Advies nr 09/2016 van 24 februari 2016

Betreft: Advies m.b.t. de keuze voor een SaaS-HR-strategie bij talentmanagementprocessen van de Vlaamse Overheid (CO-A 2016-006).

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 informeel overleg d.d. 25/11/15 en 22/01/2016 tussen vertegenwoordigers van de Vlaamse Overheid - Agentschap Overheidspersoneel (hierna het VAO) en het secretariaat van de Commissie;

Gelet op de beslissing van de Commissie d.d. 3 februari 2016 om hierover een advies uit te brengen;

Gelet op het verslag van de heer Frank De Smet;

Brengt op 24 februari 2016 het volgend advies uit:

I. VOORWERP VAN DE AANVRAAG

1. De strategische stuurgroep van de Vlaamse overheid denkt eraan om een cloudstrategie te volgen met betrekking tot de zachte HR-gegevens van het Vlaams Overheidspersoneel, meer in het bijzonder het overbrengen van die persoonsgegevens naar een van oorsprong Amerikaanse (publieke) cloudprovider met een data center op Europees grondgebied.

2. Volgens die stuurgroep zou een SaaS oplossing het meest geschikt zijn voor de ondersteuning van de HR talent management processen binnen de Vlaamse Overheid.

3. Wat de zachte HR-gegevens betreft, gaat het dan, naast een minimum aan basissignalitiek i.v.m. elk Vlaams personeelslid, over gegevens zoals cv, functieprofiel, opleiding, competentieprofiel, en informatie over rekrutering, selectie en evaluatie.

4. Het VAO werd belast met een voorstudie en heeft op basis van een Amerikaans consultancyrapport 4 mogelijke dienstverleners voor ogen om de gewenste cloudoplossing te kunnen aanbieden. Het betreft telkens van oorsprong Amerikaanse dienstverleners, maar de gegevens zouden wel in Europese data centers gestockeerd blijven. De eerste drie oplossingen worden aangeboden door drie stand-alone aanbieders (P1, P2 en P3) die transport encryptie combineren met database encryptie waarbij de encryptiesleutels zich bij de aanbieders bevinden. De vierde oplossing betreft een combinatie van de eerste aanbieder met een encryption gateway (P1 + Pe) waar de encryptiesleutel zich bij de klant bevindt.

5. Op vraag van het VAO vond er informeel overleg d.d. 25/11/15 en 22/01/2016 plaats tussen vertegenwoordigers van het VAO en het secretariaat van de Commissie en het standpunt van het secretariaat werd overgemaakt aan VAO bij brief d.d. 10/02/16, waarin tevens werd aangekondigd dat de Commissie onderhavig formeel advies zou uitbrengen.

II. ONDERZOEK VAN DE AANVRAAG

6. De Commissie neemt akte van de resultaten van de grondige technische analyse van de 4 mogelijke provideroplossingen die het VAO heeft doorgevoerd aan de hand van het “SMALS-model”[1], een referentiemodel op het vlak van criteria m.b.t. gegevensveiligheid.

7. De Commissie stelt daarbij vast dat de eigen vereisten betreffende de door het VAO gewenste oplossing – vastgesteld door zelfbeoordeling – zich globaal in het groene gebied (“cloud service

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

does satisfy") bevinden voor alle 4 componenten van het model en voor alle onderzochte oplossingen.

8. Niettemin vertonen de onderzochte oplossingen volgens dat model een aantal specifieke major gaps, dus items die niet voldoen aan de cloud policy van de Belgische sociale zekerheid. De major gaps die overblijven in de vier componenten van het model zijn:

Op vlak van governance

9. Alle stand-alone cloudproviders P1, P2, P3 die overwogen worden hebben een link met een overheid, in casu die van de VS, die de data mogelijks kan opvragen zonder dat de klant (VAO) van de provider het weet, laat staan de gegevenssubjecten. In de voorgestelde oplossingen bezit de SaaS-provider immers steeds zelf over de encryptiesleutel.

10. Enkel in het model P1 + Pe (een samenwerkingsverband tussen cloudprovider P1 en een provider van een encryption gateway Pe) zou de Amerikaanse overheid alleen geëncrypteerde persoonsgegevens kunnen verkrijgen, vermits de sleutel om de data te ontcijferen bij het VAO zit en de gegevens die de provider zou kunnen leveren in principe dus onleesbaar zijn voor de Amerikaanse overheid. De Commissie merkt wel op dat dit model als gevolg heeft dat er bij de cloudprovider geen enkele verwerking (dus ook niet mogelijk gewenste verwerkingen) kan gebeuren buiten louter opslag en back-up van de gegevens.

11. Bij gebruik van eventuele subverwerkers zullen de providers (uitgezonderd P2) de klant niet proactief inlichten, enkel responsief (op vraag).

Op vlak van IT-security

12. De data zijn weliswaar geëncrypteerd bij de providers, maar zij bezitten zelf de encryptiesleutel en bepalen het sleutelmanagement. Enkel in het model P1 + Pe zit de sleutel om de data te ontcijferen bij het VAO zelf.

13. Geen enkele oplossing verzekert de data-integriteit (data-at-rest) ten volle (enkel elementaire controles zijn beschikbaar – hashing of gebruik van een digitale handtekening zijn geen standaard functionaliteit) wat het risico van mogelijke onbetrouwbaarheid, onbruikbaarheid of zelfs verlies van gegevens inhoudt. Nochtans zullen bij P1 + Pe de geëncrypteerde gegevens onmogelijk ongemerkt kunnen worden gewijzigd op het niveau van de aanbieder zonder sleutel (die in het bezit is van het VAO).

Op het vlak van identiteits- en toegangsmanagement

14. Enkel provider 3 heeft geen adequaat gebruikers- en toegangsbeheer (maar zou kunnen verzekerd worden door de Vlaamse Overheid zelf).

Op vlak van operationele veiligheid

15. Inzake back-up and disaster recovery: bij alle oplossingen is het de provider die hierin voorziet zonder verdere inbreng van de klant. Het VAO vermoedt wel dat de voorziene standaarden of testrapporten die worden aangeboden zullen volstaan.

16. De Commissie neemt aldus akte van het feit dat zelfs de meest ideale technische oplossing P1 + Pe ook volgens het Smals-model nog specifieke major gaps oplevert.

17. De Commissie wijst erop dat de resultaten van de risicoanalyse aan de hand van dit model indicatief zijn voor de gebruiker. Het is een hulpmiddel dat de gebruiker van het model toelaat een risico-inschatting te maken van zijn cloudproject. De eindbeslissing of de onderzochte clouddienst voldoet moet echter worden gemaakt door de gebruiker van het model zelf, in casu het VAO.

18. Dit model toetst overigens niet alle mogelijke vragen of criteria die denkbaar zijn op het vlak van gegevensbeveiliging. Zo is de Commissie bijvoorbeeld van oordeel dat het VAO de gegevens best periodiek zou moeten decrypteren en opnieuw encrypteren met de nieuwste technieken, zodat de hernieuwde encryptie (en bijbehorende sleutel[2]) telkens de best mogelijke bescherming biedt, rekening houdend met de actuele stand van de techniek op het vlak van informatiebeveiliging.

19. Zij noteert bijkomend dat deze oplossing P1 + Pe eigenlijk nog niet effectief bestaat en een combinatie is van twee oplossingen die worden aangebracht door twee leveranciers die mogelijks nog niet op elkaar zijn afgestemd. Het gaat dus niet over een bestaand operationeel model maar over een mogelijke oplossing die zich in de praktijk nog niet bewezen heeft.

20. Zij bevestigt en beklemtoont ten slotte nog een aantal van de juridische aandachtspunten die het secretariaat reeds eerder maakte tijdens het informeel overleg. Zo wordt o.a. nog eens gewezen op:

[2] Sleutellengte om veilig te encrypteren moet periodiek worden herzien: wat vandaag een sleutel is met voldoende lengte is dat morgen niet meer.

- de aard van de te verwerken gegevens: het gaat hier zeker over een aantal persoonsgegevens in de zin van artikelen 6 t.e.m. 8 van de WVP, zoals etnische en raciale gegevens in het kader van het Vlaams doelgroepenbeleid (bv. in het kader van positieve acties), gezondheidsgegevens (zoals gegevens rond arbeidshandicap in functie van werkpostaanpassing), of gerechtelijke gegevens (zoals tuchtgegevens of de gerechtelijke antecedenten van een werknemer/ambtenaar wanneer betrokkene toegang wenst tot een betrekking die is onderworpen aan een regelgeving op grond waarvan een blanco strafregister of een strafregister vrij van bepaalde veroordelingen vereist is).

  Ook beoordelingsgegevens m.b.t. de werknemer zijn gevoelige gegevens. Het gaat over inschattingen omtrent de persoon van de werknemer, gaande van de professionele bekwaamheid tot en met een beschrijving van persoonskenmerken of van de persoonlijkheid van de werknemer (bv. ingevolge afname van psychologische en/of medische onderzoeken).

  Hoewel er gesteld wordt door het VAO dat "core" HR (waaronder loonverwerking) niet gedelokaliseerd zou worden, lijkt het erop dat de meest gevoelige HR-processen - door het VAO dus "zachte" HR genoemd - wel onder de noemer "talentmanagement" zouden vallen en dus het voorwerp van "cloudsourcing" zouden uitmaken.

  De Commissie vraagt het VAO bovendien na te gaan of er mogelijks geen sprake is van geclassificeerde gegevens in de zin van de wet van 11 december 1998 *betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen*. In voorkomend geval, moeten, gelet op de vereisten die gelden voor geclassificeerde gegevens, strengere normen van toepassing zijn op het vlak van hardware, software, procedures en personeel. De Commissie wijst ook op de nood aan maatregelen in het licht van de Europese Richtlijnen NIS[3] en EPCIP[4].

- de bestemmeling van de gegevens: het gaat hier over van oorsprong Amerikaanse cloudproviders, met data centers op Europees grondgebied, die dus onderworpen zijn aan mogelijke bevelen van de Amerikaanse overheid tot overlegging van deze gegevens (zelfs zonder dat de cloudklant dat zou weten, laat staan de betrokkenen).

- De Commissie wijst ten slotte op de aard van de cloudklant: een grote overheidsspeler die grote hoeveelheden strategische "human capital" informatie zou overbrengen naar

[3] Network and information security.

[4] European Programme for Critical Infrastructure Protection.

een van oorsprong Amerikaanse cloudprovider en dit op een moment dat de juridische consequenties van de nieuwe Safe Harbor-regeling onder de naam 'EU-US Privacy Shield' nog niet in hun volle draagwijdte gekend zijn.

21. Anderzijds moet vastgesteld worden dat voornoemde risico's worden gereduceerd in het model P1+Pe omdat enkel de klant over de encryptiesleutel beschikt (de oplossingen P1, P2 en P3 zijn in dit opzicht dus niet aanvaardbaar voor de Commissie) en in beperktere mate ook omdat de gegevens worden opgeslagen in Europese data centers (dit geldt trouwens ook voor P1, P2 en P3) zonder dat dit laatste echter sluitende garanties biedt. Bij gebrek aan een Europese cloud moet noodgedwongen beroep worden gedaan op een Amerikaanse cloudprovider (weliswaar met een data center op Europees grondgebied). Niettemin zijn de risico's van mogelijke inmenging door de Amerikaanse overheid door gebruik te maken van de onderzochte dienstverleners (bv. toepasselijkheid van de Amerikaanse FISA[5]) reëel, zoals heel duidelijk is gebleken uit het arrest van het Europees Hof van Justitie van 6 oktober 2015 in de zaak "Schrems". Dat arrest benadrukt het belang van het fundamentele recht op gegevensbescherming, ook bij de overdracht van persoonsgegevens aan derde landen. In dit kader is het ook nodig te onderlijnen dat zelfs als de gegevens geëncrypteerd zijn, dit niets afdoet van hun status: het blijven persoonsgegevens en die moeten worden beschermd tegen elke niet toegelaten verwerking. Bovendien gaat het hier niet over 'overheidsgegevens', maar over de persoonsgegevens van het Vlaams overheidspersoneel die de Vlaamse overheid bezit in de hoedanigheid van werkgever. In dit kader benadrukt de Commissie dat de betrokken personeelsleden en hun wettelijke vertegenwoordigers volledig moeten worden ingelicht over wat er met de talentgegevens te gebeuren staat, met inbegrip van de mogelijks risico's. De Commissie wijst ook op de GDPR[6], welke vereist dat de analyse van het risico gebeurt in functie van de betrokken gegevenssubjecten.

22. Op grond van het Amerikaans consultancyrapport zouden de inhoudelijke doelstellingen van het VAO het best uit te voeren zijn m.b.v. een HR Talent SaaS oplossing geboden door de net besproken providers en zouden er geen alternatieve Europese SaaS-providers zijn die voldoen aan de vereisten van het VAO-project. De Commissie vindt echter dat het VAO best ook eens ten rade zou gaan bij een Europese consultancyfirma die mogelijks oplossingen zou kunnen voorstellen waar de inbreng van Amerikaanse firma's minder groot is. De Commissie is er zich echter van bewust dat een volledig Europese oplossing op dit ogenblik waarschijnlijk niet realistisch is.

---

[5] Foreign Intelligence Surveillance Act.

[6] General Data Protection Regulation.

23. De Commissie meent tenslotte dat het nuttig zou zijn dat de Vlaamse Overheid een algemeen raamwerk inzake cloudoplossingen aanbiedt, bv. onder de vorm van een omzendbrief met richtlijnen en/of onder de vorm van een evaluatiemodel, waarop een entiteit van de Vlaamse Overheid zich kan baseren als het een bepaalde cloudoplossing wenst te evalueren voor operationeel gebruik.

24. De Commissie is hoe dan ook van oordeel dat het VAO de eindverantwoordelijkheid dient te dragen voor de keuze van een welbepaalde cloudstrategie.

OM DEZE REDENEN,

De Commissie,

is van oordeel dat het VAO, onder andere op grond van de reeds doorgevoerde risicoanalyse en de elementen aangehaald in dit advies, de eindverantwoordelijk dient te dragen voor het al dan niet kiezen voor een welbepaalde cloudoplossing en dient het ervoor te zorgen dat alle nodige garanties aanwezig zijn voor het respecteren van de relevante wetgeving met betrekking tot de verwerking en de beveiliging van de persoonsgegevens.

De Wnd. Administrateur, De Voorzitter,

(get.) An Machtens (get.) Willem Debeuckelaere