Vlaamse overheid

Vlaamse Toezichtcommissie voor het elektronische bestuurlijke gegevensverkeer

Advies VTC nr. 01/2018 van 31 januari 2018 aanvulling VTC 18 april 2018

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

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;

5. Gelet op het advies van 31 januari 2018;

6. Gelet op de aanvullende informatie bezorgd door het agentschap voor Hoger Onderwijs, Volwassenenonderwijs, Kwalificaties en Studietoelagen (AHOVOKS), ontvangen per mail op 30 april 2018;

7. 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

8. Brengt op 18 april 2018 het volgend aanvullend advies uit:

I. VOORWERP VAN DE ADVIESAANVRAAG

1. In antwoord op de voorwaarden gesteld in het advies, heeft AHOVOKS de VTC per mail op 30 april 2018 volgende informatie bezorgd:
- info mbt verwerkersovereenkomsten (vnl. aanvullende nota met betrekking tot de verwerkingsovereenkomsten)
- back-up strategie LED
- DPIA voor hosting LED (op basis van tool cnil)
AHOVOKS heeft hierover ook een toelichting gegeven op de zitting van de VTC van 18 april 2018.

II. ONDERZOEK

A. DPIA

2. De VTC maakt enkele opmerkingen bij de DPIA:
- gegevens in LED als type school (gewoon of buitengewoon – dit wordt vermeld bij gevolgen voor betrokkenen) en INSZ
- er wordt alleen gekeken naar het oorspronkelijk doel en niet naar de verdere verwerking door diverse afnemers (o.a. bij gegevensminimalisatie en logische toegangscontrole)
- gevolgen voor betrokkenen werden minimalistisch onderzocht bv. wat als gegevens verdwijnen: dit werd niet ingevuld.

B. ENCRYPTIE

3. De keuze van de **encryptie-bouwsteen** van het Facilitair Bedrijf (voor encryptie at rest) is positief. Er wordt ook naar encryptie als (mogelijke) maatregel verwezen in de verschillende teksten die AHOVOKS heeft bezorgd.

4. De VTC wijst er op dat het goed zou zijn dat de dynamische encryptie door alle overheden kan gebruikt worden.

C. BACK UP STRATEGIE

5. De back-up strategie zoals omschreven lijkt voldoende.

6. De VTC heeft wel opmerkingen bij de volgende punten:

7. Er zou een strikte scheiding van functies moeten toegepast worden. Dit is van belang mocht iemand moedwillig gegevens willen aanpassen. Men mag geen toegang hebben tot beide (primaire en backup) accounts. De scheiding van functies zou op alle niveau's moeten opgezet worden (niet enkel voor niveau 4 zoals vermeld in de presentatie).

8. Dit is voorzien bij AHOVOKS en Cronos, maar voor AWS kan men zich niet engageren.

9. De VTC heeft vragen bij de keuze om de backup account ook bij AWS te zetten.

10. De aanvragers hebben overwogen om dit te scheiden, maar onderzoek heeft uitgewezen dat dit toch nog meer risico's meebrengt, nl. data wordt steeds verplaatst en geëncrypteerd. De backups zijn geëncrypteerd at rest.

11. Wat beschikbaarheid betreft zou het beter zijn dat de back-up door een andere partner wordt bijgehouden.

D. OVERDRACHT GEGEVENS NAAR EEN NIET-EUROPESE OVERHEID

12. Er werd door AHOVOKS een **contractuele garantie** voorgelegd dat er **geen overdracht** zal zijn naar niet-Europese overheid (zie punt 3.3. van de aanvullende nota).

13. De AWS bepalingen stellen dat AWS de GDPR zal naleven. AHOVOKS concludeert dat dit garandeert dat contractueel wordt bepaald dat alleen data worden doorgegeven aan een land buiten de EER als dat kadert in een internationale overeenkomst voor wederzijdse rechtshulp of gelijkaardige verdragen conform **Fout! Verwijzingsbron niet gevonden.**' (waarnaar Cronos expliciet verwijst, maar AWS niet). AWS maakt echter tegelijk een voorbehoud voor wat wettelijke verplichtingen betreft, zonder dit te beperken tot Europees recht.

14. De redenering van AHOVOKS is niet overtuigend.

15. De VTC ziet ook een probleem in de beperkte **meldingsplicht** als de gegevens door de Amerikaanse overheid worden opgevraagd.

16. Dit wordt enkel voorzien via een cascadesysteem, zowel voor Cronos als voor AWS. AWS engageert zich om het te melden, tenzij verboden volgens Amerikaans recht.

17. De VTC is van oordeel dat men geen gegevens mag doorgeven zonder dat het op voorhand gemeld werd. Hier moet het Belgisch en Europees recht gelden. In het contract moet dus duidelijk gesteld worden dat er enkel geen melding vereist is indien het verboden is door het Belgisch of Europees recht (bij toepassing van artikel 48).

E. EFFECTIEF EISEN EN NEMEN VAN MAATREGELEN

18. De VTC wijst er nogmaals op dat persoonsgegevens in de cloud worden gezet als de nodige maatregelen ook geïmplementeerd worden. De contractuele bepalingen bieden mogelijkheden om technische en organisatorische maatregelen (zoals Least Privileged Principe en Encryptie) te eisen en te nemen, maar de VTC heeft nog geen kennis van de invulling van de maatregelen in de contractsvoorwaarden en in de praktijk.

De voorzitter,
Willem Debeuckelaere