toepasselijk recht

Op de bepalingen is het recht van de lidstaat van vestiging van de gegevensexporteur van toepassing, te weten …

Bepaling 10

Wijziging van het contract

De partijen verbinden zich ertoe de bepalingen niet te wijzigen. Dit vormt voor de partijen geen beletsel om indien nodig bepalingen toe te voegen betreffende met de transactie verband houdende vraagstukken, mits deze niet met de modelcontractbepalingen in strijd zijn.

Bepaling 11

Subverwerking

1. De gegevensimporteur besteedt de verwerkingsactiviteiten die hij overeenkomstig de bepalingen namens de gegevensexporteur uitvoert, niet uit zonder de voorafgaande schriftelijke toestemming van de gegevensexporteur. Indien de gegevensimporteur met toestemming van de gegevensexporteur zijn verplichtingen uit hoofde van de bepalingen uitbesteedt, dient hij met de subverwerker een schriftelijk contract te sluiten waarbij aan de subverwerker dezelfde verplichtingen worden opgelegd als die waaraan de gegevensimporteur uit hoofde van de bepalingen moet voldoen (3). Indien de subverwerker niet voldoet aan zijn verplichtingen tot gegevensbescherming uit hoofde van dat schriftelijke contract, blijft de gegevensimporteur jegens de gegevensexporteur volledig aansprakelijk voor de uitvoering van de verplichtingen van de subverwerker uit hoofde van dat contract.
2. In het tevoren tussen de gegevensimporteur en de subverwerker te sluiten schriftelijke contract dient tevens een derdenbeding te zijn opgenomen zoals vervat in bepaling 3, dat voorziet in gevallen dat de betrokkene geen vordering tot schadevergoeding als bedoeld in bepaling 6, lid 1, kan instellen tegen de gegevensexporteur of de gegevensimporteur omdat deze feitelijk zijn verdwenen, hebben opgehouden rechtens te bestaan of insolvent zijn geworden, en er geen rechtsopvolger is die contractueel of rechtens alle wettelijke verplichtingen van de gegevensexporteur of de gegevensimporteur heeft overgenomen. Deze aansprakelijkheid van de subverwerker jegens derden blijft beperkt tot de verwerkingswerkzaamheden die deze zelf heeft uitgevoerd krachtens de bepalingen.
3. Op de in lid 1 bedoelde bepalingen betreffende de gegevensbeschermingsaspecten van de subverwerking uit hoofde van het in lid 1 bedoelde contract is het recht van de lidstaat van vestiging van de gegevensexporteur van toepassing, te weten …
4. De gegevensexporteur houdt een lijst bij van subverwerkingscontracten die krachtens de bepalingen zijn gesloten en door de gegevensimporteur overeenkomstig bepaling 5, onder j), zijn aangemeld, en werkt deze ten minste eenmaal per jaar bij. Deze lijst wordt ter beschikking gesteld van de toezichthoudende autoriteit voor gegevensbescherming die op de gegevensexporteur toezicht houdt.

Bepaling 12

Verplichting na de beëindiging van de verwerking van persoonsgegevens

1. De partijen komen overeen dat de gegevensimporteur en de subverwerker na het beëindigen van de verlening van de gegevensverwerkingsdiensten alle doorgegeven persoonsgegevens en kopieën daarvan aan de gegevensexporteur terugbezorgen of, indien de gegevensexporteur dat verkiest, alle persoonsgegevens vernietigen en aan de gegevensexporteur verklaren dat de vernietiging heeft plaatsgevonden, tenzij de op de gegevensimporteur toepasselijke wetgeving hem verbiedt alle of een gedeelte van de doorgegeven persoonsgegevens terug te bezorgen of te vernietigen. In dat geval garandeert de gegevensimporteur dat hij de vertrouwelijkheid van de doorgegeven persoonsgegevens zal respecteren en dat hij de doorgegeven gegevens niet verder actief zal verwerken.
2. De gegevensimporteur en de subverwerker garanderen dat zij op verzoek van de gegevensexporteur en/of de toezichthoudende autoriteit hun verwerkingsvoorzieningen voor een controle van de in lid 1 bedoelde maatregelen beschikbaar zullen stellen.

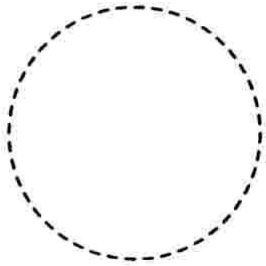
Namens de gegevensexporteur:

Naam (voluit): …

Functie: …

Adres: …

Eventuele andere inlichtingen die voor het verbindend worden van het contract noodzakelijk zijn:

	Handtekening …

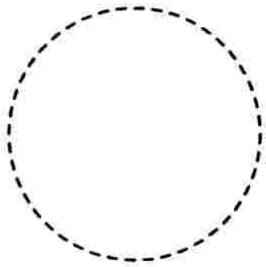
Namens de gegevensimporteur:

Naam (voluit): …

Functie: …

Adres: …

Eventuele andere inlichtingen die voor het verbindend worden van het contract noodzakelijk zijn:

	Handtekening …

(1) De partijen kunnen in deze bepaling de definities en begrippen van Richtlijn 95/46/EG herhalen, indien zij de voorkeur geven aan een autonoom contract.

(2) Vereisten van het nationale recht die op de gegevensimporteur van toepassing zijn en die niet verder gaan dan wat in een democratische samenleving noodzakelijk is op basis van een van de in artikel 13, lid 1, van Richtlijn 95/46/EG vermelde belangen, dat wil zeggen noodzakelijke maatregelen ter vrijwaring van de veiligheid van een staat, de landsverdediging, de openbare veiligheid, het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten of schendingen van de beroepscodes voor gereglementeerde beroepen, een belangrijk economisch en financieel belang van een lidstaat of de bescherming van de betrokkene of van de rechten en vrijheden van anderen, zijn niet in strijd met de bepalingen. Enkele voorbeelden van dergelijke vereisten die niet verder gaan dan wat in een democratische samenleving noodzakelijk is, zijn internationaal erkende sancties, verplichtingen in verband met de belastingaangifte en verplichtingen in verband met het melden van witwaspraktijken.

(3) Aan deze eis kan worden voldaan door medeondertekening door de subverwerker van het contract tussen de gegevensexporteur en de gegevensimporteur dat krachtens dit besluit wordt gesloten.

Aanhangsel 1

Bij de modelcontractbepalingen

Dit aanhangsel maakt deel uit van de bepalingen en moet door de partijen worden ingevuld en ondertekend.

De lidstaten kunnen overeenkomstig hun nationale procedures aanvullende of meer gedetailleerde gegevens voorschrijven die in dit aanhangsel moeten worden opgenomen.

Gegevensexporteur

De gegevensexporteur is (beschrijf in het kort de voor de doorgifte relevante activiteiten):

…

…

…

Gegevensimporteur

De gegevensimporteur is (beschrijf in het kort de voor de doorgifte relevante activiteiten):

…

…

…

Betrokkenen

De doorgegeven persoonsgegevens betreffen de volgende categorieën betrokkenen:

…

…

…

Categorieën gegevens

De doorgegeven persoonsgegevens betreffen de volgende categorieën gegevens:

…

…

…

Bijzondere categorieën gegevens (indien van toepassing)

De doorgegeven persoonsgegevens betreffen de volgende bijzondere categorieën gegevens:

…

…

…

Verwerking

De doorgegeven persoonsgegevens zullen de volgende basisverwerkingen ondergaan:

…

…

…

DE GEGEVENSEXPORTEUR

Naam: …

Handtekening van de bevoegde persoon: …

DE GEGEVENSIMPORTEUR

Naam: …

Handtekening van de bevoegde persoon: …

8.2 BIJLAGE 2: Binding Corporate Rules Siemens

Binding Corporate Rules ("BCR") – SIEMENS

This document contains in its Sections 3 – 9 all provision of the "Binding Corporate Rules (BCR) for Siemens Group Companies and Other Adopting Companies for the Protection of Personal Data" which are binding vis-à-vis data subjects, by virtue of third-party beneficiary rights.

1. Purpose of the BCR

Protecting the security and privacy of personal data is important to Siemens. Therefore, Siemens conducts its business in compliance with applicable laws on data privacy protection and data security. The BCR are internal rules adopted by Siemens, i.e. Siemens AG and its participating group companies, to adduce "adequate safeguards for the protection of the privacy and fundamental rights and freedoms of individuals" within the meaning of applicable data protection law, especially the data protection laws of member states of European Economic Area ("EEA").

2. Scope of the BCR

The BCR apply to the processing of all personal data relating to data subjects by participating companies established

· outside an EEA country to the extent that this personal data has been transferred from a participating company established in an EEA country or established in a country with an adequate level of data protection as acknowledged by a decision of the EU Commission to a participating company established outside the EEA; and

· in an EEA country or in a country with an adequate level of data protection as acknowledged by a decision of the EU Commission.

3. Substantive principles for the processing of personal data

The following principles which derive specifically from the EU Data Protection Directive 95/46/EC and the Madrid Resolution of November 5, 2009 apply to the processing of personal data by participating companies within the scope of these BCR:

3.1 Legitimacy & legality of data processing

The processing of personal data shall be done lawfully in compliance with the relevant statutory provisions and with due regard for the principles laid down in these BCR. Processing is only permissible if at least one of the following prerequisites is fulfilled:

· The data subject has freely given his/her unambiguous, effective consent; or

· Data processing is for the purpose of establishing a contractual relationship or similar relationship of trust with the data subject; or

· Processing is necessary to safeguard justified interests of the controller (for the purpose of these BCR "controller" shall mean the company which determines the purposes and means of data

processing; dependent branches, places of business and permanent establishments are part of the controller) and there are no grounds for assuming that the data subject has an overriding legitimate interest in precluding data processing; or

· Processing is stipulated or permitted by national law and regulations that apply for the controller; or

· Processing is necessary for compliance with legal obligations to which the controller is subject; or

· Processing is required, exceptionally, to protect the life, health or safety of the data subject. The controller shall provide simple, fast and efficient procedures that allow the data subject to withdraw his/her consent at any time.

3.2 Purpose

Personal data shall be processed exclusively for specified, explicit and legitimate purposes. Under no circumstances, shall personal data be processed in a way incompatible with the legitimate purposes for which the personal data was collected. Participating companies are obligated to adhere to these original purposes when storing and further processing or using data transferred to them by another participating company; the purpose of data processing may only be changed with the consent of the data subject or to the extent permitted by the national law to which the participating company transferring the data is subject.

3.3 Transparency

All participating companies shall process personal data in a transparent manner. Data subjects whose personal data is processed by a participating company shall be provided with the following information by the participating company (in consultation with the transferring company, if applicable):

· Identity of the controller and of the transferring company;

· Categories of recipients or identity of the receiving entity;

· Purpose of processing;

· Origin of the data (unless this is personal data collected directly from the data subject);

· Right of objection to the processing of personal data of the data subject for advertising purposes;

· Other information to the extent required for reasons of equity, e.g. rights of information, rectification and erasure.

To the extent that the personal data was not collected directly from the data subject, such information - as an exception - need not be provided, if this non-provision of information is necessary in order to protect the data subject or the rights of other persons, if the data subject has already been informed or if this would involve disproportionate effort.

3.4 Data quality and data economy

Personal data must be factually correct and – if necessary – kept up to date. Appropriate measures are to be taken to ensure that inaccurate or incomplete data is corrected or erased. Data processing shall be guided by the principle of data economy. The objective is to collect, process and use only such personal data as is required, i.e. as little personal data as possible. In particular, use is to be made of the possibility of anonymous or pseudonymous data, provided that the cost and effort involved is commensurate with the desired purpose. Statistical evaluations or studies based on anonymized or pseudonymized data are not relevant for data privacy protection purposes, provided that such data cannot be used to identify the data subject. Personal data which is no longer required for the business purposes for which it was originally collected and stored, is to be erased. In the event that statutory retention periods apply, the data shall be blocked rather than erased.

3.5 Onward transfer of data

The transfer of personal data from a participating company to a non participating company (i.e. a company that is not bound to the BCR) outside the EEA is only permissible under the following conditions:

· The receiving entity is endowed with an adequate level of protection for personal data within the meaning of Article 25 of the EU Data Protection Directive 95/46/EC, e.g. by concluding an EU standard contract (Standard Contractual Clauses for Data Processors 2010/87/EU or Standard Contractual Clauses between Data Controllers 2001/497/EC or 2004/915/EC) or by concluding other appropriate contractual agreements between the transferring and the receiving entity;

· The transfer is permissible under the exceptions defined in Article 26 of the EU Data Protection Directive 95/46/EC;

· If the receiving entity is a processor, the conditions set out in Article 16 and 17 of the EU Data Protection Directive 95/46/EC must additionally be satisfied.

3.6 Special categories of personal data

Special categories of personal data, in other words information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life, may not be processed as a general principle. Should the processing of special categories of personal data be necessary, the explicit consent of the data subject must be obtained, unless,

· the data subject is not in a position to give his/her consent (e.g. medical emergency) and processing is necessary to protect the vital interests of the data subject or of another person; or

· processing is required in connection with medical diagnosis, preventive medicine, the provision of care or treatment or the management of healthcare services where data processing is carried out by medical staff who are subject to the obligation of professional secrecy or by other staff subject to an equivalent obligation of secrecy, or

· the data subject has already made public the data in question; or

· processing is necessary for the establishment, exercise or defense of legal claims in court proceedings, provided that there are no grounds for assuming that the data subject has an overriding legitimate interest in ensuring that such data is not processed; or

· processing is expressly permitted by law under the applicable national legislation (e.g. for the purpose of registering/protecting minorities), and additional guarantees within the meaning of the EU Data Protection Directive 95/46/EC are provided for the processing of the data, including specifically adequate security measures for this data. The competent Data Privacy Officer (DPO) of the participating company shall be consulted prior to the processing of special categories of personal data.

3.7 Automated individual decisions

If personal data is processed for the purpose of making automated individual decisions, the legitimate interests of the data subject must be ensured through appropriate measures. Decisions which have negative legal consequences for the data subject or substantially prejudice the data subject, may not be reached exclusively on the basis of an automated individual procedure designed to evaluate an individual's personal characteristics, i.e. decisions may not be exclusively based on the use of information technology. An exception applies only if the decision

· is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as giving him/her the opportunity to put his point of view; or

· is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

3.8 Data security

Controllers are to take appropriate technical and organizational measures to ensure the requisite data security, which protects personal data against accidental or unlawful erasure, unauthorized use, alteration, against loss, destruction as well as against unauthorized disclosure or unauthorized access. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected. Special categories of personal data are to be given special protection.

The security measures to be provided relate in particular to computers (servers and workplace computers), networks, communication links and applications.

To ensure an adequate level of technical and organizational measures for data protection, Siemens introduced the Corporate Information Security Guide with binding effect for the entire Siemens group.

Specific measures used to ensure adequate protection of personal data include admission controls, system access controls, data access controls, transmission controls, input controls, job controls, availability controls and segregation controls.

All workplace computers – including mobile devices (e.g. laptops) – are password-protected. The Siemens intranet has a firewall system to protect internal company content from unauthorized external access. Transmission of personal data within the company's own network is typically encrypted – to the extent that the nature and intended purpose of the personal data requires this.

3.9 Confidentiality of data processing

Only personnel who are authorized and have been specifically instructed in compliance with data privacy protection requirements, may collect, process or use personal data. Access authorization of the individual employee will be restricted according to the nature and scope of his/her particular field of activity. The employee is prohibited from using personal data for private purposes, from transferring or from otherwise making available personal data to unauthorized persons. Unauthorized persons in this context include, for example, other employees, to the extent that they do not require the personal data to complete their specialist tasks. The confidentiality obligation continues beyond the end of the employment relationship of the employee in question.

3.10 Commissioned data processing

If a participating company commission another company ("processor") to process personal data under the terms of these BCR, the following requirements must be observed:

· The processor is to be carefully selected by the controller; a processor shall be selected who is able to ensure the necessary technical and organizational security measures required to perform data processing in compliance with data privacy protection regulations;

· The controller shall ensure and regularly verify that the processor remains fully compliant with the agreed technical and organizational security measures;

· The performance of commissioned data processing must be regulated in a written or otherwise documented contract, in which the rights and obligations of the processor are unambiguously defined;

· The processor must be bound by contract to process the data received from the controller only within the contractual framework and in accordance with the instructions issued by the controller. The processing of data for the processor's own purposes or for the purposes of a third party must be prohibited by contract;

· The controller retains responsibility for the legitimacy of processing and continues to be the point of contact for the data subject.

4. Substantive rights of the data subject

Data subjects have the inalienable rights listed below in respect of their personal data processed by a participating company within the scope of these BCR.

· The data subject can demand communication to him in an intelligible form of the personal data processed in relation to him/her, of any available information as to its source, and the purpose of the processing. The data subject also has the right to information about the identity of the controller and, in the event of the transfer of personal data, the data subject also has the right to information

about the recipients or categories of recipients. The right to information also covers the logical structure of automated processing operations, to the extent that automated decisions are affected. When provided for by applicable local law, the data subject does not have a right to information if it would involve considerable impairment of business purposes, including specifically if the disclosure of business secrets and the interest in safeguarding the business secrets outweighs the data subject's interest in disclosure. Local legal regulations may restrict the data subject's right to information if this right is exercised repeatedly within a short period of time, unless the data subject can show a legitimate reason for the repeated assertion of claims for information. The participating company may charge the data subject a reasonable fee for providing the information, to the extent that the applicable national law permits this.

· The data subject can demand rectification if his/her personal data is found to be incorrect or incomplete.

· The data subject has the right to demand that his/her personal data be blocked off if it is not possible to establish whether the data is correct or incorrect.

· The data subject has the right to demand that his/her personal data be erased if the data processing was unlawful or has become unlawful in the interim or as soon as the data is no longer required for the purpose of the processing. Justified claims by the data subject for erasure are to be acted on within a reasonable period, to the extent that statutory retention periods or contractual obligations do not prevent erasure. In the event of statutory retention periods, the data subject may demand that his/her data be blocked rather than erased. The same applies if it would be impossible to erase the data.

· The data subject has the right to object to the processing of his/her personal data for advertising purposes or for purposes of market research and/or opinion polling purposes. The data subject shall be informed of his/her right to object free of charge.

· The data subject also has a general right of objection to the processing of his/her personal data, if because of the data subject's special personal situation, the legitimate interest of the data subject outweighs the legitimate interest of the controller in processing the personal data.

The data subject can assert the above rights in writing vis-à-vis the respective participating company, the competent Data Privacy Officer (DPO) of such participating company or the Global Data Privacy function (LC CO DP) of Siemens AG. The justified request of the data subject shall receive a response from the contacted entity within a reasonable period. The response shall be in written form (e-mail is sufficient).

5. Binding nature vis-à-vis data subjects

The regulations in the BCR contained in Sections 3 - 9 of this document are also binding vis-à-vis data subjects, by virtue of third-party beneficiary rights.

Data subjects can choose to lodge a complaint for non-compliance with the regulations of the BCR contained herein by a participating company either against the participating company or against Siemens AG (LC CO DP).

In addition, data subjects are entitled to enforce compliance with one of the above-mentioned third party beneficiary rights by a participating company, by lodging a complaint before the competent data protection authority or by seeking other legal remedies in the competent courts. Data subjects may claim compensation for damages.

Data subjects can choose to lodge such a complaint

· before the jurisdiction of the participating company that transferred the data; or

· before the jurisdiction of the headquarters of Siemens AG; or

· before the competent data protection authority.

This means that in the event of a breach of the BCR regulations by a participating company established outside the EEA, courts and authorities within the EEA are also competent. The data subject holds the same rights vis-à-vis the participating company that has accepted liability, as if the breach had been committed by a participating company established in an EEA country.

The competence of courts and authorities in the EEA as described above does not apply however if the data recipient is established in a country outside the EAA but that country does have an adequate level of data protection as acknowledged by a decision of the EU Commission.

In order to ensure that data subjects enjoy legally enforceable third party beneficiary rights also in those countries where the granting of third party beneficiary rights in the BCR document might not be sufficient, Siemens AG will – to the extent necessary – draw up additional contractual agreements with the relevant participating companies allowing for this. A third party beneficiary clause granting the necessary rights to data subjects is included in the Declaration of Commitment which group companies sign to signify their acceptance and implementation of the BCR. The same applies for the Adoption Agreement which the other adopting companies conclude with Siemens AG.

6. Complaint process

Data subjects can contact the competent complaint handling department in Siemens AG (LC CO DP; for contact details, see Section 10) or the participating company's competent local point of contact for data protection (generally the Data Privacy Officer (DPO)), at any time, with complaints about a breach of the BCR by a participating company or with any questions. The data subject shall be given prompt confirmation of receipt of the complaint at the entity contacted and the complaint shall be processed within three (3) months of receipt of the complaint. This timeframe can be reasonably exceeded in case of delays not attributable to the participating company, e.g. in case of a failure of the data subject to timely provide information that is reasonably necessary. The employees involved with complaint processing in the competent complaint handling department benefit from an appropriate level of independence in the exercise of this function.

In any inquiry, the participating company and LC CO DP are obligated to cooperate with the data protection authorities of the country and to respect their opinions.

7. Mutual assistance and cooperation with the data protection authorities

Siemens AG and the participating companies will trustfully cooperate and support one another in the event of inquiries and complaints from data subjects with regard to non compliance with the BCR. Siemens AG and the participating companies further undertake to trustfully cooperate with the competent data protection authorities in the context of implementation of the BCR.

They will answer BCR-related requests from the data protection authority within an appropriate timeframe and in an appropriate fashion and will follow the advice and decisions of the competent data protection authority with regard to implementation of the BCR.

8. Relationship between BCR and local statutory regulations

The legitimacy of processing of personal data is judged on the basis of the applicable local law. To the extent that the applicable local law stipulates a higher level of protection of personal data than these BCR, data processing shall be in accordance with the applicable law. Each participating company shall check for itself (e.g. through its Data Privacy Officer (DPO) or by the Legal department), whether such local statutory regulations (e.g. data privacy laws) exist and shall ensure compliance with these. If the applicable local law provides a lower level of protection for personal data than these BCR, the present BCR shall be applied.

In the event that obligations arising from the applicable local law are in conflict with the BCR, the participating company shall inform the LC C DP without undue delay. LC C DP will record the reported conflict.

LC C DP will inform all participating companies which previously transferred data to the participating company in question, of the reported conflict between the BCR and the local law. LC C DP will also inform the competent data protection authority of the regulatory conflict and, together with the data protection authority and the participating company, will seek a practical solution that comes as close as possible to the principles in the EU Data Protection Directive 95/46/EC.

9. Liability

Siemens AG assumes liability for non-compliance with the BCR by participating companies established outside the EEA. Siemens AG undertakes to monitor BCR compliance by participating companies established outside the EEA and to ensure that participating companies established outside the EEA take the necessary corrective actions to remedy breaches of the BCR.

Siemens AG further undertakes to pay compensation for damages in the event of a proven breach of the BCR and a resulting violation of a data subject's rights.

The burden of proof lies with Siemens AG. Siemens AG shall demonstrate that no breach of the BCR has taken place or that the participating company established outside the EEA is not responsible for the breach of the BCR on which the data subject's claim for damages is based.

Contact Data subjects can raise any concerns with the Data Privacy Officer (DPO) of the relevant participating company or with the global Data Privacy function of Siemens AG: Siemens AG LC CO DP St.-Martin-Str. 76 D-81541 Munich Email: datenschutz@siemens.com Internet: http://www.siemens.com

8.3 BIJLAGE 3: Privacy Statement

DEJURISTEN

PRIVACY STATEMENT NAAM ONDERNEMING

Hoewel je er niet steeds van bewust bent geef je als Gebruiker door het gebruik van onze applicatie steeds enkele 'persoonsgegevens' vrij. Persoonsgegevens zijn die gegevens die ons toelaten jou als natuurlijke persoon te identificeren, ongeacht of we dit daadwerkelijk doen of niet. Dit zal het geval zijn zodra men een directe of indirecte link kan leggen tussen één of meerdere gegevens en jou, de natuurlijke persoon in kwestie.

De verzameling en verwerking van persoonsgegevens wordt door de wetgever aan strenge voorwaarden verbonden zoals bepaald in de wetgeving, voornamelijk de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer (Privacywet). Aangezien ook wij de bescherming van jouw privacy heel belangrijk vinden en hier heel duidelijk over willen zijn, hebben wij deze Privacy Statement opgemaakt.

Door gebruik te maken van de Applicatie en haar diensten gaan wij ervan uit dat iedere Gebruiker kennis heeft genomen van deze Privacy Statement en bijgevolg de verzameling en verwerking van zijn persoonsgegevens, op de wijze zoals hier beschreven, aanvaardt.

Het is mogelijk dat ons Privacy-beleid in de toekomst vatbaar is voor aanpassingen en wijzigingen. Deze zullen duidelijk gemaakt worden in de Privacy Statement. Het is dan ook aan de Gebruiker om op regelmatige basis kennis te nemen van dit document. Iedere substantiële wijziging zal steeds duidelijk gecommuniceerd worden.

1 Wie is de verantwoordelijke van de verwerking?

In de Privacywet wordt een onderscheid gemaakt tussen de verantwoordelijke voor de verwerking en de partijen waar men beroep op doet voor de feitelijke verwerking. Dit onderscheid is uitermate belangrijk om enige onduidelijkheid rond verantwoordelijkheden te vermijden.

1.1 Verantwoordelijke van de verwerking?

De verantwoordelijke voor de verwerking, ook wel data controller genaamd, is elke natuurlijke persoon of rechtspersoon die alleen of samen met anderen het doel en de juridische en technische middelen bepaalt voor de verwerking van persoonsgegevens. Volgende persoon is aangeduid als verantwoordelijke verwerker:

GEGEVENS VERWERKER

1.2 Feitelijke verwerker?

De feitelijke verwerker is de natuurlijke persoon of rechtspersoon die in opdracht van de verantwoordelijke voor de verwerking persoonsgegevens verwerkt. De feitelijke verwerker is verantwoordelijk voor de goede technische werking van de Applicatie (datatransmissie). De personen die onder rechtstreeks gezag van de verantwoordelijke voor de verwerking gemachtigd zijn om de gegevens te verwerken vallen hier niet onder.

Uiteraard is de verantwoordelijke voor de verwerking uitermate zorgvuldig in zijn selectie van feitelijk verwerker. Zo moet de feitelijke verwerker voldoende waarborgen bieden met betrekking tot technische en organisatorische beveiligingsmaatregelen rond de verwerking, en voldoen aan de verplichtingen van artikel 16, §1 privacywet.

De verantwoordelijke voor de verwerking draagt of neemt geen enkele aansprakelijkheid op bij verlies of corruptie van data, identiteitsdiefstal, diefstal van gegevens, virussen of Trojans, SQL-injecties of andere aanvallen op de informaticasystemen of online cloud-portalen. De feitelijke verwerker beslist autonoom over de meest technisch geschikte toepassing om de gegevens te verwerken, en doet dit vanuit zijn professionele expertise. Van de verantwoordelijke voor de verwerking kan niet verwacht worden over dezelfde expertise en specialiteit te beschikken.

2 Voor welke doeleinden worden mijn persoonsgegevens gebruikt?

NAAM ONDERNEMING is een UITLEG APPLICATIE/PLATFORM/….

Persoonsgegevens worden bijgevolg enkel verwerkt voor zover er sprake is van een toestemming of andere rechtsgrond zoals vereist door de Privacywet. De verkregen informatie wordt zichtbaar gemaakt voor andere Gebruikers van onze Applicatie. De mate van toegankelijkheid kan verschillen naargelang de aard van de informatie. Indien de Betrokkene niet akkoord gaat met deze vorm van gegevensverwerking verwijzen wij graag door naar “artikel 4: wat zijn mijn rechten”.

NAAM ONDERNEMING verzamelt de persoonsgegevens van Gebruikers daarnaast om hen een veilige, optimale en persoonlijke Gebruikerservaring aan te bieden. De verzameling van persoonsgegevens wordt uitgebreider naarmate de Gebruiker intensiever gebruik maakt van de Applicatie. Deze vorm van gegevensverwerking is dus essentieel voor de werking van de Applicatie en de daarbij horende diensten. De verwerking gebeurt slechts voor volgende (interne) doeleinden:

- De Gebruiker toegang verschaffen tot zijn Gebruikersprofiel en de daarbij horende functionaliteiten.

- Het aanbieden en verbeteren van onze gepersonaliseerde en algemene dienstverlening; inclusief eventueel aanbod van informatie, nieuwsbrieven en aanbiedingen die nuttig en/of noodzakelijk zijn voor de Gebruiker, de verkrijging en verwerking van Gebruikersbeoordelingen en het verlenen van ondersteuning.

- De detectie van en bescherming tegen fraude, fouten en/of criminele gedragingen.

Wij geven persoonsgegevens nooit door voor externe analyse zonder dat wij een voorafgaande anonimisering hebben doorgevoerd.

Door gebruik te maken van de Applicatie verklaart de Gebruiker zijn uitdrukkelijke toestemming voor de verwerking van zijn persoonsgegevens door NAAM ONDERNEMING. Voor de verwerking van persoonsgegevens van derde personen beroept NAAM ONDERNEMING zich uitdrukkelijk op het feit dat deze verwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is of voor de uitvoering van maatregelen die aan het sluiten van die overeenkomst voorafgaan en die op verzoek van de betrokkene zijn genomen.

Aangezien er geen rem op technologie en innovatie staat, is het onmogelijk een inschatting te maken van onze toekomstige Applicaties en dienstverlening. Het is bijgevolg belangrijk dat deze toestemming ook betrekking heeft op het gebruik van de persoonsgegevens in het kader van de ontwikkeling van nieuwe diensten en functionaliteiten voor zover deze binnen de oorspronkelijke doelstelling van onze Applicatie valt.

2.1 Registratie account

Het gebruik van de Applicatie vereist de aanmaak van een individueel Gebruikersprofiel en de daarbij horende Gebruikersregistratie. Dit betekent dat we alle gegevens kunnen verzamelen die nodig zijn voor de gepersonaliseerde dienstverlening zoals geslacht, leeftijd, demografische gegevens net als enkele essentiële contactgegevens zoals adres, email-adres en telefoonnummer. De betrokkene beslist zelf over de mate van informatie die hij vrij geeft via de Applicatie.

We verzamelen in geen geval gevoelige persoonsgegevens van de Gebruiker, zoals gegevens over uw ras, politieke opvattingen, gezondheid, godsdienstige en andere geloofsovertuigingen, seksuele geaardheid en dergelijke.

Deze gegevensverwerking is essentieel voor de werking van de Applicatie. Deze gegevens kunnen zichtbaar zijn voor andere Gebruikers. De mate van zichtbaarheid kan afhankelijk gemaakt worden van de hoedanigheid van de Gebruiker.

Wij kunnen deze persoonsgegevens eveneens gebruiken voor de verspreiding van commerciële berichten met betrekking tot onze eigen diensten of in opdracht van derde partijen. In dit kader krijgen deze derde partijen nooit toegang tot uw persoonsgegevens.

2.2 Goede technische werking;

Daarenboven verzamelen en verwerken we persoonsgegeven om de Gebruiker de goede technische werking van de Applicatie te garanderen. De Applicatie maakt gebruik van verscheidene middelen om de Gebruikerservaring te optimaliseren en eventuele (technische) fouten in de Applicatie te detecteren;

- Cookies; deze informatie laat ons toe de Gebruiker te herkennen en zodoende efficiënt gebruik te maken van de Applicatiefuncties zoals ingelogd blijven, navigering door de informatie, gebruik van functionaliteiten, gepersonaliseerde commerciële berichten weergeven, etc. Voor een verdere verduidelijking rond onze cookies verwijzen we u graag door naar onze Cookie Policy;

- Log-informatie: dit betreft informatie zoals het IP-adres en diverse telecommunicatie-gegevens.

- Informatie met betrekking tot het gebruikte toestel zoals hardware- en software informatie en netwerk informatie.

- Local storage informatie.

De Applicatie verzamelt eveneens anonieme gegevens, zijnde technische gegevens die uitsluitend voor interne doeleinden gebruikt worden om een beeld te krijgen van Gebruikersnavigatie op de Applicatie.

2.3 Worden mijn gegevens overgedragen aan derde partijen?

De persoonsgegevens worden in de eerste plaats enkel verwerkt voor intern gebruik binnen NAAM ONDERNEMING. We kunnen u dan ook gerust stellen dat persoonsgegevens niet verkocht, doorgegeven of meegedeeld worden aan derde partijen. Gegevens kunnen uitzonderlijk toch meegedeeld worden aan derden indien:

- Er een uitdrukkelijke toestemming is van de betrokkene;

- Wanneer de doorgifte noodzakelijk is voor de uitvoering van de overeenkomst. Dit zal het geval zijn met werknemers, medewerkers, agenten, onderaannemers, leveranciers, commerciële partners, marketingdiensten, etc.;

- Wanneer de doorgifte noodzakelijk is voor de sluiting of de uitvoering van een in het belang van de Gebruiker tussen de verantwoordelijke voor de verwerking en een derde gesloten of te sluiten overeenkomst. Bijvoorbeeld in het kader van fraude;

- Wanneer de doorgifte noodzakelijk is of wettelijk verplicht (zwaarwegend algemeen belang of recht);

De betrokkene is zeker van de vertrouwelijke verwerking van zijn persoonsgegevens in geval van een overname of verkoop van NAAM ONDERNEMING. In dit geval zal NAAM ONDERNEMING de nodige informatie aan betrokkene verschaffen.

NAAM ONDERNEMING is een Belgische onderneming. Niettemin kan er gegevensverwerking en/of –overdracht zijn naar landen buiten de Europese Unie. Ingevolge artikel 21 van de privacywet mogen persoonsgegevens alleen worden doorgegeven aan landen die eenzelfde passend beschermingsniveau waarborgen, en waar dezelfde of gelijkaardige bepalingen van de privacywet worden nageleefd. Het land, duur van de overdracht en opslag, aard van de gegevens en precieze doeleinden zijn criteria die per geval onderzocht moeten worden.

NAAM ONDERNEMING garandeert dat er geen overdracht naar derde landen voor gegevensverwerking of –opslag plaats heeft zonder dat de nodige maatregelen genomen zijn om te voldoen aan de beschermingsvereisten uit de Belgische Privacywet. Deze overdracht zal slechts plaats vinden op basis van één van de gronden zoals vermeld in artikel 2.

3 Worden er locatiegegevens opgeslagen?

De analytische data van NAAM ONDERNEMING kunnen locatiegegevens tonen. Op basis van deze gegevens kan je (vermoedelijke) locatie op een kaart ('Kaart') worden bepaald en aangegeven. Deze aanduidingen (op basis van een IP-adres) zijn echter allesbehalve nauwkeurig, en dus ruim onvoldoende om je precieze locatie te achterhalen.

Deze locatiegegevens worden dus niet gebruikt om iemand te identificeren, doch enkel om de goede technische werking van onze Applicatie te garanderen.

4 Wat zijn mijn rechten?

4.1 Garantie van een rechtmatige en veilige verwerking van de persoonsgegevens

Iedere Gebruiker kan er van uitgaan dat NAAM ONDERNEMING jouw persoonsgegevens steeds 'eerlijk en rechtmatig' verwerkt. Dit wil zeggen dat de gegevens enkel voor de bovenstaande uitdrukkelijk omschreven en gerechtvaardigde doeleinden verwerkt worden. NAAM ONDERNEMING garandeert dan ook dat de gegevensverwerking steeds toereikend, ter zake dienend en niet overmatig is.

We bewaren jouw persoonsgegevens nooit langer op dan strikt noodzakelijk. Wel houden we een archief bij van jouw gegevens, zolang je account actief is, of wanneer je persoonlijke data noodzakelijk is om je een bepaalde dienst te kunnen aanbieden.

NAAM ONDERNEMING heeft voldoende technische en organisatorische beveiligingsmaatregelen getroffen om jou een veilige verwerking van de persoonsgegevens te garanderen. Deze beveiligingsmaatregelen zijn in verhouding met de aard van de persoonsgegevens en de potentiele risico's.

De risico's van een toevallige of ongeoorloofde vernietiging, toevallig verlies, de wijziging van of de toegang tot, en iedere andere niet toegelaten verwerking zijn dan ook tot een minimum gereduceerd. Dit betekent jammer genoeg niet dat er geen risico meer bestaat. Bij een inbraak op haar informaticasystemen zal NAAM ONDERNEMING onmiddellijk alle mogelijke maatregelen nemen om schade en/of diefstal tot een minimum te beperken.

4.2 Recht op verzet

Iedere Gebruiker kan zich steeds verzetten tegen de verwerking van zijn persoonsgegevens. Dit recht van verzet bestaat slechts indien er sprake is van zwaarwegende en gerechtvaardigde redenen die verband houden met zijn bijzondere situatie. De uitzonderingen van artikel 5, (b) en (c) Privacywet zijn eveneens van toepassing op dit recht van verzet.

De Gebruiker kan zich ten allen tijde, kosteloos en zonder motivering verzetten tegen de voorgenomen verwerking van zijn persoonsgegevens indien deze persoonsgegevens verkregen werden met het oog op direct marketing.

De Gebruiker is eveneens gerechtigd om ten allen tijde, kosteloos en zonder motivering de verwijdering van of het verbod op de aanwending van alle hem betreffende persoonsgegevens te

bekomen die gelet op het doel van de verwerking, onvolledig of niet ter zake dienend zijn, of waarvan de registratie, de mededeling of de bewaring verboden zijn, of die na verloop van de toegestane duur zijn bewaard.

De Gebruiker oefent zijn recht uit via een gedagtekend, schriftelijk verzoek aan NAAM ONDERNEMING, per post of per e-mail via info@socialseeder.com. NAAM ONDERNEMING verbindt er zich toe binnen de vijftien (15) werkdagen aan jouw verzoek een gevolg te geven.

4.3 Recht op toegang

Iedere Gebruiker die zijn identiteit bewijst beschikt over een recht op toegang tot de informatie rond het al dan niet bestaan van verwerkingen van zijn persoonsgegevens, net als de doeleinden van deze verwerking, de categorieën gegevens waarop deze verwerkingen betrekking hebben en de categorieën van ontvangers aan wie de gegevens worden verstrekt.

De Gebruiker oefent zijn recht uit via een gedagtekend, schriftelijk verzoek aan NAAM ONDERNEMING, per post of per e-mail aan info@socialseeder.com. NAAM ONDERNEMING verbindt er zich toe binnen de vijftien (15) werkdagen aan jouw verzoek een gevolg te geven.

4.4 Recht op verbetering

NAAM ONDERNEMING engageert zich tot een zo nauwkeurig mogelijke gegevensverzameling. Onnauwkeurige of onvolledige persoonsgegevens kunnen bijgevolg steeds verbeterd of zelfs uitgewist worden.

Aangezien het onmogelijk is om continu op de hoogte te zijn van iedere verandering of fout in de persoonsgegevens, is het aan jou als Gebruiker om onnauwkeurigheden en onvolledigheden te melden en in de eerste plaats zelf de nodige aanpassingen te maken binnen zijn Gebruikersregistratie.

Indien dit toch niet voldoende blijkt kan men steeds een gedagtekend, schriftelijk verzoek aan NAAM ONDERNEMING richten, per post of per e-mail aan info@socialseeder.com. NAAM ONDERNEMING verbindt er zich toe binnen de vijftien (15) werkdagen aan jouw verzoek een gevolg te geven, door de persoonsgegevens geheel of gedeeltelijk aan te vullen, te verbeteren of zelfs te verwijderen. De verwijdering heeft voornamelijk betrekking op de zichtbaarheid, het is dus mogelijk dat de verwijderde persoonsgegevens toch nog tijdelijk bewaard worden.