Advies nr. 10/2016 van 24 februari 2016

Betreft: advies uit eigen beweging over de gebruikmaking van cloudcomputing door de verantwoordelijke voor de verwerking (CO-A-2015-013)

De Commissie voor de bescherming van de persoonlijke levenssfeer (hierna "de Commissie");

Gelet op de wet van *8 december 1992 betreffende de bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking* van persoonsgegevens (hierna WVP), inzonderheid art. 29 ;

Gelet op het verslag van de heer Stefan Verschuere; Ondervoorzitter;

Brengt op 24 februari 2016 volgend advies uit:

I. Inleiding

1. BETREFT :

1. Dit advies wil richtlijnen uitwerken om de verantwoordelijke voor de verwerking, die beroep wil doen op een cloudcomputingdienst, moet helpen bij het naleven van zijn verplichtingen die voortvloeien uit de WVP, omdat deze diensten ondanks de economische voordelen, risico's met zich meebrengen [1].

2. Draagwijdte

2. Dit onderzoek is gericht op de verantwoordelijke voor de verwerking die beroep doet op de diensten van een verwerker om zijn gegevens in de cloud te verwerken.

3. dit advies gaat niet over cloudgebruik voor privédoeleinden, dat in principe vrijgesteld is van de bepalingen van de WVP[2]. Deze tekst is dus niet bestemd voor particulieren die cloudcomputing gebruiken maar is bestemd voor ondernemingen en administraties.

4. Dit advies gaat ook niet over de situatie waarin de aanbieder van clouddiensten (of cloudservice provider, afgekort CSP of cloudprovider) als verantwoordelijke voor de verwerking kan worden beschouwd, met name als hij rechtmatig gebruik maakt van de gegevens voor andere doeleinden.

5. Als de verantwoordelijke voor de verwerking geen beroep doet op een verwerker maar zijn eigen cloudoplossingen uitwerkt waarover hij totale controle heeft, moet ook hij dit advies niet toepassen.

6. Het advies richt zich op de essentiële aspecten van de problematiek en is niet exhaustief, dit ten behoeve van de leesbaarheid.

---

[1] Cloudcomputing geeft ook de kleine en middelgrote ondernemingen de mogelijkheid om te genieten van technologieën die van een hoger niveau zijn dan deze waarop ze traditioneel aanspraak kunnen maken.

[2] Zie artikel 3 §2 van de WVP.

II. Definities

7. Cloudcomputing evolueert en bevat een brede waaier aan technologische oplossingen en commerciële praktijken. De term wordt in in verschillende contexten en betekenissen gebruikt. De meest aanvaarde definitie van het cloudcomputingmodel is terug te vinden in de omschrijving van het U.S. National Institute of Standards and Technology (NIST):
« Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. "[3].

8. Naargelang de bronnen die via clouddiensten worden aangeboden, kunnen er vervolgens drie dienstenmodellen worden onderscheiden : 1) Software as a service (SaaS), 2) Platform as a service (PaaS) en 3) Infrastructure as a service (IaaS)[4].

9. Naargelang de toegankelijkheid van cloudcomputing, worden *er ten slotte vier gebruiksmodellen* weerhouden: 1) de private cloud (beschikbaar voor een enkele organisatie), 2) de publieke cloud (beschikbaar voor het algemene publiek), 3) de 'community' of gemeenschapscloud (voor een bepaalde specifieke gemeenschap bestaande uit verschillende organisaties met gedeelde belangen) en 4) de hybride cloud (die kan bestaan uit twee of meer van de hiervoor genoemde gebruikersmodellen).

III. Toepassing van de WVP

1. Materieel toepassingsgebied

10. De WVP is in principe van toepassing[5] van zodra er een verwerking[6] is van persoonsgegevens[7]. Van een dergelijke verwerking zal in een cloudomgeving snel sprake zijn zodra er documenten worden opgeslagen of applicaties beheerd worden, die dienen om persoonsgegevens te verwerken.

---

[3] Voir http://www.nist.gov/itl/cloud/.

[4] Zie http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

[5] Artikel 3, §1, 1° van de WVP.

[6] Zie artikel 1, §2, 2° van de WVP.

[7] Zie artikel 1, §1, 1° van de WVP.

2. Territoriaal toepassingsgebied

11. De Commissie herinnert er aan dat de bepaling van het toepasselijke recht inzake bescherming van persoonsgegevens moet onderscheiden worden van de jurisdictie die de bevoegdheid bepaalt van nationale rechtbanken om op te treden in een zaak .[8] Enkel het eerste aspect, dat betrekking heeft op de toepasselijkheid van de WVP, wordt behandeld in deze paragraaf.

12. Het toepassingsgebied van de WVP wordt bepaald in artikel 3*bis*. Deze bepaling omvat twee territoriale toepassingscriteria. Het begrip verantwoordelijke voor de verwerking staat hierin centraal.

13. De WVP is van toepassing zodra een natuurlijke persoon of een rechtspersoon, een feitelijke vereniging of een openbaar bestuur gebruik maakt van cloudcomputing voor de daadwerkelijke activiteiten van hun vestiging in België. Zij omkadert de uitgevoerde gegevensverwerkingen, zelfs indien de cloudprovider in een andere lidstaat gevestigd is en ongeacht op welke plaats de gegevens worden bewaard[9].

14. Er is sprake van het tweede toepassingscriterium van de WVP indien het hoofdcriterium niet kan worden toegepast, dit wil zeggen als de verantwoordelijke voor de verwerking niet permanent op het grondgebied van de Europese Unie gevestigd is.

15. De WVP zal van toepassing zijn vanaf het ogenblik dat de verantwoordelijke voor de verwerking "gebruik maakt van cloudcomputingdiensten die zich op het grondgebied van België bevinden, behalve indien deze middelen op het grondgebied van België slechts voor doorvoer worden gebruikt"[10].

3. Verantwoordelijkheid voor de verwerking

16. De verplichtingen van de WVP berusten bij de verantwoordelijke voor de verwerking. Het begrip “verantwoordelijke voor de verwerking” wordt in de WVP als volgt bepaald : *Onder "verantwoordelijke voor wordt de natuurlijke persoon of de rechtspersoon, de feitelijke vereniging*

---

[8] Zie in dit verband, B. Volders, "IPR in de wolken : het toepasselijke recht op cloudcomputingovereenkomsten", *Computerrecht*, 2011/3, blz. 137 e.vv.

[9] B. Docquir, « Le ‘cloud computing’ ou l’informatique dématérialisée : la protection des données au cœur de la relation contractuelle », R.D.C., 2011/10, blz. 1007.

[10] Artikel *3bis* , 2° van de WVP.

of het openbaar bestuur verstaan die alleen of samen met anderen het doel en de middelen voor de verwerking van persoonsgegevens bepaalt[11].

17. De Commissie merkt op dat de cloudklant in principe moet worden beschouwd als verantwoordelijke voor de verwerking zodra hij de doeleinden bepaalt en beslist om zijn verwerkingen naar de cloud te outsourcen.

18. De Commissie herinnert eraan dat het onevenwicht in de contractuele relatie tussen een verantwoordelijke voor een verwerking van een kleine of middelgrote onderneming ten aanzien van een grote dienstenaanbieder geen reden is om termijnen en contractuele voorwaarden te aanvaarden die niet in overeenstemming zijn met de WVP[12].

19. Onverminderd de acties gebaseerd op andere Belgische wetgevingen, is de verantwoordelijke voor de verwerking verantwoordelijk voor de schade die hij de betrokken persoon berokkent door te handelen in strijd krachtens of door de WVP vastgestelde bepalingen[13]. Hij is van deze aansprakelijkheid ontheven indien hij bewijst dat het feit dat de schade heeft veroorzaakt, hem niet kan worden toegerekend.

4. Verwerking

20. Onder 'verwerker' of 'onderaannemer' verstaat de WVP "de *natuurlijke persoon, de rechtspersoon, (...) die ten behoeve van de voor de verwerking verantwoordelijke persoonsgegevens verwerkt, met uitsluiting van de personen die onder rechtstreeks gezag van de verantwoordelijke voor de verwerking gemachtigd zijn om de gegevens te verwerken"*[14].

21. De provider van clouddiensten moet in principe aanzien worden als verwerker hoewel er situaties zijn waarin hij al naargelang de omstandigheden, beschouwd kan worden als medeverantwoordelijke voor de verwerking of als verantwoordelijke voor de verwerking als zodanig. Dit is bijvoorbeeld het geval wanneer de provider gegevens verwerkt voor eigen doeleinden.

---

[11] Artikel 1, §4, WVP.

[12] Zie het advies van de groep 29 nr. 05/2012 van 1 juli 2012 over cloudcomputing blz. 10, https://www.privacycommission.be/sites/privacycommission/files/documents/G29-advies-cloud-computing_0.pdf, en de verwijzing naar advies 1/2010 van 16 februari 2010 over de begrippen "verantwoordelijke voor de verwerking" en de "verwerker".

[13] Artikel 15*bis* van de WVP

[14] Artikel 1, §5, WVP.

22. Wanneer een verantwoordelijke voor de verwerking beslist om verwerkingen in de cloud te verwerken, moet hij een verwerker kiezen die voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen voor de te verrichten verwerking en moet hij erover waken dat die maatregelen worden nageleefd[15].

23. De verantwoordelijkheid van de cloudprovider ten aanzien van de verantwoordelijke van de verwerking moet in een contract worden vastgesteld. Dit contract moet op zijn minst vermelden dat de de verwerker slechts handelt in opdracht van de verantwoordelijke voor de verwerking en dat de verwerker is gebonden door dezelfde verplichtingen als deze waaraan de verantwoordelijke zich moet houden inzake technische en organisatorische maatregelen voor gegevensbescherming, zoals hierboven beschreven.

5. Technische en organisatorische gegevensbeschermingsmaatregelen

24. Overeenkomstig artikel 16 van de WVP moet de verantwoordelijke voor de verwerking passende technische en organisatorische maatregelen ten uitvoer leggen om persoonsgegevens te beveiligen.

25. De informatiebeveiliging bestaat erin de door een organisatie verwerkte informatie te beschermen voor tal van risico's, hetzij bedreigingen (kwaadwillige interne of externe acties) hetzij kwetsbaarheden (risico's eigen aan de systemen en toepassingen) en laat aldus toe de vertrouwelijkheid, de integriteit alsook de beschikbaarheid van de gegevens te waarborgen.

26. Deze beveiliging moet worden verzekerd door de toepassing van passende maatregelen[16] waaronder organisatorische structuren, regels, processen, procedures maar ook technische systemen. Dit geheel van maatregelen moet welbepaald en gedocumenteerd zijn, geïmplementeerd, gecontroleerd en zo vaak als nodig verbeterd worden opdat de specifieke doelstellingen inzake veiligheid zouden worden bereikt.

27. Specifiek voor cloudcomputing, bestaat het risico op gegevenslekken uit de cloudomgeving. De Commissie verwijst hieromtrent naar haar Aanbeveling uit eigen beweging nr. 01/2013[17] *betreffende de na te leven veiligheidsmaatregelen ter voorkoming van gegevenslekken*.

---

[15] Artikel 16, §1 van de WVP.

[16] De door de Commissie gepubliceerde veiligheidsmaatregelen: zie http://www.privacycommission.be/sites/privacycommission/files/documents/referentiemaatregelen_voor_de_beveiliging_van_elke_verwerking_van_persoonsgegevens.pdf , ISAE 3402 en de ISO 27.002 norm kunnen in dit opzicht een passend algemeen referentiekader bieden.

[17] Aanbeveling uit eigen beweging 01/2013 van 21 januari 2013: http://www.privacycommission.be/sites/privacycommission/files/documents/aanbeveling_01_2013.pdf.

6. Rechten van betrokkenen

a. Informatieplicht

28. De verantwoordelijke voor de verwerking moet aan de betrokkene de informatie verstrekken bedoeld in artikel 9 van de WVP.

29. In dit geval moet de cloudklant de betrokkenen informeren van zijn identiteit, de doeleinden van de verwerking, het recht om zich kosteloos te verzetten tegen een verwerking gericht op direct marketing. De klant moet in principe[18] ook andere, bijkomende informatie verstrekken, met name over de ontvangers of de categorieën ontvangers. De Commissie beveelt hier aan dat de klant de betrokkene informeert over de identiteit van de verwerkers en de verdere verwerkers in de cloud.

30. De Commissie benadrukt dat de verantwoordelijke voor de verwerking moet blijk geven van transparantie, zowel over de verwerkte gegevens als de uitgevoerde verwerkingen.

b. Recht op toegang, verbetering en schrapping.

31. De artikelen 10 en 12 van de WVP bieden de betrokkene een recht op toegang tot de gegevens die de verantwoordelijke voor de verwerking over hem heeft verwerkt en de mogelijkheid ze te verbeteren, te schrappen of om zich tegen de verwerking te verzetten.

7. Lokalisering van de gegevens

32. De cloudklant moet erop toezien dat de gegevens verwerkt worden in landen die de gegevens een gepast beschermingsniveau bieden.

33. Persoonsgegevens kunnen binnen de Europese Unie vrij circuleren. De artikelen 21 en 22 van de WVP voorzien in de doorgifte van persoonsgegevens naar landen buiten de Europese Gemeenschap.

34. Iedere verantwoordelijke voor een verwerking die persoonsgegevens buiten de Europese Unie wenst over te zenden moet er zich eerst van vergewissen dat het land van bestemming een passend beschermingsniveau biedt [19]. Indien het beschermingsniveau van het land van

[18] Behalve indien die verdere informatie, met inachtneming van de specifieke omstandigheden waaronder de persoonsgegevens verkregen of verwerkt worden, niet nodig is om tegenover de betrokkene een eerlijke verwerking te waarborgen.

[19] https://www.privacycommission.be/nl/doorgifte-buiten-de-eu-zonder-passende-bescherming.

bestemming als passend beschouwd kan worden, kan de overzending gebeuren alsof het ging om een overzending tussen twee Belgische verantwoordelijken of naar een ander land van de Europese Unie.

35. De Europese Commissie heeft de bevoegdheid om vast te stellen of een derde land een passend beschermingsniveau biedt en heeft reeds het passend beschermingsniveau van heel wat landen erkend[20]. In een arrest van 6 oktober 2015 (arrest "Schrems"), verklaarde Het Hof van Justitie van de Europese Unie de beslissing ongeldig als zou de Verenigde Staten een passend beschermingsniveau bieden aan persoonsgegevens die worden overgedragen aan Amerikaanse ondernemingen die de veiligehavenbeginsels naleven (certification Safe Harbor)[21]. Er kan dus niet langer naar deze beschikking verwezen worden als juridische omkadering voor de gegevensdoorgiftes naar de Verenigde Staten. Momenteel wordt gewerkt aan een “EU-VS Privacyschild” om tegemoet te komen aan de opmerkingen van het Hof van Justitie van de Europese Gemeenschappen en om alzo het statuut van gepaste bescherming van de Verenigde Staten opnieuw in te voeren[22].

36. Wanneer een niet-EU-land niet erkend wordt als aanbieder van een passend beschermingsniveau, zijn er enkele mogelijkheden om toch een gegevensdoorgifte te laten plaatsvinden waaronder het afsluiten van een modelovereenkomst van de EU, of het aannemen van bindende ondernemingsregels (‘BCR’s)[23]. BCR’s zijn gedragscodes voor bedrijven die binnen hetzelfde concern gegevens overdragen.

37. De Groep 29 is van mening dat de afwijkingen die een gegevensdoorgifte zonder bijkomende garanties[24] toelaten buiten de Europese Unie, uitsluitend betrekking kunnen hebben op doorgiftes die niet recurrent, massaal of structureel zijn[25]. Hierdoor is het praktisch onmogelijk om in het kader van cloudcomputing beroep te doen op deze afwijkingen.

---

[20] Zie http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

[21] Affaire C362-14, http://curia.europa.eu/juris/liste.jsf?language=nl&num=C-362/14 ; persbericht, http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117nl.pdf.

[22] http://europa.eu/rapid/press-release_IP-16-433_nl.htm.

[23] http://www.privacycommission.be/nl/grensoverschrijdende-doorgifte-van-persoonsgegevens.

[24] Artikel 22, alinea 1 van de WVP.

[25] Werkdocument van de Groep 29 nr. 12/1998 van 24 juli 1998 betreffende de doorgifte van persoonsgegevens naar derde landen: toepassing van de artikelen 25 en 26 van de EU-richtlijn betreffende gegevensbescherming, waarvan verwijzing naar advies nr. 05/2012 van 1 juli 2012 over cloudcomputing, blz. 22, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_nl.pdf.

IV. Risico's verbonden aan de cloud

38. Aan de migratie naar een cloudcomputingoplossing zijn een aantal inherente risico's verbonden. Risicofactoren zijn afhankelijk van het servicemodel (i.e. IaaS, PaaS of SaaS) en het deployment-model (i.e. private, community, publieke of hybride cloud) die bij een migratie in overweging worden genomen. De belangrijkste risico's die bij een migratie naar een cloudoplossing geïdentificeerd kunnen worden, zijn de volgende:

1. Uit handen geven van controle op de gegevensverwerkingen

39. Met de cloud kunnen organisaties grote besparingen doorvoeren op hun informaticabudget. Ze kunnen hun informaticapark op hun site sterk verminderen en bijgevolg ook het personeel dat het moet beheren.

40. Dankzij de virtualisering, kunnen hardware- en softwaremiddelen onstoffelijk onder elkaar verdeeld en dynamisch toegewezen worden. De providers van clouddiensten kunnen tarieven aanbieden die niet in verhouding staan met de klassieke outsourcing.

41. Tezelfdertijd brengt deze virtualisering een fysieke fragmentering van de gegevens met zich mee op verschillende servers en datacenters, die zich in verschillende landen kunnen bevinden. Hierdoor geeft de cloudklant de controle over zijn gegevens uit handen met potentiële risico's voor de bescherming van die gegevens als gevolg indien er niet voldoende garanties ingebouwd zijn: lekken ("data breach"), verlies, misbruik, inzage van data door derde partijen, toegankelijkheid voor buitenlandse overheden...

2. Toegang door de overheden om de wet te handhaven (law enforcement)

42. De meest optimale beveiligingsmaatregelen kunnen niet verhinderen dat er steeds toegang mogelijk zal zijn tot de gegevens voor buitenlandse overheden. In dit kader is het ook nodig te onderlijnen dat zelfs als de gegevens geëncrypteerd zijn, dit niets afdoet van hun status: het blijven persoonsgegevens en die moeten worden beschermd tegen elke niet toegelaten verwerking. Anderzijds moet vastgesteld worden dat voornoemde risico's worden gereduceerd indien enkel de klant over de encryptiesleutel beschikt.

43. De landen hebben de mogelijkheid om informaticagegevens in beslag te nemen, op te sporen, te lokaliseren of kennis te nemen van elektronische communicaties en de gebruikers te identificeren. In België zijn dergelijke middelen bestemd voor de juridische autoriteiten (Procureur des Konings

of Onderzoekrechter naargelang de aantastingsgraad van de individuele vrijheden die daar mee samengaan) of de inlichtingendiensten.

44. Het nagestreefde doeleinde is in de meeste gevallen de wet te doen naleven[26] of terrorisme te bestrijden. Toch worden er soms bepaalde andere overheidsdoeleinden nagestreefd waardoor het risico op abusieve raadpleging van de gegevens toeneemt.

45. Een studie van het Europees Parlement had op die manier beschikkingen opgespoord van de Amerikaanse Foreign Intelligence Surveillance Amendment Act (FISAA) die aan de Amerikaanse overheden de mogelijkheid gaven om zonder juridisch mandaat toegang te hebben tot de cloudgegevens buiten de Verenigde Staten, die toebehoren aan niet-Amerikaanse personen en verwerkt werden door ondernemingen met een commerciële activiteit in de Verenigde Staten[27]. Volgens dit document kan deze toegang gebeuren zodra die gegevens worden beschouwd als belangrijk voor de uitsluitend buitenlandse belangen van de Verenigde Staten. Die toegang kan dan plaatsvinden buiten ieders medeweten zonder dat de cloudprovider daar zijn klant over inlicht. De affaire over de Amerikaanse mass surveillance programma's legden de onvermoede omvang[28] bloot van het aantal toegangen van de Amerikaanse autoriteiten tot de gegevens van grote dienstenverstrekkers van de Amerikaanse informatiemaatschappij.

46. Het is daarom aangewezen om voorzichtig te zijn met buitenlandse cloudproviders, zelfs al zijn die gevestigd in Europa of België, of met Europese providers in het buitenland die zich moeten verantwoorden bij buitenlandse overheden. Het wordt in ieder geval afgeraden om hen gevoelige gegevens toe te vertrouwen die raken aan de nationale economie. Zoals reeds gezegd kunnen deze risico's wel beperkt worden door het gebruik van state of the art encryptietechnieken gecombineerd met het feit dat de encryptiesleutel zich enkel bij de klant bevindt. Best worden de gegevens ook periodiek gedecrypteerd en opnieuw geëncrypteerd met de nieuwste technieken, zodat de hernieuwde encryptie (en bijbehorende sleutel) telkens de best mogelijke bescherming biedt, rekening houdend met de actuele stand van de techniek op het vlak van informatiebeveiliging.

---

[26] In het Engels "Law enforcement"

[27] Studie van oktober 2012 van van de 'DG for internal policies' van het : Europese Parlement, http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/462509/IPOL-LIBE_ET(2012)462509 _EN.pdf; zie ook een studie van september 2012 van de Universiteit van Amsterdam die met voorbeelden aantoont tot welke afwijkingen het juridisch arsenaal dat de Verenigde Staten op punt zette, zou kunnen leiden: Dr. J.V.J. van Hoboken, Mr. A.M. Arnbak & prof. Dr. N.A.N.A.M. Arnbak & prof. Dr. N.A.N.M. van Eijk, m.m.v. mr. mr. N. Kruijsen, *Cloud diensten in Hoger onderwijs en onderzoek en de USA Patriot Act*, Instituut voor Informatierecht, Universiteit van Amsterdam, september 2012, http://www.ivir.nl/publicaties/vanhoboken/Clouddiensten_in_HO_en_USA_Patriot_Act.pdf.

[28] Zie met name de programma's PRISM et XKeyscore.

47. De levering van cloudcomputingdiensten brengt overigens regelmatig met zich mee dat de provider beroep doet op verwerkers, wat de voormelde risico's vergroot.

3. Technologische afhankelijkheid van de cloudprovider

48. Voor een migratie naar de cloud moet de klant zich ervan verzekeren dat hij over een reële uitstapmogelijkheid beschikt bij de cloudprovider. Cloudproviders maken immers niet steeds gebruik van standaard dataformaten en service interfaces die interoperabiliteit en overdraagbaarheid tussen verschillende cloudproviders bevorderen. Indien de klant beslist om van cloudprovider te wisselen, kan het gebrek aan interoperabiliteit resulteren in moeilijkheden of zelfs de onmogelijkheid om de gegevens van de klant over te dragen naar de nieuwe cloudprovider (i.e. zogenaamde “vendor lock-in”).

4. Gebrekkig beheer van toegangsrechten

49. Eén van de voordelen van het gebruik van een clouddienst is dat de gegevens van op afstand kunnen geraadpleegd worden. Gebruikers kunnen dezelfde gegevens raadplegen, zowel van thuis uit als vanop kantoor en dit met een brede waaier aan toestellen. Dit impliceert evenwel dat de cloudklant de garantie moet krijgen dat er adequate maatregelen genomen werden om onrechtmatige toegang tot de gegevens te verhinderen.

50. In cloudomgevingen worden middelen zoals opslagruimte, geheugen en netwerken gedeeld met verschillende klanten. Dit creëert nieuwe risico’s met betrekking tot onrechtmatige toegang en/of verwerking voor andere doeleinden dan overeengekomen tussen de cloudklant en de cloudprovider.

51. Om deze risico’s te vermijden, moet er een voldoende scheiding zijn van data met de gegevens van andere klanten. Een degelijke isolering vereist onder meer een adequaat beheer van toegangsrechten en rollen voor de toegang tot persoonsgegevens, die op regelmatige basis moeten herzien worden. Daarnaast moet de implementatie van rollen met vergaande rechten vermeden worden (geen enkele gebruiker of administrator zou bijvoorbeeld toegang mogen hebben tot alle gegevens in de cloud). Bij de toekenning van toegangsrechten moet het principe van “least privilege” gelden, waarbij de gebruikers en administrators enkel toegang hebben tot de informatie die noodzakelijk is voor hun legitieme doeleinden.

5. Risico's verbonden aan het gebruik van verwerkers door de cloudprovider

52. Bij cloudcomputingdiensten kunnen meerdere partijen betrokken zijn die als verwerkers kunnen optreden. Ook is het gebruikelijk dat verwerkers activiteiten uitbesteden aan subverwerkers die daarmee toegang krijgen tot persoonsgegevens. Als verwerkers diensten uitbesteden aan subverwerkers, zijn zij verplicht deze informatie beschikbaar te maken voor de verantwoordelijke voor de verwerking, waarbij zij bijzonderheden verstrekken over het type uitbestede dienst, de kenmerken van de huidige en potentiële verwerkers, en garanties die deze entiteiten geven voor de naleving van de WVP.

53. In zijn Advies 1*/2010 "over de begrippen 'verantwoordelijke voor de verwerking' en* 'verwerker' " heeft de Groep 29 verwezen naar gevallen waarin er meerdere verwerkers zijn en deze verwerkers een rechtstreekse verhouding met de verantwoordelijke voor de verwerking hebben, of subverwerkers zijn, waaraan de verwerkers een deel van de hun opgedragen verwerkingen hebben uitbesteed. Bij dergelijke scenario's is het belangrijk dat de verplichtingen en verantwoordelijkheden die voortvloeien uit de wetgeving inzake gegevensverwerking, duidelijk worden bepaald en niet versnipperd raken over de keten van uitbesteding of onderaanneming, ten behoeve van een effectief toezicht en duidelijke verantwoordelijkheden voor de activiteiten van de verwerker. In dit opzicht is het belangrijk dat alle middelen voorzien zijn om te allen tijde te kunnen aantonen wie wat deed op een bepaald ogenblik (logging).

6. Niet-naleving van de retentieregels

54. Persoonsgegevens mogen niet langer bewaard worden dan noodzakelijk is voor de doeleinden waarvoor de gegevens oorspronkelijk werden verzameld of waarvoor ze verder worden verwerkt. Persoonsgegevens die niet langer noodzakelijk zijn, moeten vernietigd of volledig geanonimiseerd worden. Een veilige vernietiging van gegevens vereist dat opslagmedia vernietigd of gedemagnetiseerd worden of dat de opgeslagen persoonsgegevens op een doeltreffende manier worden verwijderd, bijvoorbeeld door de data meermaals te overschrijven met willekeurige data. Daar de persoonsgegevens in cloudomgevingen veelal op redundante wijze worden opgeslagen op verschillende servers op verschillende locaties moet men er zich van verzekeren dat elke van deze data-instanties verwijderd wordt op onherstelbare wijze.

7. Gebrekkig beheer met betrekking tot de rechten van de betrokkenen

55. Een cloudprovider is niet altijd in staat om de gegevens te beheren waarmee de klant zijn verplichtingen kan nakomen inzake het recht voor de betrokken personen, op toegang, verbetering, verzet en schrapping. Daarom moet de klant hier bijzondere aandacht aan besteden.

8. Onbeschikbaarheid van de dienst geleverd door de cloudprovider

56. De verantwoordelijke voor de verwerking dient over de garantie te beschikken dat hij te allen tijde toegang heeft tot de gegevens en dat de data niet verloren kunnen gaan. Bij een overweging tot migratie naar een clouddienst dient de verantwoordelijke zich van alle risico's te vergewissen met betrekking tot de beschikbaarheid van de dienst, dit zowel aangaande een eventuele onbeschikbaarheid van de clouddienst zelf (zoals hardware falen) als ook met betrekking tot de toegangsmiddelen tot de dienst. Dit laatste heeft in het bijzonder betrekking op het toevallig verlies aan netwerkconnectiviteit tussen de klant en de provider of het verlies aan serverperformance door kwaadwillige acties zoals (Distributed) Denial of Service attacks.

9. Stopzetting van de dienst door de provider of overname door een derde partij

57. De klant loopt het risico dat hij moeilijkheden zal ondervinden om zijn gegevens op te eisen wanneer zijn cloudprovider failliet is of wordt overgenomen.

58. Tegen dit risico heeft Luxemburg bijvoorbeeld het recht wettelijk ingevoerd om bij een failliete provider zijn gegevens op te eisen en dit via de wijziging van artikel 567 van de "Code de commerce" inzake faillissementen, bankbreuk en uitstel van betaling[29].

59. De verantwoordelijke voor de verwerking dient dus de zekerheid te verkrijgen dat alle betrokken gegevens gerecupereerd kunnen worden bij de stopzetting van de dienst of bij een andere vorm van beëindiging van het contract.

10. Niet-overeenstemming met de regelgeving, in het bijzonder met betrekking tot internationale doorgiftes

60. *"De onevenwichtigheid in de contractuele macht van een kleine voor de verwerking verantwoordelijke ten opzichte van grote dienstverleners [behoort] niet te worden beschouwd als*

[29] http://www.lexology.com/library/detail.aspx?g=9c1bfce5-156f-4860-97d1-95d2c020b7a7.

een rechtvaardiging voor de voor de verwerking verantwoordelijke om contractbepalingen te accepteren die niet in overeenstemming met de wetgeving voor gegevensbescherming zijn'[30].

61. Het is de klant die beslist of hij een deel of al zijn verwerkingen naar de cloud zal migreren. Als verantwoordelijke voor de verwerking, draagt hij de verantwoordelijkheid voor het kiezen van een kwalitatieve verwerker waarmee hij zijn verplichtingen kan nakomen omdat deze voldoende garanties biedt inzake bescherming van persoonsgegevens.

62. In het bijzonder, kan de verantwoordelijke voor de verwerking geen beroep doen op een verwerker die geen passende bescherming zou bieden als bedoeld in de artikelen 21 en 22 van de WVP als de persoonsgegevens worden overgezonden naar een land dat geen lid is van de Europese Unie.

11. Andere risico's

63. Naast bovenstaande risico's verwijzen we ook naar een meer uitgebreide, niet-exhaustieve lijst van 35 risico's die de ENISA identificeerde[31]. Deze risico's kunnen in overweging worden genomen bij de risicoanalyse van het migratieproject (zie punt V, richtlijn nr. 4).

V. Richtlijnen

1. Identificeer welke gegevens en verwerkingen men naar de cloud overweegt te migreren

64. De klant moet als verantwoordelijke voor de verwerking de verwerkingen die hij naar de cloud wenst te migreren, duidelijk identificeren.

65. Hij moet de beslissing om data al dan niet naar de cloud te migreren nemen in functie van het soort persoonsgegevens dat wordt verwerkt en van hun gevoeligheid, zoals bedoeld in de artikelen 6 tot 8 van de WVP.

66. In dit opzicht raadt de Commissie ook een stapsgewijze (in plaats van een volledige) migratie naar de cloud aan, te beginnen met niet-gevoelige en niet-confidentiële gegevens.

---

[30] Advies van de Groep 29 nr. 1/2010 van 16 februari 2010 over de begrippen "verantwoordelijke voor de verwerking" en "verwerker", http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_nl.pdf, blz. 28, vermeld in het advies van de Groep 29 n° 05/2012 van 1 juli 2012 over cloudcomputing.

[31] Zie https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment.

2. Bepaal de eigen technische en juridische vereisten

67. Hoewel de Commissie hieronder een aantal minimale contractuele, organisatorische en technische vereisten meegeeft, blijft de finale verantwoordelijkheid hiervoor bij de cloudklant zelf liggen in zijn hoedanigheid als verantwoordelijke voor de verwerking. Het staat hem aldus vrij om hogere standaarden te vereisen van de cloudprovider dan de hier opgesomde contractuele, organisatorische en technische vereisten.

a. Minimale contractuele garanties

- *Rechtszekerheid*

68. Het is niet uitzonderlijk dat de gebruiksvoorwaarden van de clouddiensten de cloudprovider toelaten om de bedoelde voorwaarden eenzijdig te wijzigen. De commissie beveelt aan om geen contracten af te sluiten dat dergelijke clausules bevat.

- *Vertrouwelijkheid van de gegevens*

69. De toegang tot de gegevens door de cloudprovider moet beperkt worden tot wat strikt noodzakelijk is om de dienst te kunnen leveren en onderhouden. De werknemers van de cloudprovider moeten daartoe met hun werkgever een vertrouwelijkheidsovereenkomst afsluiten.

70. De overeenkomst moet bepalen dat de cloudprovider geen gegevens mag meedelen aan derden tenzij hij beroep wil doen op verdere verwerkers.

- *Verdere verwerking*

71. De verdere verwerking is alleen toegestaan als de verantwoordelijke voor de verwerking vooraf zijn schriftelijke toestemming heeft gegeven (zie punt IV, risico nr. 5).

72. De klant moet erop toezien dat de verplichtingen van de provider ten aanzien van zijn klant worden overgeheveld naar de verwerkers. Wanneer de provider beroep doet op een verwerker, blijft de eerste volledig verantwoordelijk.

73. De klant moet worden ingelicht van de identiteit van de verwerkers en landen waar ze gevestigd zijn. Telkens beroep wordt gedaan op een nieuwe verwerker van buiten de Europese Unie, moet de provider dit melden aan de klant die de mogelijkheid moet krijgen zich daartegen te verzetten.

- *Rechten van betrokkenen*

74. De cloudklant moet erop toezien dat de omstandigheden waarin de verwerking in de cloud wordt verricht, geen obstakels vormen op technisch of organisatorisch gebied, zodat hij zijn verplichtingen kan vervullen (zie punt IV, risico nr. 7).

- *Lokalisering van de gegevens*

75. In de overeenkomst met de cloudprovider moet de verantwoordelijke voor de verwerking erover waken op voorhand over een volledige lijst van fysieke locaties te beschikken waar tijdens de duur van de overeenkomst de data opgeslagen of verwerkt kunnen worden door de cloudprovider en/of één van zijn onderaannemers (inclusief back-up).

76. In de overeenkomst met de cloudprovider moet de verantwoordelijke van de verwerking zich ervan verzekeren dat noch de cloudprovider, noch één van zijn verwerkers gegevens overbrengen naar andere fysieke locaties dan aangegeven in de overeenkomst.

77. De verantwoordelijke voor de verwerking dient over de mogelijkheid te beschikken om bij de cloudprovider “location audit trails” op te vragen. De “location audit trails” moeten automatisch worden geregistreerd en de fysieke locatie en het tijdstip weergeven waar en wanneer persoonsgegevens werden opgeslagen en verwerkt.

- *Doorgiftes buiten de Europese Unie*

78. De klant moet erop toezien dat de persoonsgegevens passend worden beschermd wanneer ze buiten de Europese Unie worden doorgegeven, meer bepaald met bindende ondernemingsregels voor de verwerking of door het ondertekenen modelcontractbepalingen[32] (zie punt IV hierboven, risico nr. 10).

79. Aangezien de verdere verwerker van de cloudprovider dezelfde verplichtingen heeft als die laatste, moeten de internationale doorgiftes tussen de providers en zijn verdere verwerkers omkaderd zijn door instrumenten als de modelcontractbepalingen.

[32] Zie hiervoor https://www.privacycommission.be/nl/doorgifte-buiten-de-eu-zonder-passende-bescherming.

- *Audit en certificatie*

80. In de overeenkomst moet een auditmechanisme worden ingeschreven voor de verplichtingen van de provider bij de levering van de clouddiensten. Dit zou door een derde, onafhankelijke dienstverlener kunnen uitgevoerd worden.

81. De klant kan ook nagaan of de service provider gecertificeerd is.

- *Data breach*

82. Bij problemen die gevolgen kunnen hebben voor de gegevens, moet worden voorzien in een kennisgevingsplicht voor de cloudprovider ten aanzien van de klant (zie punt IV, risico nr. 1).

- *Andere overheden*

83. In principe moet de provider de klant inlichten als overheden toegang hadden tot de gegevens die in de cloud worden verwerkt (zie punt IV, risico nr. 2).

84. In geen geval mogen de doorgiftes van een verwerker naar een overheid niet massaal zijn, disproportioneel en zonder onderscheid op een wijze die verder gaat dan wat noodzakelijk is in een democratische samenleving[33].

b. Technische vereisten

85. Volgens art. 16 §4 dient de verantwoordelijke voor de verwerking de veiligheid van de persoonsgegevens te waarborgen "door de gepaste technische en organisatorische maatregelen te treffen die nodig zijn voor de bescherming van de persoonsgegevens tegen toevallige of ongeoorloofde vernietiging, tegen toevallig verlies, evenals tegen de wijziging van of de toegang tot, en iedere andere niet toegelaten verwerking van persoonsgegevens*".*

86. In het geval de verantwoordelijke voor de verwerking een migratie naar de cloud overweegt voor de verwerking van persoonsgegevens, dient hij dus te verifiëren of de verwerker voldoende technische, organisatorische en juridische garanties biedt en deze af te toetsen in een

[33] Zie het Explanatory Document on the Processor Binding Corporate Rules' du Groupe 29 goegekeurd op 19 april 2013 en herzien op 22 mei 2015, blz. 13, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp204.rev_en.pdf, en vermeld in het advies 02/2015 van 22 september 2015 'on C-SIG Code of Conduct on Cloud Computing', blz. 8, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp232_en.pdf.

risicoanalyse. Ter begeleiding hiervoor verwijst de Commissie onder meer naar haar referentiemaatregelen en haar richtsnoeren inzake informatiebeveiliging[34].

87. Naast de cruciale veiligheidseisen betreffende de kwaliteit van de diensten, de beschikbaarheid, de confidentialiteit en de integriteit, wenst de Commissie ook de aandacht te vestigen op bijkomende garanties betreffende gegevensbescherming zoals transparantie, isolatie van data, verantwoordelijkheid bij incidenten, reversibiliteit, overdraagbaarheid en uitwissing van de gegevens. De cloudklant dient met betrekking tot deze punten voldoende garanties te verkrijgen van de cloudprovider.

- *Kwaliteit van de diensten*

88. De kwaliteit van de verleende diensten kan een weerslag hebben op de verwerking van persoonsgegevens en op de verwerkte gegevens. Het contract moet het dienstenniveau bepalen (service level agreement) dat de cloudprovider aan zijn klant moet verstrekken, alsook de sancties bij non conformiteit (zie punt IV, risico nr. 8).

- *Beschikbaarheid*

89. De cloudprovider dient, naast onvoorziene omstandigheden langs de kant de cloudklant (zoals connectieproblemen), voldoende garanties te bieden dat de gegevens steeds beschikbaar zijn (zie punt IV, risico nr. 8).

- *Confidentialiteit*

90. In een cloudomgeving kan encryptie een zeer belangrijke rol spelen – zeker bij de verwerking van gevoelige gegevens - bij de vertrouwelijkheid van de persoonsgegevens. Het gebruikte encryptieprotocol moet minstens voldoen aan erkende en actuele industriële standaarden. De Commissie wenst erop te wijzen dat encryptie in alle gevallen gebruikt dient te worden bij de overdracht van persoonsgegevens (dus ook bij de overdracht tussen de verschillende data centers van de cloudprovider) en, indien mogelijk, bij opslag in de cloud (waarbij het sleutelmanagement best ook niet in handen ligt bij de cloudprovider zelf) . In het geval van een SaaS-omgeving moet men zich er duidelijk van bewust zijn dat encryptie bij opslag minder compatibel is met de noodzakelijke verwerkingen. Er moet bij het gebruik van encryptie duidelijke garanties bestaan van een degelijk sleutelbeheer (niet bij de cloudprovider zelf, maar wel bij de sysadmins van de klant of bij een TTP), daar de veiligheid van de gegevens ultiem afhankelijk is van de

[34] Zowel de referentiemaatregelen als de richtsnoeren kunnen geraadpleegd worden via https://www.privacycommission.be/nl/informatiebeveiliging.

confidentialiteit van de encryptiesleutels. Bijkomende technische maatregelen om de confidentialiteit van de persoonsgegevens in de cloud te garanderen bestaan ook uit het inbouwen van een adequaat toegangs- en gebruikersbeheer met o.a. sterke authenticatiemechanismen (zoals two-factor authenticatie).

- *Integriteit*

91. De integriteit van gegevens kan gedefinieerd worden als de eigenschap dat de data authentiek zijn en dus niet kwaadwillig of toevallig werden gewijzigd tijdens het verwerken, de opslag of overdracht. De integriteit van gegevens kan gegarandeerd worden met cryptografische authenticatiemechanismen zoals digitale handtekeningen of 'message authentication codes' (MAC). Storingen met betrekking tot de integriteit van IT-systemen in de cloud kunnen verhinderd of gedetecteerd worden door zogenaamde "intrusion detection / prevention systems" (IPS/IDS).

- *Transparentie*

92. De technische en organisatorische maatregelen die de cloudprovider heeft opgezet, dienen op een transparante wijze open te staan voor inspectie. Cloudproviders dienen hun klanten een mechanisme aan te bieden om de technische en organisatorische maatregelen te inspecteren waar individuele audits door de klant technisch niet mogelijk zijn en/of bijkomende risico's inhouden.

- *Isolatie van de data*

93. In cloudomgevingen worden middelen zoals opslagruimte, geheugen en netwerken gedeeld tussen verschillende klanten, waardoor een degelijke isolatie van data nodig is om risico's zoals onrechtmatige toegang en verder verwerking voor niet-legitieme doeleinden te vermijden (zie punt 4 in de lijst met risico's verbonden aan de cloud).

- *Verantwoordelijkheid bij incidenten*

94. In het geval van cloudomgevingen kunnen de cloudprovider en eventuele verwerkers elk een zekere mate operationele verantwoordelijkheid dragen. In dit opzicht is het belangrijk dat alle middelen voorzien zijn om te achterhalen welke entiteit wat deed op welk bepaald ogenblik (logging). Dit is in het bijzonder van belang in het geval van een data breach.

- *Omkeerbaarheid van de gegevens*

95. Bij het einde van het contract moet de klant zijn gegevens kunnen recupereren en zijn activiteiten hervatten. In dit opzicht moet het cloudcontract bepalen dat de klant een integrale kopie van zijn gegevens kan verkrijgen in een gestructureerde en veel gebruikte vorm (zie punt IV, risico nr. 9).

- *Overdraagbaarheid van de gegevens*

96. Cloudproviders dienen waar mogelijk gebruik te maken van standaard dataformaten en systeeminterfaces die de interoperabiliteit en de overdraagbaarheid van gegevens bevorderen teneinde te vermijden dat data niet of moeilijk overdraagbaar zijn naar een andere cloudprovider (zie. punt IV, risico nr. 3).

- *Uitwissing van de gegevens*

97. Uitwissing: als de klant bij het beëindigen van de verbintenis zijn gegevens recupereert, dienen alle sporen van vroegere verwerkingen in de cloud door de cloudprovider vernietigd te worden (zie punt IV, risico nr. 7). De klant kan een beveiligde schrapping van zijn gegevens eisen zodat de schrapping onomkeerbaar is.

3. Identificeer het geschikte type cloudoplossing

98. De Commissie wenst er nadrukkelijk op te wijzen dat een verantwoordelijke voor de verwerking die gegevens naar de cloud wil migreren niet voor alle data dezelfde dienst of hetzelfde deploymentmodel moet kiezen. Eén bepaald dienstenmodel kan bovenop een ander dienstenmodel toegepast worden. De cloudprovider die één bepaalde component van de dienst aanbiedt, zoals de software, hoeft niet dezelfde provider te zijn die een andere component aanbiedt, zoals de cloudinfrastructuur.

99. Het dient opgemerkt te worden dat het gebruik van gelaagde diensten, zoals in bovenstaand randnummer beschreven, kan resulteren in een meer complexe keten van cloudproviders. De cloudklant dient er zich bewust van te zijn dat dit extra risico's met zich meebrengt.

100. Er bestaat een brede waaier aan clouddiensten om zeer uiteenlopende doeleinden te bereiken. Het is bij de keuze ook belangrijk om rekening te houden met het maturiteitsniveau van de aangeboden dienst.

4. Voer een risicoanalyse uit

101. Een gegarandeerde objectieve analyse wordt idealiter uitgevoerd door een onafhankelijk orgaan, gespecialiseerd in informatiebeveiligingen.

102. Naast het juridisch kader inzake de beveiliging vermeld onder punt III.5, wil de Commissie als voorbeeld verwijzen naar een evaluatiemodel voor de beveiliging van clouddiensten[35] onder andere aanbevolen door de afdeling Gezondheid van het Sectoraal comité voor de Sociale Zekerheid en van de Gezondheid[36], waarnaar de Commissie heeft verwezen in haar advies nr. 04/2015 van 25 februari 2015[37] en haar advies nr. 09/2016 van 24 februari 2016[38]. Het gaat om een praktische en kwantitatieve methode waarmee de veiligheid van de clouddiensten kan worden geëvalueerd t.o.v. de behoeften van de klant.

5. Kies een geschikte cloudprovider (CSP)

a. Principes

103. Op basis van de risicoanalyse is de klant verantwoordelijke voor de keuze van de cloudprovider die garanties biedt op juridisch en technisch gebied waarmee hij de WVP kan naleven.

104. Hij moet erop toezien dat hij vanwege de cloudprovider beschikt over alle transparantie en dus van alle informatie die noodzakelijk is om de voor- en nadelen van een clouddienst te kunnen beoordelen.

105. Teneinde de betrokkenen hun rechten te laten uitvoeren, beveelt de Commissie aan dat de klant alle betrokkenen op een transparante wijze informeert over de migratie naar de cloud nadat deze een geschikte cloudprovider heeft gekozen.

---

[35] https://www.smalsresearch.be/tools/cloud-security-model-nl.

[36] Zie de aanbeveling nr. 15/01 van 20 januari 2015 *betreffende een ontwerp van omzendbrief van de FOD Volksgezondheid inzake het gebruik van cloud diensten in ziekenhuizen.*

[37] Advies *betreffende een ontwerp van omzendbrief over het gebruik van de "cloud" door de ziekenhuizen*, https://www.privacycommission.be/sites/privacycommission/files/documents/advies_04_2015.pdf.

[38] Advies m.b.t. de keuze voor een SaaS-HR-strategie bij talentmanagementprocessen van de Vlaamse Overheid, https://www.privacycommission.be/sites/privacycommission/files/documents/advies_09_2016.pdf.

b. Certificatie

106. Een certificatie van een cloudprovider door een onafhankelijke derde partij kan een betrouwbaar middel bieden voor cloudproviders om de naleving van hun verplichtingen aan te tonen en het vertrouwen van cloudklanten te winnen. Een certificatie toont minstens aan dat de maatregelen inzake informatieveiligheid onderworpen werden aan een onafhankelijke audit ten opzichte van een aantal verplichtingen. Mogelijke relevante certificaties zijn onder meer deze op basis van de ISO/IEC 27001[39] en de ISO/IEC 27018[40] normen.

107. Echter, zoals ook uiteengezet in de opinie van de Groep 29 over cloud computing[41], dienen potentiële cloudklanten na te gaan of cloud service providers een kopie kunnen bezorgen van het desbetreffende auditrapport teneinde de certificatie te kunnen verifiëren met betrekking tot de verplichtingen van de cloudproviders en de vereisten van de cloudklant.

108. In 2014 heeft de ISO een specifieke norm uitgebracht voor Cloud Service Providers met het oog op de bescherming van persoonsgegevens in publieke clouds. Het gaat hier om ISO norm "ISO/IEC 27018:2014 – Information technology - Security techniques - Code of Practice for protection of personally identifiable information (PII) in public clouds acting as PII processors". Deze internationale standaard streeft volgende doelstellingen na:

- hulp aan publieke cloudproviders bij naleving van hun verplichtingen als verwerkers van persoonsgegevens;
- hulp aan publieke cloudproviders om transparantie te bieden op relevante aspecten zodat cloudklanten goed beheerde op cloud gebaseerde diensten kunnen kiezen;
- ondersteuning bieden aan de cloudklant en de cloudprovider om tot een contractuele overeenkomst te komen;
- cloudklanten een mechanisme aan te bieden voor het uitvoeren van audits in gevallen waar individuele audits door de klant technisch moeilijk zijn en/of risico's inhouden.

109. De standaard vormt een aanvulling op de maatregelen zoals beschreven in de ISO/IEC 27002 norm om tegemoet te komen aan de gedistribueerde aard van de risico's en het bestaan van de contractuele relatie tussen de cloudklant en de cloud service provider.

---

[39] Zie http://www.iso.org/iso/home/standards/management-standards/iso27001.htm.

[40] Zie http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=61498.

[41] Advies nr. 05/2012 van 1 juli 2012, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_nl.pdf.

110. Cloudproviders kunnen gecertificeerd worden voor deze ISO-norm. Een dergelijke certificatie kan aldus bijkomende, specifieke garanties bieden naast een eventuele certificatie onder de ISO/IEC 27001-norm.

111. Net zoals de Groep 29[42], benadrukt de Commissie dat de norm ISO/IEC 27018 een catalogus is van goede praktijken voor de cloud service provider die handelt als verwerker. Deze beschrijft een controlelijst die de bescherming van de privacy moet verbeteren. Deze standaardnorm is niet meer dan een goed geheel van niet verplichte, niet-exhaustieve en niet-maximalistische controles die kunnen worden uitgevoerd. De norm ISO/IEC 27018 is dus niet bedacht om gebruikt te worden als een autonoom document voor een certificering. Ze kan gebruikt worden in combinatie met de norm ISO/IEC 27001 die een certificering toelaat. De norm ISO/IEC 27001 houdt geen rekening met de bijzonderheden van de privacybescherming, zoals de impact voor de individuen, maar staat in voor een hoger niveau van informatiebescherming in het belang van de organisatie. De toevoeging van goede praktijken gebaseerd op de norm ISO/IEC 27018, kan er bijgevolg toe bijdragen dat de privacybescherming beter wordt uitgevoerd maar dit bewijst niet dat rekening werd gehouden met de risico's die samengaan met de privacy. De norm ISO/IEC 27018 zou idealiter gebruikt moeten worden nadat de risico's op privacy-schending van de betrokkenen werden beoordeeld door ze proportioneel te verwerken. Vandaag is er geen enkele standaardnorm bekend die de manier beschrijft waarop dit proces moet worden uitgevoerd. De lopende werkzaamheden van ISO kunnen helpen om in de komende jaren die lacune te dichten.

112. De Commissie wenst ook een belangrijke kanttekening bij deze standaard te maken, met name met betrekking tot toegangsaanvragen door buitenlandse autoriteiten. De standaard bepaalt hierover het volgende:

"The contract between the public cloud PII processor and the cloud service customer should require the public cloud PII processor to notify the cloud service customer, in accordance with any procedure and time periods agreed in the contract, of any legally binding request for disclosure of PII by a law enforcement authority, unless such a disclosure is otherwise prohibited."

(eigen nadruk).

113. Gezien bepaalde buitenlandse wetgeving veelal bepaalt dat dergelijke toegangsaanvragen niet bekend mogen gemaakt worden omwille van geheimhoudingsverplichtingen (zoals bijvoorbeeld bepaald in de Fisaa-wetgeving) geeft deze bepaling onvoldoende garantie inzake transparantie op het gebied van onrechtmatige toegangsaanvragen door buitenlandse overheden. In het bijzonder in geval van gevoelige gegevens dient de cloudklant dit aspect in zijn risicobeoordeling mee te nemen.

---

[42] Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing, adopted on 22 September 2015, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp232_en.pdf.

6. Volg wijzigingen op doorheen de tijd

114. Clouddienstmodellen wijzigen doorheen de tijd. In dit licht hiervan is het belangrijk om de gemaakte risicoanalyses periodiek te herhalen, rekening houdend met eventuele nieuwe risico's, het aanbod op de markt en andere relevante aspecten.

115. De Commissie beveelt in ieder geval aan de gemaakte risicoanalyse opnieuw uit te voeren bij significante wijzigingen met betrekking tot de gekozen clouddienst. Relevante wijzigingen kunnen bijvoorbeeld betrekking hebben op nieuwe datacentra, wijzigingen in het veiligheidsbeleid, in de verwerkingen door de cloudklant etc.

De Wnd. Administrateur, De Voorzitter,

(get.) An Machtens (get.) Willem Debeuckelaere