Vlaamse overheid

Vlaamse Toezichtcommissie voor het elektronische bestuurlijke gegevensverkeer

Boudewijnlaan 30, bus 47, 1000 Brussel

aan de, algemeen directeur van het agentschap Binnenlands Bestuur

aan de algemeen directeur van het Agentschap Integratie en Inburgering

PER MAIL

uw bericht van	**uw kenmerk**	**ons kenmerk**	**bijlagen**
22 maart 2016		VTC/A/2016/03/2	/
vragen naar / e-mail	**telefoonnummer**	**datum**	

Betreft: uw vraag om advies in verband met het insourcen van persoonsgegevens in de Virtual Private Cloud van de Vlaamse overheid – aanvullend advies

Geachte mevrouw, geachte heer,

Ik verwijs naar het vorige negatieve advies van de VTC van 22 maart 2016 en de conclusies (in cursief hieronder) van de zitting van de VTC van 25 mei 2016, die werden bezorgd per mail van 26 mei 2016 aan de informatieveiligheidsconsulent van de KBI (verder aangeduid als “veiligheidsconsulent”). De VTC verwijst naar de voorgaande mails die ze gestuurd heeft aan ABB (op 24 december 2015 en 19 februari 2016) en naar de documentatie die de veiligheidsconsulent aan de VTC bezorgd heeft en die in het bijzonder alle mitigerende maatregelen inhoudt.

Voor een goede lezing wordt eerst de probleemstelling hernomen: de vraag komt erop neer of de gegevens van inburgeraars, dus persoonsgegevens, in een datacenter, concreet het VPC, mogen geplaatst worden dat eigendom is van een bedrijf dat duidelijk banden heeft met een Amerikaans bedrijf (HPE US) en beheerd wordt door dat bedrijf.

Concreet wat de vraag van ABB betreft, werd door de VTC gesteld dat als er geen zekerheid is dat niemand anders aan de persoonsgegevens van de inburgeraars kan en als er geen zekerheid is dat de persoonsgegevens niet kunnen verloren gaan, de gegevens niet aan die verwerker kunnen toevertrouwd worden.

De VTC geeft haar advies op basis van een reeks elementen, waaronder:

- het feit dat de data door een Europees bedrijf (HP Belgium) en in Europa (hoofdzakelijk België) worden verwerkt door Europese werknemers;
- het resultaat van de cloudevaluatie door ABB op basis van het model van SMALS;
- de uitgebreide analyse door de veiligheidsconsulent van de beveiliging inzake externe toegang;
- het uitgewerkte plan van aanpak zowel wat de eenmalige overdracht als de verdere verwerking betreft;
- de procedure die gevolgd moet worden bij een gerechtelijk bevel via de Belgische overheid;
- het uitdrukkelijke schriftelijke engagement van de verwerker (HP Belgium) om geen persoonsgegevens door te geven aan het Amerikaanse moederbedrijf/de Amerikaanse overheid zonder toestemming van de verantwoordelijke voor de verwerking;
- de contractuele voorwaarden, waaronder het verbod om de persoonsgegevens door te geven en een exitstrategie;
- de organisatorische maatregelen, waaronder functiescheiding en sleutelbeheer;
- de technische maatregelen, waaronder implementatie van een systeem dat de toepassing van het least privileged principe afdwingt, logging van gebruikers en beheerders, encryptie van de data in rust en in transit.

Hierna worden de overgebleven knelpunten conform de conclusies van de VTC van 25 mei 2016 weergegeven zoals besproken op de zitting van de VTC van 22 juni 2016:

A. *De VTC vindt de analyse door de veiligheidsconsulent degelijk*.

De algemeen directeur van ABB heeft per mail van 14 juni 2016 de analyse en de voorgestelde maatregelen goedgekeurd.

B. *CyberArk wordt met de toepassing van het least privileged principe en logging als goede methodologie beschouwd. De VTC adviseert dit gunstig. (Beheer van logging door (ander team van) HP blijft risico).*

Dit wordt bij deze nog eens bevestigd door de VTC. Ze wijst er wel op dat deze tool ook correct moet geïmplementeerd worden.

C. *Er zijn nog vragen in verband met de modaliteiten van de encryptie. Hiervoor kan nog geen advies worden gegeven.*

De VTC heeft vastgesteld (in de brief van HP Belgium van 17 juni 2016 aan de leidend ambtenaar van het Facilitair Bedrijf, dat verantwoordelijk is voor het VPC) dat encryptie door de verwerker HP Belgium zelf, naast contractuele voorwaarden die de overdracht verbieden, als voorwaarde wordt gesteld om te kunnen garanderen dat HP Belgium geen persoonsgegevens zal doorgeven aan de Amerikaanse overheid via het Amerikaanse moederbedrijf. Dit lijkt tegemoet te komen aan de opmerkingen van de VTC. Volgens de VTC moet de verwerker er inderdaad voor zorgen dat er technische maatregelen worden genomen om die doorgave onmogelijk te maken. Dit is een verplichting van de verwerker zelf die dan ook niet de verantwoordelijke voor de verwerking, in casu de Vlaamse Overheid, ten laste zou mogen komen.
De VTC merkt op dat er nog geen duidelijkheid is over de geplande naleving van de eis om regelmatig opnieuw te encrypteren. Ze stelt anderzijds vast dat ook HP Belgium het essentieel vindt dat de encryptiesleutel zich bij de Vlaamse Overheid zelf bevindt (bij het Facilitair Bedrijf).

D. *Een aantal procedures moeten nog verder uitgetekend worden zodat er nu nog geen volledig beeld is.*

De VTC vertrouwt erop dat dit alsnog gebeurt onder het toezicht van de verantwoordelijke voor de verwerking en diens veiligheidsconsulent. Zij wijst op het belang van het correct uitvoeren van de geplande dataclassificatie.

E. *Volgende informatie wordt opgevraagd:*

a. *I.k.v. encryptieoplossing: wat is de omgeving waarop de applicatie draait? (antwoord bezorgd door de veiligheidsconsulent op 26/05/2016)*

b. *De evaluatie door de verantwoordelijke van de verwerking (20/05 gevraagd, nog niet ontvangen)*

Zie onder A. De uiteindelijke beslissing door de verantwoordelijken voor de verwerking moet nog genomen worden (zie ook verder).

c. *Brief HP 5 februari 2014 naar minister-president. Schriftelijke bevestiging nodig van HP dat dit ook de vervangende en aanvullende wetgeving dekt (FISAA, Freedom Act,…)*

De VTC heeft de brief met dit engagement ontvangen op 21 juni 2016. Het engagement is voorwaardelijk geformuleerd (zie onder C).

d. *De VTC stelt scheiding van 3 functies als best practice: beheerder structuur van de database, beheerder toegangsrechten en mensen die encryptiesleutels parametriseren. Akkoord van de drie nodig voor toegang tot data. Is in dergelijke functiescheiding voorzien?*

De VTC heeft kennis genomen van de geplande functiescheiding via de nota opgesteld door de veiligheidsconsulent vermeld hieronder.

e. *Een samenvattende nota/overzicht voor niet-technici.*

Deze nota werd door de veiligheidsconsulent aan de VTC bezorgd op 17 juni 2016.

De VTC is van oordeel dat er belangrijke stappen gezet werden naar een veilige verwerking.

Op grond van artikel 16 van de Wet Verwerking Persoonsgegevens moet de verantwoordelijke voor de verwerking een verwerker kiezen die voldoende waarborgen biedt.[1]
De VTC benadrukt dat de verantwoordelijken voor de verwerking, met name de leidinggevenden van het Agentschap Binnenlands Bestuur en het Agentschap Integratie en Inburgering, dus verantwoordelijk zijn voor de keuze van de verwerkers-beheerders van de KBI en dat zij er over moeten waken dat de nodige maatregelen ter bescherming van de persoonsgegevens worden genomen en permanent onderhouden of aangepast. Het komt er voor de verantwoordelijken voor de verwerking dus op aan om op basis van alle beschikbare informatie te beslissen of de gevraagde zekerheid (zie inleidende paragrafen) er is.

[1] **"Art. 16.** § 1. Indien de verwerking wordt toevertrouwd aan een verwerker, moet de verantwoordelijke voor de verwerking, en in voorkomend geval zijn vertegenwoordiger in België :
1° een verwerker kiezen die voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerking;
3° de aansprakelijkheid van de verwerker ten aanzien van de verantwoordelijke voor de verwerking vaststellen in de overeenkomst;"

De VTC gaat ervan uit dat indien er voor andere toepassingen en databanken met persoonsgegevens van de Vlaamse Overheid voor de VPC/HP zou gekozen worden, minstens de voor dit dossier gestelde voorwaarden zullen worden nageleefd (contractueel, technisch, organisatorisch en engagement verwerker en verantwoordelijke voor de verwerking).

Met de meeste hoogachting,

Willem Debeuckelaere
Voorzitter Vlaamse Toezichtcommissie

cc de administrateur-generaal van het Facilitair Bedrijf