Vlaamse Toezichtcommissie voor de verwerking van persoonsgegevens

Reactie van 20 oktober 2020 in verband met advies en waarschuwing VTC nr. 2020/05

De VTC heeft via diverse kanalen kennis genomen van een aantal reacties op haar recente advies Advies en waarschuwing VTC nr. 2020/05 van 8 september 2020, over informatieveiligheid en GDPR-conformiteit bij publieke cloud hosting. Veel van deze reacties wijzen er terecht op dat clouddiensten sterk beveiligd kunnen worden, inclusief bij wege van encryptiemethodes, dat er gebruik wordt gemaakt van GDPR-conforme contracten, en dat data in deze clouds niet verplaatst zullen worden uit de (Europese) regio's die gekozen worden door de klant.

De VTC stelt deze standpunten niet in vraag, integendeel: de VTC is zich wel degelijk bewust dat moderne cloud diensten state-of-the-art technologie voorzien om gegevens te beschermen. Dit vereist dan wel de implementatie van al de nodige maatregelen, zoals de volledige encryptie van de data voordat ze bij de dienstverlener worden geplaatst, en dat de encryptiesleutels volledig in eigen controle worden gehouden door de Vlaamse bestuursinstantie. **Aan deze voorwaarden werd tot nog toe niet voldaan in de betrokken dossiers:** de data zijn bijvoorbeeld niet allemaal versleuteld voordat ze bij de dienstverlener worden geplaatst, en wanneer dat wel gebeurt, dan is dat met het encryptiesysteem van de dienstverlener. Op termijn biedt deze aanpak geen afdoende garanties.

De VTC wijst er op dat het basisprobleem de hoeveelheid aan gevoelige data betreft en de aard van de verwerking in de cloud (niet enkel storage/data at rest, maar ook data in use).

De bezwaren van VTC reiken verder dan de technische aspecten alleen. Zo wijst de VTC in het advies naar het belang van een risico-analyse waarbij de risico's voor de minderjarige betrokkene, zoals het risico op profilering, voldoende in kaart wordt gebracht en dat (soms ook, maar niet uitsluitend technische) maatregelen ertoe moeten leiden dat deze risico's worden uitgesloten. Dat het in de voorgestelde casussen over een grote hoeveelheid gevoelige gegevens gaat, versterkt deze noodzaak. Naast de technische maatregelen vraagt de VTC naar de governance strategie die de risico's bewaakt en beheerst en voldoende aandacht voor bedrijfsrisico's zoals een vendor-lock in. In de betrokken dossiers zijn deze risico's niet of onvoldoende meegenomen.

Tot slot herhaalt de VTC dat een engagement van de cloud leverancier om de data niet te verplaatsen uit de gekozen regio niet sluitend is. Zelfs als de data op Europese servers blijven staan, maar beheerd door een niet-Europese dienstverlener, kan toegang en kopiëren nog steeds mogelijk gemaakt worden. Dit kan zelfs verplicht worden opgelegd aan de dienstverlener onder Amerikaans recht. Tegen dit risico kan een dienstverlener geen sluitende garanties bieden, tenzij met technische maatregelen die in de betrokken dossiers niet steeds aanwezig zijn. Om dezelfde redenen is het gebruik van Europese modelcontracten die conform de GDPR zijn ook niet voldoende: zoals ook het Europese Hof van Justitie opmerkte in zijn Schrems II-arrest, zijn de Amerikaanse autoriteiten niet gebonden door deze contractuele garanties, en biedt hun regelgeving ook voor het overige ook onvoldoende garanties om de eerbiediging van Europese gegevensbeschermingsregels sluitend te verzekeren.

De VTC zal voorstellen van de Vlaamse instanties betreffende cloud computing afwegen aan haar advies opdat ze voldoen aan AVG en voldoende veiligheidsgaranties bieden. Ze zal daarbij de evoluties in de dienstverlening volgen.

Op basis van de huidige reacties blijft het advies van de VTC dus integraal gehandhaafd.