

*Avez-vous des questions ou souhaitez-vous des informations supplémentaires?*

*Envoyez un courriel au frontdesk à l’adresse suivante**question@mi-is.be*

*Ou prenez contact avec nous au****02 508 85 86***

|  |  |
| --- | --- |
| SPP Intégration Sociale, Lutte contre la Pauvreté, Economie Sociale et Politique des Grandes VillesBld Roi Albert II – 30 – 1000 Bruxelles – <http://www.mi-is.be>tel +32 2 508 85 86– fax +32 2 508 85 10– question@mi-is.be  | logos |

-

|  |
| --- |
|  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Service | Votre lettre du | Vos références | Non références | date | Annexe(s) |
|  |  |  |  |  |  |

**Réponse à la question posée par les CPAS concernant la conservation des données dans le cloud.**

En ce qui concerne les dispositions légales en vigueur en matière de données personnelles, l'article 16 §4 de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (également appelée 'loi vie privée') prévoit que le responsable du traitement ainsi que le sous-traitant doivent prendre les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel[[1]](#footnote-1). Voir également l'article 17 de la directive européenne 95/46/CE sur la vie privée[[2]](#footnote-2).

Dans un souci de fournir des directives en matière de sécurité relative à des services de cloud aux institutions de sécurité sociale traitant des données confidentielles, le SPF Sécurité Sociale a élaboré en concertation avec le 'Groupe de travail Sécurité de l'information' organisé au sein de la BCSS ainsi qu’avec FEDICT une « Politique de sécurité relative à des services de Cloud Computing » [[3]](#footnote-3).

Les fournisseurs de services en cloud (nuage) font des efforts au niveau de la sécurisation des connexions ainsi que du cryptage des données (pas toujours standard ou sans frais supplémentaire) pour les données confidentielles. Il n'est toutefois pas certain que les solutions proposées offrent une protection adaptée. Qui a la clé ? Quelles sont les garanties pour pouvoir décrypter après une longue période ? Est-ce simple et facile d'utilisation (sans quoi ce ne sera de toute façon pas appliqué) ? ...

Il est positif que les fournisseurs de services en nuage commencent à utiliser la sécurité de l'information comme un argument de vente. En ce moment, plusieurs gros fournisseurs de services en nuage utilisent l’argument de la sécurité mais il est difficile de dire lequel offre des garanties satisfaisantes.

Les entreprises commerciales penseraient également proposer des services ou des produits visant la création d'un nuage privé (ou hybride), qui permet au responsable du traitement de rester propriétaire de l'infrastructure et donc aussi des données.

Les choses bougent donc un peu chez les fournisseurs commerciaux mais aussi du côté des autorités. Quelques autorités belges[[4]](#footnote-4) préparent la mise en place de cloud (FEDICT, LNE) ou projettent de le faire (SPF Finances).

Dans le même ordre d'idée, citons le « Good Practice guide for securely deploying Governmental Clouds »[[5]](#footnote-5) de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), qui regorge de recommandations en matière de protection de la vie privée et de sécurité de l'information.

Conclusion : bien que la protection et la confidentialité progressent mais considérant que Microsoft et les autres sociétés américaines ne peuvent actuellement pas s’opposer aux demandes de leur gouvernement d’obtenir accès aux données stockées dans leurs clouds, il est fortement déconseillé dans l’état actuel des choses de faire appel à leurs services de cloud. »

Pour information, les principaux problèmes liés au nuage public sont :

• l’utilisation des données pour créer des profils d'utilisateurs qui sont ensuite exploités à des fins de marketing propres (cf. événement récent avec une banque néerlandaise et une « belge »[[6]](#footnote-6)) transmis à des « entreprises liées » ou vendus[[7]](#footnote-7) ;

• le piratage et l’utilisation de portes d’accès cachées (back doors) ;

• avec la plupart des solutions, perte totale de la maitrise des données par le responsable du traitement (gestion des accès, protection contre les pertes de données gérées, migrations de données vers un autre système souvent non prévu, reprise des données si le fournisseur cesse son activité) et manque de visibilité sur les responsabilités légales encadrant la conservation et la protection de ces données ;

• une mise en œuvre complexe des contrats et garanties, même si des SLA sont possible, car le préjudice est difficile à chiffrer ;

* • le transfert des coûts des comptes d’investissements vers les comptes d’exploitation qui rend un financement par emprunt compliqué voire impossible ;les activités d'espionnage de la NSA (en vertu ou non de la législation américaine citée ci-après) via des firmes proposant des services en nuage ;

• les points d'attention dans les contrats « nuage » et, en général, dans les contrats d'externalisation, voir notamment la publication de l'ENISA[[8]](#footnote-8) et les directives déjà nombreuses publiées par des avocats et consultants ;

• un juge - même européen - peut demander des données au fournisseur de services en nuage sans que le propriétaire des données n'en soit averti (malgré les dispositions contractuelles ou une éventuelle réserve explicite)[[9]](#footnote-9)

• les fournisseurs américains de services en nuage : analyse à grande échelle des nuages comportant des données de citoyens européens conservées par des entreprises américaines ou ayant un lien avec l'Amérique. L'emplacement de stockage n'est pas déterminant ! La législation américaine, plus particulièrement le Patriot Act et le FISA Amendments Act, l'autorisent, il ne doit même pas être question de terrorisme ni de grande criminalité[[10]](#footnote-10).

1. Art. 16, § 4. Afin de garantir la sécurité des données à caractère personnel, le responsable du traitement et, le cas échéant, son représentant en Belgique, ainsi que le sous-traitant doivent prendre 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.

<http://www.privacycommission.be/fr/node/3790> [↑](#footnote-ref-1)
2. Art. 17, 2. Les États membres prévoient que le responsable du traitement, lorsque le traitement est effectué pour son compte, doit choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements à effectuer et qu'il doit veiller au respect de ces mesures.

http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:31995L0046 [↑](#footnote-ref-2)
3. <https://www.bcss.fgov.be/binaries/documentation/fr/securite/policies/isms_050_cloud_computing_policy_fr.pdf> [↑](#footnote-ref-3)
4. Voir le rapport d’activités 2013 de la Smals : p. 19 concernant le Community Cloud et p. 52 concernant l’Infrastructure Cloud : <https://www.smals.be/sites/default/files/assets/rapportsmalsfrweb11-06-2014.pdf>.

 Voir sur le site de Datanews, l’actualité du 03/04/2014 concernant le projet « Government Cloud » ou « G-Cloud » de Fedict : <http://datanews.levif.be/ict/actualite/le-nuage-public-sera-en-fin-de-compte-developpe-en-interne/article-4000580731852.htm>. [↑](#footnote-ref-4)
5. <http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds> [↑](#footnote-ref-5)
6. <http://www.lecho.be/actualite/entreprises_finance/Qui_achete_quoi_ING_va_devoiler_les_donnees_clients.9476021-3028.art?ckc=1> [↑](#footnote-ref-6)
7. <http://www.lemonde.fr/technologies/article/2014/03/19/google-critique-pour-avoir-scanne-les-mails-de-millions-d-etudiants_4385358_651865.html> [↑](#footnote-ref-7)
8. <http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment> [↑](#footnote-ref-8)
9. Pour le cas d’un juge américain : <http://www.reuters.com/article/2014/04/25/us-usa-tech-warrants-idUSBREA3O24P20140425> [↑](#footnote-ref-9)
10. <http://business.lesechos.fr/directions-numeriques/0203680050698-le-cloud-europeen-de-microsoft-reste-sous-loi-americaine-102117.php>

<http://www.01net.com/editorial/584637/comment-les-etats-unis-legitiment-la-cybersurveillance-mondiale/> [↑](#footnote-ref-10)