CCBE Richtlijnen voor het gebruik van CLOUD COMPUTING SERVICES door advocaten

(vrije vertaling van officiële Engelstalige versie)
(v1.0 d.d. 5 december 2012)

Inhoud

I. INLEIDING

1. Reikwijdte van de richtlijnen

Dit document is bedoeld voor het creëren van meer bewustzijn onder de advocaten over de verschillende risico's verbonden aan Cloud Computing. Als zodanig, zijn de richtlijnen in deel II van dit document gericht op de advocatenorden van de CCBE-lidstaten om de aandacht te vestigen op de problemen waarmee individuele advocaten mogelijk worden geconfronteerd bij het maken/overwegen van beslissingen ten aanzien van het gebruik van Cloud Computing-diensten.

2. Cloud Computing

Cloud Computing is een algemene term voor de IT-infrastructuur waarbij de opslag en verwerking van data en software op afstand in het datacenter van de cloud provider of onderling met elkaar verbonden centra, als een dienst wordt benadert met behulp van het Internet. Volgens de Amerikaanse National Institute of Standards and Technology (NIST), maakt Cloud Computing hiermee alomtegenwoordige, gemakkelijke, on-demand netwerktoegang mogelijk tot een gedeelde pool van configureerbare computerbronnen, zoals netwerken, servers, opslag, toepassingen en diensten, die kunnen worden snel vrijgegeven met minimale beheer inspanning of service provider interactie[1].

3. Cloud Computing op de agenda van de Europese Commissie

De noodzaak om een EU-brede strategie op Cloud Computing te ontwikkelen is benadrukt in de Europese Commissie Digitale Agenda voor Europa. De drie brede gebieden die in dit verband worden aangepakt om ervoor te zorgen dat Europa de voordelen van Cloud Computing maximaliseert omvatten:

- **Het juridische kader**: dit betreft gegevensbescherming en privacy, met inbegrip van de internationale dimensie. Het gaat ook om wetgeving en andere regels die een invloed hebben op de implementatie van Cloud Computing in openbare en particuliere organisaties.
- **Technische en commerciële grondslagen**: het doel is de ondersteuning voor de uitbreiding van het onderzoek van de EU gericht op kritieke problemen, zoals beveiliging en beschikbaarheid van cloud-diensten.
- **De markt**: proefprojecten die gericht zijn op cloud-implementatie zullen worden gesteund. Om echt te profiteren van de kracht van de overheidsopdrachten, zal de Commissie samenwerken met partners van de openbare sector in de lidstaten en op regionaal niveau om te werken aan gemeenschappelijke benaderingen van Cloud Computing.

Zoals de Commissie reeds heeft gerapporteerd, is het werk al begonnen binnen sommige van deze gebieden, met inbegrip van een openbare raadpleging in 2011 waarop de CCBE heeft gereageerd[2].

4. Cloud Computing voor advocaten: voordelen en risico's

Advocatenkantoren, evenals andere bedrijven, gebruiken Cloud Computing om uiteenlopende redenen. De vermindering van de kosten is één overweging. Cloud Computing zou een afname kunnen inhouden van de kosten om servers en software te kopen of te huren en de kosten van personeel om de servers te handhaven. Bovendien, aangezien veel Cloud Computing toepassingen toegang vanaf elke locatie omvatten, kan een eenvoudige setup van off-site werk in een besparing op huur en reiskosten resulteren als ook gezamenlijke werken binnen meerdere vestigingen van een advocatenkantoren vergemakkelijken.

---

[1] P. Mell en T. Grance, de NIST definitie van Cloud Computing, Nationaal Instituut voor normen en technologie, US Department of Commerce (januari 2011).

[2] CCBE reactie met betrekking tot de openbare raadpleging van de EuropeseCommissie over Cloud Computing.

Bovendien kan Cloud Computing computerwerk voor vele advocatenkantoren vereenvoudigen. Voor bedrijven met een bestaande IT-infrastructuur, kunnen cloud-gebaseerde software programma's de complexiteit verminderen. Ook voor startende advocatenkantoren, zonder bestaande software-systemen, is het relatief eenvoudig om een effectieve practice-management-systeem (PMS) van de grond af met behulp van cloud-gebaseerde software programma's op te bouwen.

Cloud Computing systemen bieden meestal meer flexibiliteit voor de eindgebruiker, aangezien Cloud Computing diensten via een internetverbinding vanaf elke locatie op elk gewenst moment toegankelijk zijn. Ook, in tegenstelling tot de desktop of server gebaseerde softwaresystemen, kunnen cloud-gebaseerde platforms op elk type computer met internet toegang worden gebruikt, met behulp van elk type besturingssysteem. Zolang de gebruikers toegang tot het internet hebben, kunnen ze toegang krijgen tot bestanden die zijn opgeslagen in de cloud. Als zodanig, Cloud Computing advocaten om hun diensten in nieuwe en efficiëntere manieren, in het voordeel van hun klanten in staat kan stellen.

Niettemin, naast vele aanzienlijke voordelen, brengt Cloud Computing ook een eigen set van risico's en uitdagingen voor advocaten met zich mee, belangrijkst in verband, allereerst met betrekking tot de gegevensbescherming, ten tweede, de professionele verplichtingen van vertrouwelijkheid en, ten derde, de andere professionele en regelgevende verplichtingen van de advocaat. Hoewel de eerste en de tweede van deze gebieden nauw gerelateerd zijn, zijn ze niet per se identiek. De advocaat wordt ook verwacht gevoelig te zijn voor de zuiver commerciële risico's waaraan hij kan worden blootgesteld, bijvoorbeeld door een tijdelijke onbeschikbaarheid van zijn cloud-dienst veroorzaakt verstoring van zijn bedrijf.

De essentie van Cloud Computing is het gebruik van een derde partij, een externe provider van computerdiensten met inbegrip van de opslag van gegevens, in tegenstelling tot het gebruik van computers of servers binnen het kantoor van de gebruiker of die volledig onder controle is van de gebruiker. De cloud-provider beschikt vaak zelf over of huurt van andere aanbieders een reusachtige datacenter, in het geval van de grootste cloud providers kunnen deze onderling verbonden zijn om een netwerk van servers te vormen die zich ook in landen buiten de EEA kunnen bevinden, waar mogelijk verschillende vormen en een lager niveau van gegevensbescherming toepassing kunnen zijn. In enkele gevallen kunnen dergelijke centra gevestigd zijn in landen die niet volledig de rechtsstaat respecteren. Bovendien, waar een netwerk van cloud-servers is, kunnen mogelijk gegevens worden uitgesplitst en opgeslagen op verschillende servers (zelfs in verschillende landen) en zelfs voortdurend tussen die servers migreren. In de meeste gevallen zullen zelfs de controllers van dergelijke netwerken zich niet bewust zijn van waar in het netwerk een gegevensitem op een bepaald moment opgeslagen is. Deze omstandigheden verhogen de aandacht voor specifieke kwesties en eventuele zorgen voor de juridische beroepen met betrekking tot normen voor bescherming en potentieel diefstal van gegevens, verlies of openbaarmaking van vertrouwelijke informatie.

De meest directe zorgen van advocaten die voortvloeien uit de Cloud Computing bevatten[3]:

Kwesties met betrekking tot professionele geheimhouding en gegevensbescherming:

- De verantwoordelijkheid van advocaten met betrekking tot de betrouwbaarheid en de veiligheid van de cloud waarop zij hun klanten gegevens opslaan zou moeten worden verduidelijkt

[3] Verschillende van deze onderwerpen werden geïdentificeerd in de volgende kranten: de Law Society of Scotland van Cloud Computing - advies voor het beroep (2012) en de American Bar Association Commissie over ethiek 20/20 Working Group op de gevolgen van nieuwe technologieën onderwerpen papier betreffende Cliënt vertrouwelijkheid en advocaten gebruik van technologie (20 September 2010).

- Cloud Computing kan verduidelijking nodig hebben van de mate waarin dat advocaten van de cliënt toestemming moeten verkrijgen voordat men Cloud Computing-diensten gebruikt om vertrouwelijke informatie op te slaan of te verzenden.
- Gegevens die zijn opgeslagen in een Cloud Computing omgeving kunnen gevoelig zijn voor de risico's van onbevoegde toegang of fysiek onbevoegde toegang tot de ruimten waar de servers zich bevinden of elektronisch, hetzij door de provider werknemers of onderaannemers, of door derden, bijvoorbeeld hackers, via het Internet.

Kwesties met betrekking tot 'extra- territorialeit':

- Cloud Computing zou verwerking van persoonsgegevens kunnen inhouden op servers in landen die minder of minder doeltreffende juridische beschermingsmechanismen hebben voor elektronisch opgeslagen informatie dan in de EU/EER zijn gemandateerd en die niet onder de EU-regelgeving vallen. Cloud Computing aanbieders kunnen lokale regels verplichten hen te overhandigen van Europese advocaten gegevens die zijn opgeslagen op een cloud-server, zoals het geval zou kunnen zijn, nationale autoriteiten uit derde landen gelden.
- Een extra risicofactor is 'long-arm' buitenlandse wetgeving die opleggen van verplichtingen willen misschien tot het verstrekken van gegevens op verzoek aan de nationale autoriteiten, niet alleen op de staat van herkomst bedrijven die cloud-diensten verlenen, maar ook op buitenlandse bedrijven die zijn uiteindelijk eigendom van bedrijven van de staat van herkomst. In dit opzicht Cloud Computing kan worden onder onduidelijke procedures bestuur reactie of weigering van de provider regering verzoeken om toegang tot informatie.

Kwesties met betrekking tot de (lokale) deontologische/regelgevende vereisten:

- Problemen misschien ook uit het feit dat er kan zijn uiteenlopende en tegenstrijdige lokale vereisten van de nationale staven of wet samenlevingen dat advocaten moeten voldoen met betrekking tot de behandeling van vertrouwelijke gegevens.

Kwesties met betrekking tot contracten met Cloud Computing-aanbieders:

- Cloud Computing kan worden onderworpen aan onduidelijk beleid met betrekking tot de eigendom van opgeslagen gegevens.
- Cloud Computing aanbieders niet kan back-up gegevens adequaat en/of permanente beschikbaarheid van hun cloud-diensten.
- Cloud Computing kan gelden onvoldoende gegevenscodering.
- Cloud Computing onduidelijk beleid voor het melden van klanten van inbreuken op de beveiliging kan gelden.
- Cloud Computing kan worden onderworpen aan onduidelijk beleid met betrekking tot de duur van de gegevensopslag.
- Cloud Computing mogelijk onduidelijk beleidsinstellingen voor gegevensvernietiging in gevallen wanneer een advocatenkantoor niet langer wenst de relevante gegevens beschikbaar zijn op de Cloud Computing server of wanneer zij de gegevens die worden overgedragen aan een ander advocatenkantoor wenst.
- Cloud Computing-problemen met betrekking tot toegang tot de gegevens met behulp van gemakkelijk toegankelijke software in het geval dat een advocatenkantoor haar relatie beëindigt met de on-demand aanbieder of wanneer de provider wijzigingen of failliet zou kunnen inhouden.

5. De CCBE richtlijnen voor Cloud Computing

Als beschreven boven, biedt Cloud Computing een constructief alternatief voor de traditionele IT-infrastructuur systemen voor advocaten. Echter naast vele aanzienlijke voordelen, zij leidt ook tot een aantal risico's en uitdagingen op het gebied van advocaten vermogen om te voldoen aan hun wettelijke verplichtingen als verwerking verantwoordelijken onder de richtlijnen

gegevensbescherming, hun professionele gedragscodes, met name wat betreft de verplichtingen van de klant vertrouwelijkheid, en hun verantwoordelijkheden onder de regelgevende regimes die moeten kunnen worden onderworpen, bijvoorbeeld in het handhaven van de boekhouding die gecontroleerd kunnen worden door hun toezichthouder, of het bieden voor de continuïteit van het bedrijfsleven in het geval dat hun advocatenkantoor ophoudt te kunnen om zijn diensten te verlenen. Het is noodzakelijk dat advocaten, bij het overwegen van implementeren van Cloud Computing in hun kantoren, nemen de nodige maatregelen om ervoor te zorgen dat de klantgegevens is beveiligd, dat cliënt vertrouwelijkheid wordt gehandhaafd en dat de bezorgdheid die in bovenstaand lid 2 geïdentificeerde adequaat worden aangepakt. Niettemin, zoals andere consumenten, advocaten zal vaak niet weten genoeg om er zeker van zijn dat er veiligheidsmaatregelen voldoende zijn. In deze context heeft de CCBE deze set van richtlijnen inzake het gebruik van on-demand diensten door advocaten ontwikkeld. Deze richtlijnen zijn bedoeld om te maken advocaten meer bewust van de verschillende risico's verbonden met Cloud Computing en hen te helpen bij maken weloverwogen beslissingen van de technologie.

II. CCBE RICHTLIJNEN INZAKE HET GEBRUIK VAN CLOUD COMPUTING DIENSTEN DOOR ADVOCATEN

Nationale Bars en Law Societies, die hun leden, die overwegen Cloud Computing in hun kantoren te implementeren, willen adviseren moeten trachten hun aandacht te vestigen op de volgende overwegingen:

A. wetten op gegevensbescherming en beroepsgeheim

Als algemene regel moet als een primaire stap bij de overweging van het invoeren van Cloud Computing-diensten door advocaten rekening gehouden worden met de wetten op het gebied van gegevensbescherming en beroepsgeheim.
In het bijzonder moeten advocaten nagaan of zij volgens de regels van hun 'Nationale Bar en Law Society' toestemming hebben voor het opslaan van gegevens buiten hun advocatenkantoor.
En, zo ja, zorgen dat de Cloud Computing dienstverlener niet onderworpen is aan een jurisdictie met 'long-arm'-wetgeving waardoor zij verplicht zijn gegevens van Europese advocaten die zijn opgeslagen op een cloud-server te overhandigen , zoals het geval zou kunnen zijn, aan nationale autoriteiten van landen buiten de EU.
Advocaten zouden kunnen overwegen of, met het oog op deze zorgen, het in bepaald gevallen niet beter zou zijn om een cloud-service provider te gebruiken die in de EER gevestigd is en (waar ook gelegen) zo ver als praktisch mogelijk niet bloot staat aan dergelijke 'long-arm'-wetgeving.

B. voorbereidend onderzoek van Cloud Computing-diensten

Advocatenkantoren zijn altijd bezig met verwerking van verschillende soorten gegevens waaraan verschillende eisen op het gebied van behandeling en bescherming van toepassing zijn met inachtneming van de dwingende verplichting ten aanzien van beroepsgeheim/vertrouwelijkheid.
Advocaten die overwegen gebruik te willen maken van Cloud Computing-diensten moeten eerst nadenken over het soort servicemodel. Hetgeen zou moeten voldoen aan de huidige en toekomstige behoeften van hun kantoor. Wanneer advocaten Cloud Software as a Service (SaaS)[4] of Cloud Infrastructure as a Service (IaaS)[5] gebruiken zullen zij zich ervan moeten verzekeren dat beide de verwerking en opslag van gegevens bevatten, waaronder eventueel ook persoonlijke gegevens en gevoelige persoonlijke gegevens, evenals informatie beschermd door klantvertrouwelijkheid.
Advocaten dienen dus te worden geïnformeerd en zich bewust te zijn van deze overwegingen bij de externe verwerking van gegevens. Vaststelling van procedures voor codering van gegevens in gegevensoverdracht en -opslag moet ook worden overwogen.

In deze omstandigheden, als een advocaat wil gebruiken Cloud Computing, zullen

---

[4] SaaS (Cloud Software as a Service): een provider levert, via het web, toepassing van de verschillende diensten en maakt ze beschikbaar voor eindgebruikers. Deze diensten zijn vaak bedoeld ter vervanging van conventionele toepassingen worden geïnstalleerd door gebruikers op hun lokale systemen; dienovereenkomstig, zijn gebruikers uiteindelijk bedoeld om het uitbesteden van hun gegevens naar de individuele provider. Dit is het geval, bijvoorbeeld, van typische web-based office-toepassingen zoals spreadsheets, tekstverwerking tools, geautomatiseerde registers en agenda's, gedeelde agenda's, enz.; echter, de betrokken diensten omvatten ook cloudbased e-mailtoepassingen. Bron: De Groep gegevensbescherming artikel 29, 05/2012 advies over Cloud Computing

[5]IaaS: een aanbieder van leaseovereenkomsten een technologische infrastructuur, d.w.z. virtuele externe servers de eindgebruiker overeenkomstig mechanismen en regelingen zoals rekenen kan zodat het eenvoudig, effectief ook als heilzaam vervangen de corporate IT-systemen op de bedrijfsterreinen en/of de gehuurde infrastructuur naast de corporate systemen gebruiken. Dergelijke aanbieders zijn meestal gespecialiseerde marktspelers en eigenlijk kunnen rekenen op een fysieke, complexe infrastructuur die vaak over verschillende geografische gebieden overspant. Bron: De Groep gegevensbescherming artikel 29, 05/2012 advies over Cloud Computing.

De eerste beslissing die een advocaat moet nemen indien hij gebruik wil maken van Cloud Computing is de keuze tussen het SaaS of de IaaS model.

Verder, Cloud Computing diensten kunnen worden verleend door een openbare cloud-provider of een particuliere cloud-provider. Een openbare cloud-provider biedt zijn diensten aan iedereen aan. Terwijl een particuliere cloud-provider meestal eigendom is of gecontroleerd wordt door een kleine groep. Bijvoorbeeld, in sommige lidstaten hebben advocaten zich gegroepeerd om een 'Private Cloud' te vormen. Het onderscheid tussen de publiek/private Cloud kan zeer relevant zijn bij een evaluatie van welke provider een lagere risicofactor heeft, bijvoorbeeld in verband met de mogelijkheid van opslag van gegevens op servers buiten de EER of op servers die onderworpen zijn aan zgn. 'long arm'-wetgving. Het gebruik van een openbaar Cloud moet in geen geval per definitie beschouwd worden als zijnde ongeschikt, mits de advocaat eerst een due diligence heeft uitgevoerd op de leverancier zelf en de veiligheid van het gegevenscentrum die door de provider wordt gebruikt en over de details van de Service Level Agreement. In het geval dat uit een dergelijke due diligence bezorgdheid blijkt, kan het goed zijn dat aanbieders (met name kleine en middelgrote) bereid zijn om hun diensten aan te passen en/of te onderhandelen over contractvoorwaarden om deze bezorgdheid aan te pakken.

Voordat een contract gesloten wordt dient de advocaat, als de eindgebruiker van de cloud-service, de volgende punten te controleren:

a) de ervaring,
b) de reputatie,
c) de specialisatie,
d) het geregistreerd adres en locatie van de Cloud Computing service provider.

Bovendien moet een afzonderlijke controle uitgevoerd op:

a) de toereikendheid van de solvabiliteit, betrouwbaarheid, eigendom en kapitaal van de provider,
b) potentiële conflicten van belangen,
c) risico's van misbruik van de opgeslagen informatie,
d) exacte locatie van de opslag-servers
e) voor zover doenlijk, de veiligheid van de servers en het gegevenscentrum waarin ze zich bevinden (zowel fysiek als elektronisch),
f) de toepassing civiele, strafrechtelijke en openbare wetten en verordeningen

C. Pre-evaluatie van gevoeligheid van de gegevens

Advocatenkantoren zijn altijd bezig met verwerken van verschillende typen gegevens waarop verschillende eisen op het gebied van de verwerking en bescherming van toepassing zijn. Elk besluit om informatie op te slaan op de cloud-server moet noodzakelijkerwijs gepaard gaan met overwegingen op het type gegevens (gegevens over werknemers, strafrechtelijke gegevens, algemene juridische archieven, enz.) en het niveau van bescherming die dienovereenkomstig moeten worden vastgesteld.

D. beoordeling van veiligheidsmaatregelen

Elke beoordeling van cloud-dienstverleners moet tenminste een evaluatie bevatten van goedgekeurde technische, fysieke en organisatorische veiligheidsmaatregelen overeenkomstig de nationale en internationale IT-risico-management-normen, zoals ISO 27001: 2005 (veiligheidsbeheer) en ISO 9001 (kwaliteitsmanagement). Certificaten die door erkende IT-auditors zijn verstrekt kunnen ook dienen als een testcriterium.

Indien van toepassing, zou een advocaat ook de betrouwbaarheid van zijn eigen in-house beveiligingsnormen moeten beoordelen door het opzetten van ICT regels, informatie en opleiding van het personeel. Aangezien effectief wachtwoordbeheer zelden in zijn geheel door

advocatenkantoren gebeurt, moet tokenisatie of invoering van elektronische identiteitskaart registratie worden overwogen.

Over het algemeen, moet een advocaat altijd de inzet van professionele ondersteuning en advies overwegen bij het selecteren van en het toezicht op cloud-dienstverleners.

E. Vergelijking bestaande in-house IT-infrastructuur met cloud services

Bij de beoordeling van cloud diensten, moeten advocaten een vergelijking maken met hun huidige in-house IT-infrastructuur. Een dergelijke evaluatie zou het advocatenkantoor in de gelegenheid stellen te beoordelen of overschakeling naar een aparte cloud service de risico's zal verhogen of verlagen.

F. Beoordeling van het vermogen om gegevensverlies te herstellen in geval van het falen van de cloud dienstverlener, fouten van het advocatenkantoor of contractuele geschillen tussen de dienstverlener en het advocatenkantoor

Een advocaat zal niet willen lijden onder de verstoring van haar zakelijke dienstverlening in geval van een storing van zijn cloud service provider.
Daarnaast dienen de advocaten bij vele rechtsgebieden onder de professionele en regelgevende vereisten in staat te zijn om klantgegevens en andere materiaal niet zijnde persoonlijke- of klantgegevens (zoals hun bedrijfsboekhouding) beschikbaar te stellen voor inspectie door regelgevende instanties. Indien dergelijke gegevens niet beschikbaar gesteld kunnen worden wanneer deze door autoriteiten worden vereist, als gevolg van of het falen van de cloud service provider, het fouten van het advocatenkantoor zelf (wat leidt tot een inbreuk of de beëindiging van het contract met de cloud-dienstverlener) of door een contractuele geschil met de cloud-dienstverlener hetgeen aanleiding zou kunnen geven tot een pandrecht of recht van retentie door de provider met betrekking tot de gegevens van de advocaat, zou dit kunnen leiden tot professioneel wangedrag of tot de machtiging van een regelgevende strafbaar feit door de advocaat, als gevolg van het dat hij niet in staat is de gegevens of ander materiaal te reproduceren.
Dergelijke overtreding of wangedrag kan doorlopend of herhaaldelijk zijn zo lang als het onvermogen om de gegevens te reproduceren voortduurt.

Daarom dient een advocaat, bij de evaluatie van de cloud dienstverleners, zijn eigen kwetsbaarheid te beoordelen voor de ongunstige beroeps- of regelgevende gevolgen door een dergelijk onvermogen om data te reproduceren. Hij moet overwegen of het noodzakelijk is om over passende contractuele voorwaarden te onderhandelen om voor continue beschikbaar van data te zorgen, zelfs in geval van een contractuele geschil of een falen van de aanbieder of zijn eigen advocatenkantoor. Hij kan ook eisen om te beoordelen of het ook noodzakelijk is om te zoeken naar technische middelen om dergelijke onbeschikbaarheid van data te voorkomen. Bijvoorbeeld doordat een contractueel recht om gegevens te herstellen van beperkt nut blijkt doordat de gegevens in een vorm zijn opgeslagen die niet gemakkelijk leesbaar is. Het kan dan nodig zijn om ervoor te zorgen voor een voortdurende beschikbaarheid van de software die nodig is om de gegevens te lezen, bijvoorbeeld doordat de vergunning van de desbetreffende software in borg (escrow) wordt gehouden ten behoeve van de advocaat.

G. contractuele voorzorgsmaatregelen

Het is belangrijk om op zijn minst de volgende aspecten te overwegen vast te leggen:

a) omvang van de dienst,
b) beschikbaarheid van het systeem,
c) termijnen voor foutcorrecties en verwijdering van storingen,
d) contractuele boetes voor niet-nakoming en vertragingen (indien uitvoerbaar overeenkomstig de van toepassing zijnde nationale wetgeving),
e) veranderingen in servicevereisten,

f) de verplichting van de service provider tot aanpassing van het systeem als gevolg van regelgevende of wetgevende amendementen,
g) uitsluiting van betrokkenheid van onderaannemers zonder voorafgaande toestemming,
h) licenties, met name de zekerheid dat de software gebruikt door de provider correct is gelicenceerd
i) het eigendom van de gegevens die zijn opgeslagen en het exclusieve recht op toegang tot deze gegevens,
j) overeenkomsten ten behoeven van de bescherming van de gegevens, met name indien en voor zover dit vereist wordt door de toepasselijke nationale wetten[6],
k) de veiligheidsmaatregelen en de verantwoordelijkheid,
l) de niet-openbaarmaking verplichtingen (non-disclosure),
m) bewaking en rapportage,
n) technische documentatie, procesdocumentatie en gebruiker-/systeembeheer documentatie,
o) recht op controle en audit, inclusief standaard certificeringen
p) back-up, rampen herstelplan bij onvoorziene gebeurtenissen,
q) voorziening voor Software-ESCROW in geval van insolventie of zakelijke onvermogen van de cloud-dienstverlener
r) locatie van servers - nationale, EER of buiten de EER, maar ook met de Europese normen met betrekking tot privacy en vertrouwelijkheid,
s) verzekeringen, garanties, schade,
t) contracttermijn, contractbeëindiging,
u) bepalingen met betrekking tot het einde van de service en exit-management, met inbegrip van transmissie en verwijdering van gegevens,
v) bemiddeling, conciliatie en/of arbitrage,
w) toepasselijk recht en bevoegdheid.

H. Voorwaardelijke gebeurtenissen

Er dient altijd aandacht besteed te worden op het feit dat cloud-service beschikbaarheid hangt af van een ononderbroken netwerkverbinding. De advocaat moet overwegen of het noodzakelijk te beschikken over een alternatieve of back-up technieken voor verbinding met het internet, in het geval dat zijn primaire verbinding niet meer werkt.

I. Transparantie

Met het oog op de transparantie van juridische diensten dient een advocaat te overwegen zijn toekomstige klanten te informeren over het feit dat het advocatenkantoor gebruik maakt van Cloud Computing-diensten. Dit kan worden bereikt door het invoegen van de informatie in de algemene voorwaarden van de juridische dienstverleningsovereenkomst, hetgeen onderhevig is aan veranderingen overeengekomen met individuele cliënten. Deze formulering beperkt het geven van meer gedetailleerde informatie over Cloud Computing uitsluitend tot individueel verzoek. Opgemerkt moet worden dat er wellicht bepaalde rechtsgebieden zijn waar toestemming van de cliënt noodzakelijk is.

Het invoegen van informatie over de algemene voorwaarden van een juridische serviceovereenkomst zou met name raadzaam zijn in gevallen waarin een advocatenkantoor diensten van een Clould provider afneemt met servers die zich fysiek bevinden in een ander rechtsgebied. In dat geval moet een advocaat mogelijk toestemming verkrijgen van zijn (geïnformeerde) cliënt om vertrouwelijke gegevens op dergelijke servers op te slaan. Informatie over de cloud-dienstverlener en wettelijke normen inzake gegevensbescherming, wet op privacy en professionele privileges van advocaten in een land waar de servers zich bevinden moeten aan de cliënt worden verstrekt.

[6] Dergelijke sectie bijvoorbeeld als onder 11 van de Duitse wet voor de bescherming van de persoonsgegevens.

J. algemene overwegingen

Cloud Computing omvat vele risico's en problemen, zoals uiteengezet in deze richtlijnen, met name ten aanzien van de vertrouwelijkheid/wettelijke professionele voorrecht en het behoud van gegevens. De CCBE moedigt Nationale Bars en Law Societies aan om de bewustwording onder hun leden met betrekking tot het vergroten van de waakzaamheid en te nemen voorzorgsmaatregelen op een hoog niveau te brengen. Juridische en technische waarborgen moeten door hun Cloud Computing aanbieders aan hen worden geboden (bijv. lange termijn data backup-garanties, etc.).

In de praktijk, is het voor individuele advocaten(kantoren) niet altijd mogelijk om te voldoen aan al deze overwegingen. Nationale Bars en Law Societies worden daarom aangemoedigd om mechanismen te faciliteren waardoor advocaten kunnen voldoen aan deze richtlijnen, zoals de ontwikkeling van in-house Cloud Computing infrastructuur met inachtneming van de hierboven genoemde overwegingen bepalen. In dit geval kunnen zij overwegen om een impact assessment uit te voeren.