Avis n°10/2016 du 24 février 2016

Objet : avis d'initiative relatif au recours au cloud computing par les responsables du traitement (CO-A-2015-013)

La Commission de la protection de la vie privée (ci-après "la Commission") ;

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (ci-après "la LVP"), en particulier l'article 29 ;

Vu le rapport de Monsieur Stefan Verschuere, Vice-Président ;

Émet, le 24 février 2016, l'avis suivant :

I. Introduction

1. Objet

1. Cet avis a pour objet d'établir des lignes directrices afin d'aider les responsables du traitement qui souhaitent recourir à de services de cloud computing à respecter leurs obligations découlant de la LVP, étant donné les risques induits par ces services malgré leurs avantages notamment du point de vue économique[1].

2. Portée

2. L'analyse s'intéresse aux responsables du traitement qui recourent aux services de sous-traitants pour traiter leurs données dans le cloud.

3. Il n'est pas question dans le présent avis d'aborder les utilisations du cloud à des fins privées qui sont en principe exemptées des dispositions de la LVP[2]. Les particuliers qui utilisent des solutions de cloud computing ne sont dès lors pas concernés par le présent texte qui a vocation à s'adresser aux entreprises et administrations.

4. L'avis ne s'intéresse pas non plus aux situations dans lesquelles le fournisseur de services cloud (ou Cloud Service Provider, en abrégé CSP) peut être considéré comme responsable du traitement, notamment dès lors qu'il utilise légitimement les données pour d'autres finalités.

5. Si le responsable du traitement ne recourt pas à un sous-traitant mais développe sa propre solution de cloud computing sur laquelle il a le contrôle total, le présent avis ne trouve pas non plus à s'appliquer.

6. L'avis se focalise sur les aspects essentiels de la problématique et ne se veut pas exhaustif afin de gagner en lisibilité.

II. Définitions

7. Le cloud computing évolue et comprend un large éventail de solutions technologiques et de pratiques commerciales. Le terme est utilisé avec différentes significations dans différents

[1] Le cloud computing permet également aux petites et moyennes entreprises de bénéficier de technologies de plus haut niveau que celles auxquelles elles pourraient prétendre de manière traditionnelle.

[2] Voir l'article 3, § 2 de la LVP.

contextes. Une définition largement acceptée du cloud computing est la définition suivante établie par le National Institute of Standards and Technology américain (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. Selon les sources qui sont proposées via les services cloud, on peut distinguer trois catégories principales de services : 1) Software as a Service (SaaS), 2) Platform as a Service (PaaS) et 3) Infrastructure as a Service (IaaS)[4].

9. Enfin, selon l'accessibilité du cloud computing, *quatre catégories d'utilisation* sont distinguées : 1) le cloud privé (disponible pour une seule organisation), 2) le cloud public (disponible pour le grand public), 3) le cloud 'community' ou communautaire (pour une communauté spécifique déterminée se composant de différentes organisations avec des intérêts partagés) et 4) le cloud hybride (qui peut se composer de deux ou de plusieurs des catégories d'utilisation susmentionnées).

III. Application de la LVP

1. Champ d'application matériel

10. La LVP s'applique[5] en principe dès lors qu'on est en présence d'un traitement[6] de données à caractère personnel[7]. Dans un environnement de cloud, il sera rapidement question de tels traitements dès lors que l'on y stocke des documents ou que l'on y gère des applications destinées à travailler sur des données à caractère personnel.

2. Champ d'application territorial

11. La Commission rappelle que la détermination du régime juridique relatif à la protection des données à caractère personnel applicable doit être distinguée de la compétence judiciaire qui

[3] Voir http://www.nist.gov/itl/cloud/.
[4] Voir http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.
[5] Article 3, § 1 de la LVP.
[6] Voir l'article 1, § 2 de la LVP.
[7] Voir l'article 1, § 1 de la LVP.

établit l'aptitude des tribunaux nationaux à connaître d'une affaire[8]. Seul le premier aspect qui intéresse l'applicabilité de la LVP est traité dans cette section.

12. Le champ d'application de la LVP est défini en son article 3*bis*. Cette disposition prévoit deux critères d'application territoriale. La notion de responsable du traitement y est centrale.

13. La LVP s'applique dès lors qu'une personne physique ou morale, une association de fait ou une administration publique utilise le cloud computing dans le cadre des activités réelles et effectives de son établissement situé en Belgique. Elle encadre les traitements de données effectués même si le fournisseur de services cloud est également établi dans un autre État, et quel que soit le lieu où sont conservées les données[9].

14. Il est question du critère secondaire d'applicabilité de la LVP lorsque le critère principal ne trouve pas à s'appliquer, c'est-à-dire que le responsable du traitement n'est pas établi de manière permanente sur le territoire de la Communauté européenne.

15. La LVP s'appliquera dès lors que le responsable du traitement recourt, à des fins de traitement de données à caractère personnel, à des services de cloud computing situés sur le territoire belge, autres que ceux qui sont exclusivement utilisés à des fins de transit sur le territoire belge[10].

3. Responsabilité du traitement

16. Les obligations découlant de la LVP sont à charge du responsable du traitement. La notion de "responsable du traitement" est définie comme suit dans la LVP : "*la personne physique ou morale, l'association de fait ou l'administration publique qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel*"[11].

17. La Commission note que le client de services cloud doit être en principe considéré comme le responsable du traitement dès lors qu'il détermine les finalités et décide d'externaliser ou non ses traitements dans le cloud.

18. La Commission rappelle à cet égard que le déséquilibre dans les relations contractuelles entre un responsable du traitement de petite ou moyenne importance par rapport à un fournisseur de

---

[8] Voir à ce dernier égard, B. Volders, "IPR in de wolken : het toepasselijke recht op Cloud computing-overeenkomsten", *Computerrecht*, 2011/3, p. 137 et sv.

[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, p. 1007.

[10] Article 3*bis*, 2° de la LVP.

[11] Article 1, § 4 de la LVP.

services de grande taille ne pourrait justifier d'accepter des termes et conditions contractuelles non conformes avec la LVP[12].

19. Sans préjudice d'actions fondées sur d'autres dispositions légales, le responsable du traitement est responsable du dommage causé à la personne concernée par un acte contraire aux dispositions déterminées par ou en vertu de la LVP[13]. Il ne peut être exonéré de cette responsabilité que s'il prouve que le fait qui a provoqué le dommage ne lui est pas imputable.

4. Sous-traitance

20. Par "sous-traitant" ou "sous-contractant", la LVP entend "*la personne physique ou morale, (…) qui traite des données à caractère personnel pour le compte du responsable du traitement et est autre que la personne qui, placée sous l'autorité directe du responsable du traitement, est habilitée à traiter les données*"[14].

21. Le fournisseur de services cloud doit en principe être appréhendé comme sous-traitant bien qu'il y ait des situations où il peut être considéré comme responsable conjoint du traitement ou responsable du traitement en tant que tel, en fonction des circonstances. C'est par exemple le cas quand le fournisseur traite des données à des fins propres.

22. Lorsqu'un responsable du traitement décide de sous-traiter des traitements dans le cloud, il doit choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures techniques et organisationnelles de sécurité relatives aux traitements et doit veiller au respect de ces mesures[15].

23. La responsabilité du fournisseur de services cloud à l'égard du responsable du traitement doit être fixée par un contrat. Ce contrat doit par ailleurs au minimum indiquer que le sous-traitant n'agit que sur la seule instruction du responsable du traitement et est tenu par les mêmes obligations que celles auxquelles le responsable du traitement est tenu en ce qui concerne les mesures techniques et organisationnelles de protection des données telles que précisées ci-dessous.

---

[12] Voir l'avis du Groupe 29 n° 05/2012 du 1er juillet 2012 *sur l'informatique en nuage*, p. 10, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_fr.pdf, et la référence à son avis 1/2010 du 16 février 2010 sur les notions de "responsable du traitement" et de "sous-traitant".

[13] Article 15*bis* de la LVP.

[14] Article 1, § 5 de la LVP.

[15] Article 16, § 1er de la LVP.

5. Mesures techniques et organisationnelles de protection des données

24. Conformément à l'article 16 de la LVP, le responsable du traitement doit mettre en œuvre les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel.

25. La sécurité de l'information consiste à protéger les informations traitées par une organisation de nombreux risques, soit des menaces (actions malveillantes internes ou externes), soit des vulnérabilités (risques propres aux systèmes et aux applications), et permet donc de garantir la confidentialité, l'intégrité ainsi que la disponibilité des données.

26. Cette sécurité doit être assurée par l'application de mesures adéquates[16] dont des structures organisationnelles, des règles, des processus, des procédures mais également des systèmes techniques. Cet ensemble de mesures doit être déterminé et documenté, mis en œuvre, contrôlé et amélioré aussi souvent que possible afin que les finalités spécifiques en matière de sécurité soient atteintes.

27. Spécifiquement en ce qui concerne le cloud computing, il existe le risque de fuites de données dans l'environnement du cloud. À cet égard, la Commission renvoie à sa recommandation d'initiative n° 01/2013[17] *relative aux mesures de sécurité à respecter afin de prévenir les fuites de données*.

6. Droits des personnes concernées

a. Devoir d'information

28. Le responsable du traitement doit fournir à la personne concernée les informations visées à l'article 9 de la LVP.

29. En l'espèce, le client de services cloud doit informer les personnes concernées de son identité, des finalités du traitement, du droit de s'opposer gratuitement à un traitement envisagé à des fins de

[16] Les mesures de sécurité publiées par la Commission (http://www.privacycommission.be/sites/privacycommission/files/documents/mesures_de_reference_en_matiere_de_securite_applicables_a_tout_traitement_de_donnees_a_caractere_personnel.pdf), l'ISAE 3402 et la norme ISO 27.002 peuvent à cet égard offrir un cadre de référence approprié.

[17] Recommandation d'initiative n° 01/2013 du 21 janvier 2013 : https://www.privacycommission.be/sites/privacycommission/files/documents/recommandation_01_2013_0.pdf.

marketing direct. Le client devrait en principe [18] également fournir d'autres informations supplémentaires notamment les destinataires ou catégories de destinataires. La Commission recommande à cet égard que le client informe la personne concernée sur l'identité de ses sous-traitants et sous-traitants ultérieurs dans le cloud.

30. La Commission insiste sur le fait que le responsable du traitement doit se montrer transparent à la fois en ce qui concerne les données traitées et les traitements appliqués.

b. Droits d'accès, de rectification, d'opposition et de suppression

31. Les articles 10 et 12 de la LVP offrent aux personnes concernées un droit d'accès aux données les concernant traitées par le responsable du traitement et la possibilité d'en obtenir la rectification, l'effacement ou encore de s'opposer à leur traitement.

7. Localisation des données

32. Le client de services cloud doit veiller à ce que les données soient traitées dans des pays assurant un niveau de protection de données adéquat.

33. Les données à caractère personnel peuvent circuler librement au sein de l'Union européenne. Les articles 21 et 22 de la LVP régissent le transfert de données à caractère personnel vers des pays non membres de l'Union européenne.

34. Tout responsable de traitement qui souhaite exporter des données à caractère personnel hors de l'Union européenne doit d'abord se renseigner sur le niveau de protection adéquat du pays destinataire[19]. En effet, lorsque le pays tiers est considéré comme offrant un niveau de protection adéquat, le transfert peut être effectué comme s'il s'agissait d'un transfert entre deux responsables en Belgique, ou vers un autre pays de l'Union européenne.

35. La Commission européenne a la compétence de constater qu'un pays tiers offre un niveau de protection adéquat et a déjà reconnu le niveau de protection adéquat de nombreux pays[20]. Dans un arrêt du 6 octobre 2015 (arrêt "Schrems"), la Cour de Justice de l'Union européenne a invalidé la décision d'adéquation constatant que les États-Unis assurent un niveau de protection adéquat aux données à caractère personnel transférées vers des entreprises américaines respectant les

[18] Sauf dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont obtenues ou traitées, ces informations supplémentaires ne sont pas nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données.

[19] https://www.privacycommission.be/fr/en-dehors-ue-protection-adequate.

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

principes de la sphère de sécurité (certification Safe Harbor)[21]. Il ne peut donc être référé à cette décision pour encadrer juridiquement des transferts de données vers les États-Unis. Un paquet « bouclier de protection des données UE-États-Unis » (« EU-U.S. Privacy Shield ») est actuellement en préparation afin de répondre aux critiques de la Cour de Justice de l'Union européenne et ainsi restaurer l'adéquation des Etats-Unis[22].

36. Lorsqu'un pays qui n'est pas membre de l'Union européenne n'est pas reconnu comme offrant un niveau de protection adéquat, il existe cependant différentes possibilités pour un transfert de données, dont signer un contrat type mis à disposition par l'Union européenne ou accepter des règles d'entreprise contraignantes ('BCR')[23]. Les BCR constituent un code de conduite pour les entreprises qui transfèrent des données au sein du même groupe.

37. Le groupe 29 considère que les dérogations permettant de transférer des données en dehors de l'Union européenne sans garanties supplémentaires[24] ne doivent concerner que les cas où les transferts ne sont ni récurrents, ni massifs, ni structurels[25]. Partant, il est pratiquement impossible de se prévaloir de ces dérogations dans le cadre du cloud computing.

IV. Risques liés au cloud

38. Plusieurs risques inhérents sont liés à la migration vers une solution de cloud computing. Les facteurs de risque dépendent du modèle de service (à savoir IaaS, PaaS ou Saas) et du modèle de déploiement (à savoir cloud privé, communautaire, public ou hybride) envisagés lors d'une migration. Les principaux risques pouvant être identifiés lors d'une migration vers une solution de cloud sont les suivants :

1. Renonciation au contrôle sur les traitements et les données

39. Le cloud permet aux organisations d'effectuer des économies importantes sur leur budget informatique. Elles peuvent réduire leur parc informatique maintenu sur site et partant, l'effectif chargé de sa gestion.

---

[21] Affaire C362-14., http://curia.europa.eu/juris/liste.jsf?language=fr&num=C-362/14 ; communiqué de presse, http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117fr.pdf.

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

[23] http://www.privacycommission.be/fr/flux-transfrontieres.

[24] Article 22, alinéa 1 de la LVP.

[25] Document de travail du Groupe 29 n° 12/1998 du 24 juillet 1998 intitulé *Transferts de données personnelles vers des pays tiers : Application des articles 25 et 26 de la directive relative à la protection des données*, référencé dans son avis n° 05/2012 du 1er juillet 2012 *sur l'informatique en nuage*, p. 22 : http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_fr.pdf..

40. Grâce à la virtualisation, les ressources physiques et logicielles peuvent être abstraites, mutualisées et allouées dynamiquement. Les fournisseurs de services cloud sont en mesure de proposer des tarifs sans commune mesure avec l'infogérance classique.

41. Dans le même temps, cette virtualisation implique une fragmentation physique des données sur différents serveurs et centres de données, qui peuvent être situés dans différents pays. Partant, le client de cloud renonce au contrôle sur ses données avec comme conséquence des risques potentiels pour la protection de celles-ci si des garanties suffisantes ne sont pas prévues : fuite ("data breach"), perte, abus, consultation par des tiers, accès par des autorités étrangères, ...

2. Accès afin de faire respecter la loi (law enforcement) par les autorités

42. Des mesures de protection optimales ne peuvent pas empêcher un possible accès aux données par des autorités étrangères. Dans ce cadre, il est également nécessaire de souligner que même si les données sont cryptées, cela n'affecte en rien leur statut : elles restent des données à caractère personnel et doivent être protégées de tout traitement non autorisé. D'autre part, il faut constater que les risques précités sont réduits à condition que seul le client dispose de la clé de cryptage.

43. Les pays se sont dotés de possibilités de saisir des données informatiques ainsi que de repérer, de localiser ou de prendre connaissance des communications électroniques et d'identifier les utilisateurs. En Belgique, de telles facultés sont placées entre les mains des autorités judiciaires (Procureur du Roi ou Juge d'instruction en fonction du degré d'atteinte aux libertés individuelles qu'elles impliquent) ou des services de renseignement.

44. La finalité poursuivie est dans la plupart des cas de faire respecter la loi[26] ou de lutter contre le terrorisme. Cependant, certaines autres fins publiques sont parfois poursuivies faisant accroître le risque de consultation abusive des données.

45. Une étude du Parlement européen avait ainsi épinglé des dispositions du Foreign Intelligence Surveillance Amendment Act (FISAA) américain permettant aux autorités américaines d'accéder sans mandat judiciaire aux données du cloud situées en dehors des États-Unis, appartenant à des personnes non-américaines et traitées par des sociétés ayant une activité commerciale aux États-Unis[27]. Selon ce document, cet accès peut en effet intervenir dès lors que ces données sont

---

[26] "Law enforcement" en anglais.

[27] Étude d'octobre 2012 de la 'DG for internal policies' (Direction générale des politiques internes de l'Union) du Parlement européen : http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/462509/IPOL-LIBE_ET(2012)462509_EN.pdf ; voir également une étude de septembre 2012 de l'Université d'Amsterdam qui illustre au travers d'exemples les dérives auxquelles pourraient amener l'arsenal juridique mis au point par les États-Unis : Dr. J.V.J. van Hoboken, Mr. A.M. Arnbak &

considérées comme importantes pour les seuls intérêts étrangers des États-Unis et peut intervenir en dehors de toute suspicion et sans que le fournisseur de services cloud puisse en informer son client. L'affaire des programmes américains de surveillance de masse[28] a montré l'étendue insoupçonnée des accès ayant été opérés par les autorités américaines sur les données des grands fournisseurs de services de la société de l'information américains.

46. Il convient dès lors d'être prudent vis-à-vis de fournisseurs de cloud étrangers, même établis en Europe ou en Belgique, ou de fournisseurs européens implantés à l'étranger et devant rendre des comptes à des autorités étrangères. Il est déconseillé en tout cas de leur confier des données sensibles touchant à la sécurité et à l'économie nationales. Comme déjà mentionné ces risques peuvent être limités par l'utilisation de techniques de cryptage actuelles à condition que seul le client de cloud dispose de la clé de cryptage. Idéalement les données seront périodiquement décryptées et à nouveau cryptées avec les techniques les plus récentes, de sorte que le cryptage renouvelé (et la clé associée) offre la meilleure protection eu égard à l'état actuel de la technique en matière de sécurité de l'information.

47. Par ailleurs, la fourniture de services de cloud computing entraîne régulièrement le recours à des sous-traitants de la part du fournisseur, ce qui augmente les risques précités.

3. Dépendance technologique du Cloud Service Provider

48. Pour une migration vers le cloud, le client doit s'assurer qu'il dispose d'une réelle possibilité de désengagement auprès du Cloud Service Provider. Les Cloud Service Providers n'utilisent en effet pas toujours des formats de données et des interfaces de service standard favorisant l'interopérabilité et la portabilité entre différents Cloud Service Providers. Si le client décide de changer de Cloud Service Provider, l'absence d'interopérabilité peut occasionner des difficultés, voire même l'impossibilité de transférer les données du client vers le nouveau Cloud Service Provider (ce qu'on appelle le "vendor lock-in").

4. Mauvaise gestion des droits d'accès

49. Un des avantages de l'utilisation d'un service cloud est la possibilité de consulter les données à distance. Les utilisateurs peuvent consulter les mêmes données, tant par exemple de la maison que du bureau, et ce au moyen d'un large éventail d'appareils. Cela implique toutefois que le client

---

prof. Dr. N.A.N.M. van Eijk, m.m.v. 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] Voir notamment les programmes PRISM et XKeyscore.

de services cloud doit avoir la garantie que des mesures adéquates ont été prises afin d'empêcher un accès illicite aux données.

50. Dans les environnements de cloud, des moyens tels qu'un espace de stockage, de la mémoire et des réseaux sont partagés avec plusieurs clients. Cela crée de nouveaux risques relatifs à un accès et/ou un traitement illicites pour d'autres finalités que celles convenues entre le client de services cloud et le Cloud Service Provider.

51. Afin de faire face à ces risques, il faut créer une séparation suffisante entre les données et celles d'autres clients. Un bon isolement requiert notamment une gestion adéquate des droits d'accès et des rôles pour l'accès aux données à caractère personnel, qui doivent être réexaminés régulièrement. En outre, il faut éviter de créer des rôles disposant de droits considérables (aucun utilisateur ou administrateur ne pourrait par exemple avoir accès à l'ensemble du cloud). Lors de l'octroi des droits d'accès, il faut appliquer le principe du "least privilege" (de moindre privilège), selon lequel les utilisateurs et les administrateurs n'ont accès qu'aux informations nécessaires à leurs finalités légitimes.

5. Risques liés au recours à des sous-traitants par le Cloud Service Provider

52. Dans le cas de services de cloud computing, plusieurs parties intervenant en tant que sous-traitants peuvent être impliquées. Il est également habituel que des sous-traitants confient des activités à des sous-sous-traitants (appelés également sous-traitants de deuxième niveau ou sous-traitants ultérieurs) qui peuvent ainsi avoir accès à des données à caractère personnel. Si des sous-traitants confient des services à des sous-traitants ultérieurs, ils sont obligés de rendre cette information disponible à l'attention du responsable du traitement en fournissant des détails quant au type de service confié, aux caractéristiques des sous-contractants actuels et futurs et aux garanties que ces entités donnent en matière de respect de la législation vie privée.

53. Dans son avis 1/2010 *sur les notions de "responsable du traitement" et de "sous-traitant"*, le Groupe 29 a fait référence aux cas où il y a plusieurs sous-traitants et où ceux-ci entretiennent une relation directe avec le responsable du traitement des données ou sont des sous-contractants auxquels les sous-traitants ont délégué une partie des activités de traitement qui leur ont été confiées. Dans de tels scénarios, il est important que les obligations et responsabilités qui découlent de la législation en matière de traitement de données soient clairement définies et ne puissent pas être fragmentées à travers la chaîne de délégation ou de sous-traitance, au profit d'un contrôle effectif et de responsabilités claires en ce qui concerne les activités de sous-traitance. À cet égard, il importe de prévoir tous les moyens permettant d'établir à tout moment qui a fait quoi à un moment donné (journalisation).

6. Non-respect des règles de conservation

54. Les données à caractère personnel peuvent être conservées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles ont été collectées initialement ou pour lesquelles elles sont traitées ultérieurement. Les données à caractère personnel qui ne sont plus nécessaires doivent être détruites ou être tout à fait anonymisées. Une destruction sûre de données requiert que le support de stockage soit détruit ou démagnétisé ou que les données à caractère personnel enregistrées soient supprimées de manière efficace, par exemple en écrasant à plusieurs reprises les données au moyen de données aléatoires. Étant donné que dans des environnements de cloud, les données à caractère personnel sont généralement enregistrées de manière redondante sur différents serveurs à différents endroits, il faut s'assurer que chacune de ces instances de données soit supprimée de manière définitive.

7. Mauvaise gestion concernant les droits des personnes concernées

55. Un fournisseur de services cloud ne propose pas toujours les possibilités de gestion des données qui vont permettre au client de remplir ses obligations en matière de droit d’accès, de rectification, d'opposition et de suppression des personnes concernées. Une attention particulière du client doit dès lors porter sur ce point.

8. Indisponibilité du service fourni par le Cloud Service Provider.

56. Le responsable du traitement doit disposer de la garantie qu'il a accès à tout moment aux données et que les données ne peuvent pas se perdre. Au moment d'envisager une migration vers un service cloud, le responsable doit s'informer de tous les risques concernant la disponibilité du service, et ce tant vis-à-vis d'une éventuelle indisponibilité du service cloud proprement dit (comme une défaillance du matériel) que vis-à-vis des moyens d'accès au service. Ce dernier aspect concerne en particulier la perte fortuite de connectivité au réseau entre le client et le fournisseur ou la perte de performance du serveur en raison d'actions malveillantes comme des (Distributed) Denial of Service attacks (attaques par déni de service).

9. Cessation du service par le fournisseur ou reprise par un tiers

57. Le client risque d'être confronté à des difficultés pour revendiquer ses données en cas de faillite ou de reprise de son fournisseur de services cloud.

58. Face à ce risque, le Luxembourg a par exemple instauré légalement un droit de revendiquer ses données auprès d'un fournisseur de services en faillite par une modification de l'article 567 du Code de Commerce relatif aux faillites, banqueroutes et sursis[29].

59. Le responsable du traitement doit donc avoir la certitude que toutes les données concernées peuvent être récupérées en cas de cessation du service ou d'une autre forme de fin du contrat.

10. Non-conformité avec la réglementation, en particulier concernant les transferts internationaux

60. *"Le faible poids contractuel d'un petit responsable du traitement face à d'importants prestataires de services ne doit pas lui servir de justification pour accepter des clauses et conditions contractuelles contraires à la législation sur la protection des données"*[30].

61. C'est le client qui prend la décision de migrer tout ou partie de ses traitements dans le cloud. En tant que responsable du traitement, il porte la responsabilité de choisir un sous-traitant de qualité qui va lui permettre de respecter ses obligations en apportant des garanties suffisantes en matière de protection des données à caractère personnel.

62. Singulièrement, le responsable du traitement ne peut recourir aux services d'un sous-traitant qui n'offrirait pas de protection adéquate au sens des articles 21 et 22 de la LVP dès lors que des données à caractère personnel sont transférées vers des pays non membres de l'Union européenne.

11. Autres risques

63. Outre les risques susmentionnés, on peut notamment renvoyer à une liste plus étendue - mais non exhaustive - de 35 risques identifiés par ENISA[31]. Ces risques peuvent être pris en considération lors de l'analyse de risques du projet de migration (voir point V, ligne **Fout! Verwijzingsbron niet gevonden.**

---

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

[30] Avis du Groupe 29 n° 1/2010 du 16 février 2010 sur les notions de "responsable du traitement" et de "sous-traitant", http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_fr.pdf, p. 28, cité dans l'avis du Groupe 29 n° 05/2012 du 1er juillet 2012 sur l'informatique en nuage.

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

V. Lignes directrices

1. Identifier quelles données et quels traitements on envisage de migrer vers le cloud

64. Le client en sa qualité de responsable du traitement doit clairement identifier les traitements qu'il envisage de transférer dans le cloud.

65. Il doit prendre la décision de migrer ou non des données vers le cloud en fonction des types de données à caractère personnel concernées par ces traitements et de leur sensibilité notamment s'il s'agit de données visées aux articles 6 à 8 de la LVP.

66. À cet égard, la Commission recommande également toujours une migration progressive (plutôt qu'une migration complète) vers le cloud, en commençant par des données non sensibles et non confidentielles.

2. Définir les exigences techniques et juridiques propres

67. Bien que la Commission formule ci-après plusieurs exigences contractuelles organisationnelles et techniques minimales, la responsabilité finale incombe toujours au client de services cloud lui-même, en sa qualité de responsable du traitement. Il est donc libre d'exiger du Cloud Service Provider des normes plus strictes que les exigences contractuelles, organisationnelles et techniques énumérées ici.

a. Garanties contractuelles minimales

- *Sécurité juridique*

68. Il n'est pas rare que les conditions d'utilisation des services cloud permettent au prestataire de services cloud de modifier unilatéralement ces dernières. La Commission recommande de ne pas s'engager dans des contrats comprenant de telles clauses.

- *Confidentialité des données*

69. L'accès aux données par le fournisseur de services cloud doit être limité au strict nécessaire pour assurer la fourniture et la maintenance du service. Les employés du fournisseur de services cloud doivent à cet égard signer une clause de confidentialité avec leur employeur.

70. Le contrat doit prévoir que le fournisseur de cloud ne peut pas communiquer les données à des tiers sauf s'il prévoit le recours à des sous-traitants ultérieurs.

- *Sous-traitance ultérieure*

71. La sous-traitance ultérieure ne peut être autorisée que si le responsable du traitement a donné son accord écrit préalable (cf. point IV, risque n° 5).

72. Le client doit veiller à ce que les obligations du fournisseur à son égard soient reportées sur les sous-traitants. La responsabilité du fournisseur doit rester entière à son égard quand celui-ci recourt à la sous-traitance.

73. Le client doit être informé de l'identité et des pays d'établissement des sous-traitants. Le recours à tout nouveau sous-traitant établi hors de l'Union européenne par le fournisseur doit être notifiée au client qui doit pouvoir s'y opposer.

- *Droits des personnes concernées*

74. Le client de services cloud doit veiller à ce que les conditions du traitement dans le cloud ne présentent pas d'obstacles notamment au niveau technique ou organisationnel, afin de pouvoir remplir ses obligations à cet égard (cf. point IV, risque n° 7).

- *Localisation des données*

75. Dans le contrat avec le Cloud Service Provider, le responsable du traitement doit veiller à disposer à l'avance d'une liste complète des lieux physiques où des données peuvent être enregistrées ou traitées par le Cloud Service Provider et/ou un de ses sous-traitants (y compris back-up) pendant la durée du contrat.

76. Dans le cadre du contrat avec le Cloud Service Provider, le responsable du traitement doit s'assurer que ni le Cloud Service Provider, ni un de ses sous-traitants ne transfèrent des données vers des lieux physiques différents de ceux indiqués dans le contrat.

77. Le responsable du traitement doit disposer de la possibilité de réclamer auprès du Cloud Service Provider des "location audit trails" (pistes de vérification du lieu). Les "location audit trails" doivent être automatiquement enregistrés et indiquer le lieu physique et le moment où des données à caractère personnel ont été enregistrées et traitées.

- *Transferts hors de l'Union européenne*

78. Le client doit s'assurer de la protection adéquate des données à caractère personnel si celles-ci sont transférées en dehors de l'Union européenne, notamment par la mise en œuvre de règles d'entreprises contraignantes par les sous-traitants ou par la signature de clauses contractuelles types[32] (cf. point IV ci-dessous, risque n° 10).

79. Dès lors que les sous-traitants ultérieurs du fournisseur de services cloud doivent être tenus aux mêmes obligations que ce dernier, les transferts internationaux entre le fournisseur et ses sous-traitants ultérieurs doivent être encadrés par des instruments tels que des clauses contractuelles types.

- *Audit et certification*

80. Le contrat doit prévoir un mécanisme d'audit des obligations du fournisseur dans la fourniture des services cloud. Celui-ci pourra être opéré par un prestataire tiers indépendant.

81. Le client pourra également s'assurer que les services du fournisseur bénéficient d'une certification.

- *Fuite de données*

82. En cas de problèmes susceptibles d'affecter les données, une obligation de notification au client dans le chef du fournisseur de services cloud doit être prévue (cf. point IV, risque n° 1).

- *Accès des autorités*

83. Le fournisseur doit en principe avertir son client en cas d'accès aux données traitées dans le cloud par les autorités (cf. point IV, risque n° 2).

84. En aucun cas, les transferts d'un sous-traitant vers une autorité publique ne peuvent être massifs, disproportionnés et sans distinction d'une manière excédant ce qui est nécessaire dans une société démocratique[33].

---

[32] Voir à cet égard https://www.privacycommission.be/fr/en-dehors-de-ue-sans-protection-adequate.

[33] Voir l' 'Explanatory Document on the Processor Binding Corporate Rules' du Groupe 29 adopté le 19 avril 2013 et révisé le 22 mai 2015, p.13, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp232_fr.pdf., et référencé dans son avis 02/2015 du 22 septembre 2015 'on C-SIG Code of Conduct on Cloud Computing', p. 8 : http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp232_fr.pdf..

b. Exigences techniques

85. L'article 16, § 4 de la LVP oblige le responsable du traitement à garantir la sécurité des données à caractère personnel en prenant "*les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification, l'accès et tout autre traitement non autorisé de données à caractère personnel*".

86. Si le responsable du traitement envisage une migration vers le cloud pour le traitement de données à caractère personnel, il doit vérifier si le sous-traitant offre des garanties techniques, organisationnelles et juridiques suffisantes et les évaluer dans une analyse de risques. Pour accompagner cette démarche, la Commission renvoie notamment à ses mesures de référence et à ses lignes directrices en matière de sécurité de l'information[34].

87. Outre les exigences cruciales de sécurité en matière de qualité des services, de disponibilité, de confidentialité et d'intégrité, la Commission souhaite également attirer l'attention sur des garanties supplémentaires relatives à la protection des données comme la transparence, l'isolement des données, la responsabilité en cas d'incidents, la réversibilité, la portabilité et l'effacement des données. Concernant ces points, le client de services cloud doit avoir suffisamment de garanties de la part du Cloud Service Provider.

- *Qualité des services*

88. La qualité des services fournis est susceptible d'avoir des répercussions sur les traitements de données à caractère personnel et sur les données traitées. Le contrat doit prévoir cet ensemble de niveaux de services (service level agreement) à fournir par le fournisseur de services cloud à son client et les sanctions en cas de non-conformité (cf. point IV, risque n° 8).

- *Disponibilité*

89. Le Cloud Service Provider doit, outre des circonstances imprévues du côté du client de services cloud (comme des problèmes de connexion), offrir suffisamment de garanties que les données sont toujours disponibles (cf. le point 8 de la liste des risques liés au cloud).

[34] Les mesures de référence ainsi que les lignes directrices peuvent être consultées via https://www.privacycommission.be/fr/securite-information.

- *Confidentialité*

90. Dans un environnement de cloud, le cryptage peut jouer un rôle très important dans le cadre de la confidentialité des données à caractère personnel. Le protocole de cryptage utilisé doit au moins répondre à des normes industrielles agréées. La Commission souhaite attirer l'attention sur le fait que le cryptage doit en tout cas être utilisé lors du transfert de données (donc également lors du transfert entre les différents centres de données du Cloud Service Provider) et, si possible, lors du stockage dans le cloud. Dans le cas d'un environnement SaaS, il faut être clairement conscient du fait que le cryptage lors du stockage est généralement plus difficile à réaliser en raison des traitements nécessaires (sauf cas exceptionnels). Il s'agit d'une considération essentielle, notamment pour le traitement de données sensibles. Dans d'autres environnements de cloud, comme un environnement IaaS, le responsable du traitement peut bien plus facilement veiller à ce que les données soient stockées de manière cryptée et sécurisée. En tout cas, lors de l'utilisation d'un cryptage, il doit y avoir des garanties claires d'une gestion de clés appropriée, étant donné que la sécurité des données dépend au final de la confidentialité des clés de cryptage. Des mesures techniques complémentaires visant à garantir la confidentialité des données à caractère personnel dans le cloud consistent à intégrer des mécanismes d'autorisation et des mécanismes d'authentification forte (comme une authentification à deux facteurs).

- *Intégrité*

91. L'intégrité des données peut être définie comme étant la caractéristique que les données sont authentiques et n'ont donc pas été modifiées de manière malveillante ou fortuite lors du traitement, du stockage ou du transfert. L'intégrité des données peut être garantie au moyen de mécanismes d'authentification cryptographiques comme les signatures numériques ou les 'message authentication codes' (MAC) (codes d'authentification de message). Des perturbations liées à l'intégrité de systèmes IR dans le cloud peuvent être empêchées ou détectées grâce à ce qu'on appelle des "intrusion detection / prevention systems" (IPS/IDS) (systèmes de prévention/détection d'intrusion).

- *Transparence*

92. Les mesures techniques et organisationnelles que le Cloud Service Provider a mises en oeuvre doivent rester disponibles de manière transparente pour une inspection. Les Cloud Service Providers doivent proposer à leurs clients un mécanisme permettant d'inspecter les mesures techniques et organisationnelles pour lesquelles des audits individuels par le client ne sont techniquement pas possibles et/ou impliquent des risques supplémentaires.

- *Isolement des données*

93. Dans les environnements de cloud, des moyens comme un espace de stockage, de la mémoire et des réseaux, sont partagés entre plusieurs clients, rendant nécessaire un isolement correct des données afin d'éviter des risques tels qu'un accès illicite et un traitement ultérieur pour des finalités non légitimes (cf. le point 4 dans la liste des risques liés au cloud).

- *Responsabilité en cas d'incidents*

94. Dans le cas d'environnements de cloud, le Cloud Service Provider et d'éventuels sous-traitants peuvent chacun porter une certaine responsabilité opérationnelle. À cet égard, il importe de prévoir tous les moyens pour retrouver quelle entité a fait quoi à quel moment précis (journalisation). C'est particulièrement important dans le cas d'une fuite de données ("data breach").

- *Réversibilité des données*

95. Le client doit être en position de pouvoir récupérer ses données et réintégrer son activité à la fin du contrat. À cet égard, le contrat de cloud doit prévoir que ce dernier pourra obtenir une copie de l'intégralité de ses données dans un format structuré et couramment utilisé (cf. le point 9 de la liste des risques liés au cloud).

- *Portabilité des données*

96. Les Cloud Service Providers doivent si possible utiliser des formats de données standard et des interfaces système qui favorisent l'interopérabilité et la portabilité des données afin d'éviter que des données ne soient pas ou difficilement transférables à un autre Cloud Service Provider (cf. point IV, risque n° 3).

- *Effacement des données*

97. Quand le client a récupéré ses données à la fin du contrat, toutes traces des données traitées précédemment dans le cloud doivent être détruites par le prestataire de services cloud (cf. point IV, risque n° 7). Le client est en droit d'exiger un effacement sécurisé de ses données afin de les rendre irrécupérables.

3. Identifier le type de solution de cloud approprié

98. La Commission souhaite attirer l'attention avec insistance sur le fait qu'un responsable du traitement qui veut migrer des données dans le cloud ne doit pas choisir le même modèle de service ou de déploiement pour toutes les données. Un modèle de service déterminé peut être appliqué par-dessus un autre modèle de service. Le Cloud Service Provider qui propose un composant déterminé du service, comme le logiciel, ne doit pas nécessairement être le même fournisseur que celui qui propose un autre composant, comme l'infrastructure du cloud.

99. Il convient de signaler que l'utilisation de services par couche, comme cela est décrit au point susmentionné, peut aboutir à une chaîne plus complexe de Cloud Service Providers. Le client de services cloud doit être conscient que cela engendre des risques supplémentaires.

100. Il existe un large éventail de services cloud permettant d'atteindre des finalités très diverses. Au moment de choisir, il importe également de tenir compte du niveau de maturité du service proposé.

4. Mener une analyse de risques

101. Idéalement, elle sera opérée par un organe indépendant spécialisé dans la sécurité de l'information pour garantir son objectivité.

102. À côté du cadre juridique relatif à la sécurité mentionné au point III.5., la Commission souhaite faire référence, à titre d'exemple, à un modèle d'évaluation de sécurité des services cloud[35] recommandé entre autres par la section Santé du Comité sectoriel de la Sécurité sociale et de la Santé[36] et référencé par la Commission dans son avis n° 04/2015 du 25 février 2015[37] et son avis n° 09/2016 du 24 février 2016[38]. Il s'agit d'une méthode pratique et quantitative visant à évaluer la sécurité des services cloud par rapport aux besoins du client.

---

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

[36] Voir la recommandation n° 15/01 du 20 janvier 2015 *relative à un projet de circulaire du SPF Santé publique portant sur l'utilisation de services "cloud" dans les hôpitaux.*

[37] Avis *relatif à un projet de circulaire portant sur l'utilisation du "cloud" par les hôpitaux*, http://www.privacycommission.be/sites/privacycommission/files/documents/avis_15_2015.pdf.

[38] Avis concernant le choix d'une stratégie HR SaaS dans le cadre des processus de gestion des talents de l'Autorité flamande, https://www.privacycommission.be/sites/privacycommission/files/documents/avis_09_2016.pdf.

5. Choisir un Cloud Service Provider (CSP) approprié

a. Principes

103. Sur la base de l'analyse de risques, le client est responsable du choix d'un fournisseur de services cloud qui fournit des garanties sur le plan juridique et technique lui permettant de respecter la LVP.

104. Il doit veiller à disposer de toute la transparence de la part du fournisseur de services cloud et partant, de toutes les informations nécessaires pour évaluer les avantages et inconvénients d'un service cloud.

105. Afin que les personnes concernées puissent exercer leurs droits, la Commission recommande que le client informe toutes les personnes concernées de manière transparente quant à la migration vers le cloud après avoir choisi un Cloud Service Provider approprié.

b. Certification

106. Une certification d'un Cloud Service Provider par un tiers indépendant peut offrir un moyen fiable aux Cloud Service Providers de prouver le respect de leurs obligations et de gagner la confiance de clients de services cloud. Une certification indique au moins que les mesures en matière de sécurité de l'information ont été soumises à un audit indépendant à l'égard d'un certain nombre d'obligations. D'éventuelles certifications pertinentes sont notamment celles réalisées sur la base des normes ISO/IEC 27001[39] et ISO/IEC 27018[40].

107. Toutefois, comme cela est également exposé dans l'avis du Groupe 29 *sur l'informatique en nuage*[41]*, les potentiels clients de services cloud doivent contrôler si les Cloud Service Providers peuvent fournir une copie du rapport d'audit en question afin de pouvoir vérifier la certification relative aux obligations des Cloud Service Providers et aux exigences du client de services cloud.*

108. En 2014, l'ISO a émis une norme spécifique pour les Cloud Service Providers en vue de protéger les données à caractère personnel dans les clouds publics. Il s'agit ici de la norme "ISO/IEC 27018:2014 – Code of Practice for protection of personally identifiable information (PII)

---

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

[40] Voir http://www.iso.org/iso/fr/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=61498.

[41] Avis n° 05/2012 du 1er juillet 2012 : http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_fr.pdf.

in public clouds acting as PII processors" (ISO/IEC 27018:2014 Technologies de l'information -- Techniques de sécurité -- Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII). Cette norme internationale poursuit les finalités suivantes :

- aider les Cloud Service Providers à respecter leurs obligations en tant que sous-traitants de données à caractère personnel ;
- aider les Cloud Service Providers publics à être transparents quant aux aspects pertinents afin que les clients de services cloud puissent choisir des services basés sur le cloud qui soient bien gérés ;
- soutenir le client de services cloud et le Cloud Service Provider afin de parvenir à un accord contractuel ;
- proposer aux clients de services cloud un mécanisme pour exécuter des audits dans les cas où des audits individuels par le client seraient techniquement difficiles et/ou comporteraient des risques.

109. La norme constitue un complément aux mesures telles que définies dans la norme ISO/IEC 27002 afin de tenir compte de la nature répartie des risques et de l'existence de la relation contractuelle entre le client de services cloud et le Cloud Service Provider.

110. Les Cloud Service Providers peuvent être certifiés pour cette norme ISO. Une telle certification peut donc offrir des garanties spécifiques complémentaires en plus d'une éventuelle certification en vertu de la norme ISO/IEC 27001.

111. A l'instar du Groupe 29[42], la Commission souligne que la norme ISO/IEC 27018 est un catalogue de bonnes pratiques pour les fournisseurs de services cloud agissant en qualité de sous-traitants. Elle décrit une liste de contrôle pour améliorer la protection de la vie privée. Ce standard est seulement un bon ensemble de contrôles non obligatoires, non exhaustifs et non maximalistes qui peuvent être mis en œuvre. Donc la norme ISO/IEC 27018 n'est pas conçue pour être utilisée comme un document autonome pour une certification. Elle peut être utilisée en combinaison avec la norme ISO/IEC 27001 qui permet une certification. La norme ISO/IEC 27001 ne prend pas en compte les spécificités de la protection de la vie privée tels que les incidences sur les individus, mais elle assure un niveau élevé de protection de l'information dans l'intérêt de l'organisation. L'addition des bonnes pratiques basées sur la norme ISO/IEC 27018 peut dès lors aider à assurer que la protection de la vie privée soit mieux prise en compte mais cela ne prouve pas que les risques liés à la vie privée sont pris en compte. La norme ISO/IEC 27018 devrait idéalement être utilisée après avoir évalué les risques d'atteinte à la vie privée des personnes concernées, de

[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.

manière à les traiter d'une manière proportionnée. A l'heure actuelle, aucun standard publié ne décrit le manière de mener ce processus. Les travaux en cours au niveau de l'ISO pourront aider à combler cette lacune dans les prochaines années

112. La Commission souhaite également formuler une remarque importante sur cette norme, à savoir concernant les demandes d'accès par des autorités étrangères. À cet égard, la norme dispose ce qui suit :

"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."
(soulignement propre).

113. Étant donné que certaines législations étrangères disposent généralement que de telles demandes d'accès ne peuvent pas être admises en raison d'obligations de secret (comme par exemple celles définies dans la législation FISAA), cette disposition n'offre pas suffisamment de garanties en matière de transparence dans le domaine des demandes d'accès illégitimes par des autorités étrangères. C'est spécialement en cas de données sensibles que le client de services cloud doit tenir compte de cet aspect dans son évaluation des risques.

6. Assurer le suivi des modifications à travers le temps

114. Les modèles de services cloud changent à travers le temps. À la lumière de cet élément, il importe de répéter périodiquement les analyses de risques réalisées, en tenant compte de nouveaux risques éventuels, de l'offre sur le marché et d'autres aspects pertinents.

115. La Commission recommande en tout cas de procéder à nouveau à l'analyse de risques réalisée lors de modifications significatives concernant le service cloud choisi. Des modifications pertinentes peuvent par exemple concerner de nouveaux centres de données, la politique de sécurité, les traitements par le client de services cloud, etc.

L'Administrateur f.f., Le Président,

(sé) An Machtens (sé) Willem Debeuckelaere