Vlaamse overheid

Vlaamse Toezichtcommissie

voor de verwerking van persoonsgegevens

Richtlijnen voor verwerking van persoonsgegevens met algemene kantoortoepassingen in de cloud bij lokale besturen (en andere kleinere Vlaamse bestuursinstanties)

INLEIDING

De VTC heeft al verschillende adviezen en aanbevelingen uitgebracht over cloud computing of het beroep doen op Amerikaanse IT-leveranciers.[1] Naar aanleiding van haar advies VTC/A/2020/05 met daarin een matrix die aangeeft wat je als Vlaamse bestuursinstantie wel en niet mag doen in een cloudomgeving en onder welke voorwaarden, duiken er frequent vragen op naar het gebruik van het algemene kantoortoepassingen (officepakketten/bureautica) door Vlaamse bestuursinstanties en in het bijzonder lokale besturen.

De VTC wil benadrukken dat dit advies werd opgesteld voor **alle leveranciers van algemene kantoortoepassingen in een cloud-model** en dat het steeds aangewezen is om alternatieve oplossingen te bekijken (zie hierna).

Het moet ook duidelijk zijn dat dit advies het gebruik van een kantoortoepassing in de publieke cloud niet zonder meer goedkeurt. Het bestuur blijft verantwoordelijk, zowel voor de keuze van haar dienstenleveranciers als voor het correct gebruik van hun diensten, en moet een eigen afweging maken.

WAT IS HET PROBLEEM?

De bedoelde kantoortoepassingen houden in de regel in dat de gegevens **niet louter lokaal** maar in de publieke cloud worden verwerkt. Bovendien is de cloud dienstverlener meestal een **niet-Europese groep**, ongeacht de gekozen datalocatie. De leverancier kan daarbij niet sluitend en afdwingbaar garanderen dat de **Europese gegevensbeschermingseisen** steeds zullen worden gerespecteerd. Problemen kunnen zich bijvoorbeeld stellen doordat wetgeving die op de leverancier van toepassing is, zoals die van de Verenigde Staten, de overheid (in het bijzonder de inlichtingendiensten) de mogelijkheid geeft om de data die beheerd worden door deze cloud providers massaal op te vragen,

[1] https://overheid.vlaanderen.be/digitale-overheid/informatieveiligheid/vlaamse-toezichtcommissie-cloud
Een samenvatting vindt u hier: https://overheid.vlaanderen.be/vlaamse-toezichtcommissie-actueel-cloud

ook als de servers zich niet in de VS bevinden. Op die manier wordt niet alleen afbreuk gedaan aan de vertrouwelijkheid, maar ook aan het principe van proportionaliteit.

Als verwerkingsverantwoordelijke heb je bij zo'n grote speler op de markt ook zeer weinig impact op hoe die de verwerking uitvoert en welke maatregelen die neemt.

HOE GA JE HIER ALS BESTUUR MEE OM?

Artikelen 5.1.f), 24.1 en 32 van de AVG vermelden uitdrukkelijk de verplichting voor de verwerkingsverantwoordelijke om gepaste technische en organisatorische maatregelen te treffen die nodig zijn voor de bescherming van de persoonsgegevens.

De verwerkingsverantwoordelijke, dus ook elk lokaal bestuur, moet erop toezien dat de **veiligheidsmaatregelen** altijd worden nageleefd. Dit is een algemene verplichting die van toepassing is bij elke verwerking, en dus ook bij elke verwerking in de cloud. Wanneer er daarbij gekozen wordt voor een **publieke clouddienst**, dient de **lat hoger** gelegd te worden om het risico van misbruik door of via de dienstverlener te minimaliseren.

De VTC wijst er nog eens op dat de lokale besturen in de meeste gevallen niet afhankelijk zijn van toestemming van de burger en op basis van wettelijke regelingen en openbaar gezag persoonsgegevens kunnen of moeten verwerken. Dat geeft hun een **grotere verantwoordelijkheid** dan privé-organisaties.

Eerst moet er gekeken worden voor welke verwerkingen het gebruik van een publieke cloudtoepassing **wel of niet aanvaardbaar** is. Daarna moet nagegaan worden welke **maatregelen** kunnen genomen worden om de verwerking van de persoonsgegevens met de toepassing te beschermen. Het betreft dan maatregelen die ook nuttig zijn voor het voorkomen van datalekken in het algemeen.

WANNEER WEL EN WANNEER NIET?

RISICO'S AFWEGEN

Het is belangrijk dat er conform de AVG een **risicoanalyse** gebeurt. De VTC verwijst naar de tools op haar website en de motivering van haar advies A/2020/05 die daarbij kunnen helpen. Het advies van de **functionaris voor gegevensbescherming/DPO** is daarbij altijd vereist.

WELKE VRAGEN MOET U ZICH STELLEN?

Overeenkomstig de matrix die de VTC heeft opgenomen in haar advies A/2020/05 en zonder aan de daar gehanteerde richtlijnen afbreuk te doen, zijn de belangrijkste vragen die u zich moet stellen om te bepalen of informatie in de publieke cloud kan verwerkt worden de volgende (elke vraag telt apart):

- **Hoe gestructureerd zijn de data/persoonsgegevens?**

  Gaat het om databases of digitale dossiers?

  Worden er terloops gegevens van personen in verwerkt (bv. contactpersonen van een organisatie) of gaat het om dossiers over personen (bv. debiteurenbeheer)?

- **Wat is de schaal van de verwerking?**

  Betreft het een groot deel of de hele populatie van de inwoners van een gemeente?

- **Hoe gevoelig is de informatie?**

  Worden er gegevens verwerkt van kwetsbare personen of gevoelige gegevens (in ruime zin) van de burger.

  Hierbij moet er ook rekening gehouden worden met de **context** waarin ogenschijnlijk neutrale informatie wordt verwerkt, maar waar gevoelige informatie uit kan afgeleid worden bv. het onderhouden van contact met een dienst die voor drugspreventie instaat (problematiek van zogenaamde **metadata**).

CRITERIA

Volgende richtlijnen zijn bedoeld als houvast om te bepalen of het gebruik van algemene kantoorapplicaties in de publieke cloud AVG-conform is:

- **in principe niet aanvaardbaar voor** structureel dossierbeheer met persoonsgegevens. Daarvoor zijn specifieke applicaties met specifieke beveiliging vereist: de bedoelde kantoortoepassingen zijn daar niet voor bedoeld en de standaardbeveiliging is daar niet op afgesteld. Algemene kantoorapplicaties zijn niet bedoeld of geschikt als surrogaat voor een grootschalig verwerkingssysteem van persoonsgegevens;

- **in principe wel bruikbaar voor** het uitwisselen van ontwerpdocumenten zonder vertrouwelijke informatie en het uitvoeren van praktische taken, bv. samenwerken aan een beleidsplan. Daarbij kunnen incidenteel persoonsgegevens worden uitgewisseld, zoals de naam of het emailadres van een collega of beperkte informatie over de medewerker;

- **in principe niet aanvaardbaar voor** het delen of uitwisselen van gevoelige persoonsgegevens zoals het uitwisselen van vaccinatiestatus;

- **in principe geen** applicatie voor participatie van de burger bv. met gedeelde mappen in de cloud.

CONCLUSIE

In principe te gebruiken als algemene kantoortoepassing en niet voor dossierbehandeling. Doe de risicoanalyse per geplande verwerking.

HOE EEN KANTOORTOEPASSING IN DE PUBLIEKE CLOUD OMKADEREN?

Als je een algemene kantoortoepassing (tekstverwerking, spreadsheets, e-mail, documentbeheer) in de publieke cloud gebruikt waarbij een beperkte verwerking van persoonsgegevens niet uitgesloten is, waar hou je dan rekening mee?

Hierna een aantal richtinggevende tips en ook enkele minimumvereisten. De VTC is er zich van bewust dat hiermee niet alle aspecten afgedekt worden en dat de specifieke contractuele bepalingen en technische instellingen een grondiger benadering vragen.

CONTRACT

De AVG vereist dat u als verwerkingsverantwoordelijke een **verwerkersovereenkomst** sluit. Om die afdwingbaar te maken is het nodig om het beroep op de cloudleverancier ook te kaderen in een **contract** en niet zonder kritische reflectie in te schrijven op basis van standaardvoorwaarden. Bovendien zijn er meestal verschillende **licentiemogelijkheden** en voldoen de goedkoopste bijna zeker niet aan de AVG-eisen.

SERVERS

Er mogen enkel gegevens verwerkt worden in datacenters/servers in Europa. Dit is een minimale vereiste. Dit geldt ook voor back-ups.

Om lock in-risico's te beheren (vastzitten aan een leverancier) is het uitermate belangrijk ook een **backup** te voorzien van alle gegevens die in de toepassing worden opgeslagen. Als u als bestuur vastzit aan een bepaalde leverancier en deze blijk niet te voldoen (aan de AVG), moet het mogelijk zijn om van leverancier te veranderen. Er zijn verschillende oplossingen op de markt voor back-ups.

Belangrijk bij deze backups is dat:

- deze binnen Europa gehost worden, met op hun beurt ook de nodige garanties;
- snel herstelbaar zijn (liefst lokaal);
- de afhankelijkheid van één leverancier niet bestendigen als er alternatieven zijn. M.a.w. het vormt een groot risico om back-ups enkel te bewaren bij de leverancier die ook de primaire data bewaart;
- volgens de regels van de kunst ingericht zijn met tests, controles, enz.

MULTIFACTORAUTHENTICATIE

Er moet **2(of meer)-factorauthenticatie** worden geïnstalleerd voor de toegang tot de accounts. Dit is een minimumvoorwaarde. Er worden nog regelmatig datalekken vastgesteld op basis van accounts die enkel met een paswoord beveiligd zijn. De keuze voor de authentificatiefactoren moet ook zorgvuldig gebeuren. Niet alle mogelijkheden zijn aanvaardbaar in een overheidscontext.

ROLLENBEHEER

Er mag enkel toegang zijn op basis van **rechten toegekend aan de gepaste rollen** voor wat toegang tot documenten met persoonsgegevens betreft, zodat iedere medewerker (ongeacht de plaats in de hiërarchie) enkel toegang heeft tot de persoonsgegevens die deze nodig heeft om de eigen taken uit te voeren. Idealiter wordt er gebruik gemaakt van een volledig Role-based Acccess controle-systeem dat mee geïntegreerd is in de verdere rechtenstructuur van het bestuur.

ENCRYPTIE

Als er toch gedacht wordt aan uitwisseling van persoonsgegevens die niet louter incidenteel is (bijvoorbeeld een namenlijst mailen) kan dat enkel als dit gebeurt in een bestand dat volgens de regels van de kunst versleuteld is door gebruik te maken van een erkend encryptiealgoritme (voordat je het oplaadt in een kantoortoepassing).

PRIVACY-INSTELLINGEN

Vermijd dat medewerkers en burgers gemonitord worden (*metering*) op een manier die niet wordt gecontroleerd en bepaald door de Vlaamse instantie zelf of die om een andere reden onrechtmatig zou zijn: o.m. via cookies en automatische evaluatie van activiteit.

Kijk de standaardinstellingen na en pas ze aan.

Bied de medewerkers en burgers minstens transparantie over wat niet kan vermeden worden. Het gaat hier om online gedrag en onderlinge relaties op basis van metagegevens.

ACCOUNT BURGER?

De burger verplichten om een account aan te maken bij een privébedrijf is in principe niet toelaatbaar.

PET

Voor bepaalde toepassingen kan er gebruik worden gemaakt van privacy bevorderende technologieën.

Zie https://www.smalsresearch.be/webinar-pets/
https://www.smalsresearch.be/wanneer-is-welke-privacybevorderende-technologie-nuttig/

TOEZICHT

Garandeer toezicht van de functionaris voor gegevensbescherming (DPO) op het proces van de introductie van een toepassing en van de wijzigingen achteraf. Dit is wel geen overdracht van het beheer aan de functionaris.

HOE JE ER ALS MEDEWERKER MEE OM?

GEVOELIGE PERSOONSGEGEVENS

Kom niet in de verleiding om een kantoortoepassing in de cloud occasioneel te gebruiken voor gevoelige (in ruime zin) gegevens of dossiers.

VIDEOCONFERENTIES

Wees voorzichtig met het gebruik van online videoconferenties voor vergaderingen waar gevoelige elementen besproken worden zoals sociale raden, tuchtprocedures, benoemingen, etc.

Opnames

- hou er rekening mee dat deelnemers ook opnames kunnen maken zonder de opnamefuncties van Teams, en zelfs zonder dat dit gemerkt wordt;
- hou rekening met een mogelijke transcriptietool die van het overleg (live) een geschreven verslag maakt (en eventueel audio-opnames) en wat daarmee verder gebeurt.

Vergaderhygiëne

Doe bij online (en andere vergaderingen) aan vergaderhygiëne:

- zorg dat iedereen sterk geïdentificeerd is voor hij kan deelnemen;
- bespreek enkel niet-persoonsgebonden materies;
- voor zover het onvermijdelijk is om over persoonsgebonden materies te spreken, vermeld dan voor zover mogelijk geen namen of andere identificatoren: spreek of schrijf bv. over een dossiernummer en “de klant”; zorg er wel voor dat er geen verwisselingen van persoon kunnen gebeuren.

ALTERNATIEVEN

De VTC heeft al meerdere keren de vraag gekregen of er dan wel alternatieven zijn voor de cloudtoepassing(en).

Er zijn zeker mogelijkheden.

De gegevens die niet in de publieke cloud kunnen verwerkt worden, kunnen dat eventueel wel (nog altijd) **on premise/lokaal** in een beveiligde omgeving. Dit geldt voor de verschillende toepassingen die deel uitmaken van een algemene kantoortoepassing.

Overweeg alternatieven zoals Jitsi, en andere jabberafhankelijken, enz.

Kijk naar de mogelijkheden van vrije software: bv. Zimbra-mail, collaboratietools.

Alternatieven kan je vinden op gespecialiseerde sites zoals: https://dasprive.be/dasprive-business-tooltip/

De alternatieven bieden meestal een minder omvattend pakket, maar verminderen daardoor ook de afhankelijkheid van die ene leverancier.

MEER WETEN? VRAGEN?

Contacteer de Vlaamse Toezichtcommissie
https://overheid.vlaanderen.be/vlaamse-toezichtcommissie