Avis n° 09/2016 du 24 février 2016

Objet : avis concernant le choix d'une stratégie HR SaaS dans le cadre des processus de gestion des talents de l'Autorité flamande (CO-A-2016-006)

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 la concertation informelle des 25/11/2015 et 22/01/2016 entre des représentants de l'Autorité flamande - Vlaams Agentschap Overheidspersoneel (Agence flamande de la Fonction publique) (ci-après "la VAO") et le Secrétariat de la Commission ;

Vu la décision de la Commission du 3 février 2016 de formuler un avis en la matière ;

Vu le rapport de Monsieur Frank De Smet ;

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

I. OBJET DE LA DEMANDE

1. Le groupe de pilotage stratégique de l'Autorité flamande envisage une stratégie de cloud pour les données HR "douces" du personnel de l'Autorité flamande, plus particulièrement le transfert de ces données à caractère personnel vers un fournisseur de cloud (public) d'origine américaine possédant un centre de données (data center) sur le territoire européen.

2. D'après ce groupe de pilotage, une solution SaaS serait la plus appropriée pour le soutien des processus de gestion des talents HR au sein de l'Autorité flamande.

3. Les données HR "douces" recouvrent donc, outre une signalétique de base concernant chaque membre du personnel flamand, des données telles que le CV, le profil de fonction, la formation, le profil de compétences ainsi que des informations sur le recrutement, la sélection et l'évaluation.

4. La VAO a été chargée d'une étude préparatoire et, sur la base d'un rapport de consultance américain, elle a retenu 4 fournisseurs de service possibles pouvant offrir la solution de cloud souhaitée. Il s'agit à chaque fois de fournisseurs de services américains, mais les données resteraient par contre stockées dans des centres de données européens. Les trois premières solutions sont proposées par trois fournisseurs autonomes (stand-alone) (P1, P2 et P3), combinant le cryptage du transport et le cryptage de la base de données et où les clés de cryptage sont conservées chez les fournisseurs. La quatrième solution consiste en une combinaison du premier fournisseur et d'un "encryption gateway" (P1 + Pe), où la clé de cryptage se trouve chez le client.

5. À la demande de la VAO, une concertation informelle a eu lieu le 25/11/2015 et le 22/01/2016 entre des représentants de la VAO et du Secrétariat de la Commission, et la position du Secrétariat a été communiquée à la VAO par courrier du 10/02/2016, annonçant également la promulgation du présent avis officiel par la Commission.

II. EXAMEN DE LA DEMANDE

6. La Commission prend acte des résultats de l'analyse technique approfondie des 4 solutions de fournisseurs possibles que la VAO a effectuée à l'aide du "modèle SMALS"[1], un modèle de référence dans le domaine des critères relatifs à la sécurité des données.

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

7. La Commission constate à cet égard que les exigences propres concernant la solution souhaitée par la VAO - définies par auto-évaluation - se situent globalement dans la zone verte ("cloud service does satisfy") pour l'ensemble des 4 composants du modèle ainsi que pour l'ensemble des solutions analysées.

8. Néanmoins, d'après ce modèle, les solutions analysées présentent plusieurs lacunes majeures, donc des éléments ne répondant pas à la politique en matière de cloud de la sécurité sociale belge. Les lacunes majeures qui subsistent dans les quatre éléments du modèle sont les suivantes :

Au niveau de la governance

9. Tous les fournisseurs de cloud stand-alone P1, P2, P3 envisagés ont un lien avec des autorités, en l'occurrence les autorités américaines, qui peuvent éventuellement réclamer les données à l'insu du client (la VAO) du fournisseur, sans parler des personnes concernées. Dans les solutions proposées, le fournisseur SaaS dispose en effet toujours lui-même de la clé de cryptage.

10. Ce n'est que dans le modèle P1 + Pe (un partenariat entre le fournisseur de cloud P1 et un fournisseur d'un "encryption gateway" Pe) que les autorités américaines ne pourraient recevoir que des données à caractère personnel cryptées, vu que la clé de décryptage des données se trouverait au niveau de la VAO et que les données que le fournisseur pourrait livrer seraient donc en principe illisibles pour les autorités américaines. La Commission remarque toutefois que ce modèle a pour conséquence qu'au niveau du fournisseur de cloud, aucun traitement ne peut avoir lieu (y compris donc les traitements éventuellement souhaités) en dehors de la simple conservation et de la simple sauvegarde des données.

11. En cas de recours à d'éventuels sous-traitants, les fournisseurs (excepté P2) n'informeront pas le client de manière proactive, uniquement de manière réactive (à la demande).

Au niveau de la sécurité IT

12. Les données sont certes cryptées au niveau des fournisseurs, mais ils possèdent eux-mêmes la clé de cryptage et en définissent la gestion. Ce n'est que dans le modèle P1 + Pe que la clé pour décrypter les données se trouve au niveau de la VAO elle-même.

13. Aucune solution ne garantit totalement l'intégrité des données (data-at-rest) (seuls des contrôles élémentaires sont disponibles - le hashage ou l'utilisation d'une signature numérique ne sont pas des fonctionnalités standard), ce qui implique le risque de ne pas pouvoir se fier aux données,

de ne pas pouvoir les utiliser ou même d'en perdre. Néanmoins, la solution P1 + Pe rendra impossible toute modification cachée des données cryptées au niveau du fournisseur si on ne dispose pas de la clé (qui se trouve en la possession de la VAO).

Au niveau de la gestion de l'identité et de l'accès

14. Seul le fournisseur 3 ne dispose pas d'une gestion adéquate des utilisateurs et des accès (mais elle pourrait être assurée par l'Autorité flamande elle-même).

Au niveau de la sécurité opérationnelle

15. En ce qui concerne la sauvegarde (back-up) et la reprise d'activité (disaster recovery) : dans toutes les solutions, c'est le fournisseur qui s'en occupe, sans autre contribution du client. La VAO suppose que les normes prévues ou les rapports de test proposés suffiront.

16. La Commission prend donc acte du fait que même la solution P1+Pe, la meilleure possible du point de vue technique, présente encore aussi des lacunes majeures spécifiques au regard du modèle Smals.

17. La Commission souligne que les résultats de l'analyse des risques effectuée à l'aide de ce modèle sont indicatifs pour l'utilisateur. Il s'agit d'un outil permettant à l'utilisateur du modèle d'effectuer une analyse des risques de son projet de cloud. La décision finale de savoir si le service cloud examiné convient doit toutefois être prise par l'utilisateur du modèle lui-même, en l'occurrence la VAO.

18. Ce modèle n'évalue d'ailleurs pas toutes les questions ni tous les critères possibles au niveau de la sécurité de données. Ainsi, la Commission estime par exemple que la VAO devrait périodiquement décrypter et recrypter les données à l'aide des dernières techniques, de sorte que le nouveau cryptage (et la clé y afférente) offre [2]à chaque fois la meilleure protection possible, compte tenu de l'état actuel de la technique en matière de sécurité de l'information.

19. Elle note également que cette solution P1 + Pe n'existe en fait pas encore concrètement et constitue une combinaison de deux solutions apportées par deux fournisseurs qui ne sont peut-être pas encore compatibles. Il ne s'agit donc pas d'un modèle opérationnel existant mais d'une solution possible n'ayant pas encore fait ses preuves dans la pratique.

[2] La longueur de clé permettant un cryptage sûr doit être périodiquement reconsidérée : ce qui constitue aujourd'hui une clé d'une longueur suffisante ne le sera plus demain.

20. Enfin, elle confirme et souligne encore plusieurs des problèmes juridiques soulevés précédemment par le Secrétariat lors de la concertation informelle. Elle attire ainsi une nouvelle fois l'attention notamment sur :

- la nature des données à traiter : il s'agit certainement ici de plusieurs données à caractère personnel au sens des articles 6 à 8 inclus de la LVP, telles que des données ethniques et raciales dans le cadre de la politique flamande relative aux groupes cibles (par ex. dans le cadre d'actions positives), de données de santé (telles que des données relatives au handicap à l'emploi en vue d'une adaptation du poste de travail), ou encore de données judiciaires (telles que des données disciplinaires ou les antécédents judiciaires d'un travailleur/fonctionnaire lorsque la personne concernée souhaite accéder à une fonction soumise à une réglementation en vertu de laquelle un casier judiciaire vierge ou exempt de certaines condamnations est requis).

  Des données relatives à l'évaluation du travailleur sont aussi des données sensibles. Il s'agit d'appréciations concernant la personne du travailleur, allant de son aptitude professionnelle à une description des caractéristiques de la personne ou de la personnalité du travailleur (par ex. suite au passage d'examens psychologiques et/ou médicaux).

  Bien que la VAO affirme que le "core HR" (comprenant le traitement des salaires) ne serait pas délocalisé, il semble que les processus HR les plus sensibles - qui sont donc appelés "soft HR" par la VAO - relèvent bel et bien de la "gestion des talents" et feraient donc l'objet de "cloudsourcing".

  La Commission demande en outre à la VAO de vérifier s'il ne s'agirait pas éventuellement de données classifiées au sens de la loi du 11 décembre 1998 *relative à la classification et aux habilitations, attestations et avis de sécurité*. Le cas échéant, vu les exigences applicables aux données classifiées, des normes plus sévères devront être respectées au niveau du hardware, du software, des procédures et du personnel. La Commission attire également l'attention sur le besoin de mesures à la lumière des Directives européennes NIS[3] et EPCIP[4].

- le destinataire des données : il s'agit ici d'un fournisseur de cloud d'origine américaine avec des centres de données se trouvant sur le territoire européen, qui sont donc soumis

[3] Network and information security.

[4] European Programme for Critical Infrastructure Protection.

à d'éventuelles injonctions des autorités américaines de présenter ces données (même à l'insu du client cloud, sans parler des personnes concernées).

- La Commission attire enfin l'attention sur la nature du client cloud : un important acteur public qui transférerait de grandes quantités d'informations stratégiques de type "human capital" vers un fournisseur de cloud d'origine américaine, et ce à un moment où l'ampleur totale des conséquences juridiques du nouveau régime de "Safe Harbor" désigné sous le nom de "EU-US Privacy Shield" n'est pas encore connue.

21. D'autre part, force est de constater que les risques susmentionnés sont réduits dans le modèle P1+Pe parce que seul le client dispose de la clé de cryptage (à cet égard, les solutions P1, P2 et P3 ne sont donc pas acceptables pour la Commission) et aussi, dans une moindre mesure, parce que les données sont stockées dans des centres de données européens (cela vaut d'ailleurs aussi pour P1, P2 et P3), sans que ce modèle n'offre toutefois de garanties concluantes. À défaut de cloud européen, on est contraint de faire appel à un fournisseur de cloud américain (ayant certes un centre de données sur le territoire européen). Néanmoins, les risques d'ingérence par les autorités américaines en ayant recours aux fournisseurs de services examinés (par ex. applicabilité du FISA américain[5]) sont réels, comme il ressort très clairement de l'arrêt de la Cour de Justice européenne du 6 octobre 2015 dans l'affaire "Schrems". Cet arrêt accentue l'importance du droit fondamental à la protection des données, y compris lors du transfert de données à caractère personnel vers des pays tiers. Dans ce cadre, il est aussi nécessaire de souligner que même si les données sont cryptées, cela n'enlève rien à leur statut : il s'agit toujours de données à caractère personnel et il convient de les protéger contre tout traitement non autorisé. En outre, il ne s'agit pas ici de "données publiques" mais de données à caractère personnel des fonctionnaires flamands dont l'Autorité flamande dispose en sa qualité d'employeur. Dans ce cadre, la Commission insiste sur le fait que les membres du personnel concernés et leurs représentants légaux doivent être totalement informés de ce qu'il adviendra des données relatives aux talents, y compris des risques éventuels. La Commission se réfère également au GDPR[6] qui requiert que l'analyse du risque s'effectue en fonction des personnes concernées.

22. Sur la base du rapport de consultance américain, le meilleur moyen d'atteindre les objectifs concrets de la VAO serait de recourir à une solution SaaS pour la gestion HR des talents proposée par les fournisseurs précités et il n'existerait aucun fournisseur SaaS européen alternatif qui répondrait aux exigences du projet de la VAO. La Commission estime cependant que la VAO

[5] Foreign Intelligence Surveillance Act.

[6] General Data Protection Regulation.

devrait également prendre conseil auprès d'une société de consultance européenne qui pourrait peut-être proposer des solutions où la contribution de sociétés américaines serait moins importante. La Commission est toutefois consciente du fait qu'à l'heure actuelle, une solution totalement européenne n'est probablement pas réaliste.

23. La Commission considère enfin qu'il serait utile que l'Autorité flamande adopte un cadre général en matière de cloud, par exemple sous la forme d'une circulaire reprenant des directives et/ou d'un modèle d'évaluation pouvant servir de base à une entité de l'Autorité flamande qui souhaiterait évaluer une solution de cloud déterminée pour un usage opérationnel.

24. La Commission estime quoi qu'il en soit que la VAO doit porter la responsabilité finale pour le choix d'une stratégie de cloud bien déterminée.

PAR CES MOTIFS,

la Commission,

considère, notamment sur la base de l'analyse des risques déjà effectuée et des éléments évoqués dans le présent avis, que la VAO doit porter la responsabilité finale pour le choix éventuel d'une solution de cloud bien déterminée et veiller à ce que toutes les garanties nécessaires soient présentes pour respecter la législation pertinente relative au traitement et à la sécurité des données à caractère personnel.

L'Administrateur f.f. Le Président,

(sé) An Machtens (sé) Willem Debeuckelaere