Vlaamse overheid

aan de leidend ambtenaren van de departementen en agentschappen van de Vlaamse Overheid

Vlaamse Toezichtcommissie voor het elektronische bestuurlijke gegevensverkeer

Boudewijnlaan 30, bus 47, 1000 Brussel
Tel. 02 553 50 47

PER MAIL

uw bericht van	**uw kenmerk**	**ons kenmerk**	**bijlagen**
/	/	VTC/AB/2016/01	/

vragen naar / e-mail	**telefoonnummer**	**datum**
	02 553 20 85	

toezichtcommissie@vlaanderen.be

Betreft: Aanbeveling betreffende het beheer van persoonsgegevens in een datacenter door een niet-Europese firma.

Geachte mevrouw, geachte heer,

Hierbij vindt u de aanbeveling van de Vlaamse Toezichtcommissie (VTC) zoals besproken op de zitting van 12 oktober 2016.

Inleiding

De VTC heeft op 29 juni 2016 een advies verleend aan het agentschap Binnenlands Bestuur en het agentschap Integratie en Inburgering inzake het “insourcen van persoonsgegevens in de Virtual Private Cloud (VPC) van de Vlaamse Overheid”.
Doordat de Vlaamse Toezichtcommissie heeft vastgesteld dat dit advies ongenuanceerd wordt voorgesteld als een “gunstig advies voor het VPC”, heeft zij besloten deze aanbeveling te schrijven zodat duidelijk wordt welke criteria gehanteerd worden.

Deze aanbeveling omvat richtlijnen voor contracten met verwerkers (IT-bedrijven), zowel voor cloud als voor niet-cloudtoepassingen.

Op grond van artikel 16 van de Wet Verwerking Persoonsgegevens (privacywet) moet de verantwoordelijke voor de verwerking een verwerker kiezen die voldoende waarborgen biedt.[1]
De VTC benadrukt dat de verantwoordelijken voor de verwerking[2], met name de leidinggevenden van de betrokken Vlaamse instanties, verantwoordelijk zijn voor de keuze van de verwerkers en dat zij er over moeten waken dat de nodige maatregelen ter bescherming van de persoonsgegevens worden genomen en permanent onderhouden of aangepast.

Aan de vermelde adviesvraag gingen een aantal gesprekken en vragen en antwoorden vooraf.
Daarbij werden al een aantal (niet limitatieve) eisen meegegeven waaraan een (cloud)verwerkerscontract inzake persoonsgegevens moet voldoen:

- zekerheid over de beschikbaarheid: dat je te allen tijde toegang hebt tot de gegevens; dat de data niet kwijt kunnen geraken;
- zekerheid over de beveiliging: dat de data niet geconsulteerd worden door een derde of de cloudaanbieder zelf; dat de encryptiesleutel niet in handen is van de cloudaanbieder;
- zekerheid dat de data kunnen gerecupereerd worden bij het stopzetten van de dienst/ het beëindigen van het contract; een exitstrategie die getest wordt;
- de mogelijkheid van een onafhankelijke audit;
- garanties inzake integriteit van de gegevens;
- transparantie;
- uitgewerkte incidentregeling;
- een voldoende scheiding van data van andere klanten.

Het probleem is dat de meeste cloudproviders of andere externe verwerkers deze principes niet (volledig) kunnen of willen garanderen.

De VTC benadrukt dat een dergelijk dossier aandacht en een weloverwogen beoordeling vraagt. Wanneer een niet-Europese verwerker wordt gekozen, moeten extra maatregelen worden genomen.

Probleemstelling:
De kernvraag is**: mogen persoonsgegevens** (in casus ging het om de gegevens van inburgeraars), **in een datacenter**, concreet het VPC, **geplaatst worden dat eigendom is van een bedrijf dat duidelijk banden heeft met een Amerikaans bedrijf** (HPE US) **en beheerd wordt door dat bedrijf?**
Achtergrond bij die vraag waren de onthullingen van Edward Snowden en de problemen met de Safe Harbour overeenkomst tussen de Europese Commissie en de VS en de opvolger ervan, de Privacy Shield overeenkomst.

[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;" Dit principe wordt overgenomen in de nieuwe Algemene Verordening Gegevensbescherming van 25 mei 2016 (GDPR, artikel 32).
[2] De verantwoordelijke voor de verwerking is de Vlaamse instantie die verantwoordelijk is voor de door haar verzamelde gegevens.

Principe
Door de VTC wordt gesteld dat **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, de gegevens niet aan die verwerker kunnen toevertrouwd worden**.

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 er is.

Toepassing
De VTC heeft haar advies gegeven op basis van een reeks elementen, waaronder de belangrijkste hierna worden vermeld. Sommige van deze elementen kunnen voor alle verwerkersrelaties van belang zijn, andere zijn specifiek voor het VPC beheerd door HP Belgium en weer andere moeten per toepassing bekeken worden:

- 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 de veiligheidsconsulent op basis van het model van SMALS[3];
- 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;
- goedkeuring van de analyse en de voorgestelde maatregelen door de leidinggevende van de Vlaamse instantie;
- 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 en ;(zie verder over encryptie);
- de contractuele voorwaarden, waaronder het verbod om de persoonsgegevens door te geven en een exitstrategie voor bij de beëindiging van het contract;
- de organisatorische maatregelen, waaronder functiescheiding en sleutelbeheer (bij de verantwoordelijke);
- de technische maatregelen, waaronder implementatie van een systeem dat de toepassing van het *least priviledged* principe[4] afdwingt, logging van gebruikers en beheerders, encryptie (zie verder over encryptie);
- de encryptiesleutel zich bij de Vlaamse Overheid zelf bevindt (bij het Facilitair Bedrijf voor het VPC);
- scheiding van 3 functies als *best practice*: beheerder structuur van de database, beheerder toegangsrechten en mensen die encryptiesleutels parametriseren. Er is een akkoord van de drie nodig voor toegang tot data.

In het dossier waarvan sprake waren nog enkele risicoaspecten niet helemaal afgedekt, maar deze werden in dit dossier niet als beslissend beschouwd:
– de toepassing die gebruikt zou worden voor de implementatie van het least privileged principe en logging werd als goede methodologie beschouwd, maar beheer van logging door

[3] http://vtc.corve.be/infoveiligheid.php
[4] Slechts toegang verlenen tot de data voor zover noodzakelijk voor de taak.

een ander team van dezelfde firma blijft een risico. De VTC wees er ook op dat deze tool ook correct moet geïmplementeerd worden.
- een aantal procedures moesten nog verder uitgetekend worden zodat er nog geen volledig beeld is. De VTC heeft gesteld erop te vertrouwen dat dit alsnog zou gebeuren onder het toezicht van de verantwoordelijke voor de verwerking en diens veiligheidsconsulent. Zij wees op het belang van het correct uitvoeren van de geplande dataclassificatie.
- de voorwaarden voor het engagement van de betrokken firma (zie hoger) moeten vervuld zijn. De VTC eiste een schriftelijke bevestiging van HP dat het engagement dat vroeger was gegeven in het kader van de Patriot Act ook de vervangende en aanvullende wetgeving dekt (FISAA, Freedom Act,…). De VTC heeft de brief met dit engagement voor VPC (t.a.v. het Facilitair Bedrijf) ontvangen op 21 juni 2016. Daarin werd encryptie door de verwerker (HP Belgium) zelf, naast contractuele voorwaarden die de overdracht verbieden, als voorwaarde gesteld om te kunnen garanderen dat HP Belgium geen persoonsgegevens zal doorgeven aan de Amerikaanse overheid via het Amerikaanse moederbedrijf. Het komt er dus op neer dat als er via HP ooit naar data van de Vlaamse overheid zou worden gevraagd, deze kan inbrengen dat ze er geen (leesbare) data kán leveren. 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. Het is nog niet duidelijk of de gestelde voorwaarden gerealiseerd zijn.
De VTC merkte ook op dat er nog geen duidelijkheid is over de geplande naleving van de eis om regelmatig opnieuw te encrypteren.

Besluit

De VTC gaat ervan uit dat indien er voor andere toepassingen en databanken met persoonsgegevens van de Vlaamse Overheid voor het 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).

Mutatis mutandis gelden hoger gestelde voorwaarden ook voor contracten met andere niet-Europese leveranciers.

Met de meeste hoogachting,

Willem Debeuckelaere
Voorzitter Vlaamse Toezichtcommissie

cc. de heer voorzitter van het Vlaams Parlement