Vlaamse overheid

Vlaamse Toezichtcommissie voor de verwerking van persoonsgegevens
Autonome dienst met rechtspersoonlijkheid

Koning Albert II-laan 15
1210 Brussel
https://overheid.vlaanderen.be/vlaamse-toezichtcommissie

Aan de heer Frank Geets, administrateur-generaal
Facilitair Bedrijf

PER MAIL

uw bericht van	uw kenmerk	ons kenmerk	bijlagen
25/02/2023		VTC/A/2022/11	

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

contact@toezichtcommissie.be

Betreft: Digipost – advies

Mijnheer de administrateur-generaal,

De VTC verwijst naar het overleg dat heeft plaatsgevonden op 2 maart 2023 en waarbij de vraag werd gesteld naar een geschreven advies. Het advies beperkt zich tot de use-case van het inscannen van papieren poststukken.

De VTC wil beginnen met te zeggen dat ze de constructieve houding en de openheid van het Facilitair Bedrijf zeer apprecieert.

De VTC is van oordeel dat het gebruik van de publieke cloud voor de specifieke casus van Digipost van het Facilitair Bedrijf aanvaardbaar is, rekening houdend met de specifieke karakteristieken van de casus, en onder bepaalde voorwaarden die hierna besproken worden.

Specifieke kenmerken van Digipost die, als geheel genomen en door hun combinatie, het gebruik van publieke cloud zoals hier toegepast aanvaardbaar maken

DUUR VAN DE OPSLAG

- er is geen permanente grootschalige opslag van persoonsgegevens in de cloud (max 16 dagen);
- het verwerkingspatroon is onvoorspelbaar, vermits briefstukken worden ingescand en doorgestuurd in de volgorde waarin zij worden voorgelegd, en deze volgorde is voor een derde niet redelijkerwijs te voorpellen. Een aanvaller kan bijgevolg geen specifieke poststukken als doelwit kiezen.
- de persoonsgegevens in de poststukken worden niet gestructureerd op een manier die ze makkelijk doorzoekbaar maakt voor een derde. De ingescande documenten worden bewaard met beperkte metadata (zie punt 7.3.1 modelGEB[1][2]), die niet toelaten om een aanval op een specifieke verzender te richten, of om bepaalde soorten briefstukken te viseren.

ENCRYPTIE EN CONTAINERS

- de data at rest bevinden zich in een confidential compute (of vergelijkbaar) omgeving; aanvallen zijn complex, en bij een memory dump kan je in principe geen bruikbare informatie uit de data halen;
- er zijn geen emergency keys bij de cloudleverancier;
- er werd een onafhankelijke derde partij ingeschakeld om de beveiligingsoplossing van de dienstverlener te beoordelen[3];
- er worden geen databases met persoonsgegevens in de cloud gezet en dus ook niet gedecrypteerd bij data in use;
- zelfs indien deze maatregelen falen, dan zou deze aanval op relatief korte termijn detecteerbaar moeten zijn, en door de beperkte opslagtermijn zou zelfs een succesvolle aanval ongericht moeten blijken.

OPT-OUT MOGELIJKHEDEN

- opt-out is mogelijk op initiatief van de verzender door een vermelding op de briefomslag - decretaal verankerd (ontwerp digitaliseringsdecreet), waardoor het systeem niet dwingend in alle gevallen opgedrongen kan worden;
- opt-out is mogelijk door de ontvanger/verwerkingsverantwoordelijke via een (extra) postbusnummer waarbij er geen documenten ingescand worden (GEBmodel, 10.11); deze opt-out kan granulair ingezet worden, naargelang de voorkeuren van de ontvanger/verantwoordelijke;
- opt-out is mogelijk door de ontvanger middels weigeren van OCRscan van de printjob (cf. GEBmodel, 8.2. en 10.2)

ANDERE MAATREGELEN (specifiek of essentieel voor Digipost)

- vertrouwelijkheidsverplichtingen decretaal verankerd (ontwerp digitaliseringsdecreet).

---

1 Versie 2.0 ontvangen op 2 maart 2023.

2 Dit metadatabestand bevat minimaal de volgende gegevens: bestandsnaam, datum- en tijdsstempel (het moment dat de scanoperator de batch afsluit), aantal pagina's, code postvak, Code posttype (bv. gewone poststukken, aangetekend, retour gewoon, retour aangetekend), Sequencer (extra QR code om grote bundels te splitsen), aangemelde gebruiker die oplaadt, documenttype, barcode van Bpost, ID van de archiefdoos waarin de originelen bewaard worden.

3 "*De vragen van Het Facilitair Bedrijf gaan over de dienst, DigiPost, die door de dienstverlener Cronos verder ontwikkeld wordt. Het verzoek is aan Cumundi om het technische voorstel van dienstverlener Cronos te beoordelen. De concrete vragen zijn:*
1) of Cumundi kan inschatten of de voorgestelde oplossing correct is en
2) of deze oplossing ook effectief doorgiften buiten de EU onmogelijk maakt."

Voorwaarden waaraan de verwerkingsverantwoordelijken moeten voldoen

INFORMATIECLASSIFICATIE en GEB

- ontvangers die het systeem wensen te gebruiken dienen een informatieclassificatie uit te voeren zodat het duidelijk is welke verwerkingen gevoelige gegevens verwerken; voor verwerkingen die dat doen op grote schaal het centraal laten inscannen uitsluiten/onmogelijk maken;
- ontvangers die het systeem wensen te gebruiken dienen een GEB (DPIA) op te stellen om de risico's voor de betrokkenen in kaart te brengen, waarbij minimaal dezelfde elementen als uit de model-GEB die het Facilitair Bedrijf heeft aangebracht ter sprake komen;
- opt-out mogelijkheid implementeren voor verwerkingen die niet onder het eerste punt vallen maar om andere redenen gevoelig/risicovol kunnen zijn: de mogelijkheid voorzien voor de afzender om voor niet centraal inscannen te kiezen (vermelden persoonlijk e.d. en/of apart busnummer te gebruiken);
- mening betrokkenen/vertegenwoordigers over de verwerking wel bevragen.

BESLISSING

- de verwerkingsverantwoordelijke houdt er rekening mee dat (rest)risico's voor de rechten en vrijheden van de betrokkenen niet kunnen geaccepteerd worden.

Voorwaarden waaraan Digipost nog moet voldoen

ARCHITECTUUR

- de architectuur met de cryptografische oplossing moet gevalideerd worden door een externe partij;
- er moet een waarschuwing ingebouwd zijn in de SOC SIEM(bouwsteen) bij toegang door de leverancier (naast die van andere derden - hacking) en er moeten acties aan gekoppeld worden; (punt 14.1.7 modelGEB[4])
- de PAMaas bouwsteen Cyberark (veiligheidsbouwsteen Digitaal Vlaanderen (of equivalent) wordt in productie gekoppeld vooraleer de oplossing naar alle VO-entiteiten wordt uitgerold (zie 10.5.2. GEBmodel);
- de KMSaaS bouwsteen voor Azure (veiligheidsbouwsteen Digitaal Vlaanderen of equivalent) wordt in productie gekoppeld vooraleer de oplossing naar alle VO-entiteiten wordt uitgerold (zie 10.5.2. GEBmodel).
- in verband met dit HSM-alternatief[5]: de KMSaaS-bouwblok moet garanderen dat ongeoorloofde toegang wordt gedetecteerd en een expertenreview moet de gelijkwaardigheid van dit alternatief bevestigen.

---

4 "Elke activiteit van een gebruiker (technisch, privileged of gewoon) wordt gelogd in het systeem. Zo is het niet enkel mogelijk om te zien wie er wat gedaan heeft met een document, maar ook wie wanneer een document bekeken, gedownload of doorgestuurd heeft. Deze gegevens worden gekoppeld aan SOC/SIEM (veiligheidsbouwsteen Digitaal Vlaanderen).

Ook de activiteiten die via PAMaas (Cyberark), KMSaaS of de Azure Premium key vault gedaan worden, worden doorgespeeld aan SOC/SIEM.

Daarnaast wordt elke actie op het niveau van een document bijgehouden en getoond in het DigiPost-platform. Op die manier is de logging op het niveau van een document ook steeds beschikbaar voor de eindgebruiker."

5 Softwarematig i.p.v. met hardware omwille van de hoge kost.

TRANSPARANTIE

- de gebruikers/verwerkingsverantwoordelijken moeten toegang krijgen tot het detail van de architectuur (voor zover dit de veiligheid niet in het gedrang brengt);

IMPLEMENTATIE

- alles moet correct geïmplementeerd worden (zie advies externe partij van 17 februari 2023 en voorbehoud daarin);
- er is een engagement nodig van de verwerker(s) om zich aan de vereiste garanties te houden, in eerste instantie van het Facilitair Bedrijf in een verwerkersovereenkomst.

De VTC hoopt u hiermee meer duidelijkheid te hebben gegeven over de aanvaardbaarheidscriteria voor de geplande verwerkingen. Ze is beschikbaar voor verdere vragen en overleg.

Hoogachtend,

Hans Graux
Voorzitter VTC

Getekend door:Hans Graux (Signature)
Getekend op:2023-03-24 22:20:30 +01:0
Reden:Ik keur dit document goed