Vlaamse overheid

Vlaamse Toezichtcommissie voor het elektronische bestuurlijke gegevensverkeer

Advies VTC nr. 01/2018 van 31 januari 2018

Betreft: Vraag om advies inzake de migratie van de Leer- en ervaringsbewijzendatabank (hierna "LED") naar een publieke cloud

De Vlaamse Toezichtcommissie (hierna: "de VTC");

1. Gelet op het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer (hierna: "het e-govdecreet"), inzonderheid artikel 9 en 11;

2. Gelet op de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (hierna: "WVP");

3. Gelet op de wet van 5 mei 2014 houdende verankering van het principe van de unieke gegevensinzameling in de werking van de diensten en instanties die behoren tot of taken uitvoeren voor de overheid en tot vereenvoudiging en gelijkschakeling van elektronische en papieren formulieren (hierna "wet van 5 mei 2014"), inzonderheid artikel 5;

4. Gelet op het verzoek om advies van het agentschap voor Hoger Onderwijs, Volwassenenonderwijs, Kwalificaties en Studietoelagen (AHOVOKS), ontvangen op 15 december 2017 per mail;

5. Gelet op de voorstelling en bespreking van het project op de zitting van de VTC van 20 december 2017 en de bespreking op de zitting van 31 januari 2018;

6. Brengt op 31 januari 2018 het volgend advies uit:

I. VOORWERP VAN DE ADVIESAANVRAAG

7. De LED is de databank waarin kwalificatiebewijzen (diploma's, certificaten, getuigschriften, etc.) uitgereikt door o.a. onderwijsinstellingen worden geregistreerd.

De kwalificatiebewijzen worden in de LED opgenomen van zodra deze instellingen ze hebben uitgereikt en dit voor de meeste bronnen sinds 1999. De LED is opgericht bij artikel 20 van het decreet van 30 april 2009 en wordt beheerd door AHOVOKS. De LED is bedoeld om snel betrouwbare informatie te verschaffen en onnodige administratie te vermijden. De LED wordt gebruikt door diverse Vlaamse en Federale overheidsinstellingen (VDAB, FOD BOZA, etc.) en kan geconsulteerd worden door de burger (i.e. inkijken van eigen kwalificatiebewijzen).

8. De beheerder van de LED, AHOVOKS, vraagt aan de VTC advies inzake de geplande migratie naar een publieke cloud in casu van Amazon Web Services (AWS).

II. VOORGAANDEN

9. De VTC heeft op 18 januari 2017 een advies verleend in het kader van de erkenning van de LED als authentieke bron[1].

10. Inzake de hosting en beveiliging werden toen volgende elementen bekeken:

11. Voor de erkenning als authentieke gegevensbron zijn er ook criteria die verband houden met de informatieveiligheid[2]. De criteria zijn de volgende:

- de gepaste fysieke, technische en organisatorische maatregelen zijn genomen om de opslag, de toegang tot en het gebruik van de gegevens te beveiligen;
- het is mogelijk de gegevens te auditen, d.w.z. wijzigingen in de gegevens op te sporen (en de historiek van de toegang tot en het gebruik van de gegevens op te vragen);
- de gegevensbronhouder beschikt over een veiligheidsplan (dat voldoet aan de binnen Vlaanderen geldende veiligheidsstandaarden);
- de gegevensbronhouder laat op regelmatige basis een veiligheidsaudit uitvoeren om na te gaan of de veiligheidsmaatregelen nageleefd worden (zoals voorzien in de binnen Vlaanderen geldende veiligheidsstandaarden);

12. De VTC heeft deze criteria besproken op basis van de evaluatie in het evaluatierapport:

13. Inzake beveiligingsmaatregelen:

14. Aansluitend bij wat het evaluatierapport had gesteld i.v.m. de verwijzing naar de verantwoordelijkheid van de outsourcer op basis van het outsourcing raamcontract, heeft de VTC in haar advies benadrukt dat de beheerder van de LED, als verantwoordelijke voor de verwerking, de verantwoordelijkheid draagt voor de naleving van de principes van de WVP (en van de Algemene Verordening Gegevensbescherming, van toepassing vanaf 25 mei 2018) en voor de keuze van de verwerkers waarop hij beroep doet voor de verwerking van persoonsgegevens. De beheerder van de LED moet er bijgevolg over waken dat aan de gepaste voorwaarden wordt voldaan.

[1] Advies VTC/A/2017/01 inzake de erkenning van de Leer- en ervaringsbewijzendatabank (LED) als authentieke bron van persoonsgegevens.
[2] Cf. blz. 24 evaluatierapport.

15. De VTC was van oordeel dat conform wat gesteld werd in vorige paragraaf, duidelijke afspraken dienden gemaakt te worden tussen de LED veiligheidsconsulent en het Facilitair Bedrijf voor wat betreft de naleving van de verplichtingen van de externe verwerker.

16. AHOVOKS had al aangegeven dat een infrastructuurtraject werd opgezet om de LED (public) cloud klaar te maken, waarmee men bedoelde de LED klaar te maken voor een migratie naar eender welke omgeving. Het omvatte o.a. een aantal updates, vervangen van verouderde technologie en de overschakeling naar het gebruik van certificaten in de communicatie. In het evaluatierapport werd vermeld dat een migratie naar Virtual Private Cloud (VPC) van de Vlaamse Overheid wordt voorzien[3]. Bij de behandeling van de adviesvraag werd echter gesteld dat recent bij een adviesbureau een studie werd besteld om na te gaan waarheen de LED het best verhuisd werd.

17. De VTC heeft dan gevraagd op de hoogte te worden gehouden van de keuze van de omgeving, zodat ze haar advies zo nodig kon aanpassen.

18. Aangezien het Virtual Private Cloud (VPC) [4] werd vernoemd als mogelijke bestemming, wees de VTC op haar aanbeveling nr. 01/2016[5] waarbij haar advies met betrekking tot de mogelijkheid om persoonsgegevens van inburgeraars over te brengen naar een datacenter in België dat beheerd wordt door een bedrijf dat verbonden is met een Amerikaans moederbedrijf, zoals VPC van de Vlaamse overheid, voor een goed begrip en een betere toepassing veralgemeend werd.

19. De VTC benadrukte dat de voorwaarden, gesteld in de aanbeveling VTC/A/01/2016, zeker ook gelden in het geval beslist zou worden de LED te migreren naar een public cloud, wat niet evident werd geacht om te realiseren.

20. Voor de LED moeten dezelfde eisen gesteld worden als voor de "Kruispuntbank Inburgering". Het gaat hier ook om persoonsgegevens (met inbegrip van het rijksregisternummer) die in principe vertrouwelijk moeten behandeld worden. Bovendien zijn opleidings- en diploma-getuigschriftgegevens heel belangrijk voor onder meer werk, verloning en maatschappelijke positie van de betrokkenen. Op basis van opleidings- en diplomagegevens kan er ook profilering gebeuren met het risico van discriminatie en dus een risico voor de rechten en vrijheden van de betrokkenen. Extra bescherming is ook nodig omdat de LED als authentieke bron nog belangrijker wordt, zowel voor de betrokkenen als voor de afnemers van de LED doordat het voor de entiteiten van de Vlaamse administratie verplicht wordt, op grond van artikel 3 van het e-govdecreet (zolang dat nog niet vervangen is), om de gegevens bij de LED op te vragen.

21. Inzake het veiligheidsplan:

---

[3] cf. p. 19 van het rapport.
[4] De VTC merkte op dat 'Virtual Private Cloud' betekent dat men gebruik maakt van een geëncrypteerde cloud in een public cloud. Dergelijke werkwijze wordt niet aangeraden daar de encryptie slechts voor beperkte tijd als veilig kan beschouwd worden en voor longitudinale gegevens betekent dit hetzelfde als bijhouden in een public cloud. Het VPC waarover hier sprake is geen cloud als dusdanig, maar een datacenter.
[5] http://vtc.corve.be/docs/adviezen/VTC_AB_2016_01_aanbeveling_outsourcing_datacenter_def_vrpubl.pdf

22. Uit het evaluatierapport bleek dat het informatieveiligheidsplan dateert van 2014 en geldt voor het hele beleidsdomein. De VTC was van oordeel dat er een update moest worden gemaakt, zeker in het kader van de beslissing die wordt genomen m.b.t. al dan niet toetreding tot een bepaald datacenter of cloudtoepassing.

23. Het veiligheidsplan intussen aan de VTC bezorgd. De laatste versie werd goedgekeurd door AHOVOKS op 4 december 2017.

24. Inzake de mogelijkheid van veiligheidsaudits:

25. De VTC sloot zich aan bij de aanbeveling uit het rapport en herhaalde dat dit in eerste instantie een verantwoordelijkheid is van de verantwoordelijke van de verwerking, de beheerder van de LED.

26. De VTC benadrukte dat het de taak van de informatieveiligheidsconsulent is om op regelmatige tijdstippen een veiligheidsaudit uit (te laten) voeren en nadien de verantwoordelijke voor de verwerking te adviseren.

Besluiten in het advies inzake informatieveiligheid:

27. De VTC besliste dat een gunstige beoordeling voor de erkenning van de LED als authentieke bron voorbarig was zolang een aantal elementen niet zijn uitgewerkt en opgezet. Wat het informatieveiligheid betreft waren dat:

- duidelijke afspraken over het opvolgen van de externe verwerker (randnummer 40-41);
- updaten van het informatieveiligheidsplan, rekening houdend met de gevolgen van een migratie naar een datacenter of cloudtoepassing (randnummer 43-47 en 53).
- de beheerder van de LED rechtstreeks de logs kan raadplegen zonder tussenkomst van de externe verwerker (randnummer 50);
- interne veiligheidsaudit op geregelde tijdstippen (randnummer 56);

28. De VTC besliste dat haar advies opnieuw zou worden ingewonnen wanneer in de hiervoor vermelde elementen voorzien zouden zijn.

29. Op 10 november 2017 erkende de Vlaamse Regering de LED als authentieke bron. Er werd voorafgaand niet opnieuw een advies gevraagd aan de VTC. Door de erkenning zijn Vlaamse overheden verplicht om de LED te gebruiken en mogen ze niet langer papieren afschriften van diploma's opvragen bij burgers.

IV. ONDERZOEK VAN DE ADVIESAANVRAAG

30. Vandaag wordt de LED gehost in het Colt datacenter. Deze hosting wordt evenwel stopgezet met ingang vanaf november 2018. Het Facilitair Bedrijf vraagt echter in 2017 een engagement van de entiteiten om te migreren, zoniet verhogen de kosten. AHOVOKS diende bijgevolg op zoek te gaan naar een andere oplossing en wenst in dit kader over te gaan tot een migratie van de LED naar een publieke cloud met het oog op

kostenbeperking, beweegbaarheid, flexibiliteit, schaalbaarheid, performantie en beschikbaarheid. AHOVOKS heeft hiertoe een onderzoek opgestart en een minicompetitie gelanceerd binnen het raamcontract "clouddiensten".

31. Hoewel de officiële gunning nog moe(s)t gebeuren, is AHOVOKS van oordeel dat op basis van het voorliggend dossier kan besloten worden dat de offerte aangeboden door Cronos Public Services NV de beste voorwaarden biedt voor volgende diensten:
- Opzet van een omgeving in de AWS publieke cloud en ondersteuning bij de migratie van LED
- Hosting van de LED-applicatie in de AWS publieke cloud.

32. Dit maakt dat AHOVOKS verantwoordelijk is voor de toepassing en deze beheert. Cronos is verantwoordelijk voor het platform waar deze toepassing op draait. Waar in het verleden in het exploitatiecontract met HB+ (inmiddels DXC) gewerkt werd met een AMAAS-model stapt men hier dus over op een meer marktconform model, PAAS, waarbij AHOVOKS zelf instaat voor het applicatiebeheer.

33. Het kiezen van Cronos, een in België gevestigde "kleinere" speler, als aanbieder van de AWS publiek cloud, geeft AHOVOKS meer flexibiliteit om ad hoc bijkomende (contractuele) voorwaarden op te leggen wat betreft de bescherming van persoonsgegevens, alsook om te garanderen dat er geen potentiele conflicten zijn wat betreft de specifiek na te leven regels als overheidsinstelling.

34. AHOVOKS is zich ervan bewust dat zij, op grond van artikel 16 van de Wet Verwerking Persoonsgegevens en artikel 28 van de Algemene Verordening Gegevensbescherming, een verwerker moet kiezen die voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen van de persoonsgegevens en zal hiermee rekening houden bij de selectie van de AWS publieke cloud aangeboden door Cronos Public Services NV. In de mate van het mogelijke worden al de bepalingen van de Algemene Verordening Gegevensbescherming in acht genomen.

35. Een aantal afgevaardigden van AHOVOKS heeft op de zitting in januari het project voorgesteld en uitvoerig alle technische, juridische en organisatorische maatregelen binnen AHOVOKS en specifiek voor de toepassing LED besproken. Er werden verschillende documenten aan de VTC bezorgd. Na de zitting werd ook de presentatie werd aan de VTC bezorgd. De aanvragers beschikken nog niet over de tekst van het contract met AWS.

36. De VTC behandelt de volgende aandachtspunten:

A. Backups

37. Het betreft een authentieke bron en men moet dus zeker elders een backup voorzien. Als authentieke bron is het ondenkbaar dan men niet meer aan zijn gegevens zou kunnen.

38. Op de vraag naar de bewaartermijn voor de backups antwoordt AHOVOKS dat de standaard bewaartermijn 7 dagen bedraagt, maar vanuit AHOVOKS 30 dagen zullen gevraagd worden. Het betreft wel services die door AWS worden aangeboden.

39. De VTC geeft aan dat het belangrijk is dat zeer regelmatig een backup wordt genomen bv. elke dag en dat men best over 3 'generaties' beschikt. Dan is een termijn van 30 dagen niet nodig.

40. De VTC merkt op dat een statische backup zonder omgeving niet voldoende is.

41. Voor de volledigheid merkt de VTC op dat de data in het slechtste geval nog beschikbaar zijn bij de onderwijsinstellingen.

B. Exitstrategie

42. De aanvrager antwoordt dat er qua exitstrategie contractueel 2 mogelijkheden zijn voorzien met Cronos. Daarnaast wil AHOVOKS regelmatig oefeningen uitvoeren om data over te zetten naar andere platformen.

43. De VTC stelt dat er sowieso met 2 partners moet gewerkt worden, zoniet wordt men als uitbestedende overheid gegijzeld.

C. Encryptie

44. De VTC benadrukt het belang van de encryptiesleutel om te verzekeren dat AWS niet aan de data kan.

45. AHOVOKS meldt dat het Facilitair Bedrijf werkt aan een cryptomodule.

46. De VTC vraagt toch nog aandacht voor het feit dat sleutels doorheen de tijd onveilig worden. Er moeten dus structurele maatregelen genomen worden zodat er regelmatig herencryptie is en de gegevens op elk ogenblik veilig zijn.

47. Er moet ook voor gezorgd worden dat de gegevens ook niet meer als backup met een verouderde sleutel ter beschikking zijn.

48. Het standaardadvies inzake encryptie moet worden gevolgd, ook al zijn het niet gevoelige oude data.

49. De VTC wijst er op dat (i.t.t. data at rest en data in motion) encryptie van data in use niet/zeer moeilijk te organiseren is. Daarom moeten er degelijke auditsystemen komen en programma's die gegevens zo verwerken dat er niet gekopieerd wordt (en het beveiligen van de verspreide gegevens moeilijk wordt).

50. AHOVOKS is verantwoordelijk voor dit bestaand risico. Onder de AVG/GDPR wordt de verantwoordelijkheid nog meer beklemtoond.

51. De masterkey zal bewaard worden door het Facilitair Bedrijf. Dit zou ook kunnen bij Onderwijs en Vorming, maar het lijkt niet de beste practice het beheer zelf te organiseren. De VTC bevestigt dat.

D. Noodzaak cloudgebruik

52. De aanvragers kunnen geen cijfers geven over het aantal opvragingen dat jaarlijks zal gebeuren. Er zitten momenteel 11 miljoen diploma's in en jaarlijks komen daar ongeveer 1 miljoen bij. De gegevens veranderen niet veel, er komen er in principe enkel bij. Het gaat om een beperkt aantal gegevens.

53. De VTC concludeert dat het dus om een kleine toepassing gaat en maakt de bedenking of dit wel economisch interessant is.

54. Op de vraag of het de bedoeling is ook andere applicaties naar AWS te verhuizen antwoordt de aanvrager dat dit niet de bedoeling is. Men plant bijvoorbeeld niet om studietoelagen ook te migreren naar AWS. Voor de LED lijkt dit een goed oplossing, omdat
- het een stabiele toepassing is
- er een redelijk constant volume aan vragen (men kent de piekperiodes) is en dus *cloud scalable*
- er weinig interfaces zijn.

E. Voorgestelde maatregelen

55. Het is niet de bedoeling om te zeggen dat er niet mag gewerkt met een private cloudprovider, maar de VTC moet wel policies kunnen zien. De aanvrager moet een antwoord kunnen geven op evidente risico's. De gegevens in de LED zijn geen "gevoelige gegevens", maar er zou een globale policy voor de Vlaamse Overheid moeten zijn.

56. Absolute veiligheid bestaat niet, de verantwoordelijke voor de verwerking moet door risico-analyse nagaan welke risico's die wil aanvaarden.

57. Positief in dit dossier is de maturiteit die Onderwijs en Vorming heeft met het beheer van persoonsgegevens en haar uitgewerkte veiligheidsbeleid zoals aangetoond in de presentatie.

58. Het probleem is dat de VTC meestal geen uitgebreid gedocumenteerde dossiers krijgt.

59. Op basis van de voor de zitting bezorgde documenten wordt geoordeeld dat AHOVOKS de situatie zo goed als mogelijk heeft 'dichtgetimmerd'.

60. AHOVOKS heeft op de zitting laten weten dat niet gemigreerd wordt zolang niet aan de voorwaarden is voldaan (zie hierna).

V. BESLUIT

- een aantal **maatregelen** o.a. rond encryptie, backup termijn, een systeem dat de toepassing van het *least priviledged* principe afdwingt, zijn nog niet gerealiseerd: er kunnen maar

persoonsgegevens in de cloud worden gezet als de nodige maatregelen geïmplementeerd worden. De VTC vraagt haar dit te melden.

- de contractvoorwaarden met en de auditrapporten van de **verwerker**, Amazon Web Services (AWS), worden aan de VTC bezorgd, zodra ze ter beschikking zijn.

- de VTC benadrukt dat haar conclusies dit dossier betreffen en niet algemeen gelden. Er mag dan ook niet voorbijgegaan worden aan de algemene richtlijnen zoals beschreven in de reeds vermelde aanbeveling van de VTC en in de volgende documenten:
  - het cloudevaluatiemodel van SMALS[6];
  - het advies inzake cloud van de CBPL[7].

- er zou **best vanuit Vlaanderen** een **globale policy** inzake het gebruik van (publieke) cloudtoepassingen opgemaakt worden. Op die manier staan de Vlaamse overheidsinstanties sterker. Voor de specifieke applicaties kan een instantie dan nog specifieke maatregelen toevoegen.

De voorzitter,
Willem Debeuckelaere

[6] https://www.smalsresearch.be/tools/cloud-security-model-nl/ en toelichting http://vtc.corve.be/docs/Presentation-Cloud-Security-Guidance-EN-SMALLS.pdf
[7] https://www.privacycommission.be/sites/privacycommission/files/documents/advies_10_2016.pdf