Vlaamse overheid

Vlaamse Toezichtcommissie voor de verwerking van persoonsgegevens

Advies VTC nr. 2020/05 van 8 september 2020

betreffende

Informatieveiligheid en GDPR-conformiteit

4 Platformen Onderwijs – Amazon Web Services (AWS)

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

Gelet op het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer (hierna: “het e-govdecreet”), inzonderheid artikel 10/4, §1 en 10/7;

Gelet op de Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (hierna AVG), inzonderheid artikel 57, 1, c) en artikel 58, 2, a) en 3, AVG;

Gelet op het verzoek om advies van het departement Onderwijs en Vorming (DOV), het Agentschap voor Onderwijsdiensten (AGODI) en het Agentschap Hoger Onderwijs, Volwassenenonderwijs, Kwalificaties en Studietoelagen (AHOVOKS), samen aangeduid als “Onderwijs en Vorming”, ontvangen per mail door de VTC op 9 juni 2020;

Gelet op het horen van vertegenwoordigers van de adviesvragers op de zitting van de VTC van 30 juni 2020;

Gelet op de bespreking van de adviesvraag op de zitting van de VTC van 28 juli 2020 en 8 september 2020;

Brengt op 8 september 2020 het volgend advies met waarschuwing uit:

Voorbehoud

1. De VTC beklemtoont dat in de mate dat het advies dit niet als een soort machtiging van de VTC mag worden beschouwd. Het houdt voor alle duidelijkheid (voor de instanties die over de geformuleerde bezwaren en voorwaarden zouden overlezen) zeker geen goedkeuring in voor de Vlaamse instanties om over te stappen naar AWS.

2. Het gaat in de adviesvraag over vier concrete casussen. De VTC vraagt dat voor andere casussen terug naar de VTC gekomen wordt.

3. Omdat de VTC vernomen heeft dat haar advies inzake de Leer- en Ervaringsbewijzendatabank (LED) in het verleden voor andere projecten werd beschouwd als een positief advies voor andere toepassingen in AWS, wil ze nog eens verduidelijken dat de LED-casus aan enkele specifieke en noodzakelijke voorwaarden voldeed: het ging om redelijk statische informatie (die in vergelijking met andere informatie noch veel wijzigt, noch veel wordt opgevraagd en dus weinig *data in use* creëert) en alhoewel het over belangrijke info gaat voor de burger, is deze niet echt 'gevoelig'. De VTC heeft dat dossier behandeld als een – eenmalige - POC, maar heeft geen evaluatie gekregen over het al dan niet behaald zijn van de doelstellingen die door de adviesvragers gesteld werden.

4. De VTC wijst er ook op dat zij de hoogste toezichthouder is wat de verwerking van persoonsgegevens betreft voor de rechterlijke macht. Zij kan in dat licht in de toekomst van oordeel zijn dat de beoordeling strenger moet zijn op basis van voortschrijdend inzicht, zoals nu naar aanleiding van het arrest Schrems II van het Hof van Justitie (zie verder).

INLEIDING

5. Het dossier en de manier waarop het aangebracht werd, doen de VTC beseffen dat de principes achter haar vorige adviezen (https://overheid.vlaanderen.be/vlaamse-toezichtcommissie-actueel-cloud) of niet gevat werden of bewust genegeerd werden. Ze staat er dan ook op om deze verder te herhalen en verduidelijken.

UITGANGSPUNTEN

AVG: vertrouwelijkheid en veiligheid

6. De VTC heeft de principes van vertrouwelijkheid en veiligheid ondermeer vertaald in de volgende regel: geen toegang tot data voor beheerders van infrastructuur buiten wat strikt nodig is (*problem solving*).

7. Dat geldt voor binnenlandse en buitenlandse IT-leveranciers.

AVG: proportionaliteit

8. Een belangrijke regel van de AVG is die van de minimale gegevensverwerking. De proportionaliteit van de verwerking wordt afgewogen aan het (wettelijke en gerechtvaardigde) doel van de verwerking.

9. Een probleem wordt gevormd door de leveranciers die niet kunnen garanderen dat ze zich aan de Europese gegevensbeschermingseisen en in het bijzonder dit principe kunnen houden. Dit kan bijvoorbeeld omdat wetgeving die op hen van toepassing is, zoals die van de Verenigde Staten[1], de

[1] Zie o.a. Amerikaanse Cloud Act van 2018: *"(1) AMENDMENT.—Chapter 121 of title 18, United States Code, is amended by adding at the end the following:*
"§ 2713. Required preservation and disclosure of communications and records

overheid (in het bijzonder de inlichtingendiensten) de mogelijkheid geeft om de data die beheerd worden door deze cloudproviders massaal op te vragen[2], ook als de servers zich niet in de VS bevinden[3]. Op die manier wordt niet alleen afbreuk gedaan aan de vertrouwelijkheid, maar ook aan het principe van proportionaliteit. Dat is een van de punten waar het Hof van Justitie over struikelt (arresten Schrems I en II[4]).

AVG: risico-inschatting

10. De VTC constateert, in het algemeen en ook bij deze adviesvraag, dat de risico-evaluaties onvoldoende rekening houden met het risico voor de betrokken burgers en te veel geconcentreerd zijn op de bedrijfsrisico's van de betrokken Vlaamse instantie.

11. Dit blijkt ondermeer uit de DPIA[5] die werd voorgelegd en die meer de bedrijfsrisico's dan de risico's voor de betrokkenen aanwijst. De VTC concludeert dat dit geen DPIA is zoals bedoeld in de AVG. Bovendien worden de restrisico's als eenvoudig te accepteren voorgesteld (zie hierover verder).

HET RISICO

12. De VTC wil dat de verwerkingsverantwoordelijken, zijnde de leidinggevenden van de diensten van de Vlaamse Regering, en de politiek verantwoordelijken, goed verstaan wat het risico is van het mogelijk ongelimiteerd/massaal doorgeven van persoonsgegevens van de burgers waarvoor ze verantwoordelijk zijn.

Gegevens en betrokkenen

13. Het gaat om gegevens over en ook het op die manier categoriseren van lerenden, voornamelijk van kinderen en jongeren. Al deze informatie kan later in het leven van de betrokkenen een rol spelen. **De mogelijkheid van vergaande profilering is aanwezig**.

14. De VTC had op haar vergadering van 30 juni 2020 aan de vertegenwoordigers van O&V de volledige lijst van de gegevens die in de platformen zouden terechtkomen opgevraagd met de aanduiding van de gevoeligheid van de gegevens. Op 27 juli 2020 heeft zij enkel een standaardlijst van ruime categorieën ontvangen waarbij O&V heeft aangeduid welke van toepassing zijn voor de 4 platformen. Op basis van deze lijst kan de VTC niet controleren of de aanduiding van de categorieën juist is uitgevoerd. Het is evenwel duidelijk dat het ook om **gevoelige gegevens** in strikte en in ruime zin gaat zoals bedoeld door de European Data Protection Board (EDPB)[6].

"A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States."."
Zie ook

[2] Voor de VTC zijn puntbevragingen n.a.v. strafrechtelijke onderzoeken, in dit dossier niet grootste bezorgdheid.

[3] *Cloud diensten in hoger onderwijs en onderzoek en de USA Patriot Act*, Universiteit Amsterdam, 2012*:*
"The United States [...] takes the position that it can use its own legal mechanisms to request data from any Cloud server located anywhere around the world so long as the Cloud service provider is subject U.S. jurisdiction: that is, when the entity is based in the United States, has a subsidiary or office in the United States, or otherwise conducts continuous and systematic business in the United States."

[4] Arrest van 6 oktober 2015, Schrems, C-362/14 en Arrest van het Hof van Justitie van 16 juli 2020, zaak C-311/18 (http://curia.europa.eu/juris/celex.jsf?celex=62018CJ0311&lang1=nl&type=TXT&ancre=). Samenvatting: https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091nl.pdf

[5] Gegevensbeschermingseffectbeoordeling (GEB).

[6] Richtsnoeren van de Groep Gegevensbescherming Artikel 29 ("Working Party 29" intussen "European Data Protection Board") van 4 oktober 2017 over de Gegevensbeschermingseffectbeoordeling.

15. De VTC weet op basis van door haar behandelde machtigingsdossiers dat een groot deel van de studies die gedaan worden met overheidsdata betrekking hebben op leerlingkenmerken als thuistaal en hoogste opleiding van de moeder. Ook schoolprestaties zijn als gevoelige gegevens in de ruime zin te beschouwen.

16. De VTC wijst er ook op dat vragen die gesteld worden in studies aan de hand van enquêtes dikwijls zeer persoonlijk zijn. In de mate dat deze op de platformen zouden kunnen terechtkomen[7], moet hiermee ook rekening worden gehouden.

17. De grote toepassingen van OV, Discimus (alle leerlingen en leerkrachten) en eveneens DaVinci (volwassenenonderwijs) waar ook gegevens van kwetsbare groepen inzitten, blijken een bron voor de geplande dataplatformen. Zie verzoek om informatie op het einde van deze tekst.

Deze basisgegevens over potentieel alle inwoners van Vlaanderen en studerenden in het onderwijs van de Vlaamse Gemeenschap worden potentieel aan een buitenlandse mogendheid doorgegeven.

18. De dataclassificatie die meestal gehanteerd wordt en een onderscheid maakt tussen gevoelige gegevens (zoals bedoeld in artikel 9 en 10 en aanvullend zoals bepaald door de European Data Protection Board) en andere is richtinggevend, maar niet beslissend op zich.

19. Ook de hoeveelheid en aard van de betrokkenen en de hoeveelheid (omvattendheid) van de gegevens en de bewaartermijn op het AWS-platform zou een rol moeten spelen bij de risicoanalyse.

Beleidsdatabanken / datawarehouses

20. Aansluitend bij het vorige punt wil de VTC duidelijk stellen dat ze ervan overtuigd is dat al deze gegevens tot nu toe niet door de (Vlaamse) overheid verzameld worden in (beleids)databanken om specifieke personen te volgen (“surveillance”).

21. Het moet de leidend ambtenaren echter duidelijk zijn dat in de mate een min of meer volledig profiel van de burger wordt gemaakt, het **risico** hierin ligt dat **deze omvattende informatie kan gebruikt en misbruikt worden**: profilering is mogelijk en uit sommige informatie blijkt de kwetsbaarheid en mogelijke beïnvloedbaarheid van de betrokken personen. Andere informatie kan leiden tot discriminatie en er is zeker ook informatie die de personen (kinderen, jongeren, lerenden) kan stigmatiseren[8].

Alternatieven hosting

22. Het beroep doen op AWS wordt als de enige valabele mogelijkheid voorgesteld. De VTC heeft hier ernstige vragen bij.

23. Ter illustratie van de **mogelijkheid van het gebruik van ‘Europese’ infrastructuur** verwijst de VTC naar twee casussen:

24. Ten eerste is er de vergelijkbare dataset die in België wordt samengebracht in het Datawarehouse Arbeidsmarkt en Sociale Bescherming. Deze verwerking van gevoelige persoonsgegevens gebeurt op een Belgische cloudinfrastructuur met de nodige organisatorische, technische en wettelijke omkadering.

[7] Soms blijven deze data (bij voorkeur en tijdelijk) bij de onderzoekers.

[8] *Databases: Over ICT-beloftes, informatiehonger en digitale autonomie*, Munnichs, G., Schuijff, M., Besters, M., 2012, The Rathenau Institute, Den Haag.

25. Ten tweede heeft de VTC kennis genomen van het feit dat er een massa aan Vlaamse leerlinggegevens in handen is van private IT-leveranciers van de onderwijsinstellingen, maar dat die de data toevertrouwen aan Europese datacenters in buurlanden in plaats van aan niet-Europese spelers.

26. De VTC wijst er ook op dat er toepassingen/platformen mogelijk zijn die (externe)cloudcapaciteit benutten en persoonsgegevens toch lokaal houden.

Beschermingsmaatregelen

27. Artikelen 5.1.f), 24.1 en 32 van de AVG vermelden uitdrukkelijk de verplichting voor de verwerkingsverantwoordelijke(n) om gepaste technische en organisatorische maatregelen te treffen die nodig zijn voor de bescherming van de persoonsgegevens. Deze maatregelen moeten een passend beveiligingsniveau verzekeren rekening houdend, enerzijds, met de stand van de techniek ter zake en de kosten voor het toepassen van de maatregelen en, anderzijds, met de aard van de te beveiligen gegevens en de potentiële risico's.

28. De verwerkingsverantwoordelijke, dus elke entiteit van de Vlaamse overheid, moet erop toezien dat voormelde veiligheidsmaatregelen te allen tijde worden nageleefd.

29. Voor zover persoonsgegevens verkregen worden via de KSZ, zullen maatregelen voor sector van de sociale zekerheid moeten gevolgd worden. Dit geldt in ieder geval voor de entiteiten van O&V die behoren tot het secundair netwerk van de KSZ. Deze maatregelen sluiten het beroep doen op publieke en private clouddiensten uit[9].

INFORMATIEVEILIGHEID

Veiligheid

30. De vertegenwoordigers van O&V hechten zoveel belang aan hackingproblematiek dat de conclusie niet anders kan zijn dat die toch wel een zeer hoog risico inhoudt volgens de adviesvragers.

31. De VTC merkt op dat de bescherming tegen hackers dus veel aandacht krijgt, maar dat andere potentiële spelers gewoon de sleutel tot de data gegeven wordt.

32. Encryptie is voorlopig de belangrijkste maatregel, maar deze is niet 100% sluitend: er is een kans dat 10% van de data lekt, maar ook een kans dat 100% van de data lekt.

33. De VTC heeft in haar advies A/2020/04 en 05 inzake een andere cloudaanbieder (Microsoft Azure) besloten dat:

– de voorgestelde encryptiemodule van het Facilitair Bedrijf– mits correct geïmplementeerd en beheerd – het risico van het massaal data inhalen van de burger op redelijke wijze beperkt;

– er anderzijds wel nog de mogelijkheid is van toegang tot leesbare data in use, dus van zodra er bewerkingen op worden uitgevoerd;

- de VTC adviseert om de voorgestelde cloudtoepassingen (tenzij er toch sluitende maatregelen worden geïmplementeerd) niet aan te wenden voor bepaalde categorieën van informatie: strategische geheime informatie (op zich geen bevoegdheid van de VTC) en informatie die een groot risico kan vormen voor

[9] Tenzij een toelating van de KSZ wordt verkregen.

de betrokkenen: 'gevoelige' informatie, profilerende informatie, informatie over kwetsbare personen, …

34. De VTC wenst voor een goed begrip aan de verantwoordelijken nog te verduidelijken dat ze met "massaal data inhalen", verwijst naar de praktijken van de Amerikaanse inlichtingendiensten die de data van de grote cloudaanbieders in hun eigen (enorme) datacenter(s) kunnen opslaan om daar bewerkingen (screening) op uit te voeren. Encryptie verhindert niet het binnenhalen van de data, maar enkel (als ze goed werkt) het lezen ervan. De data van de Vlaamse lerenden komen daarbij dus potentieel wel in het datacenter van de inlichtingendienst terecht.

Het grote probleem is dat de verwerkingsverantwoordelijke, hier OV, geen controle heeft.

Controle

35. De VTC heeft de optie bekeken van door de verantwoordelijken zelf op te stellen gedragscodes waarin ook rekening wordt gehouden met het ethische aspect. Ze is echter van oordeel dat het opstellen van een gedragscode te veel tijd vraagt. Anderzijds is de VTC er van overtuigd dat vooral controles nodig zijn en wel van onafhankelijke partijen op grond van de vereisten volgens de VTC. Deze vereisten zullen vooral gebaseerd zijn op de aard van de gegevens/de informatie.

36. In dat kader is het aangewezen dat er een controle komt op een al bestaande cloudtoepassing, namelijk de LED (met het voorbehoud dat de impact van Schrems II op dit bestaande project moet bekeken worden).

ALLE PRINCIPES OPZIJ

37. De VTC stelt vast dat voor de voorgestelde dataplatformen verschillende principes en richtlijnen opzij worden gezet:

- pseudonimisering
- anonimisering
- trusted third party
- back-up
- exit-strategie.

Pseudonimisering

38. De VTC had tijdens het overleg een duidelijke vraag gesteld naar al dan niet voorafgaande pseudonimisering, maar had een zeer onduidelijk antwoord gekregen. De adviesvragers stelden dat de dynamische encryptie binnen het platform voldoende waarborgen bood.

39. Pseudonimisering wordt voor 2 van de 4 dataplatformen voorgesteld. Dit lijkt bij nader inzien echter enkel de pseudonomisering te betreffen die uitgevoerd wordt voor de data naar de onderzoekers gaat en niet zoals de richtlijn het vraagt, voordat de data aan het platform en de verwerker (AWS) worden toevertrouwd. De andere twee platformen zijn voor "operationele analyse" bedoeld, ze betreffen operationele doelstellingen en data. Er wordt dan duidelijk niet gepseudonimiseerd voor ze op de platformen worden opgeladen noch naar de eindgebruikers toe. Dit terwijl pseudonimisering een basis beschermingsmaatregel is in deze publieke cloud context.

40. De VTC wijst er op dat wat wetenschappelijk en statistisch onderzoek betreft, de regeling van artikel 198 e.v. van de kaderwet Verwerking Persoonsgegevens (WVG) gelden, in het bijzonder artikel 202.

Anonimisering

41. Anonimisering is natuurlijk de maatregel die veel mogelijk maakt, aangezien het dan niet meer om persoonsgegevens gaat en ze dus ook niet meer de vereiste bescherming behoeven. Wat onderwijsdata betreft is al door (andere) vertegenwoordigers van O&V aangehaald dat de massa aan gedetailleerde data echte anonimisering moeilijk maakt. Voor bepaalde analyses echter, moet het mogelijk zijn om met geanonimiseerde data te verwerken, maar hier wordt door de adviesvragers aan voorbijgegaan.

Trusted Third Party (TTP)

42. **Voor pseudonimisering en anonimisering** is een basisvereiste om **een trusted third party** in te schakelen. Zie aanbeveling 02/2010 van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer[10].

43. De VTC wijst er op dat er naar aanleiding van de machtiging van de beleidsdatabank op het oude platform wegens capaciteitsproblemen werd toegestaan om de pseudonimisering bij een afgescheiden, maar dus interne dienst van O&V te laten gebeuren. Ze wijst er op dat dat in een heel andere context werd toegelaten dan deze van de nu voorgestelde dataplatformen op AWS.

Back-up

44. Voor back-up van de data lijken de onderwijsplatformen ook afhankelijk van AWS. Het is de VTC nog niet duidelijk waar de brondatabanken gehost worden of zullen gehost worden en hoe de back-up geregeld is.

Exit strategie

45. De VTC is ten zeerste verontrust over het feit dat voor de dataplatformen **geen betrouwbare exitstrategie** wordt voorgesteld. Er moeten minstens twee providers worden ingeschakeld. AWS kan failliet gaan. De vertegenwoordigers van O&V hebben dit risico bekeken. Ze aanvaarden het risico dat AWS ineens failliet zou gaan.

46. Het is niet ondenkbaar dat er zich een *black swan event* (eerder dan een ingeschat risico) voordoet dat impact heeft op de beveiliging.

47. Doordat in het voorstel alles bij één monopolist zit zijn er heel veel afhankelijkheden.

48. De VTC beschouwt dit als **niet aanvaardbaar**.

49. De vertegenwoordigers van O&V leggen uit dat ze liever niet met duplicaten werken omdat dat een risico inhoudt.

50. De VTC gaat er echter van uit dat een **dagelijkse back-up naar een neutrale locatie vereist** is. De VTC wijst er op dat de vertegenwoordigers van Onderwijs & Vorming aangeven dat er een exit-strategie is, maar dat deze alleen geldt als AWS meewerkt.

[10] https://www.gegevensbeschermingsautoriteit.be/publications/aanbeveling-nr.-02-2010.pdf

CLOUD FIRST STRATEGIE

Monocloud strategie

51. De VTC begrijpt dat de eindconclusie van de oefening van Onderwijs & Vorming is, dat de verwerking in de publieke cloud moet gebeuren en dat er maar een enkele mogelijke kandidaat is, AWS. Dat komt dan neer op een **publieke cloud first strategie**. **Dit voor alle cases, alle data.** Bovendien wordt ook Snowflake aangeduid als verwerker, wat eveneens een niet-Europees bedrijf is. Dit maakt een correcte risico-inschatting noodzakelijk. De vertegenwoordigers van O&V zeggen nu dat O&V alle data bij AWS willen zetten en alles ontsluiten met Snowflake. Dit alles brengt een zeer grote afhankelijkheid met zich mee.

52. De VTC vindt het noodzakelijk dat er een case by case benadering komt. Nu is het eindresultaat "alles bij AWS" en dus bij een dienstverlener die moeilijk te beheersen valt.

53. Er is zeker ook het risico van een **vendor lock in**. Deze afhankelijkheid brengt mee dat in het geval problemen met de verwerking opduiken/zichtbaar worden, stel inzake vertrouwelijkheid van de gegevens, niet of te moeilijk naar een andere verwerker kan overgestapt worden.

54. De alternatieven (G-cloud, VPC met datacenters op Belgisch grondgebied en dus beter onder controle te houden) worden als onaanvaardbaar voorgesteld op basis van minder technische beschermingsmaatregelen, minder performantie en schaalbaarheid, maar zonder dat dit aangetoond wordt. Dat is een heel drastische conclusie waaruit dus een **zeer grote afhankelijkheid van AWS en Snowflake** voortvloeit. Alle alternatieven worden afgesloten. O&V heeft ook geen validatie laten doen door de andere leveranciers.

Wat de VTC dus vaststelt, is dat alle kroonjuwelen, met name de Vlaamse onderwijsdata, aan een externe provider worden toevertrouwd die bovendien ook nog Amerikaans is.

55. Volgens de VTC wordt er een **enorm risico** wordt genomen. Er moet rekening worden gehouden met de maatregelen, de data, de vereiste van pseudonimisering en sluitende encryptie. **Er is dan geen ruimte meer voor risico-aanvaarding**.

56. Wanneer de vertegenwoordigers van Onderwijs & Vorming voorstellen om een risico accepteren, redeneren zij niet vanuit de betrokkenen.

57. De **brondatabanken** (Discimus, Davinci) worden potentieel in AWS gezet, dus ook de leerlingengegevens (waaronder bv. C-attest en anderstaligheid). De gegevens betreffen dan misschien geen openbare veiligheid, maar het is wel **ongeveer alles aan onderwijsdata**. Dit heeft een zware impact op het risico.

    De VTC wenst daarom een sluitend volledig overzicht van alle data die momenteel reeds bij AWS wordt gehost en welke maatregelen er op pseudonimisering werden genomen.

58. Er kan nog een risico geaccepteerd worden als het om de gegevens van vijf personen gaat, maar als voor deze platformen een verkeerde inschatting wordt gemaakt, wordt ongeveer de hele bevolking getroffen. Ook Onderwijs & Vorming sluit dat niet uit. Het is dus aan te bevelen om niet alles in een *masterbucket* te steken die kan omvallen. De lijn van de VTC is te kijken naar wat de gevolgen zijn als het misloopt. Door alles bij eenzelfde provider te zetten wordt men zeer afhankelijk van de securitymaatregelen.

59. Bijkomend wijst de VTC er op dat ook het key-management (beheer encryptiesleutel) van AWS is en de loggings grotendeels ook. Dat er een extern (niet van de VO) key-management is, roept bijkomend vragen op bij de VTC.

60. De VTC vermoedt dat voor bijkomende use cases ook een beroep gedaan zal worden op **dezelfde leverancier**. Bovendien zal er waarschijnlijk ook een trickle down zijn naar andere overheidsdiensten als een entiteit als Onderwijs & Vorming met dergelijke leveranciers in zee gaat.

61. De VTC bepaalt niet het beleid en doet niet aan politiek, maar het is wel een zaak van de VTC **als er maar een enkele optie als valabel wordt gezien** voor de gegevensverwerking, AWS, en maar een voor de software, Snowflake.

De VTC wil zeer duidelijk stellen dat een **monocloudstrategie niet aanvaardbaar** is.

ALGEMENE STRATEGIE

Technologische evoluties

62. VTC wil liever niet de rem zijn op het implementeren van technologische verbeteringen, maar het is haar taak om te waarschuwen voor de mogelijke ongewenste gevolgen. We beseffen dat de VO/O&V geavanceerde analytics wil toepassen, maar alles naar AWS en de boodschap dat het kan nergens beter dan daar, kan niet, dus zijn een aantal richtlijnen nodig.

63. Voor de VTC is het permanent en zonder grenzen de bedoelde datasets door AWS laten hosten niet aanvaardbaar.

64. Het feit dat er geen benchmark en geen enkele verwijzing is naar andere aanbieders als HB+ (waaronder het Belgische Proximus) of het eveneens Belgische Smals, is een indicator dat de zoektocht naar een verwerker niet correct is gebeurd en mogelijk teveel onder de invloed van AWS.

65. De VTC wijst er op dat sommige entiteiten dezelfde oefening hebben gemaakt en om die reden AWS uitgesloten hebben (en Smals gekozen hebben).

66. Een evolutie in de IT-sector is dat de softwareaanbieders richting cloud duwen, terwijl er geen absolute redenen zijn om naar de cloud te gaan. Bovendien is private cloud ook een mogelijkheid.

Alternatieven

67. De alternatieven moeten gezocht worden bij Europese cloudproviders/datacenters, Belgische cloudproviders/datacenters en eigen (of gehuurde) infrastructuur (en diensten).

68. **De VTC blijft in ieder geval pleiten voor een Belgische of Europese overheidscloud**.

Beslissingsmatrix

69. De VTC gaat ervan uit dat haar antwoord op deze adviesvraag de nood aan een beslissingskader voor deze platformen en andere projecten nodig maakt. Daarom legt ze een beslissingsmatrix **voor de Vlaamse Overheid** voor, met daarin de voornaamste criteria qua risico's en maatregelen die de mogelijke hostingoplossingen duidelijk maken.

	Niet Europese leverancier*	Europese externe leverancier**	Belgische overheid	Intern Vlaamse Overheid
Grootschaligheid: veel data van veel personen (ook over projecten en beleidsdomeinen heen)	X	**Encryptie of vergelijkbare maatregel + externe controle**	Beveiliging + externe controle	Beveiliging + externe controle
Risicogevoelige personen	X	X (tenzij specifieke wetgeving)	Beveiliging + externe controle	Beveiliging + externe controle
Gegevens die een zware negatieve impact kunnen hebben	X	**Encryptie of vergelijkbare maatregel + externe controle**	Beveiliging + externe controle	Beveiliging + externe controle
Gevoelige gegevens sensu lato - niet grootschalig en - tijdelijk	**Encryptie of vergelijkbare maatregel + externe controle**	**Encryptie of vergelijkbare maatregel + externe controle**	Beveiliging + externe controle	Beveiliging + interne controle
Unieke identificatoren	X	**Encryptie of vergelijkbare maatregel + externe controle**	Beveiliging + externe controle	Beveiliging + interne controle
Andere personen/persoonsgegevens	**Encryptie of vergelijkbare maatregel + externe controle**	Beveiliging + externe controle	Beveiliging + interne controle	Beveiliging + interne controle

* - ongeacht locatie data/servers

- bedoeld worden: landen die niet voldoen aan de Europese beschermingsstandaarden

- om het eenvoudig te houden, te lezen als noch bedrijf, noch moederbedrijf is Europees.

**en locatie data/servers in Europa

Kleurcodes:

Rood = onaanvaardbaar: no go

Oranje = aanvaardbaar mits extra maatregelen die toegang leverancier (en derden) verhinderen en melding problemen aan VTC

Lichtgroen = aanvaardbaar mits normale beveiliging en externe controle

Donkergroen = aanvaardbaar mits normale beveiliging en minstens interne controle

Externe controle = niet door de verwerkingsverantwoordelijke en ook niet door zijn verwerker.

ETHISCHE DIMENSIE

Verantwoordelijke overheid

70. De VTC is er zich van bewust dat zeer grote ondernemingen al hun gegevens (buiten bedrijfsgeheimen!) in de publieke cloud zetten, ook gevoelige gegevens. Hier gaat het evenwel over de overheid en de overheid heeft andere verantwoordelijkheden en een andere verhouding met haar burgers. I.v.m. het tweede punt is een belangrijk verschil dat de overheid in de meeste gevallen niet afhankelijk is van toestemming van de burger en via wettelijke regelingen en openbaar gezag persoonsgegevens kan verwerken.

Governance mechanisme

71. De VTC beveelt wel aan dat er een (nieuw of ander) governance mechanisme wordt opgezet voor de IT-projecten van de Vlaamse Overheid dat de IT-vereisten en de gewone compliance vereisten overstijgt en een ethische dimensie toevoegt. Dit lijkt nu in belangrijke mate te ontbreken.

72. Een onafhankelijk ethisch comité kan zich buigen over de grote lijnen, maar ook over deelaspecten als de beoordeling van een informatieclassificatie (zodat niet alles in categorie 3 terechtkomt). Voor de huidige adviesvraag is dan bijvoorbeeld het probleem aan de orde dat er verschillende verwerkingen zijn, waarbij elke nieuwe het risico nog groter maakt.

73. In principe zouden de DPO's hier een belangrijke rol moeten spelen. De VTC vraagt dat ze dat ook doen, maar heeft recent meerder signalen gekregen dat hun onafhankelijkheid onvoldoende gegarandeerd is. (https://overheid.vlaanderen.be/digitale-overheid/data-protection-officer-dpo/onafhankelijkheid-van-de-dpo). Wat dit dossier betreft, verwijst de VTC naar de opmerkingen bij de DPIA (die geen DPIA is).

CONCLUSIE

74. De VTC adviseert het volgende op de belangrijkste punten:

- de beslissingsmatrix van de VTC moet gevolgd worden;

- een monocloudstrategie is niet aanvaardbaar;

- voor wat de beleidsdatabank betreft, is pseudonimisering vóór verwerking op een (aanvaardbaar) dataplatform een basisvereiste; door de hoeveelheid gegeven is identificatie altijd opnieuw mogelijk zolang er niet volop ingezet wordt op anonimisering, aggregatie en andere gelijkwaardige maatregelen;

- de exit-strategie moet aangepast worden;

- encryptie moet extern geaudit worden conform de beslissingsmatrix;

- de ethische dimensie moet structureel opgenomen worden.

75. Aangezien wat AWS en Snowflake betreft, volgens het Hof van Justitie bewezen is dat het niveau van bescherming niet voldoet voor bedrijven die onder de wetgeving van de Verenigde Staten vallen, is dus het laten hosten van platformen als dat van de beleidsdatabank van O&V, niet toegelaten.

76. De VTC vraagt dat haar tegen 30 oktober 2020 een overzicht wordt gegeven van alle datavelden van alle toepassingen/databestanden die al door AWS gehost worden en van die die men plant te migreren.

WAARSCHUWING

77. **Overeenkomstig artikel 58, a), AVG, spreekt de VTC een waarschuwing uit tegenover de verwerkingsverantwoordelijken van de Vlaamse instanties**:

> Het overdragen van veel persoonsgegevens van veel personen (ook over projecten heen) aan eenzelfde niet-Europese cloudprovider, terwijl niet bewezen is dat de gegevensbescherming van het land van de ontvanger van de gegevens vergelijkbaar is met de Europese, is niet conform de principes en bepalingen van de AVG, in het bijzonder het proportionaliteits- en vertrouwelijkheidsbeginsel en dus verboden.

Hans Graux,

Voorzitter VTC