Vlaamse overheid

Vlaamse Toezichtcommissie voor de verwerking van persoonsgegevens

Advies VTC nr. 2019/04 en 05 van 3 december 2019

betreffende

Veiligheidsmaatregelen tegen ongeoorloofde toegang tot persoonsgegevens door het Facilitair Bedrijf (FB) voor Microsoft Azure en Microsoft PowerApps

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;

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, 3;

Gelet op het verzoek om advies van het agentschap Facilitair Bedrijf (verder: FB), ontvangen per mail door de VTC op 24 mei 2019.

Brengt op 3 december 2019 het volgend advies uit:

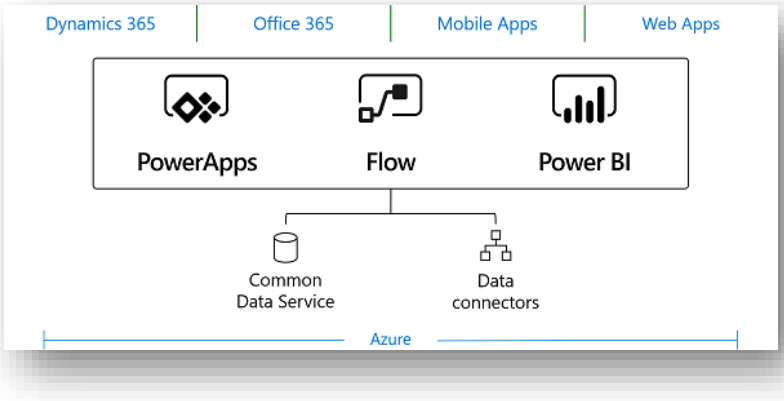
I. VOORWERP VAN DE ADVIESAANVRAAG

1. De adviesvragen van het agentschap Facilitair Bedrijf betreffen twee cloudgebaseerde toepassingen:

- Adviesvraag VTC/A/2019/04 : "Het FB wenst voor de uitbreiding van zijn HB+[1] dienstenaanbod op Microsoft Azure cloud services een overzicht van de genomen veiligheidsmaatregelen met het oog op ongeautoriseerde toegang tot de gegevens te komen voorstellen. Deze maatregelen zijn gebaseerd op de afspraken die we gemaakt hebben bij de invoering van de Vo informatieclassificatie en zijn functioneel vergelijkbaar met het positieve advies die we hebben gekregen in context van het HB+ dienstenaanbod op Amazon cloud services (AWS)."

- VTC/A/2019/05 : "WVG[2] wenst voor een specifieke informatieverwerking beroep te doen op een Microsoft SaaS aanbod (PowerApps) en wenst een advies over de voorgestelde oplossing. Conform de Vo informatieclassificatie heeft HFB de genomen veiligheidsmaatregelen geëvalueerd en wenst zijn bevindingen met jullie te delen."

Volgend schema geeft ondermeer de verhouding tussen de MS Power Apps en MS Azure aan.



[1] Tijdelijke vereniging HP en Belgacom (Proximus) die als leverancier voor de Vlaamse Overheid optreedt.

[2] Het Departement Welzijn, Volksgezondheid en Gezin.

2. De MS PowerApps worden gebruikt in combinatie met Microsoft Azure en Microsoft O365. Voor Microsoft Azure wordt de encryptieproblematiek hier behandeld, voor O365 werden er aan de VTC apart vragen gesteld door andere instanties over de *metering*problematiek die hier niet besproken worden maar ook relevant zijn.[3]"

3. De adviesvraag betreft de ongeautoriseerde toegang tot informatie en encryptiesleutels en de controle en toezicht die/dat op deze toegang wordt uitgeoefend. Ze betreft ook de door het FB voorgestelde maatregelen. Het FB presenteerde zowel technische maatregelen op basis van de gebruikte architectuur als de organisatorische maatregelen (zoals de principes van het sleutelbeheer). De VTC kreeg een toelichting van de gebruikte encryptietechnieken toegelicht, inclusief het daarbij horende sleutelbeheer. Daarnaast wordt het gebruikersbeheer en de toegangscontrole verduidelijkt. Tijdens een volgende zitting maakte het VTC kennis met het beheer van geprivilegieerde toegangen (PAM)[4]. Tot slot werd het gebruikte monitoring systeem (SIEM[5]) toegelicht.

4. De VTC wijst er op dat de voorgestelde (technische en organisatorische) maatregelen enkel zijn beoordeeld vanuit het principe van 'ongeoorloofde toegang'. De risico's bij een cloud omgeving beperken zich uiteraard niet enkel tot dit thema.

5. Daarnaast wijst het VTC er op dat enkel de architectuur van het cloud platform is toegelicht en niet de concrete toepassingen die op het platform zal worden geïnstalleerd en gebruikt. De VTC heeft kennis genomen van de voorgestelde architectuur en de organisatorische maatregelen om deze te borgen (waaronder sleutelbeheer). De VTC heeft hier (slechts) ontwerpen en onderdelen van gezien. Het uitgangspunt is dat het in ieder geval gaat om persoonsgegevens en dat die in principe integer en vertrouwelijk moeten behandeld worden en waarvoor maatregelen inzake continuïteit moeten worden voorzien

6. Een belangrijk deel van de risico's bevinden zich op niveau van de concrete toepassing. Daarom is het belangrijk dat elke toepassing individueel wordt onderworpen aan een risico-evaluatie. Hierbij moet steeds ook (maar dus niet uitsluitend) de interactie van de applicatie met het onderliggende platform worden bekeken. Met andere woorden:

---

[3] De VTC stelt vast dat met het gebruik van MS Power Apps via het beroep doen op het Common Data Model ook metering gebeurt volgens de privacyverklaring: "*Met Common Data Model van Microsoft PowerApps worden aangepaste entiteits- en veldnamen in onze diagnostische systemen verzameld en bewaard*". (cf. Privacyverklaring).

[4] Priviledged Access Management of Privileged Accountmanagement betreft typisch de toegang van personen met een administrator account:
"*Privileged Account Management (kortweg PAM) heeft tot doel de geprivilegieerde toegang tot systemen te regelen en te controleren en maakt deel uit van het arsenaal aan tools beschikbaar voor security governance*."
https://www.smalsresearch.be/download/research_reports/management_summary/Privileged%20Account%20Management%20(PAM).pdf

[5] Security information and event management (SIM + SEM).

de evaluatie van de risico's van het onderliggende cloud platform dienen integraal te worden meegenomen in de evaluatie van de risico's van een individuele toepassing die wordt gehost. Deze specifieke verwerkingen worden in het kader van deze adviesvragen niet aan de VTC voorgelegd, waardoor de VTC op dat punt een voorbehoud maakt.

7. De VTC wijst er ook op dat de toepassingen/platformen die nu worden voorgelegd (MS Azure, MS Power Apps en hier impliciet Microsoft O365), onderling verschillen en dus ook de vereiste beveiligingsmaatregelen.

8. De voorgestelde maatregelen houden rekening met het informatieclassificatiemodel[6] dat het Stuurorgaan Vlaams Informatie- en ICT Beleid heeft goedgekeurd.

9. Een ander voorbehoud betreft de motivering van de noodzaak van cloudgebruik. Over de noodzaak van het (publieke of semi-publieke) cloudgebruik (de Vlaamse Overheid zou een "*cloud first*"-strategie volgen) kunnen vragen worden gesteld, maar die komen in deze adviesvragen ook niet aan bod.

10. Aangezien de adviesbevoegdheid van de VTC op grond van artikel 10/4, § 1 van het e-govdecreet betrekking heeft op de verwerkingen van persoonsgegevens, is haar adviesverlening hiertoe beperkt.

II. ONDERZOEK VAN DE ADVIESAANVRAAG

A. Principes

11. 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.

12. De verwerkingsverantwoordelijke, dus elke entiteit van de Vlaamse overheid, moet erop toezien dat voormelde veiligheidsmaatregelen altijd worden nageleefd.

13. De VTC herhaalt de **voornaamste principes** uit haar aanbevelingen en adviezen:
- als er geen redelijke zekerheid is dat niemand anders aan de persoonsgegevens kan of als er geen redelijke zekerheid is dat de persoonsgegevens niet kunnen verloren gaan, mogen de gegevens niet aan die verwerker kunnen toevertrouwd worden;
- wanneer een niet-Europese verwerker wordt gekozen, moeten extra maatregelen worden genomen.

[6] https://overheid.vlaanderen.be/informatieclassificatiemodel

14. De adviezen die de VTC al heeft verleend waren **voorwaardelijk** gunstig: ze waren afhankelijk van uitdrukkelijk gestelde contractuele, technische en organisatorisch voorwaarden en een schriftelijk engagement van de verwerker en de verantwoordelijke voor de verwerking.

15. Een belangrijke technische (en organisatorische) voorwaarde is **encryptie** met de encryptiesleutel bij de Vlaamse Overheid zelf. De voorliggende adviesvragen betreffen enkel of voornamelijk deze component. De maatregelen zoals gebruikersbeheer, toegangscontrole en log management worden niet verder in detail besproken maar maken wel deel uit van de architectuur.

16. De verstrekte informatie aan de VTC, met name de architectuur en beleidsprincipes voor encryptie, beschrijft de maatregelen die worden genomen met het oog op ongeoorloofde toegang. Om in te schatten of de genomen maatregelen volstaan, is het evenwel belangrijk om de kwetsbaarheden, hun impact en frequentie te benoemen en in te schatten met welke **restrisico's** moet worden rekening gehouden, evenals de inschatting van deze restrisico's (i.e. risicoanalyse).

17. De verwerkingsverantwoordelijken die gebruikt maken van de aangeboden cloud oplossing dienen de restrisico's te evalueren in relatie met de verwerkingsactiviteiten die zullen worden aangeboden. Een oplijsting van deze restrisico's is met andere woorden noodzakelijk.

18. Op basis van de verstrekte informatie heeft de VTC zelf enkele mogelijke kwetsbaarheden benoemd en risico's ingeschat (zie verder), maar ze heeft aangedrongen op het verder uitwerken van de risicoanalyse door het Facilitair bedrijf[7]. De VTC wijst er op dat met de AVG *accountability* en risicobenadering belangrijker zijn geworden.

19. FB heeft maatregelen gepresenteerd op basis van de risico's die ze koppelt aan het informatieclassificatiemodel. Hierdoor werden aanvankelijk specifieke cloud gerelateerde risico's niet benoemd. De VTC wijst er op dat de risico's die gekoppeld worden aan de informatieclassificatie niet noodzakelijk dezelfde zijn als de risico's gerelateerd aan de gehanteerde techniek (in dit geval hosting in een cloudomgeving). De VTC heeft bijgevolg zelf enkele cloud specifieke risico's opgesomd, zonder hierbij volledig te (willen) zijn[8]. Ze heeft die voor commentaar aan het FB bezorgd. Het Facilitair Bedrijf heeft op 21 november 2019 informeel opmerkingen bij die tekst gegeven (maar nog niet de uitgewerkte risicoanalyse[9]).

---

[7] De VTC had een risicoanalyse gevraagd aan het FB, maar tot de zitting van december enkel een overzicht van de acties en maatregelen ontvangen (en de communicatie met de VTC).

[8] Zo heeft de VTC bijvoorbeeld niet gesproken over de contractuele risico's. De risico's bij het afsluiten van een contract voor een applicatie in de cloud zijn nu eenmaal anders dan bij een on-premise applicatie. Denk bijvoorbeeld aan continuïteit. Deze risico's kwamen niet aan bod.

[9] De VTC heeft alleen een algemeen overzicht van de risico's voor cloudcomputing ontvangen en geen dat specifiek de hier bedoelde verwerker betreft. Dit is een bewuste keuze van het Facilitair Bedrijf, maar maakt het moeilijk om de concrete verwerker te beoordelen voor de verantwoordelijke en de toezichthouder.

20. Het Facilitair Bedrijf heeft op de zitting van de VTC van 3 december 2019 een nieuwe presentatie gegeven die meer informatie gaf m.b.t. de risico's voor en na maatregelen. Het heeft daarbij uitgebreid stilgestaan bij het Priviledged Access Management (PAM) bij het gebruik van de encryptiesleutels en de toegang tot de cloudomgeving.

21. De VTC benadrukt dat het restrisico dynamisch is en bijgevolg steeds onderwerp is van een **permanente her-evaluatie**. Het is belangrijk dat het Facilitair Bedrijf elke wijziging in het restrisico kenbaar maakt aan de verwerkingsverantwoordelijken.

22. De VTC wijst er op dat er naast encryptie ook de (nog niet door de VTC gevalideerde) mogelijkheid bestaat om de toegang tot de data toe te vertrouwen aan een Europese *trusted third party* zoals de opzet was met MS Cloud Germany (voor bepaalde datacenters).

B. Te beoordelen maatregel: encryptiemodule Facilitair Bedrijf voor Microsoft Azure

a) Het risico

23. Het risico dat moet beperkt worden, is dus de toegang van en via (voor derden zoals de Amerikaanse Overheid) de verwerker, cloudprovider Microsoft, tot de data van burgers ("betrokkenen" genoemd in de AVG) waarvan gegevens in toepassingen van de Vlaamse Overheid zijn opgenomen. Het betreft de vraag of er voldoende bescherming is tegen

    - punctuele opvragingen via gerechtelijke procedures;
    - het massaal screenen van de data (buiten gerechtelijke procedure) door de inlichtingendiensten.

b) Encryptie technisch

24. De beoogde maatregel betreft encryptie *at rest*. De VTC merkt op dat wat de vereisten inzake het sleutelbeheer betreft, er om redenen van betaalbaarheid (en daarmee samengaande implementatiebereidheid) niet voor een *'dedicated' Hardware Security Module* (HSM) wordt gekozen, maar een *shared Hardware Security Module* (HSM) van het sleutelmateriaal. Dit is begrijpelijk maar dus niet optimaal.

25. Op vraag van de VTC erkent het Facilitair Bedrijf dat de onmogelijkheid van de inzet van *dedicated HSM's* in elk use-case scenario een tekortkoming is van de Azure architectuur.

26. Positief is dat de meeste realisaties onmiddellijk zullen kunnen gebruik maken van een geoptimaliseerd aanbod.

c) Encryptie organisatorisch

27. Er zijn beheersmaatregelen voor *key management* beschreven. Dit is een belangrijk item en het VTC beveelt aan voldoende audit en controle uit te voeren op dit aspect. De nodige systeemcomponenten hiervoor zijn voorzien in de

architectuur. Het beheer van geprivilegieerde toegangen (PAM – Privileged access management) worden hieronder gerekend.

d) Proof of concept

28. Er werd een POC uitgevoerd: het Facilitair Bedrijf deelde mee dat alle technische componenten werden voltooid zoals het had voorgesteld in zijn referentiearchitectuur voor de Microsoftomgeving.

29. De VTC merkt op dat de POC natuurlijk niet geldt voor de punten die nog niet door Microsoft worden aangeboden. Niet alle maatregelen die in de architectuur zijn voorzien, waren reeds beschikbaar in productie (bijvoorbeeld Storage Encryption for Managed disks, gebruik makende van Customer keys).

e) Beoordeling encryptie

30. De VTC is dus (zie hiervoor) van oordeel dat het gaat om een **goede architectuur**.

31. De VTC is van oordeel dat de het risico van het massaal screenen van de data door het correct inzetten van encyrptie en PAM wel beperkt wordt, maar dat de toegang tot (specifieke) data niet is uitgesloten.

32. Het Facilitair bedrijf heeft het best mogelijke gedaan, maar dergelijke risico's blijven bestaan. Dat wordt hierna nog eens verduidelijkt.

f) Restrisico's

33. De risico's op technisch niveau werden maximaal behandeld door gebruik te maken van een goede architectuur. Deze architectuur maakt gebruik van alle (op dit moment) voor handen zijnde technische componenten (deze technische componenten zijn trouwens leverancier afhankelijk)[10].

34. De restrisico's liggen voornamelijk op niveau van de organisatorische maatregelen (zie hierna). Hierbij is het belangrijk dat alle actoren (met name zowel de verwerkers, als bij de verwerkingsverantwoordelijken, de Vlaamse bestuursinstanties) op een correcte manier omgaan met de organisatorische maatregelen. Hier hebben de Vlaamse bestuursinstanties zeker nog een impact op.

35. Het Facilitair Bedrijf wijst er op dat conform de RACI afspraken binnen het classificatie model de restrisico's geïdentificeerd moeten worden door de opdrachtgever. Dit lijkt de VTC niet correct. De opdrachtgevers, waaronder

[10] Er zijn bijvoorbeeld verschillen tussen Amazon Web Services en Microsoft Azure.

mogelijk ook zeer kleine entiteiten, zijn in deze in belangrijke mate afhankelijk van de informatie die de verwerker en het Facilitair Bedrijf aanbieden. Ze kunnen wel eisen dat ze correcte informatie over het restrisico krijgen en over eventuele verdere maatregelen en alternatieven.

36. Volgens het Facilitair Bedrijf zijn de restrisico's meestal te vinden bij de toepassingen zelf en niet bij het feit dat ze in een cloud draaien. De VTC heeft in haar adviezen en aanbevelingen de risico's niet beperkt tot cloud, maar ook gesteld voor het verwerken in datacenters (in Europa) beheerd door firma's die door de Amerikaanse overheid als vallende onder de Amerikaanse wetgeving worden beschouwd (zonder andere niet-Europese verwerkers als betrouwbaar te beschouwen).

37. Het Facilitair Bedrijf stelt dat datacenters *on premise* op zich minstens even grote veiligheidsrisco's vertonen omdat er meestal een beperktere inzet van maatregelen is wegens de hogere kostprijs. De VTC wijst er op dat de massale screening van data in Amerikaanse (en mogelijk andere niet-Europese) cloudomgevingen een specifiek probleem is (en gerelateerd aan de Amerikaanse wetgeving daaromtrent). De risico's zijn qua aard niet vergelijkbaar, waardoor het moeilijk te zeggen dat ze dan groter of kleiner zijn.

38. FB heeft aangegeven dat volgens haar de restrisico's bij de toepassing van PAM bestaan uit:

    - de personen die elkaar controleren bij de toepassing van het 4-eyes principe gaan "samenzweren";
    - het technisch fouten in de administratie bij het toekennen van autorisaties niet uit te sluiten zijn. Dit kan enkel op organisatorische basis bewaakt worden;
    - in het algemeen processen die niet worden gevolgd.

39. Hierna beschrijft de VTC enkele risico's de het Facilitair Bedrijf niet aanhaalt:

40. Er is ook nog het theoretisch risico dat Microsoft aan de sleutels kan, onder meer door impersonalisatie (bijvoorbeeld op Active Directory). In literatuur worden bijvoorbeeld (ook) scenario's beschreven waarbij een werknemer van bijvoorbeeld Microsoft, geprivilegieerde toegang heeft tot de onderliggende componenten van de cloud omgeving en kan die de PAM alsnog omzeilen Dit risico werd niet besproken. Er is een 'veronderstelling' gemaakt dat de encryptie-maatregelen dit wel zullen oplossen, maar dat brengt dit risico niet naar nul.

41. De VTC duidt als restrisico ook de mogelijkheid aan van toegang tot data *in use* . Het Facilitair Bedrijf doet dit af als illegale praktijken die nooit uit te sluiten zijn, maar de VTC wil dit toch onder de aandacht van de verwerkingsverantwoordelijkenbrengen.

42. In verband met het restrisico van de gedecrypteerde data *in use*, stelt het Facilitair Bedrijf terecht dat maatregelen (nog) niet implementeerbaar zijn wegens redenen van financiële haalbaarheid en technologische beschikbaarheid[11]. Anderzijds blijft het een restrisico dat moet opgegeven en in overweging genomen worden. De VTC geeft hiervoor al een aanzet:

43. Het is niet zeker dat als Microsoft de sleutels niet heeft (omdat ze vanuit een *on premise HSM* beheerd door de Vlaamse overheid telkens worden geüploaded naar de OneDrive cloud) men geen andere middelen heeft om toegang tot de data te geven om de Amerikaanse overheid tegemoet te komen.

44. Uiteindelijk worden de gegevens tijdens de verwerking in in *plaintext* ingeladen in de servers van Microsoft: RAM, cache, swap. Dus de gegevens kunnen al minstens daar (hardwarematig) geïntercepteerd worden zonder sporen (tenzij men heel dure fraudebestendige servers zou gebruiken).

45. Dus, tenzij alles geëncrypteerd is en de sleutels volledig in handen blijven van de Vlaamse Overheid (dus ook niet tijdelijk in de cloud voor de bewerkingen), is het altijd mogelijk dat je *cloud provider* de gegevens kan lezen, omdat ze dan niet geëncrypteerd zijn.

46. Deze oplossing met Customer Key blijft een kwestie van vertrouwen in Microsoft en wat het bedrijf op papier wil beloven. Hetzelfde probleem stelt zich ook bij andere cloud providers.

47. Het is niet omdat het Facilitair Bedrijf en de verwerker hier geen antwoord op hebben, dat deze risico's niet moet bekeken worden, specifiek wanneer het gebruik van deze architectuur voor een bepaalde *use case* wordt overwogen.

III. BESLUIT

48. De VTC is van oordeel dat de encryptiemodule – mits correct geïmplementeerd en beheerd – het risico van het massaal data inhalen van de burger op redelijke wijze beperkt.

49. Anderzijds blijven er nog restrisico's bestaan zoals beschreven.

50. Daarom adviseert de VTC om de voorgestelde cloudtoepassingen (tenzij er toch sluitende maatregelen worden geïmplementeerd) niet aan te wenden voor bepaalde categorieën van informatie: strategische geheime informatie

[11] "1. Er zijn geen DIU standaarden, er is dus geen uitwisseling mogelijk tussen producten van verschillende leveranciers. 2. Er is geen garantie op lange termijn van beschikbaarheid van toegepaste technologie."(uit reactie Facilitair Bedrijf).

(op zich geen bevoegdheid van de VTC) en informatie die een groot risico kan vormen voor de betrokkenen: 'gevoelige' informatie, profilerende informatie, informatie over kwetsbare personen,…

51. Het is dus positief dat de maatregelen er zijn, maar de VTC heeft zeker ook bedenkingen. Voor de restrisico's moeten de instanties de inschatting doen, met name een *risk assessment* per type verwerking.

52. Er moet daarbij minstens rekening gehouden worden met:

– de gevoeligheid van de informatie;
– het doel van de verwerking;
– de technologie;
– richtlijnen van andere toezichthouders;
– sectorspecifieke richtlijnen.

53. Aanvullend herhaalt de VTC dat de applicaties en de nodige maatregelen ook kunnen wijzigen in de tijd en dat bijgevolg ook uitspraken daarover beperkt moeten zijn in de tijd.

Hans Graux

Voorzitter