

*Heeft u vragen? Nood aan bijkomende info?*

*Mail naar onze frontdesk via* [***vraag@mi-is.be***](mailto:vraag@mi-is.be)

*Of bel naar* ***02 508 85 85***

|  |  |
| --- | --- |
| POD Maatschappelijke Integratie, Armoedebestrijding, Sociale Economie en Grootstedenbeleid  Koning Albert II – laan 30 - B1000 Brussel – <http://www.mi-is.be> tel +32 2 508 85 85 – fax +32 2 508 85 10 – vraag@mi-is.be | logos |

-

|  |
| --- |
|  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Dienst | uw brief van | uw kenmerk | Ons kenmerk | datum | Bjlage(n) |
|  |  |  |  |  |  |

**Antwoord op de vraag van de OCMW's in verband met het bewaren van de gegevens in de cloud.**

Wat de wettelijke bepalingen betreft die van kracht zijn in verband met persoonsgegevens voorziet artikel 16 §4 van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte va, de verwerking van persoonsgegevens (eveneens "wet op het privéleven" genoemd) erin dat de verantwoordelijke van de behandeling en de onderaannemer de vereiste technische en organisatorische maatregelen moeten nemen om de persoonsgegevens te beschermen[[1]](#footnote-1). Zie eveneens artikel 17 van de Europese richtlijn 95/46/CE over het privéleven[[2]](#footnote-2).

Om veiligheidsrichtlijnen te bezorgen in verband met de cloud services aan de socialezekerheidsinstellingen die vertrouwelijke gegevens behandelen, heeft de FOD Sociale Zekerheid, in overleg met de "werkgroep Informatieveiligheid" die georganiseerd wordt binnen de KSZ en met FEDICT een "Veiligheidsbeleid in verband met de diensten voor Cloud Computing" opgesteld[[3]](#footnote-3).

De leveranciers van "cloud services" doen inspanningen op het vlak van beveiliging van de verbindingen en van de versleuteling van de gegevens (niet steeds standaard of zonder extra kosten) voor de vertrouwelijke gegevens. Het is echter niet zeker dat de voorgestelde oplossingen een aangepaste bescherming bieden. Wie heeft de sleutel? Wat zijn de waarborgen om te kunnen versleutelen na een lange periode? Is het eenvoudig en makkelijk in gebruik (anders zal het in geen geval worden toegepast)? ...

Het is positief dat de leveranciers van de cloud services de informatieveiligheid beginnen te gebruiken als een verkoopargument. Momenteel gebruiken verschillende grote leveranciers van cloud services het argument van de veiligheid, maar het is moeilijk te zeggen welk argument bevredigende waarborgen biedt.

De commerciële ondernemingen denken er eveneens aan om diensten of producten voor te stellen die de aanmaak tot doel hebben van een privé (of hybride) cloud, waardoor de verantwoordelijke van de behandeling eigenaar blijft van de infrastructuur en dus ook van de gegevens.

Er beweegt dus wat bij de commerciële leveranciers, maar ook bij de overheden. Enkele Belgische overheden[[4]](#footnote-4) bereiden de invoering van de cloud voor (FEDICT, LNE) of zijn dit van plan (FOD Financiën).

In verband hiermee halen we de "Good Practice guide for securely deploying Governmental Clouds"[[5]](#footnote-5) aan van het Europees Agentschap voor Netwerk en Informatieveiligheid (ENISA), dat aanbevelingen doet inzake bescherming van het privéleven en van de informatieveiligheid.

Besluit: hoewel de bescherming en de vertrouwelijkheid erop vooruitgaan, maar overwegende dat Microsoft en de andere Amerikaans ondernemingen zich momenteel niet kunnen verzetten tegen de aanvragen van hun regering om toegang te hebben tot de gegevens die in hun clouds zijn opgeslagen, is het sterk af te raden om in de huidige toestand een beroep te doen op hun cloud services. "

Ter informatie: de belangrijkste problemen in verband met de openbare cloud zijn:

• het gebruik van de gegevens om gebruikersprofielen aan te maken die vervolgens gebruikt worden voor eigen marketingdoeleinden (cf. recente gebeurtenis met een Nederlandse bank en een "Belg"[[6]](#footnote-6)) die aan "verbonden ondernemingen" bezorgd worden of worden verkocht[[7]](#footnote-7);

• piraterij en het gebruik van verborgen toegangspoorten (back doors);

• met de meeste oplossingen, totaalverlies van de gegevensmatrix door de verantwoordelijke van de behandeling (toegangsbeheer, bescherming tegen de verliezen van beheerde gegevens, migraties van gegevens naar een vaak niet voorzien systeem, overname van gegevens wanneer de leverancier zijn activiteit stopzet) en gebrek aan zichtbaarheid over de wettelijke verantwoordelijkheden die de opslag en de bescherming van deze gegevens omkaderen;

• een complexe uitvoering van de contracten en garanties, hoewel de SLA beschikbaar zijn, aangezien de schade moeilijk te becijferen is;

* de overdracht van de kosten van de investeringsrekeningen naar de exploitatierekeningen hetgeen een financiering per lening moeilijk, zelfs onmogelijk maakt; de spionageactiviteiten van NSA (al dan niet krachtens de hieronder vermelde Amerikaanse wetgeving) via firma's die cloud services aanbieden;

• de aandachtspunten in de "cloudcontracten" en, over het algemeen in de contracten voor outsourcing, zie meer bepaald de publicatie van ENISA[[8]](#footnote-8) en de richtlijnen die reeds talrijk werden gepubliceerd door advocaten en consultants;

• een rechter - zelfs een Europese - kan gegevens vragen aan de leverancier van cloud services zonder dat de eigenaar van de gegevens hierover wordt ingelicht (ondanks de contractuele bepalingen of een eventueel uitdrukkelijk voorbehoud)[[9]](#footnote-9)

• de Amerikaanse leveranciers van cloud services: grootschalige analyse van de clouds die gegevens bevatten van Europese burgers die worden bewaard door Amerikaanse ondernemingen of die verband houden met Amerika. De opslagplaats is niet bepalend! De Amerikaanse wetgeving, meer bepaald de "Patriot Act" en de "FISA Amendments Act", staan dit toe, er moet zelfs geen sprake zijn van terrorisme of grote criminaliteit[[10]](#footnote-10).

1. Art. 16, 4. Om de veiligheid te bepalen van de persoonsgegevens moeten de verantwoordelijke van de behandeling en, in dit geval, de vertegenwoordiger ervan in België de passende technische en organisatorische maatregelen ten uitvoer leggen om persoonsgegevens te beveiligen tegen vernietiging, hetzij per ongeluk, hetzij onrechtmatig, tegen verlies, vervalsing, niet-toegelaten verspreiding of toegang, met name wanneer de verwerking doorzending van gegevens in een netwerk omvat, dan wel tegen enige andere vorm van onwettige verwerking.

   <http://www.privacycommission.be/fr/node/3790> [↑](#footnote-ref-1)
2. Art. 17, 2. De Lidstaten bepalen dat de voor de verwerking verantwoordelijke, in geval van verwerking te zijnen behoeve, een verwerker moet kiezen die voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerking en moet toezien op de naleving van die maatregelen.

   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](file:///C:\Users\kempgens_gilles\AppData\Local\Microsoft\Windows\Temporary%20Internet%20Files\Content.Outlook\GSSC63UH\*https:\www.bcss.fgov.be\binaries\documentation\fr\securite\policies\isms_050_cloud_computing_policy_fr.pdf) [↑](#footnote-ref-3)
4. Zie het activiteitenverslag 2013 van Smals: p. 19 over de Community Cloud en p. 52 over de Cloud Infrastructuur: <https://www.smals.be/sites/default/files/assets/rapportsmalsfrweb11-06-2014.pdf>.

   Kijk op de site van Datanews, de actualiteit van 03/04/2014 in verband met het project "Government Cloud" of "G-Cloud" van 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. Voor het geval van een Amerikaanse rechter: <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)