Advies nr 04/2015 van 25 februari 2015

Betreft: Advies over een ontwerp van Omzendbrief betreffende het gebruik van de "cloud" door de ziekenhuizen (CO-A-2014-053)

De Commissie voor de bescherming van de persoonlijke levenssfeer;

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

Gelet op het verzoek om advies van Mevr. L. Onkelinx, Minister van Sociale Zaken en Volksgezondheid, belast met Beliris en de Federale Culturele Instellingen ontvangen op 18/09/2014; Gelet op een eerste bespreking van het dossier op de plenaire vergadering van de Commissie van 5 november 2014; Gelet op het feit dat de Commissie het alsdan, na beraadslaging, raadzaam achtte het dossier voor bijkomend advies over te maken aan de afdeling Gezondheid van het Sectoraal comité van de Sociale Zekerheid en van de Gezondheid, wat gebeurde bij schrijven van 12 november 2014; Gelet op ontvangst van 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* ontvangen op 2 februari 2015.

Gelet op het verslag van de heer F. De Smet;

Brengt op 25 februari 2015 het volgend advies uit:

I. VOORWERP VAN DE ADVIESAANVRAAG

1. De Minister van Sociale Zaken en Volksgezondheid, belast met Beliris en de Federale Culturele Instellingen, hierna de aanvrager, verzoekt om het advies van de Commissie aangaande een ontwerp van Omzendbrief betreffende het gebruik van de "cloud" door de ziekenhuizen.

2. Op 10 april 2014 werd artikel 20, §1, van de gecoördineerde wet van 10 juli 2008 *betreffende de ziekenhuizen en andere verzorgingsinrichtingen* gewijzigd, waardoor de bewaring van patiëntendossiers en de registratie van de medische activiteit niet langer "in" het ziekenhuis, maar wel "door" het ziekenhuis moet gebeuren. Deze wijziging laat de ziekenhuizen en andere verzorgingsinrichtingen in principe toe een beroep te doen op cloud computing.

3. Met het ontwerp van omzendbrief dat het voorwerp uitmaakt van onderhavig advies, wenst de aanvrager een referentiedocument inzake cloud computing ter beschikking te stellen van voormelde ziekenhuisinstellingen.
   De aanvrager vermeldt volgende doelstellingen van de omzendbrief:
   - bepalen welke informatie en welke diensten kunnen worden geëxternaliseerd;
   - nagaan welke kwaliteit en garanties de cloud provider moet bieden op het vlak van gegevensbescherming.

4. Gelet op de specifieke bevoegdheid en competentie op het vlak van de bescherming van gezondheidsgegevens, o.a. in de ziekenhuissector, heeft de Commissie het ontwerp van omzendbrief voor voorafgaandelijk advies overgemaakt aan de afdeling Gezondheid van het Sectoraal comité van de Sociale Zekerheid en van de Gezondheid.

5. Rekening houdend met 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*, is de Commissie van oordeel dat volgende overwegingen en aanbevelingen inzake de bescherming van persoonsgegevens van belang zijn in een cloud computing context in ziekenhuizen.

II. ONDERZOEK VAN DE ADVIESAANVRAAG

6. Het ontwerp van omzendbrief geeft een tekstuele beschrijving van de context van cloud diensten, van de mogelijke risico's en van een aantal aandachtspunten. De Commissie is van oordeel dat het ontwerp van omzendbrief een nuttig instrument is dat tot op zekere hoogte kan beantwoorden een nood aan omkadering bij de ziekenhuizen. De Commissie stelt echter wel

vast dat in het ontwerp een operationeel bruikbare evaluatietool ontbreekt die de ziekenhuizen kan begeleiden in concrete situaties bij het doorvoeren van de risico-analyse waarover hierna sprake.

7. Het gebruik van cloud diensten houdt een aantal inherente risico's in. De verwerking van gegevens in de cloud kan tot een fysieke fragmentering van de gegevens leiden op verschillende servers en gegevenscentra die zich in verschillende landen kunnen bevinden. Hierdoor verliest de cloudklant als verantwoordelijke voor de verwerking[1] potentieel een stuk de controle over zijn gegevens en kan de bescherming van die gegevens in gevaar komen (onvoldoende bescherming, verlies, misbruik, raadpleging door derden of buitenlandse overheden,…). Bovendien bestaat de mogelijkheid dat buitenlandse overheden die gegevens kunnen raadplegen en opvragen naargelang hun eigen wetgeving[2].

8. De ziekenhuizen of andere verzorgingsinrichtingen die overwegen om cloud computing in te voeren, moeten aan de hand van een risicoanalyse nagaan welke de weerslag zal zijn op de beveiliging en de vertrouwelijkheid als er persoonsgegevens van de betrokken personen in de cloud worden gezet.

   Deze risicoanalyse moet onder andere betrekking hebben op de hiernavolgende punten:

   - nauwgezette evaluatie van de persoonsgegevens die al dan niet worden opgeslagen in de cloud, dit geldt in het bijzonder voor de zogenaamde "gevoelige gegevens" als bedoeld in de WVP, waaronder persoonsgegevens betreffende de gezondheid;
   - analyse van de contractuele voorwaarden;
   - evaluatie van de overeenstemming van de door de cloud provider voorgestelde beveiligingsvoorwaarden, waarbij de door de Commissie vereiste beveiligingsmaatregelen als minimum standaard moeten gelden[3];

---

[1] In haar advies 05/2012 over cloud computing stelt de Groep 29 dat in principe de cloud klant (in casu het ziekenhuis) als verantwoordelijke voor de verwerking dient te worden beschouwd en de cloud provider als een verwerker. (zie http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_nl.pdf#h2-3.)

[2] Andere landen zijn uitgerust om in het bezit te komen van informaticagegevens maar ook om elektronische communicaties op te sporen, te lokaliseren of er kennis van te nemen en de gebruikers ervan te identificeren. Het doeleinde dat wordt nagestreefd is in de meeste gevallen de wet doen naleven of terrorisme bestrijden. Er worden evenwel soms andere openbare doelen nagestreefd die het risico op abusieve raadpleging vermeerderen. De zaak PRISM en XKeyscore (Amerikaanse mass surveillance programma's) legden de onvermoede omvang bloot van het aantal toegangen van de Amerikaanse autoriteiten tot de gegevens van grote dienstenverstrekkers van de Amerikaanse informatiemaatschappij.

[3] Hierbij kan o.m. verwezen worden naar:

- *Referentiemaatregelen voor de beveiliging van elke verwerking van persoonsgegevens* waarin de Commissie de verplichting inzake informatiebeveiliging van artikel 16, §4, WVP concretiseert (zie http://www.privacycommission.be/sites/privacycommission/files/documents/referentiemaatregelen_voor_de_beveiliging_van_elke_verwerking_van_persoonsgegevens_0.pdf.);
- Artikel 25 van het koninklijk besluit van 13 februari 2001 ter uitvoering van de WVP dat een aantal bijkomend na te leven beveiligingsmaatregelen oplegt aan de verantwoordelijke voor de verwerking van gevoelige persoonsgegevens, waaronder deze die de gezondheid betreffen;

- garantie van de cloud provider op bepaalde rechten, vanaf de uitvoering tot beëindiging van het contract zodat hij zich kan richten naar zijn eigen verplichtingen inzake persoonsgegevensbescherming:
  - o clausule intuitu personae[4];
  - o auditregels[5];
  - o clausule over integriteit, continuïteit, beschikbaarheid en kwaliteit van de dienstverlening;
  - o bepalingen inzake interoperabiliteit, omkeerbaarheid[6] en overdraagbaarheid[7] van de gegevens,…;
- het in aanmerking nemen van de consequenties van een mogelijke toegang tot de gegevens door personen buiten de zorginstelling, inzonderheid voor "law enforcement"[8] – en andere doeleinden;
- de mogelijkheid om tegemoet te komen aan de rechten van betrokken patiënten, zoals het recht op informatie[9], het recht op inzage[10], het recht op verbetering en, in voorkomend geval, het recht van verzet[11]; de Commissie is dienaangaande van oordeel

---

- Artikel 7, §4, WVP dat de verantwoordelijke voor de verwerking verplicht de verwerking van persoonsgegevens die de gezondheid betreffen te laten verwerken onder de verantwoordelijkheid van een beroepsbeoefenaar in de gezondheidszorg;
- Aanbeveling nr. 01/2013 van 21 januari 2013 *betreffende de na te leven veiligheidsmaatregelen ter voorkoming van gegevenslekken* (zie http://www.privacycommission.be/sites/privacycommission/files/documents/aanbeveling_01_2013.pdf);
- Toezicht op de informatiebeveiliging door de veiligheidsconsulent waarover elke ziekenhuis moet beschikken ingevolge punt 9°quater, g) van Bijlage A, III, bij het koninklijk besluit van 23 oktober 1964 *tot bepaling van de normen die door de ziekenhuizen en hun diensten moeten worden nageleefd*.

[4] De Commissie raadt aan om contractueel te verbieden dat essentiële punten van een contract door de cloud provider op zijn beurt kunnen worden toevertrouwd aan een onderaannemer; eventuele uitbesteding zal alleszins maar mogelijk zijn na akkoord van de ziekenhuisinstelling.

[5] Onafhankelijk controlesystemen (Commissie, auditeur van de ziekenhuisinstelling) moeten het systeem van de cloud provider kunnen controleren.

[6] Bij het einde van het contract moet de instelling zijn gegevens bij de cloud provider kunnen recupereren en zijn activiteiten hervatten; in dit opzicht zou het contract moeten bepalen dat de klant een integrale kopie van zijn gegevens kan verkrijgen in een gestructureerde en veel gebruikte vorm.

[7] Het moet voor de instelling mogelijk zijn om zijn gegevens over te dragen naar een andere provider.

[8] De Commissie maant alleszins aan tot voorzichtigheid tegenover buitenlandse cloud providers of providers die in het buitenland gevestigd zijn en die verantwoording moeten afleggen bij buitenlandse overheden.

Voor internationale doorgiften van persoonsgegevens moeten artikelen 21 en 22 WVP steeds voor ogen worden gehouden met het oog op het waarborgen van een passend beschermingsregime. Op de website van de Commissie kan dienaangaande bijkomende toelichting worden gevonden: http://www.privacycommission.be/nl/grensoverschrijdende-doorgifte-van-persoonsgegevens.

[9] Artikel 9 WVP.

[10] Artikel 10 WVP en artikel 9, §2, van de wet van 22 augustus 2002 *betreffende de rechten van de patiënt*. De Memorie van Toelichting bij artikel 9, §2 van de wet betreffende de rechten van de patiënt stelt uitdrukkelijk dat door de opstellers ervan principieel werd gekozen voor een rechtstreeks (zonder tussenkomst van een derde) inzagerecht in hoofde van de patiënt. De Commissie verwijst hiervoor ook naar het actieplan e-Gezondheid 2013-2018 goedgekeurd door de Interministeriële Conferentie van 29 april 2013 en meer bepaald naar het essentieel Actiepunt 10 (Toegang tot de gegevens door de patiënt – zie http://www.rtreh.be/EHEALTH/_images/20130419actieplan_egezondheidnl.pdf).

[11] Artikel 12 WVP. Er zou zelfs bijkomend kunnen overwogen worden om de patiënt toe te laten, in een speciaal daarvoor bestemd deel van zijn dossier, zelf aanvullingen en bemerkingen te doen. Hij zal uiteraard geen wijzigingen kunnen aanbrengen aan de door de zorgverleners ingevoerde gegevens en informatie. Zie ook het actieplan e-Gezondheid 2013-2018, essentieel Actiepunt 10.

dat cloud computing services bij uitstek een rechtstreekse en onmiddellijke toegang in hoofde van de patiënt tot zijn eigen dossier mogelijk moeten kunnen maken.

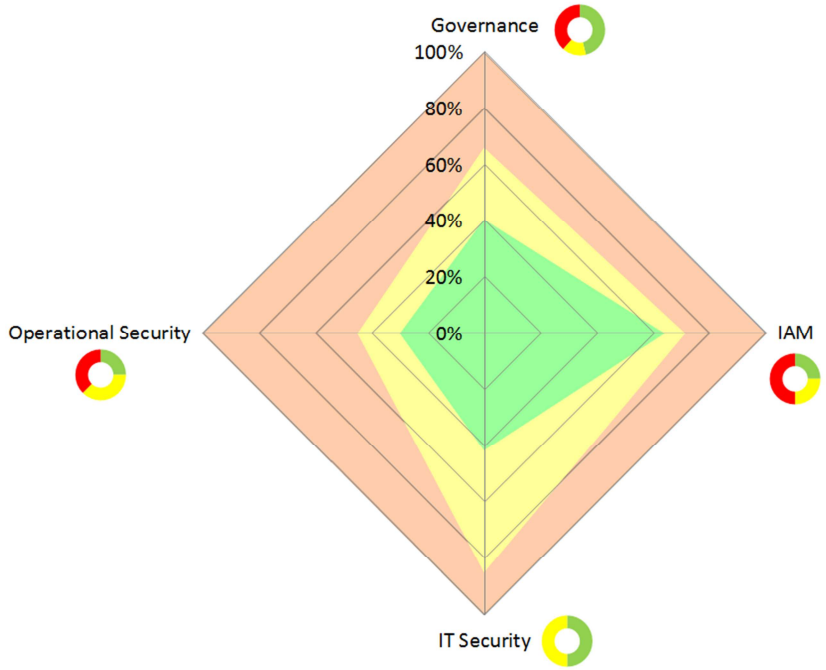
9. Teneinde de ziekenhuizen of andere verzorgingsinrichtingen toe te laten om een dergelijke risico-analyse te kunnen uitvoeren, acht de Commissie het aangewezen dat, naast de theoretische omkadering die het ontwerp van omzendbrief biedt, een praktische en kwantitatieve methode om de beveiliging van cloud diensten te evalueren, aan de ziekenhuizen en andere actoren in de gezondheidssector ter beschikking zou worden gesteld. De Commissie verwijst hiervoor, als voorbeeld, naar het door de afdeling Gezondheid van het Sectoraal comité van de Sociale Zekerheid en van de Gezondheid terzake aanbevolen evaluatiemodel[12] dat hierna wordt toegelicht.
   De Commissie merkt wel nog eerst op dat (het ontwerp van) omzendbrief inzake cloud diensten zich best onthoudt van het aanbevelen van een welbepaalde soort cloud, in casu 'community of privé-cloud', omdat die op zichzelf niet noodzakelijk meer garanties biedt op het vlak van bescherming van persoonsgegevens. Ongeacht het type cloud moet worden gefocust op de effectief geboden garanties inzake gegevensbescherming.

10. Hierna wordt het tweevoudig model beschreven dat toelaat om aan de hand van een eenvoudig, evolutief rooster enerzijds het maturiteitsniveau in verband met de beveiliging van een specifieke cloud dienst te evalueren en anderzijds het gebruik van een specifieke cloud dienst te evalueren naargelang het soort gegevens die men ernaar wil overbrengen.

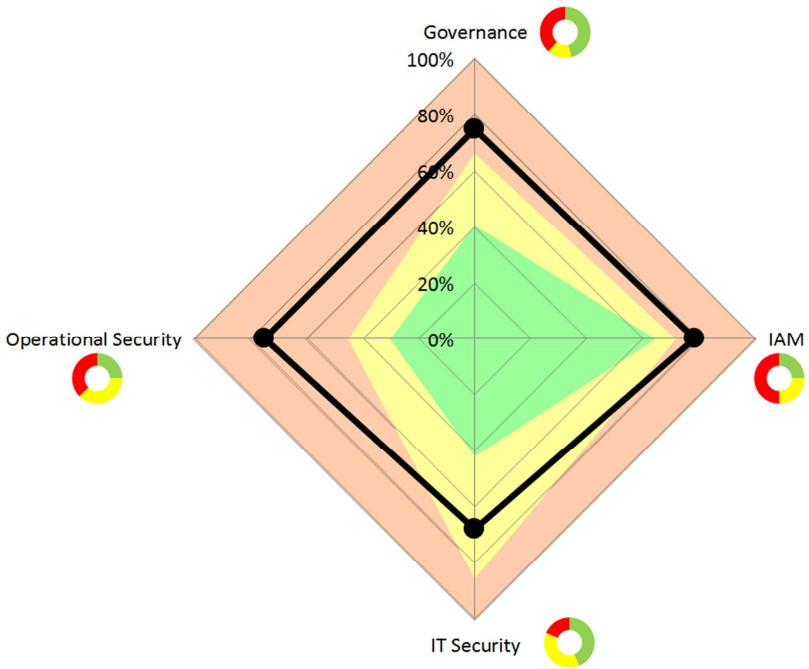
11. In concreto bestaat de voorgestelde methode uit twee luiken:

    - een luik A bestaat uit de vragenlijst "Security-assessment-cloud-service.xlsm" waarmee het maturiteitsniveau in verband met de beveiliging van een specifieke cloud dienst geëvalueerd kan worden. Deze evaluatie moet enkel steunen op de publieke gegevens die de evaluator op voorhand heeft kunnen verzamelen (bv. op de officiële website van de cloud dienst). De figuur hieronder is een voorbeeld van een analyseresultaat voor een cloud dienst zodra de vragenlijst van luik A ingevuld is. Het resultaat wordt weergegeven in de vorm van een radar.

[12] Zie 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*.



- een luik B bestaat uit de vragenlijst "Client-guide-cloud-assessment.xlsm" waarmee men de mogelijkheid kan evalueren om een specifieke clouddienst te gebruiken naargelang het soort gegevens die men ernaar wil overbrengen. De figuur hieronder is een voorbeeld van het resultaat van een vergelijking. De figuur herneemt de radar verkregen na de toepassing van luik A op een clouddienst. De zwarte lijn komt overeen met de behoeften en eisen van de gebruiker die de vragenlijst van luik B heeft ingevuld. Het eindresultaat van luik B baseert zich dus op een radar die resulteert uit luik A, aangevuld door de evaluatie van de gebruiker.



12. De belangrijkste beveiligingsaspecten die geëvalueerd worden door het model worden gegroepeerd in 4 hoofdcriteria: governance, identiteitsbeheer en toegangscontrole, IT-beveiliging en tot slot operationele beveiliging. In de context van (sociale zekerheid en) gezondheidszorg evalueert het model ook de conformiteit van de cloud dienst met de 'Veiligheidspolicy met betrekking tot Cloud Computing Services', gepubliceerd door de Kruispuntbank van de Sociale Zekerheid[13]. Deze conformiteit wordt in de luiken A en B weergegeven door de donuts (een donut per hoofdcriterium).

13. De kleurcodes zijn hetzelfde voor donuts of radars. De groene zone, genaamd "confidence zone", vertegenwoordigt het percentage dat een cloud dienst met zekerheid aan een hoofdcriterium voldoet. De gele zone, genaamd "doubt zone", vertegenwoordigt het percentage dat een cloud dienst mogelijk aan een hoofdcriterium voldoet. We spreken van "mogelijk voldoet" om de geëvalueerde cloud dienst niet te bestraffen: de "doubt zone" geeft dus de vragen van de vragenlijst "Security-assessment-cloud-service.xlsm" weer waar we onmogelijk met zekerheid op kunnen antwoorden. De rode zone, genaamd "death zone", vertegenwoordigt het percentage dat een cloud dienst niet aan een hoofdcriterium voldoet.

14. De figuren hieronder tonen een vergelijking tussen 5 verschillende cloud diensten en de behoeften/eisen van een klant die de vragenlijst van luik B ingevuld heeft. Het model vergelijkt zo de cloud dienst per criterium om de analyse te vergemakkelijken.

[13] https://www.ksz-bcss.fgov.be/binaries/documentation/nl/securite/policies/isms_050_cloud_computing_policy_nl.pdf

15. Beide vragenlijsten van luik A en luik B worden aan dit advies als bijlage toegevoegd en zullen, samen met het advies, worden gepubliceerd op de website van de Commissie.[14]

16. Het gebruik van dit model (of een ander gelijkwaardig model) door een ziekenhuis of eender welke actor in de gezondheidszorg moet toelaten om zelf te evalueren in welke mate het veiligheidsniveau van een bepaalde cloud dienst voldoet aan de specifieke behoeften. Zodoende kan de betrokken actor in de gezondheidszorg op gefundeerde wijze de diverse risico's inschatten alvorens op eigen verantwoordelijkheid gebruik te maken van een bepaalde cloud dienst.

[14] Voor de operationele 'tool' zie: http://www.privacycommission.be/nl/evaluatiemodel-voor-de-beveiliging-van-de-clouddiensten.

III. BESLUIT

17. De Commissie is van oordeel dat het ontwerp van Omzendbrief betreffende het gebruik van cloud computing door de ziekenhuizen voldoende waarborgen kan bieden wat de bescherming van de persoonsgegevens van de betrokkenen betreft[15], op voorwaarde dat
    - deze wordt aangevuld met een operationeel bruikbare evaluatietool die de ziekenhuizen en andere verzorgingsinrichtingen toelaat om op eigen verantwoordelijkheid de beveiliging van cloud diensten te evalueren; de Commissie verwijst hiervoor, als voorbeeld, naar het door het Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid terzake aanbevolen evaluatiemodel (zie randnrs. 6, 9 en 16);
    - de aanbeveling van een welbepaald soort cloud, in casu 'community of privé-cloud', uit de tekst van het ontwerp wordt verwijderd; immers de keuze voor een 'community of privé-cloud' biedt op zichzelf niet noodzakelijkerwijze meer garanties op het vlak van een betere bescherming van gegevens; ongeacht de soort cloud moet worden gefocust op de effectief geboden garanties inzake gegevensbescherming (zie randnr. 9).

OM DEZE REDENEN

Brengt de Commissie, met verwijzing naar aanbeveling nr. 15/01 van het Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid, afdeling Gezondheid, een **gunstig advies** uit over het ontwerp van Omzendbrief betreffende het gebruik van cloud computing door de ziekenhuizen, onder de uitdrukkelijke en absolute voorwaarde dat voormelde opmerkingen worden geïntegreerd in de tekst, gelet op de mogelijke gevoeligheid van de gegevens.

Voor de Wnd. Administrateur, afw. De Voorzitter,

(get.) An Machtens (get.) Willem Debeuckelaere
Wnd. Afdelingshoofd ORM

[15] De Commissie heeft wel vastgesteld dat de Nederlandstalige versie van het document qua gebruikte terminologie (waarschijnlijk het gevolg van onzorgvuldige vertaling) op sommige plaatsen vatbaar is voor optimalisatie. Bijvoorbeeld: doorheen de tekst 'behandeling' en verantwoordelijke voor de 'behandeling' vervangen door 'verwerking' en verantwoordelijke voor de 'verwerking' ('traitement' in het Frans); op p. 8, tweede alinea onder punt 6.3 'niet zinvol' vervangen door 'zinvol', ….

Cloud Service Security Assessment Model

VERSION: 1.0

Change tracking	
1.0	First release
How to use this template:	
1.	The goal of this evaluation form is for a person (called assessor) to assess the security level of a cloud service offered by a Cloud Service Provider (CSP) according to 4 main criteria: - Governance - Identity and Access Management (IAM) - IT Security - Operational Security
2.	Before filling the evaluation form, the assessor should be in possession of a standard contract and all the available datasheets that can be found on the website of the cloud service. We assume that the information found about the cloud service on the official website are correct.
3.	The "Information" tab should be filled all the general info related to the assessment: cloud service name/provider/model, the name of the assessor, and the date of the assessment.
4.	The "Assessment" tab contains all the questions necessary for the evaluation of a cloud service.
4.1.	The column "answer's value" contains the relative score of each expected response for each question (over 100) as a reference. The cells containing the relative scores must not be changed.
4.2.	The column "score" has to be filled using the possible answers.
	Note: The questions must be filled according to the given order, as some questions depend on the answers given in previous questions.
	Note: If a score is not applicable, the option "N/A" must be chosen. This will redistribute the weights for the sub questions.
	Note: If the assessor does not know the answer to a question, the option "Unknown" must be chosen. This will give two different scores for one topic.

4.3.	Each question has been defined with a specific weight. From the scores of each question, the final weighted scores are automatically filled (in combination with the defined weights).
4.4.	There are 2 different results: the **minimal weighted score** and the **maximal weighted score**. - The **minimal weighted score** corresponds to the situation where all the "Unknown" responses have been replaced by the worst answer. This is the worst case of the security evaluation, considering the uncertainty of the "Unknown" responses. - The **maximal weighted score** corresponds to the situation where all the "Unknown" responses have been replaced by the best answer. This is the best case of the security evaluation, considering the uncertainty of the "Unknown" responses.
4.5.	The two last columns grouped under "compliance with cloud policy" refer to the guarantees required by the cloud policy of the Social Security.
	The column "ignoring the data type" refers to the cloud policy guarantees that do not depend on the type of data to be stored in the cloud service.
	The column "if personal, social or medical data" refers to the additional cloud policy guarantees expected when the data to be stored in the cloud service are personal, social or medical.
5.	The "Overview" tab is a visual aide for the assessor.
5.1.	The chart represents the minimal and maximal weighted scores of each criterion.
5.2.	The donuts represent the compliance to the cloud policy per criterion when the data type is ignored.
6.	Be careful with the interpretation of the scores.

Cloud service informations	
Cloud service name:	<name>
Cloud service provider (CSP):	<CSP>
Cloud service model:	<choose a model>
Evaluated by:	<assessor name>
Evaluated date:	<dd/mm/yyyy>

Assessment of <name>

	Category Title	Answer's value	Score	Minimal weighted score	Maximal weighted score	Compliance with cloud policy	
	For more information open the outline (+ / -) left from row number	*Possibility to put some description in the question's rows*	*Select appropriate range or value for every question (select N/A if not applicable)*	*Values computed automated*	*Values computed automated*	*Ignoring the data type*	*If personal, social or medical data*
1	**Governance**			**0%**	**0%**		
1.1	Legal implication			0%	0%		
1.1.1	What is the physical location of data-at-rest?			0	0		
1.1.2	Which jurisdiction is the CSP subject to?			0	0		
1.1.3	Can the CSP accomodate with the tenant's data retention requirements?			0	0		
1.1.4	Can the data be given to governments if requested for judicial requirements without informing the tenant or without constitutional guarantees?			0	0	X	
1.1.5	Can the data be given to, shared with third parties, or used by the CSP for other purposes than the cloud service without the tenant's consent?			0	0	X	
1.1.6	If the US-EU Safe Harbor applies, is the CSP registered?			0	0		
1.2	Supply chain management			0%	0%		
1.2.1	Does the CSP use subcontrators?			0	0		
1.2.2	If so, will the CSP inform the tenant of the subcontractors hired to provide the cloud service?			0	0	X	
1.2.3	If so, will the CSP inform the tenant of any change in the course of the contract?			0	0	X	
1.2.4	If so, does the CSP guarantee contractually to remain fully responsible for his engagements, even with the hiring of subcontractors?			0	0	X	
1.3	Audit			0%	0%		
1.3.1	At which time interval is the cloud service (including all its subcontractors) audited by a third party?			0	0	X	
1.3.2	If the cloud service is audited, are the scopes of the audits accurately defined?			0	0	X	
1.3.3	At which time interval is the cloud service (including all its subcontractors) pen-tested?			0	0	X	
1.3.4	Did the cloud service define an ISP (Information Security Policy) and obtain a security-related certification?			0	0	X	
1.3.5	Is there a Tier certification of data centers (especially for physical availability and security) or equivalent certification?			0	0	X	

1.4	Business continuity					0%	0%		
1.4.1	Is the cloud service delivery managed under SLAs (Service Level Agreements)?					0	0	X	
1.4.2	Does the CSP define and implement a business continuity plan?					0	0	X	
1.4.3	Is the reversibility of the cloud service provided?					0	0	X	
1.5	Others					0%	0%		
1.5.1	Does the CSP apply a segregation of duties in the CSP organization to protect the tenants?					0	0		
1.5.2	If meta-data are extracted by the CSP from the process of tenant's data, are they used for the cloud service only?					0	0		
2	**Identity and Access Management (IAM)**					**0%**	**0%**		
2.1	Authentication level					0%	0%		
2.1.1	Are the different authentication mechanisms to access the cloud service documented?					0	0		
2.1.2	What is the strongest authentication mechanism to access the cloud service as a tenant system administrator offered by the CSP?					0	0		
2.1.3	What is the strongest authentication mechanism to access the cloud service as a tenant user offered by the CSP?					0	0		
2.1.4	Are password policy enforcements well-defined and implemented?					0	0		
2.1.5	Are secure password reset procedures well-defined and implemented?					0	0		
2.2	User management					0%	0%		
2.2.1	Who performs the tenants' user management?					0	0		
2.2.2	Is the integration with the IAM of the tenant possible?					0	0		
2.2.3	Is the integration with an ID-provider possible?					0	0		
2.2.4	Are the identification and/or authentication of the devices used to access the cloud service possible as additional enforcement of the IAM?					0	0	X	
2.3	Access management					0%	0%		
2.3.1	Does the CSP document how the IAM of its employees related to the tenants' assets is performed?					0	0		
2.3.2	Is data access of {tenant user, tenant system administrator, CSP system administrator} clearly defined?					0	0	X	

2.3.2	Is data access of {tenant user, tenant system administrator, CSP system administrator} clearly defined?			0	0	X	
2.3.3	Is data access of {CSP employees, third party, other tenants} denied?			0	0	X	
2.3.4	Is IAM management and data access logging clearly defined and available?			0	0	X	
3	**IT Security**			**0%**	**0%**		
3.1	Segregation of data			0%	0%		
3.1.1	Can the cloud service be provided as private or community?			0	0		X
3.1.2	In a multi-tenant system, are the data of the respective tenants segregated/isolated in such a way that it is technically impossible for any user of tenant A to receive entitlements to data of tenant B?			0	0	X	
3.2	Interface security			0%	0%		
3.2.1	Are APIs developed in accordance with standards?			0	0		
3.2.2	Are data integrity and security ensured for input and output?			0	0	X	
3.3	Infrastructure and virtualization security			0%	0%		
3.3.1	Is the access to hypervisors management functions and administration consoles highly controlled?			0	0	X	
3.3.2	Is data securely deleted from all storage media when the user's or tenant's account is deleted?			0	0	X	
3.3.3	Does the CSP take defense-in-depth approach to wired or wireless network security?			0	0	X	
3.3.4	Are sufficient controls in place at the hardware and virtual (if applicable) levels?			0	0	X	
3.3.5	Are security mechanisms to prevent and analyze data leakage at the hardware and virtual (if applicable) levels available?			0	0	X	
3.4	OS security (only for SaaS and PaaS cloud services)			0%	0%		
3.4.1	Are tools to prevent, detect and mitigate viruses and malwares at server stations available?			0	0	X	
3.4.2	Is harding process performed on the server stations?			0	0	X	
3.5	Cryptography			0%	0%		
3.5.1	Who is in charge of the key management?			0	0		X

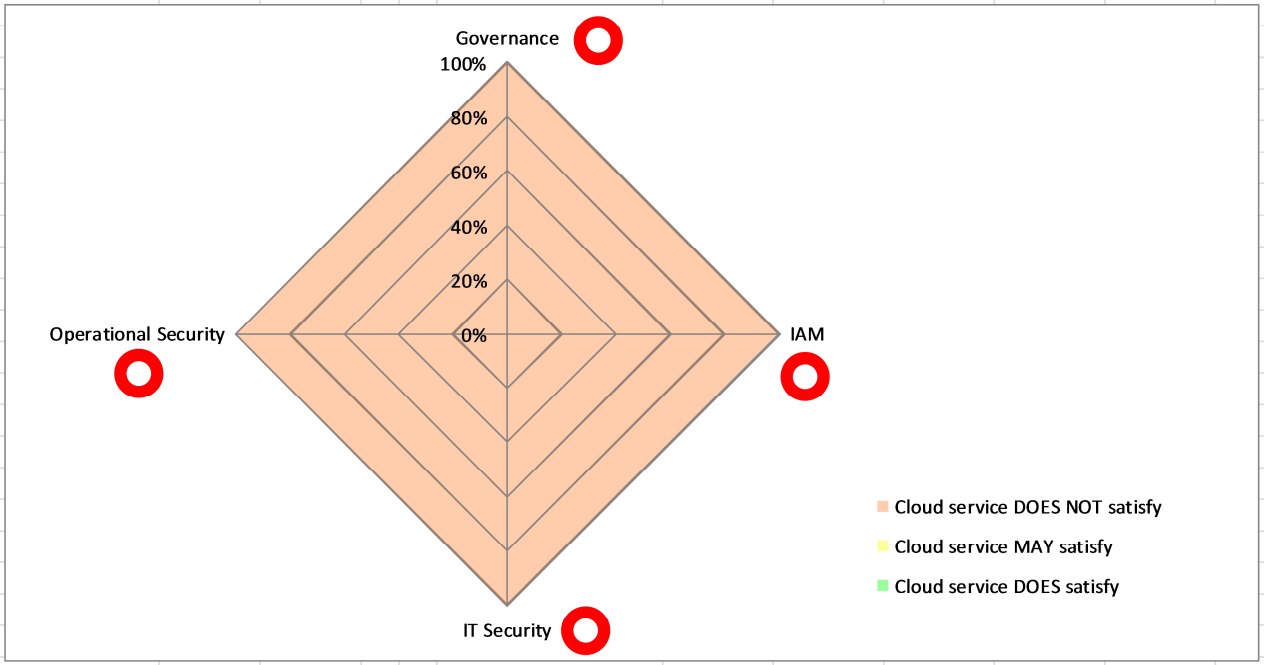
3.5.2	Has the key management been defined through policies and procedures as required by the ISO/IEC27002:2013 standard?			0	0		
3.5.3	Have the cryptographic mechanisms used for the cloud service been defined to guarantee adequate cryptographic strength?			0	0		
3.5.4	Does the CSP use HSMs (Hardware Security Modules) for the protection of keys?			0	0		
3.5.5	Is client-side encryption of data possible?			0	0		X
3.5.6	Is data-at-rest confidentiality ensured?			0	0		X
3.5.7	Is data-at-rest integrity ensured?			0	0	X	
4	**Operational Security**			**0%**	**0%**		
4.1	Backup and disaster recovery			0%	0%		
4.1.1	Can the backup retention plan be defined by the tenant?			0	0	X	
4.1.2	Are backup controls defined and adequate?			0	0	X	
4.1.3	Which RTO (Recovery Time objective) can be satisfied by the cloud service?			0	0	X	
4.1.4	Which RPO (Recovery Point objective) can be satisfied by the cloud service?			0	0	X	
4.1.5	Are tenants able to perform recovery tests, including reporting?			0	0	X	
4.2	Incident management			0%	0%		
4.2.1	Does the CSP have a SIEM (Security Information and Event Management) for analyzing the security alerts and data logs?			0	0	X	
4.2.2	Does the CSP have an adequate incident management procedure for managing and minimizing the impact of security incidents on tenants' data?			0	0	X	
4.2.3	Does the CSP have adequate security policies and procedures regarding CSP employee security?			0	0	X	
4.3	Vulnerability management (only for SaaS and PaaS cloud services)			0%	0%		
4.3.1	Is there a documented patch management process implemented in the cloud service?			0	0	X	
4.3.2	Does the CSP test patches in acceptance environments prior to deployment?			0	0	X	

Score overview of <name>

Copy **scores** for future use

	Minimal weighted score	Maximal weighted score
Governance	0%	0%
IAM	0%	0%
IT Security	0%	0%
Operational Security	0%	0%

	Compliance with cloud policy (ignoring the data type)			Compliance with cloud policy (if personal/social/medical data)		
	Does comply	May comply	Does not comply	Does comply	May comply	Does not comply
Governance	0	0	13	0	0	13
IAM	0	0	4	0	0	4
IT Security	0	0	10	0	0	14
Operational Security	0	0	8	0	0	8



Client Guide Cloud Assessment Model

VERSION: **1.0**

Change tracking	
1.0	First release
How to use this template:	
1.	The goal of this evaluation form is for a person (called client) willing to use a cloud service offered by a Cloud Service Provider (CSP) to assess if his/her wish is possible, depending on the type of data that is intended to be moved to the cloud service and according to the 4 main characteristics expected of a cloud service: - Governance - Identity and Access Management (IAM) - IT Security - Operational Security
2.	The "Assessment" tab contains all the questions necessary for the client to assess what he/she expects from a cloud service.
2.1.	First fill all the client name at the beginning.
2.2.	The column "answer's value" contains the relative score of each expected response for each question (over 100) as a reference. The cells containing the relative scores must not be changed.
2.3.	The column "score" has to be filled using the possible answers.
2.4.	Each question has been defined with a specific weight. From the scores of each question, the final weighted scores (called "**required scores**") are automatically filled (in combination with the defined weights).
3.	The "Overview" tab is a visual aide.
3.1.	The chart represents the required scores.
3.2.	It is further possible to paste the scores of a cloud service that has been assessed, and to see if it satisfies the client's requirements.
3.3.	The donuts represent the compliance to the cloud policy per criterion depending on the type of data that is intended to be moved to a cloud service.
4.	The "Comparison" tab is another visual aide where it is possible to paste the scores of several cloud services that have been assessed.
4.1.	The charts allow the client to see which cloud service fits best his/her requirements.
4.2.	Here as well, the donuts represent the compliance to the cloud policy per criterion depending on the type of data that is intended to be moved to a cloud service.
5.	Be careful with the interpretation of the scores.

<Fill client name>

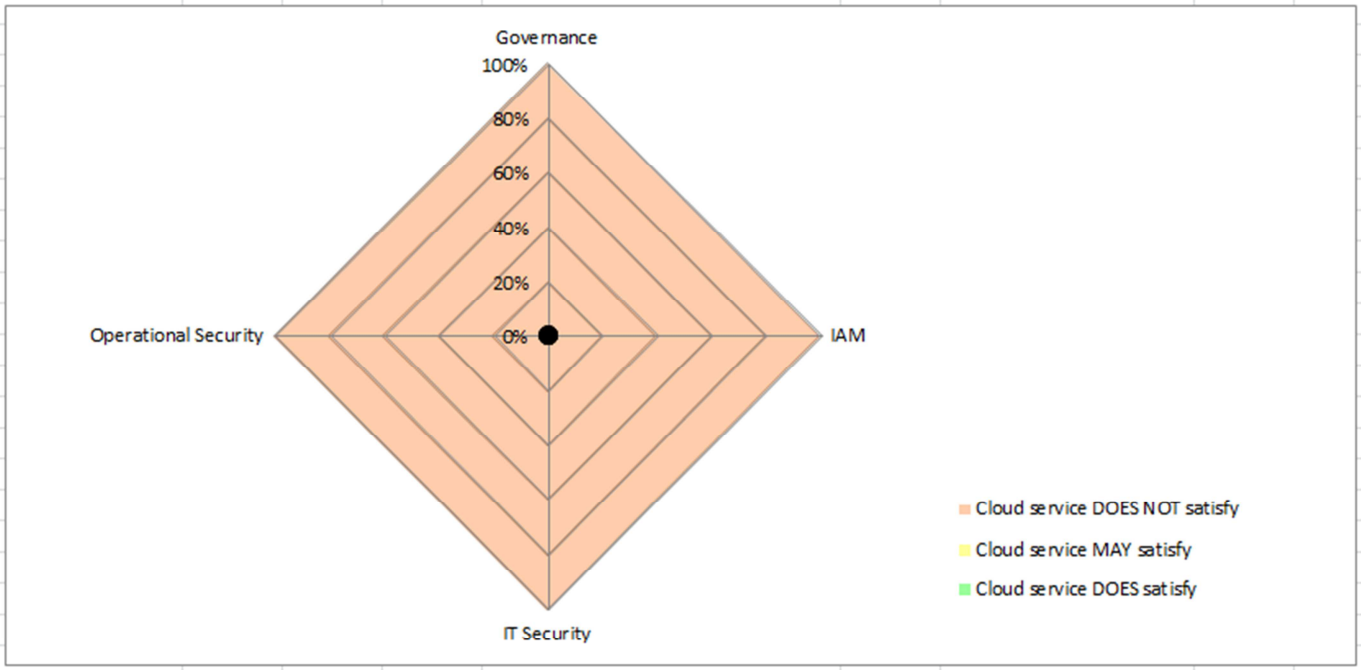
	Category Title	Answer's value	Score	Required score
	For more information open the outline (+ / -) left from row number	*Possibility to put some description in the question's rows*	*Select appropriate range or value for every question (even if not applicable N/A)*	
0	**Data Type**			
0.1	What type of data is intended to be moved to a cloud service?			
1	**Governance**			**0%**
1.1	Which level of governance must be attained by the cloud service?			0
2	**Identity and Access Management (IAM)**			**0%**
2.1	Which level of authentication must be offered by the cloud service?			0
2.2	Which level of control on the user management must be proposed by the cloud service?			0
2.3	Which level of access management must be provided by the cloud service?			0
3	**IT Security**			**0%**
3.1	Which deployment model must be provided by the cloud service?			0
3.2	Which level of interface security must be provided by the cloud service?			0
3.3	Which level of infrastructure and virtualization security must be achieved by the cloud service?			0
3.4	Which level of cryptography must be provided by the cloud service?			0
4	**Operational Security**			**0%**
4.1	Which level of backup and disaster recovery must be provided by the cloud service?			0
4.2	Which level of incident management must be provided by the cloud service?			0

Score overview of

Reset values

Paste scores	Minimal weighted score	Maximal weighted score	Required score	Does the cloud service satisfy the required score?
Governance	0%	0%	0%	Cloud service DOES satisfy
IAM	0%	0%	0%	Cloud service DOES satisfy
IT Security	0%	0%	0%	Cloud service DOES satisfy
Operational Security	0%	0%	0%	Cloud service DOES satisfy
				Cloud service DOES satisfy

	Compliance with cloud policy when data type is:		
	Does comply	May comply	Does not comply
Governance	0	0	0
IAM	0	0	0
IT Security	0	0	0
Operational Security	0	0	0



Comparison when data type is:

		<Cloud Service 1>		<Cloud Service 2>		<Cloud Service 3>		<Cloud Service 4>		<Cloud Service 5>	
	Required score	Minimal weighted score	Maximal weighted score	Minimal weighted score	Maximal weighted score	Minimal weighted score	Maximal weighted score	Minimal weighted score	Maximal weighted score	Minimal weighted score	Maximal weighted score
Governance	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
IAM	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
IT Security	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
Operational Security	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%

Reset values | Paste scores of cloud service 1 | Paste scores of cloud service 2 | Paste scores of cloud service 3 | Paste scores of cloud service 4 | Paste scores of cloud service 5