Gegevensbeschermingseffect-beoordeling (GEB/DPIA)

Gebruik DigiPost door [NaamEntiteit]

HANDLEIDING Dit document is door Het Facilitair Bedrijf opgesteld als een “White Label” GEB voor entiteiten die gebruik (gaan) maken van DigiPost. Doorheen dit document zijn bepaalde tekstonderdelen geel gemarkeerd en tussen vierkante haken ([ ]) geplaatst. Deze tekstonderdelen dienen aangepast/aangevuld of geschrapt te worden door de entiteit bij het invullen van deze GEB.

Dit document is gebaseerd op een model dat werd opgesteld door de [Vlaamse Toezichtcommissie voor de verwerking van persoonsgegevens](https://overheid.vlaanderen.be/vlaamse-toezichtcommissie) en is afgeleid van het model van het d.pia.lab van de VUB: Brussel, 2020., licentie: CC BY SA 4.0. (<https://researchportal.vub.be/files/53602836/dpialab_pb2020_1_final.pdf>) Zie ook [www.dpialab.org](http://www.dpialab.org) en [dpialab@vub.ac.be](mailto:dpialab@vub.ac.be).

# Inhoudsopgave

[Inhoudsopgave 2](#_Toc128077881)

[1. Versiebeheer 6](#_Toc128077882)

[2. GEB DigiPost 7](#_Toc128077883)

[3. Algemene omschrijving van de verwerking 8](#_Toc128077884)

[4. Projectstructuur 9](#_Toc128077885)

[4.1. Deelnemers aan GEB 9](#_Toc128077886)

[4.2. Projectwerking bij het opzetten van GEB 9](#_Toc128077887)

[4.3. Middelen voor het uitvoeren van de GEB 9](#_Toc128077888)

[5. (Her)evaluatie van GEB tijdens de verwerking 11](#_Toc128077889)

[6. Bronnen voor het opstellen van de GEB 11](#_Toc128077890)

[6.1. Wet- en regelgeving 11](#_Toc128077891)

[6.2. Aanbevelingen van EDPB/EDPS 11](#_Toc128077892)

[6.3. Aanbevelingen en standpunten van toezichthouders 11](#_Toc128077893)

[6.4. Aanbevelingen en standpunten van rechtbanken 12](#_Toc128077894)

[7. Systematische beschrijving 13](#_Toc128077895)

[7.1. Het toepassingsgebied van de GEB 13](#_Toc128077896)

[7.1.1. Het DigiPost-platform – een korte toelichting 13](#_Toc128077897)

[7.1.2. Verdeling in het DigiPost-platform (virtuele postvakken) 16](#_Toc128077898)

[7.1.3. Toegang tot het DigiPost-platform 18](#_Toc128077899)

[7.2. Beschrijving van de context van de verwerkingen 18](#_Toc128077900)

[7.3. Systematische beschrijving van de verwerkingen (en verwerkingsdoelen) 19](#_Toc128077901)

[7.3.1. Verwerking van poststukken 20](#_Toc128077902)

[7.3.2. Verwerking van postpakketten (BringMe flow) 24](#_Toc128077903)

[7.4. Categorieën van persoonsgegevens 24](#_Toc128077904)

[7.5. Beschrijving van de betrokkenen en andere actoren 25](#_Toc128077905)

[7.5.1. Betrokkenen 25](#_Toc128077906)

[7.5.2. Andere actoren 25](#_Toc128077907)

[8. Noodzakelijkheid en evenredigheid 26](#_Toc128077908)

[8.1. De rechtmatigheid van de verwerking 26](#_Toc128077909)

[8.2. De basisbeginselen van de verwerking 27](#_Toc128077910)

[8.2.1. (Eerlijkheid) Behoorlijkheid en transparantie 27](#_Toc128077911)

[8.2.2. Doelbinding 28](#_Toc128077912)

[8.2.3. Minimale gegevensverwerking 28](#_Toc128077913)

[8.2.4. Juistheid en Nauwkeurigheid 28](#_Toc128077914)

[8.2.5. Opslagbeperking 29](#_Toc128077915)

[8.2.6. Gegevensbeveiliging 30](#_Toc128077916)

[8.2.7. Gegevensbescherming door ontwerp en als standaardinstelling 30](#_Toc128077917)

[8.3. Beoordeel de noodzakelijkheid en evenredigheid 30](#_Toc128077918)

[9. Methode voor beoordeling risico’s op rechten en vrijheden van betrokkenen 32](#_Toc128077919)

[9.1. Aanvaardbaarheidscriteria van negatieve effecten 32](#_Toc128077920)

[9.2. Risicoanalyse, -evaluatie en opvolging 32](#_Toc128077921)

[9.2.1. Bepalen van de impact van een risico voor betrokkene 32](#_Toc128077922)

[9.2.2. Bepalen van de waarschijnlijkheid van een risico voor de betrokkene 34](#_Toc128077923)

[10. Beoordeling risico’s op rechten en vrijheden van betrokkenen 35](#_Toc128077924)

[10.1. Potentiële internationale doorgiftes doorgifte naar een niet-EER land/de Verenigde Staten van Amerika. 35](#_Toc128077925)

[10.1.1. Risico 35](#_Toc128077926)

[10.1.2. Maatregelen 36](#_Toc128077927)

[10.1.3. Restrisicoscore 37](#_Toc128077928)

[10.2. Gebruik OCR op binnenkomende poststukken 37](#_Toc128077929)

[10.2.1. Risico 37](#_Toc128077930)

[10.2.2. Maatregelen 38](#_Toc128077931)

[10.2.3. Restrisicoscore 38](#_Toc128077932)

[10.3. Verlies informatie door noodsituatie in scankamer 38](#_Toc128077933)

[10.3.1. Risico 38](#_Toc128077934)

[10.3.2. Maatregelen 39](#_Toc128077935)

[10.3.3. Restrisicoscore 39](#_Toc128077936)

[10.4. Substitutie 40](#_Toc128077937)

[10.4.1. Risico 40](#_Toc128077938)

[10.4.2. Maatregelen 40](#_Toc128077939)

[10.4.3. Restrisicoscore 40](#_Toc128077940)

[10.5. Ongeoorloofde toegang – kwetsbaarheden in oplossing worden uitgebuit. 40](#_Toc128077941)

[10.5.1. Risico 40](#_Toc128077942)

[10.5.2. Maatregelen 41](#_Toc128077943)

[10.5.3. Restrisicoscore: 42](#_Toc128077944)

[10.6. Ongeoorloofde toegang – scankamer 42](#_Toc128077945)

[10.6.1. Risico 42](#_Toc128077946)

[10.6.2. Maatregelen 43](#_Toc128077947)

[10.6.3. Restrisicoscore 43](#_Toc128077948)

[10.7. Ongeoorloofde toegang - gebruikersbeheer 43](#_Toc128077949)

[10.7.1. Risico 43](#_Toc128077950)

[10.7.2. Maatregelen 43](#_Toc128077951)

[10.7.3. Restrisico 44](#_Toc128077952)

[10.8. Verkeerde bezorging 44](#_Toc128077953)

[10.8.1. Risico 44](#_Toc128077954)

[10.8.2. Maatregelen 44](#_Toc128077955)

[10.8.3. Restrisicoscore 45](#_Toc128077956)

[10.9. Inbreuk na verkeerde bezorging 45](#_Toc128077957)

[10.9.1. Risico 45](#_Toc128077958)

[10.9.2. Maatregelen 45](#_Toc128077959)

[10.9.3. Restrisicoscore 46](#_Toc128077960)

[10.10. Schending briefgeheim 46](#_Toc128077961)

[10.10.1. Risico 46](#_Toc128077962)

[10.10.2. Maatregelen 46](#_Toc128077963)

[10.10.3. Restrisicoscore 46](#_Toc128077964)

[10.11. Niet naleven van de afspraken m.b.t. vertrouwelijke poststukken en gemaakte afspraken m.b.t. niet scanbare poststukken 47](#_Toc128077965)

[10.11.1. Risico 47](#_Toc128077966)

[10.11.2. Maatregelen: 47](#_Toc128077967)

[10.11.3. Restrisicoscore: 47](#_Toc128077968)

[10.12. Onethisch gebruik door personen met geoorloofde toegang – verspreiden van informatie 48](#_Toc128077969)

[10.12.1. Risico 48](#_Toc128077970)

[10.12.2. Maatregelen 48](#_Toc128077971)

[10.12.3. Restrisicoscore 48](#_Toc128077972)

[10.13. Menselijke fout in de scankamer 49](#_Toc128077973)

[10.13.1. Risico 49](#_Toc128077974)

[10.13.2. Maatregelen 49](#_Toc128077975)

[10.13.3. Restrisicoscore 49](#_Toc128077976)

[10.14. Te late reactie op ontvangen poststukken 50](#_Toc128077977)

[10.14.1. Risico 50](#_Toc128077978)

[10.14.2. Maatregelen 50](#_Toc128077979)

[10.14.3. Restrisicoscore 50](#_Toc128077980)

[11. Mening betrokkenen/vertegenwoordigers over de verwerking (verplicht) 51](#_Toc128077981)

[12. Adviezen betreffende de GEB (verplicht) 52](#_Toc128077982)

[12.1. Advies functionaris voor gegevensbescherming (FG) 52](#_Toc128077983)

[12.2. Voorafgaande raadpleging bij de toezichthouder (verplicht bij hoog restrisico) 52](#_Toc128077984)

[12.3. Overzicht van de acties die de verwerkingsverantwoordelijke neemt naaar aanleiding van het advies van de functionaris en de raapleging van de toezichthouder 52](#_Toc128077985)

[13. Besluit van de verwerkingsverantwoordelijke (verplicht) 53](#_Toc128077986)

[14. Annex I – Technische en organisatorische maatregelen (TOMs) 54](#_Toc128077987)

[14.1. TOMs op niveau van verwerker Het Facilitair Bedrijf 54](#_Toc128077988)

[14.1.1. Toegang tot het DigiPost platform voor gebruikers 54](#_Toc128077989)

[14.1.2. Geprivilegieerde toegang tot het platform 55](#_Toc128077990)

[14.1.3. Integratietoegang 56](#_Toc128077991)

[14.1.4. Encryptie 56](#_Toc128077992)

[14.1.5. Data in motion 56](#_Toc128077993)

[14.1.6. Andere maatregelen 57](#_Toc128077994)

[14.1.7. Logging en monitoring 57](#_Toc128077995)

[14.2. Aanvullende TOMs op niveau van subverwerker Cronos Public Services / FlinQ / Arxus 58](#_Toc128077996)

[14.2.1. Pentesting 58](#_Toc128077997)

[14.3. TOMs op niveau van subverwerker Bringme 58](#_Toc128077998)

[15. Annex II – Ontwerptekst aanpassing Bestuursdecreet 59](#_Toc128077999)

[15.1. Artikels in het Wijzigingsdecreet i.k.v. DigiPost 59](#_Toc128078000)

[15.2. Memorie van Toelichting bij hogervermelde artikels 60](#_Toc128078001)

[16. Annex III – Foto’s inrichting scankamer 63](#_Toc128078002)

# Versiebeheer

Deze GEB is een “actief” document. Dit betekent dat de gehanteerde maatregelen kunnen wijzigen doorheen de tijd. Bij aanpassingen aan deze maatregelen wordt de GEB geüpdatet. Stel dus steeds vast dat gebruik wordt gemaakt van de laatste versie van deze GEB wanneer u deze GEB onder ogen krijgt na de genoemde datum.

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Medewerkers** | **Commentaar** |
| 0.1. | 22/08/2022 | Bart van Buitenen | Creatie document |
| 0.2. | 17/10/2022 | Seppe Vansteelant, Quincy Oeyen | Na bespreking met VTC op 13 september 2022 zijn diverse wijzigingen aangebracht. |
| 0.3. | 27/10/2022 | Seppe Vansteelant, Quincy Oeyen | Na een eerste overleg met Microsoft tussen Cronos en Het Facilitair Bedrijf zijn een aantal verduidelijkingen aangebracht bij de risico’s en de beperkende maatregelen. |
| 1.0. | 28/10/2022 | Seppe Vansteelant, Quincy Oeyen | Eerste ontwerpversie voor feedback/aanvullingen voor de entiteiten die instappen in DigiPost. |
| 1.1. | 17/11/2022 | Quincy Oeyen | Aanpassingen n.a.v.   * feedback van Departement Omgeving * feedback van Departement Werk en Sociale Economie * wijzigingen aan de ontwerpbepalingen voor het Bestuursdecreet |
| 2.0 | 24/02/23 | Quincy Oeyen, Seppe Vansteelant, Louise De Béthune | Aanpassingen n.a.v.   * de technische maatregelen met het oog op de gekozen hosting-oplossing; * finale review i.k.v. bespreking met VTC |
| 2.1 | 07/09/23 | Quincy Oeyen | Aanpassingen n.a.v. nieuwe adequaatheidsbesluit met VS. Passages over ongeldige besluit zijn gewist. |

# GEB DigiPost

|  |  |
| --- | --- |
| **Naam/referentie van het initiatief:** | [In te vullen door de entiteit] |
| **Naam, contactinformatie en andere identificatiegegevens van:** | […] |
| **Verwerkingsverantwoordelijke(n) en hun vertegenwoordigers:** | […] |
| **Verantwoordelijke(n) voor het project (business owner):** | […] |
| **Functionaris(sen) voor gegevensbescherming (DPO)1:** | […] |
| **Versie van GEB:** | 0.1: prep template  0.2: eerste notities nalv interviews  0.3: uitwerken gegevensstroom en interviews  0.4: toevoeging risico’s, risico methodologie en placeholders beveiligingsmaatregelen  0.5: verwerking feedback Het Facilitair Bedrijf en verdere uitbreiding hoofdstukken 6 en 7.  0.6: uitbreiding risico’s o.b.v. verdere gesprekken, verwerking feedback Het Facilitair Bedrijf, uitwerking veiligheidsmaatregelen.  0.7: herziening risico’s o.b.v. maatregelen, aanvullen hoofdstuk 5 en 7  0.8: oktober 2022 – aanpassing op basis van feedback van de VTC |
| **Referentie naar pre-GEB:** | [Indien van toepassing] |
| **Classificatie:** |  Vertrouwelijk   Informatieklasse [1, 2, 3, en 4] ... |

1 Alle Vlaamse bestuursinstanties moeten een functionaris aangesteld hebben en hun verwerkers ook.

# Algemene omschrijving van de verwerking

[NaamEntiteit] zal gebruik maken van de dienstverlening DigiPost. Dit is een door Het Facilitair Bedrijf aangeboden gemeenschappelijke dienstverlening voor digitalisering van inkomende poststukken van de entiteiten van de Vlaamse overheid.

Om deze dienstverlening mogelijk te maken heeft Het Facilitair Bedrijf in het Hendrik Conscience-gebouw een centrale scankamer ingericht waar de analoge poststukken van de entiteiten van de Vlaamse overheid ontvangen worden. In de scankamer worden de poststukken scanklaar gemaakt, gescand en digitaal verdeeld naar de aangesloten entiteiten via een software-oplossing. Afhankelijk van de voorkeur per entiteit worden de poststukken in een virtuele postbus aangeleverd of rechtstreeks naar een dossiersysteem.

Poststukken die niet kunnen of mogen gedigitaliseerd worden, worden verdeeld via pakketautomaten. De volgende poststukken zijn aangemerkt als niet-digitaliseerbaar:

* Poststukken waarop op de enveloppe ‘vertrouwelijk’, ‘geheim’ of ‘medisch geheim’ vermeld wordt;
* Poststukken bestemd voor postbussen waarvan de desbetreffende entiteit heeft aangegeven dat er niet gedigitaliseerd mag worden;
* Niet digitaliseerbare objecten (bv. boeken, tijdschriften, fysieke objecten …).

Daarnaast worden de pakketautomaten ook gebruikt om die poststukken te verdelen die gedigitaliseerd werden, maar waar de bestemmeling ook het origineel van heeft opgevraagd.

Onderstaand schema geeft een overzicht op grote lijnen van de werking van DigiPost:

Diagram, schematic

Description automatically generated

De verwerking van poststukken op zich geeft geen aanleiding tot de uitvoering van een GEB maar in de context van het inzetten van digitalisering als nieuwe technologie of innovatieve toepassing en de grootschaligheid waarmee dit gaat gebeuren via Het Facilitair Bedrijf is besloten om een GEB op te stellen.

# Projectstructuur

## Deelnemers aan GEB

Onderstaande (interne en externe) medewerkers hebben deelgenomen aan deze GEB:

* [AAN TE VULLEN DEELNEMERS ENTITEIT]
* Bart van Buitenen: externe consultant gegevensbescherming
* Bernier Fierens: Solutions Architect bij FlinQ (Cronos, softwareleverancier)
* Bert Jagers: Algemeen Directeur Leo (Cronos, softwareleverancier)
* Daan Lagast: jurist (Het Facilitair Bedrijf)
* Jens Lemarcq: DPO (Het Facilitair Bedrijf)
* Johan Stessens: Senior PM/BA bij FlinQ (Cronos, softwareleverancier)
* Lore Bocken: Projectcoördinator DigiPost (Het Facilitair Bedrijf)
* Louis Malfait: DPO (Cronos - softwareleverancier)
* Louise de Béthune: privacy officer (Het Facilitair Bedrijf)
* Luc De Cock: ICT-coördinator (Het Facilitair Bedrijf )
* Quincy Oeyen: Programmamanager DigiPost (Het Facilitair Bedrijf)
* Ruben Van Driessche: Procesmanager Digitale post en Scanning (Het Facilitair Bedrijf)
* Seppe Vansteelant: voormalig DPO (Het Facilitair Bedrijf)
* Cumundi bv

## Projectwerking bij het opzetten van GEB

[HANDLEIDING: Aanvullen historiek: wanneer ging entiteit gebruik maken van DigiPost, nood aan GEB onderkend, opstart invulling GEB obv model Het Facilitair Bedrijf.]

*(kort) Voorbeeld:*

*Begin juli 2022 wordt besloten om deel te nemen aan project DigiPost. Gelet op de context van de verwerking wordt besloten dat een GEB noodzakelijk is. Samen met Het Facilitair Bedrijf stelt de relevante verantwoordelijke binnen entiteit een GEB op die op [Datum invullen] ter advies is voorgelegd aan de DPO. Etc.*

## Middelen voor het uitvoeren van de GEB

Voor de GEB zijn voldoende middelen voorzien om te garanderen dat de uitvoering objectief en correct kan plaats vinden. Als belangrijkste uitgangspunt wordt de GEB uitgevoerd voordat de uitvoering van het project van start gaat: de beslissingen of adviezen die uit de GEB voortkomen zijn cruciaal in de verder uitwerking van het project.

Om concreet de diverse aspecten te benoemen die onderbouwen dat voldoende middelen zijn ingezet:

* *Tijdsbesteding betrokkenen*: vanuit [NaamEntiteit], Het Facilitair Bedrijf en andere externe betrokken partijen zijn personen vrijgemaakt die hun input hebben gegeven voor de uitvoering van de GEB. Het betreft intern leidinggevenden, extern ingehuurde expertise, programmamanager en technische medewerkers bij externe partijen betrokken bij de uitvoering, etc.
* *Extra ondersteuning*: Specifiek voor de begeleiding bij de uitvoering van de GEB is een externe expert ingehuurd die heeft ondersteund bij de uitwerking van de GEB, bij de verzameling van informatie en voor de eerste informele beraadslaging bij de VTC. Voor het tweede gesprek met VTC werd een externe auditor aangesteld om de technische opzet door te lichten.
* *Technische onderbouwing*: Technisch inhoudelijke expertise werd ingewonnen bij het Team Informatieveiligheid van Digitaal Vlaanderen, technologieverantwoordelijken van Cronos, IT-team van Het Facilitair Bedrijf en andere operationeel verantwoordelijken.

# (Her)evaluatie van GEB tijdens de verwerking

Het is belangrijk om een GEB samen te laten evolueren met de verwerkingsactiviteit die in deze GEB wordt beoordeeld. Om die reden zal [NaamEntiteit] de GEB jaarlijks herevalueren in samenspraak met de relevante betrokkenen en de DPO om zo te kunnen valideren dat de inhoud van de GEB nog relevant is.

Indien nodig zal [NaamEntiteit] de GEB aanpassen of actualiseren. Dit kan nodig zijn in het kader van wijzigingen van het gegevensverwerkingsproces, nieuwe ontwikkelingen in de gebruikte technologie, of uitspraken en beslissingen van de bevoegde rechtbanken en toezichthoudende.

# Bronnen voor het opstellen van de GEB

Hieronder worden de bronnen opgelijst die gebruikt werden bij het opstellen van deze GEB.

## Wet- en regelgeving

* AVG: <https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32016R0679&from=EN>
* Oprichtingsbesluit Het Facilitair Bedrijf: <https://codex.vlaanderen.be/PrintDocument.ashx?id=1013222&datum=&geannoteerd=false&print=false>
* Bestuursdecreet: <https://codex.vlaanderen.be/PrintDocument.ashx?id=1030009&datum=&geannoteerd=false&print=false>
* Vlaams Personeelsstatuut: <https://overheid.vlaanderen.be/int_vertrouwelijke_behandeling>

## Aanbevelingen van EDPB/EDPS

* Aanbevelingen t.a.v. aanvullende maatregelen op de instrumenten voor doorgiftes voor een adequaat beschermingsniveau: <https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf>
* Richtsnoeren 07/2020 over de concepten van verantwoordelijke en verwerker in de AVG: <https://edpb.europa.eu/system/files/2022-02/eppb_guidelines_202007_controllerprocessor_final_nl.pdf>
* Clouddiensten bij de overheid: verslag van de EDPB: https://edpb.europa.eu/system/files/2023-01/edpb\_20230118\_cef\_cloud-basedservices\_publicsector\_en.pdf

## Aanbevelingen en standpunten van toezichthouders

* VTC: Advies VTC nr. 12/2021 van 15 februari 2022 m.b.t richtlijnen voor verwerking van persoonsgegevens met algemene kantoortoepassingen in de cloud bij lokale besturen (en andere kleinere Vlaamse bestuursinstanties): <https://overheid.vlaanderen.be/sites/default/files/media/VTC/VTC_A_2021_12_richtlijnen_kantoorpakketten_1_0_voorpub_def.pdf?timestamp=1645626166>
* VTC: Cloudadvies van 8 september 2020 (2020/05): <https://overheid.vlaanderen.be/sites/default/files/media/VTC/VTC_A_2020_05_advies.pdf?timestamp=1601969042>
* VTC: Antwoord cloudadvies van 20/10/2020: <https://overheid.vlaanderen.be/sites/default/files/media/VTC/VTC_A_2020_05_reactie_VTC_op_opmerkingen.pdf?timestamp=1603211106>

## Aanbevelingen en standpunten van rechtbanken

* Arrest Schrems 2: Zaak C‑311/18 van het Europees Hof van Justitie betreffende een verzoek om een prejudiciële beslissing krachtens artikel 267 VWEU, ingediend door de High Court (rechter in eerste aanleg, Ierland) bij beslissing van 4 mei 2018, ingekomen bij het Hof op 9 mei 2018, in de procedure: <https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:62018CJ0311>

# Systematische beschrijving

## Het toepassingsgebied van de GEB

De scope van de GEB betreft de opzet en het gebruik van de DigiPost dienstverlening van Het Facilitair Bedrijf voor de verwerking van analoge poststukken van [NaamEntiteit]. Concreet betreft dit het proces van de aankomst van analoge poststukken in de centrale scankamer van Het Facilitair Bedrijf in het Hendrik Conscience-gebouw tot en met de aanlevering door Het Facilitair Bedrijf van de gedigitaliseerde poststukken in het correcte virtuele postvak van [NaamEntiteit] in het DigiPost-platform.

### Het DigiPost-platform – een korte toelichting

De DigiPost-software is door Het Facilitair Bedrijf op 28 januari 2022 gegund aan Cronos Public Services. Deze overeenkomst is tot stand gekomen na de lancering van een werkaanvraag (CS-2021-000019) binnen het ICT-contract2, met name via Perceel 5 Applicatiediensten. Concreet neemt FlinQ, één van de bedrijven onder de Cronos koepel, de uitvoering van dit project op. De DigiPost-software bestaat uit 2 componenten zijnde 1) de scansoftware en 2) Routty - de verdeelsoftware waarin de virtuele postbussen voorzien worden.

Daarnaast is er ook nog de software die door de Bringmeboxen (pakketautomaten) gebruikt wordt.

#### Scansoftware

De scansoftware is lokaal op elke scanPC geïnstalleerd. Een scanPC is een PC in beheer van de Vlaamse overheid (cf. ICT-contract) die ‘dedicated’ is toegewezen aan een scanner. De toestellen staan in een afgesloten ruimte en zijn dus enkel toegankelijk voor geautoriseerd personeel en voorzien van Bitlocker encryptie. Inloggen kan enkel met VO credentials. De Scansoftware stuurt de scanners aan, verzamelt de beelden die gemaakt worden, laat toe aan de operatoren om een kwaliteitscontrole en eventuele rotaties of rescans te doen. De scansoftware is uitgebreid met een service die instaat voor het opladen van de resulterende bestanden naar het Digipost platform via https.

De scansoftware zorgt ook voor het OCR’en van de beelden. Dit gebeurt dus niet op een Azure-platform.

#### Routty

Routty is een SaaS platform, gehost op een Azure cloud in een specifiek VO-tenant waarmee de verdeling van de berichten kan plaatsvinden. De primaire locatie van de hosting is Amsterdam, de failover-locatie is Dublin. Contractueel is bepaald dat de hosting zich steeds binnen de Europese Economische Ruimte dient te situeren.

Routty wordt binnen het DigiPost-project gebruikt voor: routering, automatisering, datacaptatie en het biedt ook een user interface aan op de virtuele postvakken waardoor de eindgebruiker op een eenvoudige manier zijn berichten kan raadplegen.  In essentie bestaat Routty uit 2 belangrijke luiken:

1. Een Capture luik
   1. Het Capture luik is het gedeelte van het DigiPost-platform dat data uit de berichten extraheert (bv. interpretatie van de QR-codes die gebruikt worden voor de verdeling van de poststukken).
   2. Technisch draait dit luik op een virtuele machine (VM) die ondergebracht wordt op een Microsoft Azure Confidential Compute omgeving. Dit betekent concreet dat Microsoft onmogelijk toegang kan krijgen tot de informatie die aanwezig is op dit luik.
2. Distributie luik
   1. Het distributieluik is het gedeelte van het DigiPost-platform dat de berichten ter beschikking stelt aan de eindgebruikers.
   2. Technisch maakt dit luik gebruik van Microsoft Azure Functions. Dit betekent concreet dat als een gebruiker een bericht bekijkt er een function start die dat specifieke bericht ter beschikking stelt aan die specifieke gebruiker. Elk bericht dat bekeken wordt, wordt dus ter beschikking gesteld via een aparte function aan één enkele gebruiker. Het aantal actieve functions, en bijgevolg bekijkbare berichten, is dus gelijk aan het aantal gebruikers die een bericht bekijken.

Bij de initiële uitrol van de DigiPost-dienstverlening wordt Routty enkel ingezet voor het verdelen van ‘gescande analoge documenten’. Routty kan echter veel meer inputkanalen hebben zoals aangetoond wordt door onderstaande figuur. Het Facilitair Bedrijf wil deze mogelijkheden ook optimaal inzetten en geeft nu al de mogelijkheid aan klanten om specifiek voor hen een bijkomend input- of outputkanaal te activeren/integreren. Het Facilitair Bedrijf zal, samen met Digitaal Vlaanderen, investeren in een koppeling met Ebox (zodanig dat alle berichten die bestemd zijn voor een VO-entiteit  (al dan niet volledig geautomatiseerd) verdeeld kunnen worden naar het correcte postvak) en met de MAGDA-documentendienst zodat antwoorden van burgers ook gecapteerd en verdeeld kunnen worden.

Graphical user interface, chart, treemap chart

Description automatically generated  
[In deze fase zijn deze aanvullende inputkanalen nog niet actief. Passend bij het evolutieve karakter van een GEB zal deze GEB waar relevant aangevuld worden wanneer [NaamEntiteit] gebruik zal maken van aanvullende inputkanalen die leiden tot nieuwe gegevensverwerking en/of risico’s.]

De verdere verwerking van de digitale poststukken op de gewenste afleverlocatie door [NaamEntiteit] is buiten het toepassingsgebied van deze GEB.

#### Bringme (pakketautomaten)

Voor die poststukken die niet gedigitaliseerd kunnen/mogen worden plaatst Het Facilitair Bedrijf in alle grote kantoorgebouwen pakketautomaten. Concreet betreft het de volgende gebouwen:

* Hendrik Conscience-gebouw, Koning Albert II-laan 15, 1210 Brussel;
* Herman Teirlinck-gebouw, Havenlaan 88, 1000 Brussel;
* Ellips-gebouw, Koning Albert II-laan 35, 1210 Brussel;
* Anna Bijns-gebouw, Kievitplein, 2018 Antwerpen;
* Jacob Van Maerlant-gebouw, Koning Albert I-laan 1-2, 8200 Brugge;
* Virginie Loveling-gebouw, Koningin Maria Hendrikaplein 70, 9000 Gent;
* Hendrik Van Veldeke-gebouw, Koningin Astridlaan 50, 3500 Hasselt;
* Dirk Bouts-gebouw, Diestsepoort 6, 3000 Leuven;
* Arenberg-gebouw, Arenbergstraat 9, 1000 Brussel;
* Graaf de Ferraris-gebouw, Koning Albert II-laan 20, 1000 Brussel.

De pakketautomaten die Het Facilitair Bedrijf plaatst worden geleverd door Bringme. Hiervoor wordt gebruik gemaakt van de raamovereenkomst met Besteknummer 2020/HFB/MPMO/52629, namelijk de raamovereenkomst voor het leveren, plaatsen en huren van intelligente pakketautomaten en gerelateerde cloudtoepassingen in het kader van intuïtief onthaal.[[1]](#footnote-2)

De Bringme automaten laten toe dat een postbedrijf (Bpost, DHL, Post NL, Het Facilitair Bedrijf zelf …) een poststuk in de pakketautomaat achterlaat voor een bestemmeling. De pakketautomaat brengt de bestemmeling op de hoogte, via een notificatie, van het feit dat een poststuk voor hem aanwezig is in de pakketautomaat. Hiervoor verwerkt Bringme het professionele e-mailadres van de bestemmeling. Deze mailadressen zijn net als de namen van alle medewerkers van de entiteiten van de Vlaamse overheid opgeladen in de Bringme-software door een IDM-integratie. Concreet geeft een toekenning van het recht ‘DigiPost-gebruiker’ in IDM een medewerker ook het gebruiksrecht voor de pakketautomaat van Bringme.

De pakketautomaten van Bringme zijn via het bekabelde netwerk aangesloten. De authenticatie gebeurt via het 802.1x protocol. Op basis van deze authenticatie zal het toestel in het voorziene virtueel netwerk(VLAN) geplaatst worden met naam “Bringme”.

De pakketautomaten van Bringme moeten communiceren met enkele servers van Bringme. Hiervoor zijn de gevraagde datastromen opengezet. Alle andere verkeer of servers zijn niet toegestaan.

De software waarvan Bringme gebruik maakt, wordt gehost op Microsoft Azure. De locatie van de Microsoft Azure datacenters zijn West-Europa – Amsterdam.

#### Niet-scanbare poststukken

Poststukken die niet kunnen of mogen gedigitaliseerd worden, worden verdeeld via pakketautomaten. De volgende poststukken zijn aangemerkt als niet-digitaliseerbaar:

* Poststukken waarop op de enveloppe ‘vertrouwelijk’, ‘geheim’ of ‘medisch geheim’ vermeld wordt;
* Poststukken bestemd voor postbussen waarvan de desbetreffende entiteit heeft aangegeven dat er niet gedigitaliseerd mag worden. [In het geval van [NaamEntiteit] *zijn dit de volgende postbussen:* 
  + *aanvullen indien van toepassing];*
* Niet digitaliseerbare objecten (bv. boeken, tijdschriften, fysieke objecten …);
* [aanvullen door [NaamEntiteit] indien van toepassing].

### Verdeling in het DigiPost-platform (virtuele postvakken)

[NaamEntiteit] krijgt op het DigiPost-platform van Het Facilitair Bedrijf een ‘verdeelbak’ voor zijn entiteit. In deze verdeelbak komen enkel de berichten binnen voor die entiteit die door het DigiPost-team niet verder verdeeld konden worden dan op het niveau van de entiteit. Een entiteit bestaat steeds uit:

* Minimaal één postvak. Dit is een postvak dat door de entiteit vooraf is vastgelegd en ook steeds vernoemd wordt door de afzender (bv. postbus 50 van AGO op Havenlaan 88). Deze postvakken zijn steeds gekend door de scankamer en het is normaliter op dit niveau dat er gescand wordt. In concreto wordt elk fysiek postbusnummer vertaald naar een postvak
* x-aantal subpostvakken. Een subpostvak is een postvak dat door de entiteit zelf is aangemaakt met als doel om de verdeling intern te optimaliseren, maar een subpostvak is niet gekend in de scankamer. Het is wel mogelijk om documenten automatisch naar een intern postvak te sturen direct nadat ze gescand zijn, maar dan verloopt dit aan de hand van documentherkenning (in casu Maatwerk). Om documenten correct te kunnen herkennen is het een vereiste dat het om gestandaardiseerde documenten gaat (bv. formulieren, facturen …)

Daarnaast worden er ook postvakken op naam aangemaakt voor elk personeelslid van de Vlaamse overheid. Als er een bericht is toegewezen aan een individuele gebruiker krijgt deze daar een notificatie van. Om ervoor te zorgen dat er steeds opvolging mogelijk is, kan naast het personeelslid in kwestie ook de ‘verdeler’ en ‘admin’ (zie Annex I, meer bepaald onder 14.1 TOMs op niveau van verwerker Het Facilitair Bedrijf voor meer informatie over de rollen en rechten) aan dit bericht. Tijdens het pilootproject is, na bespreking met de pilootentiteiten, beslist dat Het Facilitair Bedrijf niet op naam verdeelt, aangezien dit in de praktijk verscheidene problemen met zich meebrengt:

* Het Facilitair Bedrijf weet niet of iemand met vakantie is;
* Het Facilitair Bedrijf weet niet of iemand uit dienst is;
* Heel wat poststukken zijn foutief geadresseerd door de afzender;
* Heel wat poststukken zijn geadresseerd aan personen die reeds uit dienst zijn;
* Het management doet zijn poststukken niet zelf open, maar dit gebeurt door een secretariaatsmedewerker.

In feite is dit dus dezelfde situatie als wat vandaag gebeurt. Iemand binnen de entiteit heeft de finale verantwoordelijkheid om het poststuk aan de juiste bestemmeling af te leveren (als het effectief op persoonsniveau is).

Het DigiPost-team krijgt zelf ook een eigen virtueel postvak. In het DigiPost-postvak komen alle berichten toe:

* die niet verdeeld kunnen worden o.b.v. vooraf bepaalde parameters (bv. als het poststuk geadresseerd is aan ‘de minister’, ‘de Vlaamse overheid’ …);
* die geweigerd worden door een entiteit.

Het DigiPost-team staat in voor de verdeling van die berichten die toekomen in het DigiPost-postvak.

Na de scanning wordt een bericht dus rechtstreeks afgeleverd in een postvak waarna het aan [NaamEntiteit] is om, indien nodig, de verdere verdeling (naar een specifiek persoon of een subpostvak) te doen.

Voor elk bericht zijn de volgende acties beschikbaar:

* Een bericht aanvaarden;

Bij aanvaarding wordt het bericht standaard (zonder begeleidend metadatabestand) gedownload op de PC van de persoon die het bericht aanvaard heeft. Het is ook mogelijk om het bericht na aanvaarding automatisch te laten afleveren op een vooraf gedefinieerde locatie. Concreet zijn er de volgende mogelijkheden:

* + Afleveren op een SharePoint locatie (poststuk + metadata)
  + Afleveren op een dropserver (poststuk + metadata)
  + Afleveren aan een (generieke) mailbox (poststuk + metadata)
  + Afleveren via API (poststuk + metadata)

De bovenstaande opties zijn in te stellen per (sub)postvak en worden beschouwd als Maatwerk, zijnde aanpassingen aan de software die specifieke voor 1 organisatie moet gebeuren of configuraties die verschillen per organisatie (bv. de afleverlocaties voor SharePoint …). [[2]](#footnote-3)

* Een herscan vragen van een specifiek bericht aan de scankamer (deze actie is tot 90 dagen na scanning beschikbaar)[[3]](#footnote-4);
* Het analoge originele bericht opvragen bij de scankamer (deze actie is tot 90 dagen na scanning beschikbaar)[[4]](#footnote-5);
* Een bericht doorsturen naar:
  + Een (ander) subpostvak binnen de entiteit;
  + Een andere entiteit;
  + Een specifieke persoon van de eigen entiteit (privé-postbus).
* Een bericht weigeren waardoor het, afhankelijk van de gekozen optie, teruggestuurd wordt naar ofwel:
  + het DigiPost-postvak;
  + de verdeler van de eigen entiteit.

De DigiPost-software stuurt (mail)notificaties om een gebruiker ervan te verwittigen dat in zijn ‘inbox’ één of meerdere berichten zijn toegekomen. Om te vermijden dat er een stroom aan notificaties komt, kan een gebruiker zelf kiezen op welk tijdstip of tijdstippen hij een notificatie wenst te ontvangen. Standaard is ingesteld dat om 14h op de dag van het bezorgen van het poststuk een notificatie wordt verstuurd naar de gebruiker. Deze notificatie vermeldt het aantal poststukken dat afgeleverd is, opgesplitst per type (bv. al dan niet aangetekend), en een link naar de poststukken zelf. Voor documenten die na een aanvraag tot herscannen terug aangeleverd worden in de ‘inbox’, wordt er steeds onmiddellijk een notificatie verstuurd naar de aanvrager.

De bovenstaande opties zijn in te stellen per (sub)postvak.

### Toegang tot het DigiPost-platform

De toegang tot het DigiPost-platform voor gebruikers wordt geregeld via ACM/IDM. Enkel gebruikers die de juiste rechten en rol hebben kunnen een document raadplegen. De volledige uitwerking van de rechten en rollen in het DigiPost-platform is beschreven in Annex I, meer bepaald onder 14.1 TOMs op niveau van verwerker Het Facilitair Bedrijf.

## Beschrijving van de context van de verwerkingen

De Vlaamse overheid streeft ernaar om een radicaal digitale overheid te zijn. Dit wordt duidelijk aangegeven in het Regeerakkoord 2019-2024: “*Tegelijk verhogen we de investeringen in de digitalisering van onze overheidsprocessen. We zetten in op gebruiksvriendelijkheid van de digitale platformen en zetten de agenda Radicaal Digitaal ambitieus verder.*”

Dit betekent concreet dat ernaar gestreefd wordt om elk proces volledig digitaal te laten verlopen, maar doordat niet alle actoren (burgers, andere overheden …) verplicht kunnen worden om digitaal met de Vlaamse overheid te communiceren, blijft elke Vlaamse overheidsinstantie nog analoge documenten ontvangen. Deze analoge documenten zijn zeer divers en dit zowel naar inhoud als naar vorm.

* **Divers naar inhoud** aangezien ze te maken hebben met verscheidene diensten/processen (bv. subsidieaanvragen, facturen, gerechtelijke dossiers, klachten …) of zelfs puur informatief zijn en niet gekoppeld zijn aan een specifiek proces (bv. boeken, reclamedrukwerk, kranten, tijdschriften …).
* **Divers naar vorm**, aangezien ze zowel aangetekend als niet-aangetekend kunnen zijn, ze de vorm kunnen aannemen van een postpakket.

Om de complexiteit en de administratieve lasten zo veel mogelijk weg te nemen bij  overheidsinstanties, is een gemeenschappelijke dienstverlening opgezet voor digitalisering van inkomende analoge poststukken onder de noemer ‘DigiPost’. Deze gemeenschappelijke dienstverlening is ingebed in Het Facilitair Bedrijf, aangezien artikel 4 van het oprichtingsbesluit van Het Facilitair Bedrijf duidelijk aangeeft dat dit agentschap tot taak heeft om zowel *duurzame facilitaire diensten marktconform aan te bieden* als *overheidsinstanties te ondersteunen bij de optimalisering van hun interne processen[[5]](#footnote-6)*.

Deze taken komen duidelijk tot uiting in de strategische doelstellingen van Het Facilitair Bedrijf. Deze strategische doelstellingen zijn te raadplegen op het intranet van de Vlaamse overheid.[[6]](#footnote-7)

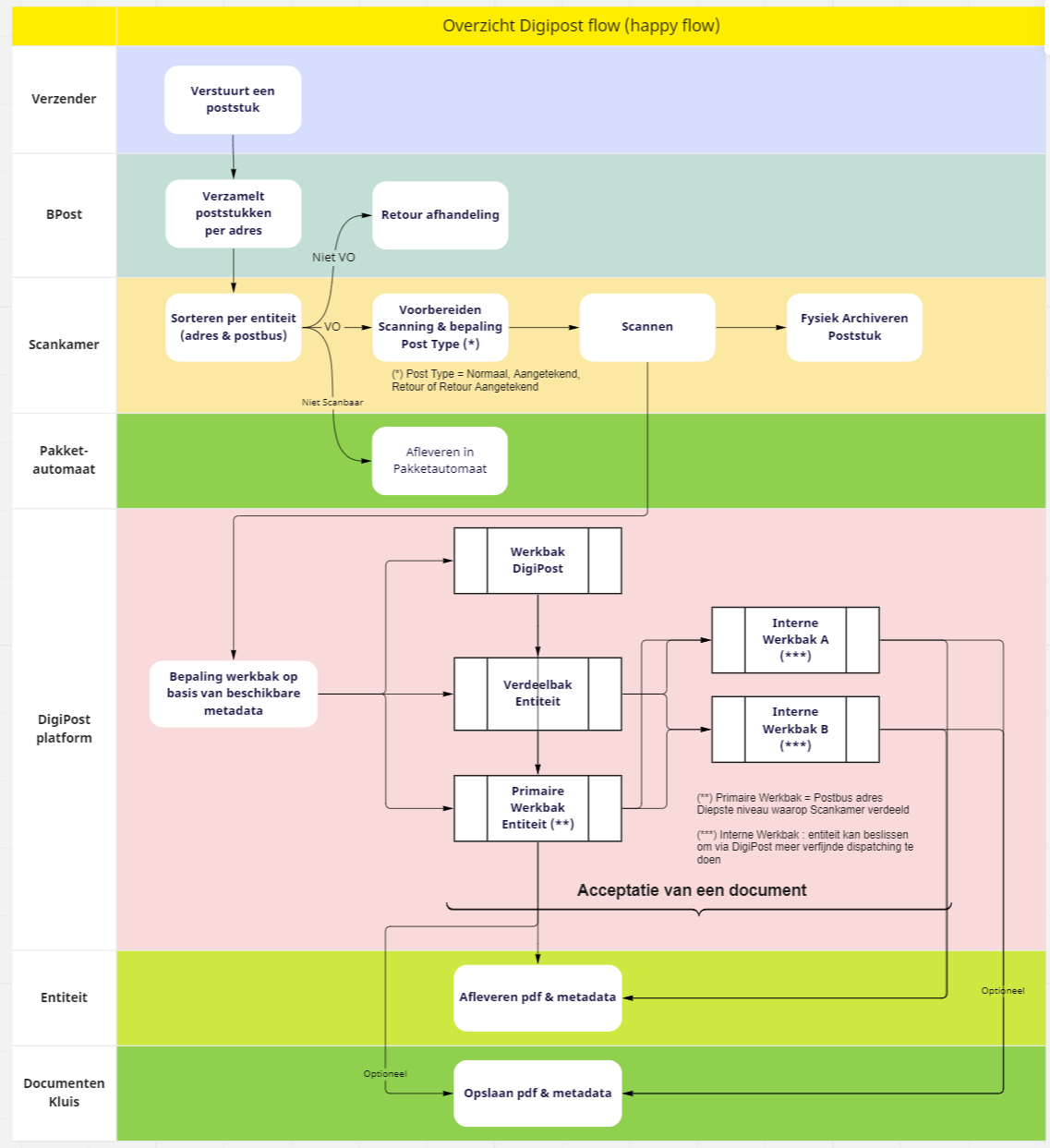
De digitalisering van analoge poststukken is een volgende evolutie in digitalisering en verhoging van efficiëntie van de VO waar [NaamEntiteit] deel van uit maakt.

De digitalisering van de inkomende poststukken heeft concreet volgende voordelen:

* **Efficiëntieverhoging**: Door in te zetten op digitalisering van inkomende poststukken, wordt een oplossing gecreëerd voor die processen die tot nu toe nog niet volledig gedigitaliseerd konden worden omdat er nog steeds analoge informatie ontvangen werd. Door de centralisatie gebeurt de verwerking van de poststukken op een gelijkaardige manier wat de verdere beheersing van bestuursdocumenten vergemakkelijkt.
* **Kostendaling door schaalgrootte**: Door digitalisering van de inkomende poststukken als een centrale/gemeenschappelijke dienstverlening op te zetten wordt een zekere schaalgrootte bereikt wat tot een kostendaling leidt op het niveau van de Vlaamse overheid.
* **Kostendaling door ‘insourcing’**: Het Facilitair Bedrijf kiest ervoor om DigiPost te organiseren met eigen mensen. Concreet betekent dit dat Het Facilitair Bedrijf de profielen die binnen Het Facilitair Bedrijf instonden voor de ontvangst en verdeling van post heroriënteert. Ook de profielen die binnen [NaamEntiteit]instonden voor de ontvangst en verdeling van post kunnen worden geheroriënteerd binnen de eigen entiteit of binnen de dienstverlening van Het Facilitair Bedrijf.
* **Flexibiliteit**: Door voor een gemeenschappelijke dienstverlening te kiezen kan er eenvoudig geschaald worden m.b.t. scanning bij piekmomenten.

## Systematische beschrijving van de verwerkingen (en verwerkingsdoelen)

Onderstaand schema bevat een weergave van het scanningsproces, onder de afbeelding wordt het proces in detail beschreven.



We maken een onderscheid in poststukken en postpakketten.

### Verwerking van poststukken[[7]](#footnote-8)

In de context van DigiPost verwerkt Het Facilitair Bedrijf poststukken binnen de 24 uur na ontvangst in de scankamer.[[8]](#footnote-9) Het verwerkingsproces verloopt als volgt:

1. **Levering van de poststukken**
   1. Het postbedrijf (in casu Bpost) levert zakken met gesloten enveloppen aan het onthaal van het Hendrik Conscience-gebouw. Bij ontvangst door het onthaal worden deze postzakken in een afgesloten ruimte geplaatst. Het onthaal geeft een signaal aan het scanteam waarna de postzakken worden opgehaald door een medewerker van het scanteam.
2. **Sortering**
   1. In de scankamer sorteren de medewerkers van het scanteam de gesloten poststukken per geadresseerde (niveau van entiteit / effectieve busnummers). Hiervoor wordt gebruik gemaakt van sorteerkasten.
   2. Als o.b.v. de enveloppe niet duidelijk is voor wie het poststuk bestemd is, wordt het poststuk geopend en wordt o.b.v. de inhoud een beoordeling gemaakt.
   3. De poststukken die niet gescand mogen/kunnen worden (bv. vertrouwelijke post) wordt hier d.m.v. de sortering uit het scanproces gehouden.
3. **Scanklaar maken**

Dit betekent dat de poststukken die gescand mogen/kunnen worden per entiteit/effectieve busnummer:

* 1. worden onderverdeeld in de volgende categorieën:
     1. Aangetekend poststuk
     2. Gewoon poststuk
     3. Aangetekend retour
     4. Gewone retour
  2. per categorie geopend worden om voor te bereiden voor scanning (bv. ontnieten, open plooien …).
  3. de enveloppes krijgen elk een eigen QR-code (deze geeft aan waar een nieuw poststuk begint en het huidige eindigt) en worden onderaan de inhoud van dat poststuk gelegd (op die manier komt de enveloppe na scanning achteraan de brief te zitten).

De poststukken zijn scanklaar als er een QR-code met aanduiding van de entiteit/busnummer bovenaan de te scannen poststukken ligt en elke categorie wordt voorafgegaan door een aparte QR-code die de desbetreffende categorie aanduidt.

De scanklare poststukken voor één entiteit/busnummer worden verder ‘batch’ genoemd.

1. **Kwaliteitscontrole** 
   1. Een controle per batch die dient om te valideren of de entiteit, het posttype, en de QR codes correct zijn;
   2. Deze controle wordt uitgevoerd door een andere medewerker dan diegene die de batch heeft samengesteld;
   3. Als er fouten worden vastgesteld dan zal de medewerker die de controle uitvoert deze fouten oplossen.
2. **Scanning** 
   1. Iedere batch wordt individueel in de scanner gelegd. De scanner verwerkt steeds één batch. Op dit ogenblik voert de scanmedewerker nog een extra (snelle) controle uit op dezelfde elementen als in stap 4.
   2. Als binnen een batch een document zit dat een buitenformaat heeft (bv. A0) wordt dit ene document met een specifiek daarvoor bedoelde scanner ingescand. A.d.h.v. een specifiek daarvoor bedoelde QR-code zal dit document nadien door de software in het juiste poststuk terecht komen.
   3. Het resultaat van een batch wordt op het scherm van een PC die aangesloten is op de scanner (scan PC) getoond. Dit laat toe dat een andere medewerker dan diegene die de scanning heeft uitgevoerd een validatie (bv. pagina’s juist, QR codes juist, alles recht gescand …) uitvoert vooraleer de batch afgesloten wordt.
3. **Behandeling analoge poststukken (‘archivering’)**
   1. Na afsluiten van de batch worden de analoge poststukken in een grote enveloppe gestopt. Op deze enveloppe wordt volgende informatie geschreven:
      1. Datum van de batch,
      2. Afkorting van de entiteit voor wie de batch bestemd is,
      3. batchnummer.
   2. De enveloppen worden nadien in een archiefdoos gestopt. Deze archiefdoos wordt in een aparte ruimte ondergebracht die grenst aan de scankamer. In deze ruimte worden alle archiefdozen van het scanningsproces tijdelijk (90 dagen) bewaard.
   3. Na 90 dagen zullen de archiefdozen verhuizen naar een ruimte in het kelderarchief van het Hendrik Conscience-gebouw.
   4. Eens DigiPost substitutie effectief in de praktijk brengt, zullen de analoge poststukken 90 dagen na scanning vernietigd worden. Deze vernietiging zal gebeuren via de afspraken voor vernietiging van vertrouwelijk papier. De binnen Het Facilitair Bedrijf gehanteerde afspraken over de vernietiging van vertrouwelijk papier zijn hier te vinden: <https://overheid.vlaanderen.be/onze-organisatie/het-facilitair-bedrijf/richtlijnen-voor-het-vernietigen-van-bestuursdocumenten>.[[9]](#footnote-10)
4. **Behandeling scans**
   1. De in stap 5 gevalideerde batch wordt door de software op de scanPC omgezet naar één PDF die de volledige batch bevat. Deze PDF wordt samen met een metadatabestand doorgestuurd naar het DigiPost platform. Dit metadatabestand bevat minimaal de volgende gegevens:
      1. Bestandsnaam;
      2. Datum- en tijdsstempel (het moment dat de scanoperator de batch afsluit);
      3. Aantal pagina’s;
      4. Code postvak;
      5. Code posttype (bv. gewone poststukken, aangetekend, retour gewoon, retour aangetekend);
      6. Sequencer (extra QR code om grote bundels te splitsen);
      7. Aangemelde gebruiker die oplaadt;
      8. Documenttype;
      9. Barcode van Bpost;
      10. ID van de archiefdoos waarin de originelen bewaard worden
   2. Vooraleer de in stap a benoemde PDF wordt opgeladen naar het DigiPost platform, wordt de samengestelde PDF op de scanPC door een OCR-applicatie verrijkt met een tekst-layer waardoor de bestemmeling later in een pdf viewer op tekst elementen kan gaan zoeken.
   3. Op het DigiPost-platform wordt de PDF die de volledige batch bevat opgedeeld in poststukken en verdeeld naar de juiste postvakken. Dit gebeurt respectievelijk a.d.h.v. van de QR-codes die op de enveloppes zijn aangebracht en de QR-codes die het postvak aanduiden.
5. **Aflevering van de gedigitaliseerde poststukken**
   1. De gebruiker krijgt een (mail)notificatie als een poststuk is:
      1. toegekend aan hem als persoon (dus op naam);
      2. toegekend aan een (sub)postvak waarvoor hij de rol ‘verdeler’ heeft.

De volledige oplijsting van de door [NaamEntiteit] gedefinieerde (sub)postvakken zijn opgenomen in titel 8.2.5.

* 1. De gebruiker voert de actie uit die van toepassing is op het desbetreffende poststuk:
     1. Aanvaarden: bevestiging dat het poststuk juist is afgeleverd. Deze actie zorgt ervoor dat het poststuk wordt afgeleverd op de juiste afleverlocatie. [[NaamEntiteit] heeft de volgende afleverlocatie(s) geactiveerd (schrappen wat niet past):
        + Standaard aflevermethode (download op PC gebruiker)
        + Afleveren op een SharePoint locatie
        + Afleveren op een dropserver
        + Afleveren aan een (generieke) mailbox
        + Afleveren via API]
     2. Afwijzen: afgewezen poststukken worden teruggestuurd naar ofwel:
        1. het DigiPost-postvak om handmatig nagekeken te worden door een DigiPost medewerkers;
        2. De verdeler van de entiteit die het dan aan de juiste bestemmeling dient toe te kennen.
     3. Doorsturen: een gebruiker ziet dat een poststuk wel degelijk voor zijn entiteit bedoeld is, maar niet voor dit specifieke postvak. Men kan een ander postvak aanduiden en het poststuk doorzenden naar dit postvak.
     4. Herscannen: het document wordt teruggestuurd naar het DigiPost-postvak met specifieke vermelding “Herscannen”. De software voorziet vervolgens een vermelding naar de archiefdoos om het document terug te vinden en een nieuwe scan uit te voeren inclusief unieke QR code die bij herscan ervoor zorgt dat de herscan terecht komt bij de aanvrager. Deze nieuwe scan komt vervolgens op het DigiPost-platform te staan en de aanvrager wordt via e-mailnotificatie op de hoogte gebracht.
     5. BringMe: een gebruiker kan ook vragen om het fysieke poststuk te ontvangen. Het fysieke poststuk wordt aan de aanvrager bezorgd via de pakketautomaten (Bringme). Deze flow wordt verder beschreven onder 7.3.2.
  2. De bestemmeling heeft zijn poststuk op de gewenste afleverlocatie.

### Verwerking van postpakketten (BringMe flow)

In detail verloopt het proces voor het verwerken van pakketten als volgt:

1. Bezorgers van pakketdiensten (bv. Bpost, DPD, PostNL, etc.) hebben rechtstreeks toegang tot de pakketautomaat om postpakketten af te leveren op naam van de bestemmeling.
2. De bezorger kan de naam van de bestemmeling opzoeken en selecteren, gezien alle werknemers van de Vlaamse overheid via IDM gekoppeld zijn aan alle pakketautomaten.
3. Via mail ontvangt de betrokken medewerker de mededeling dat een pakket klaarligt in een pakketautomaat. Via de app of *Bringme.com* kan de medewerker inloggen in het systeem van Bringme waar hij de QR-code kan ophalen die getoond moet worden op de pakketautomaat. Zonder deze QR-code kan de medewerker de pakketautomaat niet openen.
4. Wanneer een pakket niet gericht is aan een persoon, maar aan een entiteit wordt de e-mail gestuurd naar de vooraf aangeduide BringMe verantwoordelijke voor [NaamEntiteit].
5. Indien een medewerker ondanks herhaaldelijke notificaties en/of telefonisch contact een pakket niet uit de BringMe installatie haalt, zal dit pakket uit de installatie worden gehaald door Het Facilitair Bedrijf en bewaard worden door het onthaal/gebouwenteam van het desbetreffende kantoorgebouw. Het pakje wordt dan door het onthaal/gebouwenteam geregistreerd op *manager.bringme.com*. De medewerker ontvangt dan een notificatiemail dat hij/zij zijn pakje op de nieuwe locatie kan komen ophalen.

## Categorieën van persoonsgegevens

[Analoge poststukken kunnen potentieel alle mogelijke categorieën van persoonsgegevens bevatten. Het Facilitair Bedrijf is bij het opstellen van deze ‘“White Label” GEB uitgegaan van poststukken die gegevens bevatten die onder informatieklasse 4 vallen. Als dit voor jouw entiteit niet het geval is, dien je de DPIA aan te passen aan een lager classificatieniveau.] Voor poststukken die [NaamEntiteit] ontvangt die verder verwerkt worden in de gebruikelijke processen van [NaamEntiteit], zullen minstens volgende categorieën van persoonsgegevens verwerkt worden: [Vul hieronder aan welke categorieën van persoonsgegevens de gebruikelijke poststukken die jouw entiteit ontvangt bevatten].

* […]

Het is daarnaast steeds mogelijk dat poststukken worden toegezonden die niet vooraf voorzien waren. Dit kan gaan om burgers die ten onrechte besluiten om zeer gevoelige gegevens via post te versturen, of een incidentele situatie die leidt tot toezending van informatie die niet binnen een standaardproces valt. Door de aard van het poststuk in kwestie, is het niet mogelijk om voorafgaandelijk te bepalen welke categorieën van persoonsgegevens een poststuk zal bevatten.

Wat betreft Bringme worden de volgende categorieën van persoonsgegevens van medewerkers van de Vlaamse Overheid verwerkt:

* Persoonlijke identificatiegegevens (naam, familienaam)
* Contactgegevens (professioneel mailadres)
* Naam van de entiteit waarvoor de medewerker werkzaam is

## Beschrijving van de betrokkenen en andere actoren

### Betrokkenen

* Iedere burger die poststukken toezendt aan de Vlaamse overheid
* Iedere persoon die vermeld wordt in toegezonden poststukken
* Iedere medewerker van de Vlaamse overheid die poststukken ontvangt
* Gebruikers van de DigiPost software (gebruikersnaam (in casu voor- en achternaam, IDM-ID en professioneel e-mailadres)

### Andere actoren

**Het Facilitair Bedrijf**

Het Facilitair Bedrijf opereert als verwerker voor de gebruikers van het DigiPost platform, in dit geval [NaamEntiteit]. Deze hoedanigheid volgt uit het feit dat openen van poststukken voor andere entiteiten een verwerking inhoudt waarvoor Het Facilitair Bedrijf zelf geen rechtsgrond heeft, maar moet steunen op de rechtsgrond van [NaamEntiteit]voor het verwerken van binnenkomende poststukken in de context van toegekende wettelijke taken en verantwoordelijkheden (zie 8.1).

Dit is analoog aan soortgelijke verwerkingsactiviteiten in bijvoorbeeld de context van het MAGDA platform waarbij Digitaal Vlaanderen eveneens optreedt als verwerker.

**Cronos Public Services (CPS)**

Cronos Public Services is subverwerker voor Het Facilitair Bedrijf, die op hun beurt binnen de Cronos groep de firma’s FlinQ en Arxus hebben aangesteld voor de operationele uitvoering en ondersteuning binnen het DigiPost project.

**Microsoft**

Microsoft is subverwerker van Cronos Public Services. De DigiPost-software, die instaat voor de verdeling van (ingescande) documenten, is een SaaS-oplossing die gebruik maakt van Microsoft Azure voor wat betreft de hosting. De Microsoft Azure omgeving staat onder het beheer van Cronos Public Services.

**Bringme**

Bringme treedt op als subverwerker van Het Facilitair Bedrijf om de Bringme Boxen te voorzien. Bringme maakt hiervoor op zijn beurt gebruik van Microsoft Azure als subverwerker. Daarnaast treed Twilio (Sendgrid) op als subverwerker voor de notificaties en authenticatie. Voor hun klantendienst doet Bringme tot slot beroep op Zendesk als subverwerker.

# Noodzakelijkheid en evenredigheid

[Hieronder is door Het Facilitair Bedrijf een voorbereidende inschatting gemaakt van hoe de verwerking van poststukken via DigiPost voldoet aan de basisbeginselen van de AVG. Je kan hier zelf mee aan de slag. Het is uiteraard niet aan Het Facilitair Bedrijf om als verwerker een beoordeling te maken van de risico’s, bijgevolg kan alles indien gewenst aangevuld of aangepast worden. Graag wel de aanpassingen bespreken met Het Facilitair Bedrijf zodat mogelijke suggesties ook voor andere entiteiten kunnen meegenomen worden.]

## De rechtmatigheid van de verwerking

In de meeste gevallen hangt de rechtmatigheidsgrond – van een eventuele verwerking van persoonsgegevens die gepaard gaat met het openen en inscannen van poststukken – af van de verwerkingsactiviteit waarbij de via post ontvangen persoonsgegevens verder verwerkt zullen worden. Het openen en inscannen van poststukken is namelijk geen aparte verwerkingsactiviteit, maar is onderdeel van de gebruikelijke verwerkingen binnen de entiteit. De gebruikelijke en systematische verwerkingen zijn gebaseerd op [Schrappen wat niet past, vul desgewenst aan met een andere rechtsgrond indien van toepassing]:

* Art. 6, eerste lid b) AVG: de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen.
* Art. 6, eerste lid c) AVG: de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust.
* Art. 6, eerste lid e) AVG: de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen.
* […]

Voor de verwerking van bijzondere categorieën van persoonsgegevens moet de verwerking eveneens onder te brengen zijn bij een van de uitzonderingsgronden opgesomd onder art. 9 AVG. De gebruikelijke en systematische verwerkingen van bijzondere categorieën van persoonsgegevens zijn gebaseerd op [Schrappen wat niet past, vul desgewenst aan met een andere uitzonderingsgrond indien van toepassing]:

* Art. 9, tweede lid b) AVG: de verwerking is noodzakelijk met het oog op de uitvoering van verplichtingen en de uitoefening van specifieke rechten van de verwerkingsverantwoordelijke of de betrokkene op het gebied van het arbeidsrecht en het socialezekerheids- en socialebeschermingsrecht, voor zover zulks is toegestaan bij Unierecht of lidstatelijke recht of bij een collectieve overeenkomst op grond van lidstatelijk recht die passende waarborgen voor de grondrechten en de fundamentele belangen van de betrokkene biedt.
* Art. 9, tweede lid g) AVG: de verwerking is noodzakelijk om redenen van zwaarwegend algemeen belang, op grond van Unierecht of lidstatelijk recht, waarbij de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene.
* Art. 9, tweede lid i) AVG: de verwerking is noodzakelijk om redenen van algemeen belang op het gebied van de volksgezondheid, zoals bescherming tegen ernstige grensoverschrijdende gevaren voor de gezondheid of het waarborgen van hoge normen inzake kwaliteit en veiligheid van de gezondheidszorg en van geneesmiddelen of medische hulpmiddelen, op grond van Unierecht of lidstatelijk recht waarin passende en specifieke maatregelen zijn opgenomen ter bescherming van de rechten en vrijheden van de betrokkene, met name van het beroepsgeheim.
* […]

Concreet zijn de verwerkingsactiviteiten van [NaamEntiteit] gebaseerd op: [Vul hier aan welke wet- en regelgeving de basis vormt voor de taken van algemeen belang ofwel de wettelijke verplichtingen waarvoor het departement of agentschap de persoonsgegevens ontvangen via post verwerkt. Bv. oprichtingsbesluit of andere specifieke wet- en regelgeving]

* […]

## De basisbeginselen van de verwerking

### (Eerlijkheid) Behoorlijkheid en transparantie

Een verwerking is slechts behoorlijk voor zover die met de redelijke verwachtingen van de betrokkene overeenstemt. Hoewel het voor de betrokkene te verwachten is dat overheidsinstanties steeds meer digitaliseren, is het van groot belang dat de betrokkene over de geautomatiseerde verwerking van binnenkomende poststukken goed geïnformeerd wordt.

Daartoe zal Het Facilitair Bedrijf standaardteksten voorzien die op de website(s) van de Vlaamse overheid of op specifieke webpagina’s van [NaamEntiteit]geplaatst kunnen worden. Deze informatie zal door het Facilitair Bedrijf hoe dan ook gepubliceerd worden op een daarvoor voorziene webpagina in verband met DigiPost.

De standaardteksten hebben als doel om aan afzenders te verduidelijken dat hun analoge berichten bij ontvangst ingescand zullen worden door Het Facilitair Bedrijf om zo nadien aan de correcte bestemmeling te kunnen bezorgen. Onderstaande tekst, beoordeeld door Taaladvies, dient [NaamEntiteit]bij elk postadres te vermelden en ook verwerkt te worden in de privacyverklaring van [NaamEntiteit]:

*"Poststukken die naar dit adres worden gestuurd, worden ingescand en digitaal aan de geadresseerde bezorgd. Zo kan de Vlaamse overheid haar dossiers volledig digitaal behandelen. Poststukken met de vermelding ‘vertrouwelijk’ worden niet ingescand, maar ongeopend aan de geadresseerde bezorgd."*

[NaamEntiteit] heeft beslist om de betrokkene als volgt te informeren: [Beschrijf op welke manier de betrokkene door jouw entiteit geïnformeerd wordt]

* Via de algemene informatie en privacyverklaring gepubliceerd door Het Facilitair Bedrijf en door [NaamEntiteit];
* [Vul desgewenst een alternatief of aanvulling aan]
* Algemene communicatie vanuit de Vlaamse overheid, geïnitieerd door Het Facilitair Bedrijf.

### Doelbinding

[NaamEntiteit] verwerkt de persoonsgegevens uit de ontvangen poststukken voor de doeleinden die passen binnen de rechtmatigheidsgronden die onder punt 7.1 zijn opgenomen. Het gaat om de gebruikelijke processen en dus verwerkingsactiviteiten binnen de entiteit die in het verwerkingsregister zijn opgenomen, waarin de doeleinden welbepaald en uitdrukkelijk omschreven zijn. De persoonsgegevens die [NaamEntiteit] ontvangt via post worden binnen deze verwerkingsactiviteiten verwerkt.

[Indien er slechts beperkte verwerkingsactiviteiten zijn waarvoor er persoonsgegevens afkomstig uit poststukken verwerkt worden, kan hier de oplijsting van die doeleinden gemaakt worden. Indien dit een grote hoeveelheid verwerkingsactiviteiten betreft kan indien gewenst naar het verwerkingsregister van jouw entiteit verwezen worden.]

### Minimale gegevensverwerking

Bij de verwerking van poststukken worden geen aanvullende gegevens toegevoegd via andere bronnen. De verwerking van gegevens beperkt zich dus tot de gegevens die zelf door de afzender zijn toegestuurd aan [NaamEntiteit]. Dat betekent dat de betrokkene zelf in handen heeft welke gegevens hij bezorgt. In het geval het gaat om standaardformulieren die door de betrokkene zijn ingevuld in functie van de verdere verwerking in de gebruikelijke processen, dient het beginsel van minimale gegevensverwerking op dat niveau te worden beoordeeld.

Daarnaast voert de DigiPost-software *Optical Character Recognition* (verder: ‘OCR’) uit op de ingescande poststukken. Die functionaliteit scant de afbeelding van het poststuk, herkent de tekens en zet die vervolgens om in machineleesbare vorm. Op die manier wordt de tekst doorzoekbaar en kan die geselecteerd en gekopieerd worden. Deze functionaliteit laat eveneens toe poststukken automatisch toe te wijzen op basis van wat er door de software herkend wordt, bijvoorbeeld op basis van de vorm (bv. facturen).

Naast de extra functionaliteit houdt het gebruik van OCR ook een risico in, gezien naast de afbeeldingen van de poststukken ook de inhoud verwerkt wordt door de DigiPost-software. Dit risico wordt behandeld onder hoofdstuk 10.2. Desondanks doet het gebruik van OCR geen afbreuk aan het beginsel van minimale gegevensverwerking. Dat beginsel verlangt dat de verwerkte gegevens toereikend, ter zake dienend en beperkt tot wat noodzakelijk zijn voor de doeleinden waarvoor zij verwerkt worden. Hoewel het gebruik van OCR een extra gegeven oplevert, namelijk de machineleesbare tekst (in casu is deze ingebed in de PDF, het OCR’en van de poststukken genereert dus geen bijkomende file), dient dit extra gegeven nog steeds dezelfde doeleinden. De verwerkte gegevens moeten ook toereikend zijn. In de gedigitaliseerde wereld van vandaag is het namelijk moeilijk te verantwoorden dat medewerkers de tekst manueel zouden overtypen wanneer het mogelijk is die geautomatiseerd te laten verwerken. Dit komt ook de efficiënte werking van de overheid ten goede en laat toe een snelle(re) en klantvriendelijke dienstverlening uit te bouwen. In die zin is de verwerking van de machineleesbare tekst niet disproportioneel ten opzichte van het doel.

### Juistheid en Nauwkeurigheid

In de context van deze verwerking verlangt het juistheidsbeginsel dat de kwaliteit en juistheid van de scans gegarandeerd kan worden en dat er voorzien wordt in een gepast proces dat alle redelijke maatregelen voorziet om gegevens onverwijld te wissen of te verbeteren in situaties waarbij:

* Poststukken niet correct worden gescand door medewerkers DigiPost;
* Poststukken niet gescand kunnen worden;
* Poststukken verkeerd bezorgd worden.

Deze aspecten zijn benoemd in hoofdstuk 7.3. In hoofdstuk 10 zijn geïdentificeerde risico’s ten aanzien van juistheid en nauwkeurigheid benoemd.

### Opslagbeperking

Er bestaat een belangrijk onderscheid tussen de bewaartermijnen in de DigiPost-software zelf en bewaartermijnen voor de poststukken zelf zoals die in het Serieregister zijn vastgelegd. De DigiPost-software is enkel bedoeld voor het correct afleveren van het poststuk en is bijgevolg geen dossiersysteem. De poststukken worden uit DigiPost gehaald, ofwel via een automatische koppeling met een dossierbeheerssysteem, ofwel door een manuele actie (download). De stukken dienen daarna terecht komen in het dossier waartoe ze behoren.

[NaamEntiteit] zal op gebruikelijke wijze de bewaartermijnen zoals gedefinieerd in het Serieregister opvolgen, het gebruik van DigiPost heeft hier geen impact op. In de DigiPost-software wordt ervoor gekozen om met één bewaartermijn te werken voor alle poststukken die behandeld worden, met name 14 dagen. Concreet wordt het poststuk dus 14 dagen ter beschikking gehouden in de DigiPost-software.[[10]](#footnote-11) De metadata en logging, die geen persoonsgegevens van de betrokkenen bevatten, blijven na het verstrijken van de termijn wel bewaard in de DigiPost-software. Dit omwille van bewijsredenen i.k.v. substitutie.

In het kader van substitutie maakt de DigiPost-software het namelijk mogelijk om poststukken na ‘aanvaarding’ ook op te laten nemen in Documentenkluis. Dit zorgt ervoor dat de poststukken langer bewaard kunnen worden dan de hogervermelde termijn en vooral dat er duidelijke audit trail bestaat gedurende de levensduur van het poststuk. Deze audit trail is nodig o.w.v. bewijsredenen en aangezien dat de standaardafleverlocatie een hiaat doet ontstaan in de audit trail is hier een potentieel risico. Om dit risico te beperken is in de DigiPost-software voorzien dat per (sub)postvak een bewaartermijn uit een vooraf gedefinieerde lijst gekozen kan worden. Deze lijst is als volgt:

* *Geen bewaartermijn*: het document wordt 14 dagen ter beschikking gehouden in de DigiPost-software en na het verstrijken van deze termijn verwijderd. De metadata en de logging blijven wel bewaard in de DigiPost-software;
* *1 jaar*: het document + metadata + logging wordt weggeschreven naar Documentenkluis. De metadata en de logging blijft steeds ook bewaard in de DigiPost-software;
* *5 jaar*: het document + metadata + logging wordt weggeschreven naar Documentenkluis. De metadata en de logging blijft steeds ook bewaard in de DigiPost-software;
* *10 jaar*: het document + metadata + logging wordt weggeschreven naar Documentenkluis. De metadata en de logging blijft steeds ook bewaard in de DigiPost-software;
* *20 jaar*: het document + metadata + logging wordt weggeschreven naar Documentenkluis. De metadata en de logging blijft steeds ook bewaard in de DigiPost-software;
* *30 jaar*: het document + metadata + logging wordt weggeschreven naar Documentenkluis. De metadata en de logging blijft steeds ook bewaard in de DigiPost-software.

In één van de komende releases (2023) zullen de volgende mogelijkheden voorzien worden:

* Het toekennen van een zelf bepaalde termijn per (sub)postvak. Dit betekent dat de bewaartermijnen dus niet langer gelimiteerd zullen zijn tot bovenstaande opties.
* Het toekennen van een bewaartermijn op het niveau van een poststuk (zelfs als dit afwijkt van de logica die voorzien is op het niveau van het (sub)postvak waarin het poststuk zich bevindt).

Concreet kiest [NAAMENTITEIT], op moment van schrijven, voor de volgende bewaartermijnen per (sub)postvak.

[HANDLEIDING: in onderstaande tabel dient een oplijsting gemaakt te worden van alle (sub)postvakken met daarbij een aanduiding van de bewaartermijn die gehanteerd wordt.]

|  |  |  |
| --- | --- | --- |
| Naam (sub)postvak | Bewaartermijn uit keuzelijst | Bewaartermijn indien vrije keuze |
|  |  |  |

### Gegevensbeveiliging

Zie Annex I voor een overzicht van technische en organisatorische maatregelen, in aanvulling op de genomen maatregelen die genoemd worden in hoofdstuk 9 per risico.

### Gegevensbescherming door ontwerp en als standaardinstelling

De DigiPost-software is aangekocht via perceel 5 (Applicatiediensten) van de ICT-raamcontracten van de Vlaamse Overheid. Zowel in het basiscontract als in de service portfolio voor perceel 5 zijn uitgebreide afspraken opgenomen in verband met de verwerking van persoonsgegevens. Door gebruik te maken van de raamcontracten is verzekerd dat de nodige contractuele verbintenissen zoals bedoeld in art. 28 AVG met de dienstverlener tot stand zijn gekomen en dat de dienstverlener zich ertoe verbonden heeft de passende technische en organisatorische maatregelen ter beveiliging van de verwerking te nemen.

Daarnaast is zowel het opzet van DigiPost als de verwerkersovereenkomst voorgelegd aan de ‘juridische werkgroep AVG’ van het Stuurorgaan Vlaams Informatie en ICT-beleid en is aan elk beleidsdomein gevraagd feedback te verlenen door zowel hun juristen als hun DPO’s. Deze feedback is nadien uitgebreid besproken in de juridische werkgroep van 6 oktober 2022. Op basis van de opmerkingen afkomstig uit de beleidsdomeinen zijn verschillende aanpassingen gemaakt aan het ontwerp van DigiPost alsook aan het ontwerp van de verwerkersovereenkomst tussen Het Facilitair Bedrijf haar klanten. Een voorbereidend ontwerp van deze GEB is eveneens voor feedback bezorgd aan de leden van de juridische werkgroep op 28 oktober 2022. Deze feedback heeft geleid tot aanpassingen van dit document op 17 november 2022.

Standaardinstellingen:

* Gebruikersbeheer is standaard zo ingesteld dat alle medewerkers van de entiteit wel rechten hebben op de toepassing, maar in eerste instantie enkel die poststukken kunnen zien waartoe ze rechten hebben;
* Het is mogelijk om op het niveau van een scanjob eventueel te beslissen om al dan niet met OCR te scannen.

## Beoordeel de noodzakelijkheid en evenredigheid

Een verantwoording van de noodzakelijkheid en evenredigheid van de verwerking is al aan bod gekomen onder titel 8.2 en titel 8.2.3 en wordt bijgevolg hier niet hernomen.

# Methode voor beoordeling risico’s op rechten en vrijheden van betrokkenen

[Voor dit ontwerp is gebruik gemaakt van de risicoanalysemethodiek die in gebruik is bij Het Facilitair Bedrijf. Het staat je uiteraard vrij om af te wijken van de methodiek die hieronder gebruikt is en desgevallend gebruik te maken van de risicoanalyse en -beoordelingsmethodiek die in gebruik is bij je eigen entiteit.]

## Aanvaardbaarheidscriteria van negatieve effecten

De aanvaardbaarheidscriteria zijn gekoppeld aan de score die wordt toegekend aan een risico op basis van een combinatie van twee aspecten: de impact van het risico en de waarschijnlijkheid van het risico.

* Risico’s met een score “**hoog**” of “**zeer hoog**” kunnen niet geaccepteerd worden zonder bijkomende risicomaatregelen.
* Risico’s met een score “**gemiddeld**” worden idealiter nog verder behandeld. Het is mogelijk (en in bepaalde gevallen aangewezen) om hier nog bijkomende risicomaatregelen te nemen. Indien geen mogelijke aanvullende maatregelen voorhanden zijn, of bv. de kost van de maatregel niet in proportie tot het risico staat, kunnen deze risico’s geaccepteerd worden mits duidelijke en grondige motivatie.
* Risico’s met een score “**laag**” en “**zeer laag**” kunnen zonder bijkomende motivering geaccepteerd worden.

De cijferscores in het document dienen als volgt gelezen te worden:

* 1-4: zeer laag
* 5-7: laag
* 8-11: gemiddeld
* 12-15: hoog
* 16+: zeer hoog

## Risicoanalyse, -evaluatie en opvolging

De noodzaak voor de uitvoering van een GEB insinueert een context waarbinnen een verwerking gelet op de aard, de omvang, de context en de doeleinden waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

In het verdere verloop van deze GEB wordt telkens een risico besproken, welke aanvullende maatregelen er genomen worden, alsook welke beoordeling geleid heeft tot een score van het restrisico.

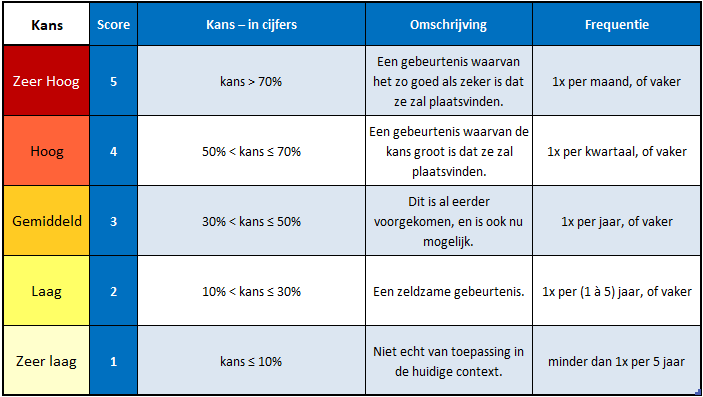
### Bepalen van de impact van een risico voor betrokkene

Om het impactniveau op de betrokkene te bepalen moet rekening gehouden worden met de rechten en vrijheden van de betrokkene, alsook met de gerechtvaardigde belangen zowel op economisch, fysiek of psychologisch vlak, zoals onder meer:

* Een mogelijk verlies aan zelfstandigheid (potentiële handelingen kunnen niet meer worden uitgevoerd);
* Vrij kunnen blijven van stigmatisering (hoe de betrokkene behandeld wordt op basis van bepaalde kenmerken);
* Gelijkheid (het op dezelfde wijze benaderen van de betrokkene);
* Bewegingsvrijheid (beperken van toegang tot bepaalde ruimtes of locaties);
* Vrij kunnen blijven van manipulatie (beïnvloeden van het gedrag op basis van de geschonden informatie);
* Integriteit (bv. door aanbieden van geschenken)
* Ongestoord leven (onaangenaam afbreken van rust en stilte)
* Eigenwaarde (afbreuk aan eigen persoonlijkheid)
* Autonomie (beperking van de vrijheid om eigen regels te volgen)
* Lichamelijke schade en bedreigingen
* Identiteitsfraude
* …



### Bepalen van de waarschijnlijkheid van een risico voor de betrokkene



# Beoordeling risico’s op rechten en vrijheden van betrokkenen

[Onderstaande risicoanalyse is een inschatting gemaakt door Het Facilitair Bedrijf op basis van poststukken die persoonsgegevens bevatten die onder informatieklasse 4 vallen. Om die reden is er van uitgegaan dat een schending van de vertrouwelijkheid door externen steeds met een hoge impact gepaard gaat. Voor een schending van de vertrouwelijkheid door internen is een gemiddelde impact geschat. De risico’s die hier in kaart gebracht zijn betreffen risico’s die gepaard gaan met het gebruik van de software en de werking van de scankamer. Het is eveneens mogelijk dat er risico’s ontstaan bij de entiteit zelf, deze risico’s zijn hier nog niet of in mindere mate uitgewerkt.

Het is uiteraard niet aan Het Facilitair Bedrijf om als verwerker een beoordeling te maken van de risico’s, bijgevolg kan alles indien gewenst aangevuld of aangepast worden. Afhankelijk van de verwachte gevoeligheid van de ontvangen poststukken kan de mogelijke impact van de betrokkene verschillen van het voorstel hieronder. De entiteit kan de impactniveaus dus naar onder bijstellen in het geval er slechts gegevens met classificatieniveau 3 of lager verwerkt worden. Het Facilitair Bedrijf adviseert om in dat geval de impact in geval van een vertrouwelijkheidsschending één niveau lager in te schatten. Graag wel de aanpassingen bespreken met Het Facilitair Bedrijf zodat mogelijke suggesties ook voor andere entiteiten kunnen meegenomen worden.

Hoewel BringMe in dit ontwerp ook besproken wordt, zijn hier geen risico’s m.b.t. het gebruik van BringMe opgenomen. Het gebruik van BringMe leidt namelijk niet tot een waarschijnlijk hoog risico voor de betrokkene.]

## Potentiële internationale doorgiftes doorgifte naar een niet-EER land/de Verenigde Staten van Amerika.

### Risico

Er wordt gebruik gemaakt van een subverwerker, in casu Microsoft, die buiten de Europese Economische Ruimte (EER) gevestigd is. Hierdoor is er een mogelijkheid tot internationale doorgifte van de verwerkte persoonsgegevens.

Zoals beschreven onder punt 6.5.2, wordt er beroep gedaan op de clouddienstverlening van Microsoft voor de hosting van de DigiPost-software. Met toepassing van de aanbevelingen van de EDPB moeten we dit als een mogelijke doorgifte naar de Verenigde Staten van Amerika beschouwen. Er dient dus beoordeeld te worden of de betrokkene als gevolg van de doorgifte van hetzelfde beschermingsniveau kan genieten, dan als wanneer er geen doorgifte zou plaatsvinden. De AVG stelt in Hoofdstuk V onder welke voorwaarden een doorgifte kan plaatsvinden.

Een doorgifte van persoonsgegevens kan onder meer plaatsvinden op basis van passende waarborgen zoals bedoeld in art. 46 AVG (de uitzonderingen bedoeld in art. 49 AVG zijn niet van toepassing voor deze GEB).

Microsoft maakt voor de gegevensdoorgifte gebruik van de Standaard Contractbepalingen (“**SCC’s**”) van de Europese Commissie, die toegevoegd worden als onderdeel van hun standaard verwerkersovereenkomst. Het is echter noodzakelijk om aanvullend het beschermingsniveau voor de betrokkene na te gaan. De VS beschikt over specifieke wetgeving (o.a. *Foreign Intelligence Surveillance Act* en *CLOUD Act*) die Amerikaanse inlichtingen- en ordediensten toe kan laten om toegang te krijgen tot gegevens in het beheer van ondernemingen die onder het toepassingsgebied van deze wetgeving vallen. Concreet zouden Amerikaanse inlichtingen- en ordediensten Microsoft kunnen verplichten om toegang te verlenen tot bepaalde gegevens. Daarnaast laat de wetgeving ook *bulk-surveillance* toe. Bovendien gaan de toegangsverzoeken meestal gepaard met zogenaamde *gagging-orders*, waardoor de onderneming (in casu Microsoft) haar klanten hier niet over kan informeren.

De wijze waarop deze toegang gebeurt en de (on)mogelijkheden die een betrokkene heeft om zich tegen deze toegang te verzetten gaan in tegen de fundamentele rechten die voorzien zijn onder artikel 7 en 8 van het Handvest van de Grondrechten van de Europese Unie en de waarborgen zoals voorzien in de AVG.

In het concrete geval van DigiPost wordt er bovendien gebruik gemaakt van optical character recognition (“OCR”) zodat tekst in documenten selecteerbaar wordt. Om dit mogelijk te maken worden ingescande documenten (die in wezen foto’s zijn) verwerkt tot tekst.[[11]](#footnote-12) Bijgevolg zal alle informatie van binnenkomende poststukken via het DigiPost platform verwerkt worden in de Microsoft Azure cloud.

Door gebruik te maken van Microsoft Azure is er dus een potentieel risico dat overheidsdiensten uit de Verenigde Staten inzage kunnen krijgen in de gegevens die door middel van DigiPost verwerkt worden. Dit zou een schending van de vertrouwelijkheid van de gegevens inhouden. De mogelijke gevolgen voor de rechten en vrijheden van de betrokkene hangen uiteraard af van de inhoud van de verwerkte poststukken, maar zijn onder meer:

* dat een verwerking van persoonsgegevens door Amerikaanse overheidsdiensten plaatsvindt zonder dat de betrokkene hierover geïnformeerd wordt;
* dat de betrokkene niet van voldoende rechtsbescherming door een onafhankelijke rechter kan genieten;
* dat de betrokkene in zijn bewegingsvrijheid beperkt wordt (bv. geen toegang meer krijgt tot het grondgebied van de Verenigde Staten);
* dat de betrokkene niet op gelijke wijze benaderd zou worden;
* dat de betrokkene bepaalde handelingen niet meer zou kunnen stellen;
* [Hier kunnen eventueel aanvullende gevolgen aangevuld worden]

### Maatregelen

Het Facilitair Bedrijf neemt minimaal volgende maatregelen:

* Er wordt voor bepaalde verwerkingen gebruik gemaakt van confidential computing. Confidential computing is een cloud computing-technologie waarbij gevoelige gegevens tijdens de verwerking worden geïsoleerd in een beschermde CPU-enclave. De inhoud van de enclave is alleen toegankelijk voor geautoriseerde gebruikers, en is onzichtbaar voor iets of iemand anders, inclusief de cloud provider, in casu Microsoft.
* De doorgifte van de persoonsgegevens wordt beperkt/bemoeilijkt doordat er gebruik gemaakt wordt van de KMSaas voor Azure die Digitaal Vlaanderen aanbiedt. Daarnaast wordt er voor het DigiPost-platform gebruik gemaakt van een Azure premium keyvault (FIPS 140-2 level 2).
* Specifieke Azure omgeving voor het DigiPost-platform met daarbinnen segmentering.
* Voor de encryptie van Data in motion worden enkel sleutels gebruikt die door de VO zelf zijn gegenereerd. Hierbij wordt gebruik gemaakt van TLS-certificaten voor HTTPS-verbindingen.
* Post die als ‘vertrouwelijk’ of ‘(medisch) geheim’ kwalificeert wordt, wordt uit het digitale circuit gehouden.
* Microsoft engageert zich er contractueel toe alle wettelijke middelen te gebruiken om zich te verzetten tegen doorgifte. Samengezien met de korte verwerkingstijd is de kans op een potentiële doorgifte minimaal.
* In de standaard verwerkersovereenkomst van Microsoft zijn de meest recente standaardcontractbepalingen van de Europese Commissie (“SCC’s”) opgenomen.
* Microsoft publiceert elke 6 maanden privacyrapporten waarin o.a. het aantal FISA-requests is opgenomen.
* Sinds 10 julii 2023 is er een nieuw adequaatheidsbesluit dat de doorgifte naar de VS positief evalueert en toelaat. Er wordt voor Digipost niet gerekend op dat adequaatheidsbesluit. Hoewel het adequaatheidsbesluit een voldoende beschermingsniveau zou kunnen verzekeren bieden die gekozen maatregelen een nog betere bescherming voor betrokkenen.

### Restrisicoscore

De kans op toegang door Amerikaanse overheden tot de gegevens wordt op laag ingeschat. Gelet op de gevoeligheid en de omvang van de gegevens (alle binnenkomende analoge poststukken van [NaamEntiteit]) wordt de impact voor de betrokkene op hoog ingeschat. Het restrisico komt op gemiddeld.

|  |  |  |
| --- | --- | --- |
| Kans |  | Laag |
| Impact |  | Hoog |
| Risico score: |  | Gemiddeld (8) |

## Gebruik OCR op binnenkomende poststukken

### Risico

De DigiPost-software voert *Optical Character Recognition* (verder: ‘OCR’) uit op de ingescande poststukken. Die functionaliteit scant de afbeelding van het poststuk, herkent de tekens en zet die vervolgens om in machineleesbare vorm. Deze machineleesbare tekst wordt als aparte ‘layer’ weggeschreven in het document en niet als een apart bestand bewaard.

Door gebruik te maken van OCR wordt de tekst doorzoekbaar en kan die geselecteerd en gekopieerd worden. Hoewel dit geen schending van het principe van minimale gegevensverwerking betekent (zie 7.2.3), houdt dit weliswaar een extra risico in voor de betrokkene, aangezien er op deze manier meer persoonsgegevens verwerkt worden dan het geval zou zijn wanneer de poststukken gewoon als scan (foto) bezorgd zouden worden aan de entiteit. De inhoud van het poststuk wordt namelijk op deze manier ook verwerkt door de DigiPost-software.

Een schending van de vertrouwelijkheid van de persoonsgegevens zou bijgevolg een grotere impact hebben op de betrokkene, dan wanneer enkel de scans van de poststukken verwerkt worden. De inhoud voor de poststukken zal namelijk niet alleen voor de diensten zelf makkelijk doorzoekbaar zijn, maar ook voor onbevoegde personen die toegang krijgen tot de gegevens.

### Maatregelen

De mogelijkheid tot het selecteren van tekst in de ingescande documenten is een vooruitgang ten opzichte van de huidige situatie waarin de inhoud van, vaak zeer lijvige, documenten manueel moet worden opgenomen. In de context van digitalisering is het tot op heden ook nadrukkelijk de verwachting van entiteiten die aansluiten op DigiPost dat OCR mogelijk is.

Dat gezegd zijnde, OCR is geen strikt noodzakelijke functie en Het Facilitair Bedrijf biedt de mogelijkheid aan entiteiten om OCR optioneel te maken in plaats van standaard. Op die manier kan per entiteit bepaald worden of OCR actief moet zijn wat hen de mogelijkheid geeft om in ieder geval zelf de afweging te maken of eventuele risico’s voldoende opwegen tegen de toegevoegde waarde van OCR.

### Restrisicoscore

De kans dat OCR een aanvullend risico voor de betrokkene betekent bovenop de vertrouwelijkheidsschending wordt als zeer laag ingeschat. Mocht er een vertrouwelijkheidsschending zijn zonder OCR, dan zou het voor malafide personen evenwel mogelijk zijn om zelf OCR op het gelekte beeldmateriaal uit te voeren. In die zin houdt dit een beperkt extra risico in. De impact van de schending blijft weliswaar hoog ingeschat.

|  |  |  |
| --- | --- | --- |
| Kans |  | Laag |
| Impact |  | Hoog |
| Risico score: |  | Gemiddeld (8) |

## Verlies informatie door noodsituatie in scankamer

### Risico

Bij een noodsituatie kan er informatie verloren gaan of tijdelijk onbeschikbaar zijn. In het geval van brand is het bijvoorbeeld mogelijk dat bepaalde nog niet ingescande poststukken verloren gaan. Een stroomuitval zou er toe kunnen leiden dat bepaalde poststukken niet snel genoeg ingescand kunnen worden. Mocht er een storing zijn met betrekking tot de Azure cloud is het mogelijk dat bepaalde poststukken niet, of niet snel genoeg, door de DigiPost-software kunnen verwerkt worden. Het is eveneens mogelijk dat er een storing is met de BringMe-software, waardoor de poststukken die normaal gezien niet door DigiPost verwerkt worden niet kunnen bezorgd worden.

Dergelijke noodsituaties kunnen nadelige gevolgen hebben voor betrokkenen. De noodzakelijke informatie zal namelijk niet beschikbaar zijn, waardoor bijvoorbeeld dossiers niet behandeld kunnen worden, bepaalde toekenningen niet of later plaatsvinden en bepaalde rechten niet (meer) uitgeoefend kunnen worden. In het geval van een tijdelijke onbeschikbaarheid van de informatie, kan dit rechtgezet worden zodra de informatie terug beschikbaar is. Het is bijvoorbeeld misschien mogelijk om een tijdelijke uitzondering op bepaalde termijnen te voorzien.

Wanneer de informatie echter permanent verloren is (zoals bij brand) kan de impact voor de betrokkene groter zijn. Het is namelijk niet eenvoudig om de betrokkene ervan op de hoogte te brengen dat de poststukken die hij of zij verstuurd heeft verloren gegaan zijn. Dit zal enkel kunnen mits algemene communicatie. Mogelijks zullen bepaalde afzenders deze informatie niet ontvangen, waardoor de situatie niet rechtgezet kan worden.

### Maatregelen

Algemeen is er door Het Facilitair Bedrijf voorzien in diverse standaardprocedures rond business continuity:

* Een eigen bedrijfscontinuiteitsplan en crisicommunicatieplan;
* Specifieke plannen in geval van o.a. elektriciteitsschaarste, pollutiepieken, verdachte pakketten met poeder.

Specifiek zijn er nog de volgende aspecten voorzien die het risico op onbeschikbaarheid van informatie of scankamer opvangen:

* Een alternatieve scanlocatie in het archiefdepot te Vilvoorde wanneer de centrale scanlocatie onbeschikbaar is.
* Bij volledige onbeschikbaarheid (bv. Uitval DigiPost platform door problemen bij hostingprovider): de mogelijkheid tot het bezorgen van fysieke poststukken voor hoogdringende zaken.
* SLA’s die zijn afgesproken met de verschillende leveranciers die garanties bieden rond de beschikbaarheid van gegevens.
* Interne werkinstructies naar medewerkers in de scankamer rond eten en drinken op de scanwerkplekken (niet toegestaan).

Er zijn brandblussers aanwezig in de scankamer.

Het Facilitair Bedrijf werkt momenteel ook de procedures uit voor het geval dat het archiefdepot te Vilvoorde de taken van de scankamer dient over te nemen.

### Restrisicoscore

De kans op een dergelijke noodsituatie wordt op zeer laag ingeschat, gezien het feit dat die tot nu toe slechts zeer zelden tot nooit zijn voorgevallen. Wanneer er zich een noodsituatie voordoet kan in het ergste geval informatie uit poststukken die op dat moment in de scankamer aanwezig zijn verloren gaan. Dit beperkt zich tot de poststukken die dezelfde week afgeleverd zijn, aangezien de overige poststukken in een andere ruimte bewaard worden. Gezien de kleine(re) groep betrokkenen wordt de impact op gemiddeld geschat. In vele gevallen zal de informatie ook hersteld kunnen worden, ofwel door ze opnieuw op te vragen, ofwel omdat de onbeschikbaarheid slechts tijdelijk is.

|  |  |  |
| --- | --- | --- |
| Kans |  | Zeer laag |
| Impact |  | Gemiddeld |
| Risico score: |  | Zeer laag (3) |

## Substitutie

### Risico

Het is de bedoeling dat DigiPost substitutie zal toepassen. Daarbij worden de analoge documenten vervangen door elektronische kopieën zonder dat de bewijskracht van het oorspronkelijke document verloren gaat. Om die reden hoeft de analoge informatie niet langer bewaard te worden.

Het is mogelijk dat er bij dit proces fouten gebeuren. Dit kan ertoe leiden dat de informatie onbeschikbaar is of dat de integriteit van de gegevens niet meer kan worden aangetoond. Dit kan nadelige gevolgen hebben voor betrokkenen doordat bijvoorbeeld dossiers niet behandeld kunnen worden, bepaalde toekenningen niet of later plaatsvinden of bepaalde rechten niet (meer) uitgeoefend kunnen worden.

### Maatregelen

Om gevolgen te beperken voor de betrokkene is besloten om voor 2023 de ingescande stukken nog fysiek te archiveren en nog niet na 90 dagen te vernietigen. Het Facilitair Bedrijf beschouwt 2023 namelijk als een jaar waarin er nog bijkomende maatregelen genomen kunnen worden en waarbij de procedure (o.b.v. feedback van klanten) bijgesteld kan worden.

De huidige aanpak en invulling van substitutie inclusief de werking van DigiPost, gedocumenteerd in de substitutieprocedure, is op 08/09/2022 goedgekeurd in de Werkgroep Archief- en Informatiebeheer die ressorteert onder het Stuurorgaan Vlaams Informatie- en ICT-beleid.[[12]](#footnote-13) Daarnaast maakt de procedure ook impliciet deel uit van de toetredingsovereenkomst waardoor elke entiteit de kans heeft om er feedback op te geven met zijn eigen procedures in het achterhoofd.

### Restrisicoscore

De mogelijkheid tot substitutie is vastgelegd in art. II.25 van het Bestuursdecreet van 7 december 2018 en verder tot uiting gebracht in het Besluit van de Vlaamse Regering van 21 mei 2021 tot regeling van de vervanging van analoge bestuursdocumenten door elektronische kopieën. Dit zorgt voor een sterke juridische basis, aangezien de bepalingen gelden voor alle bestuursdocumenten zelfs als ze ondertekend zijn met een natte handtekening. Omwille hiervan en samen met de uitgewerkte substitutieprocedure wordt de kans op een risico voor de betrokkene zeer laag ingeschat. De impact wordt op laag geschat, gezien mogelijke gevolgen voor de betrokkene steeds herstelbaar zullen zijn.

|  |  |  |
| --- | --- | --- |
| Kans |  | Zeer laag |
| Impact |  | Laag |
| Risico score: |  | Zeer laag (2) |

## Ongeoorloofde toegang – kwetsbaarheden in oplossing worden uitgebuit.

### Risico

Gekende of ongekende kwetsbaarheden in de applicatie kunnen door externen uitgebuit worden om toegang te krijgen tot de gegevens (hacking).

Diverse beveiligingsmaatregelen zijn in het huidige opzet van DigiPost nog niet volledig beschikbaar. Door het ontbreken van deze beveiligingsmaatregelen is het mogelijk dat onbevoegden toegang krijgen tot gegevens van betrokkenen.

Volgende beveiligingsmaatregelen dienen nog te worden geïmplementeerd, ofwel dient er een gelijkwaardig alternatief geïmplementeerd worden:

1. PAM oplossing Cyberark (veiligheidsbouwsteen Digitaal Vlaanderen) is nog niet actief, wat zorgt voor een onvoldoende audit trail rond gebruik geprivilegieerde toegangen.
2. Key Management via de digitale bouwsteen KMSaaS is niet beschikbaar in Azure omgevingen buiten de tenant van Digitaal Vlaanderen.
3. Fysieke beveiliging van de scankamer gebeurt vandaag aan de hand van sleutels en nog niet aan de hand van een badge-systeem.

Daarnaast is het ook mogelijk dat niet vooraf gekende kwetsbaarheden worden uitgebuit. In beide gevallen zou het om een schending van de vertrouwelijkheid van de gegevens gaan die gepaard gaat met verschillende risico’s voor de betrokkene zoals identiteitsdiefstal, financiële fraude (bv. scamming, phishing, smishing), afpersing, enz.

### Maatregelen

1. De PAMaas bouwsteen Cyberark (veiligheidsbouwsteen Digitaal Vlaanderen) wordt in productie gekoppeld vooraleer de oplossing naar alle VO-entiteiten wordt uitgerold. Dit zorgt ervoor dat er een volledige audit-trail beschikbaar is. De logs die door de PAMaas bouwsteen worden gegenereerd worden doorgegeven aan de SOC/SIEM bouwsteen van Digitaal Vlaanderen. Tijdens de pilootfase is er een alternatieve oplossing voor PAM aanwezig, namelijk dat Cronos (de leverancier van de DigiPost-software) steeds een schriftelijke goedkeuring vraagt aan een ICT-verantwoordelijke van Het Facilitair Bedrijf en de productmanager DigiPost van Het Facilitair Bedrijf. Dit is een tijdelijke oplossing waarbij de combinatie van de audit-trails in het DigiPost-platform als de schriftelijke goedkeuring van de hogergenoemde verantwoordelijken zorgen voor een duidelijk spoor van wijzigingen.
2. De KMSaaS bouwsteen voor Azure (veiligheidsbouwsteen Digitaal Vlaanderen) wordt in productie gekoppeld vooraleer de oplossing naar alle VO-entiteiten wordt uitgerold. Deze bouwsteen zal sleutels genereren voor de Azure Premium Keyvault die Het Facilitair Bedrijf zal opzetten. Tijdens de pilootfase wordt er gebruik gemaakt van default functionaliteit van Azure voor het beheren van de sleutels.
3. De fsyieke sleutels zijn beveiligd door middel van een certificaat waardoor deze niet zonder meer nagemaakt kunnen worden. Daarnaast is er een bestaand beleid rond toegangen (Link toegangsbeleid: <https://overheid.vlaanderen.be/facilitair-management/huisvesting/toegangsbeleid-grote-kantoorgebouwen>). Tenslotte worden medewerkers extra gesensibiliseerd over het verlenen van toegang tot de scankamer voor onbevoegden. Het Facilitair Bedrijf streeft ernaar om badgelezers te installeren die toegang tot de scankamer verschaft tegen 2024.
4. De volledige lijst van maatregelen (TOM’s) zijn opgelijst in Annex I – Technische en organisatorische maatregelen (TOMs).

De dienstverlener van Het Facilitair Bedrijf, Cronos Public Services, heeft een pentest uitgevoerd op de DigiPost-software (laatste versie 7 september 2022). De test heeft enkele kwetsbaarheden vastgesteld, waarvan de grootste onmiddellijk gepatcht zijn. Een gemiddelde kwetsbaarheid werd met de update van december verholpen en de lage kwetsbaarheden werden verholpen in de eerste release van 2023 (januari). Deze testen zullen periodiek herhaald worden, vandaar wordt de kans op laag ingeschat. Daarnaast worden er periodiek ook algemene security testen uitgevoerd door Digitaal Vlaanderen.

### Restrisicoscore:

De kans dat deze maatregelen niet toereikend zijn wordt als laag ingeschat. De impact van de schending blijft weliswaar hoog ingeschat, tijdens de pilootfase gezien het feit dat op dit ogenblik PAMaas nog niet geïmplementeerd is en dat er gebruik gemaakt wordt van de default functionaliteiten van Azure voor het sleutelbeheer. Deze inschatting sluit aan bij de inschatting van het reeds hoger besproken risico ‘Potentiële internationale doorgiftes doorgifte naar een niet-EER land/de Verenigde Staten van Amerika’, aangezien het hieraan gerelateerd is.

|  |  |  |
| --- | --- | --- |
| Kans |  | Laag |
| Impact |  | Hoog |
| Risico score: |  | Gemiddeld (8) |

## Ongeoorloofde toegang – scankamer

### Risico

De scankamer bevindt zich in het Hendrik Consciencegebouw. In dit gebouw zijn tevens vele andere diensten van de Vlaamse overheid gevestigd, bovendien komen vaak medewerkers van de Vlaamse overheid die elders gehuisvest zijn alsook externen op bezoek voor vergaderingen in het vergadercentrum op de eerste verdieping. Daarnaast worden ook regelmatig selectieproeven en examens van de Examencommissie georganiseerd in het gebouw. Dit alles leidt ertoe dat er veel personen in het gebouw van de scankamer kunnen zijn die geen toegang moeten en mogen hebben tot de scankamer.

In het geval de toegang tot de scankamer niet goed afgesloten wordt, of wanneer onbevoegden binnengelaten worden door de medewerkers van de scankamer, is het mogelijk dat deze onbevoegde personen kennis nemen van de informatie in de poststukken met een mogelijke schending van de vertrouwelijkheid van de informatie. Het is daarnaast ook mogelijk dat onbevoegden poststukken vernietigen. Dat kan per ongeluk zijn, omdat ze niet op de hoogte zijn van de beleidslijnen die van toepassing zijn in de scankamer (bv. i.v.m. eten en drinken), maar ook opzettelijk. Tijdens sluitingstijd van het gebouw (’s nachts) is er, ter voorkoming van inbraak, steeds een nachtwaker aanwezig in het gebouw.

Afhankelijk van de informatie kan een mogelijke schending van de vertrouwelijkheid voor de betrokkene verschillende gevolgen betekenen: identiteitsfraude, financiële fraude (scamming, phishing, smishing, …), afpersing, stigmatisering, ongelijke behandeling, enz. Een onbeschikbaarheid of vernietiging van de informatie kan er bijvoorbeeld toe leiden dat dossiers niet behandeld kunnen worden, bepaalde toekenningen niet of later plaatsvinden en bepaalde rechten niet (meer) uitgeoefend kunnen worden.

### Maatregelen

* Er zijn interne afspraken binnen het DigiPost-team dat de deur steeds gesloten wordt;
* De scankamer zit nu reeds in een (niet eenvoudig te bereiken) zone die enkel bereikbaar is met badge voor medewerkers van de Vlaamse overheid. Dit verkleint de kans op toegang voor externen aan de Vlaamse overheid;
* De deur van de scankamer zal daarnaast steeds afgesloten worden wanneer niemand aanwezig is. Vandaag hebben alle bevoegde medewerkers een sleutel. Met het gebouwenteam wordt echter onderzocht om een badgelezer te plaatsen (zie ook hoger). Dit zou de toegangscontrole verbeteren en vereenvoudigen;
* Er zijn interne afspraken binnen het DigiPost-team dat enkel bevoegde medewerkers toegelaten zijn in de scankamer.

### Restrisicoscore

Er zijn verschillende afspraken gemaakt binnen het DigiPost-team, desondanks blijft de menselijke factor spelen. Het is steeds mogelijk dat iemand vergeet de deur dicht te doen of af te sluiten wanneer er niemand meer aanwezig is. Vandaar wordt de kans als gemiddeld ingeschat. De kans kan verlagen wanneer een badgelezer geïnstalleerd zou worden. De scankamer is in principe niet bereikbaar voor externen. Als het risico zich voordoet zullen het dus doorgaans interne medewerkers van de Vlaamse overheid zijn die in de scankamer kunnen binnenkomen. Alle interne medewerkers zijn gehouden tot vertrouwelijkheid, ook de deontologische code is op hen van toepassing. Om die reden wordt de impact gemiddeld ingeschat.

|  |  |  |
| --- | --- | --- |
| Kans |  | Gemiddeld |
| Impact |  | Gemiddeld |
| Risico score: |  | Gemiddeld (9) |

## Ongeoorloofde toegang - gebruikersbeheer

### Risico

Het gebruikersbeheer voor de toegangen tot de DigiPost-software verloopt via het Vlaams toegangsbeheer ACM. Elke entiteit moet er zelf voor zorgen dat de gebruikersrechten actueel en op orde blijven. Het is echter mogelijk dat er ofwel bij Het Facilitair Bedrijf, ofwel bij [NaamEntiteit], foutieve of niet-proportionele toegangsrechten zijn toegekend. Daardoor zouden de medewerkers potentieel te veel rechten krijgen in de applicatie en meer gegevens te zien krijgen dan strikt noodzakelijk voor hun werk. Zo wordt de vertrouwelijkheid van de informatie geschonden. Afhankelijk van de informatie kan een mogelijke schending van de vertrouwelijkheid voor de betrokkene verschillende gevolgen betekenen: identiteitsfraude, financiële fraude (scamming, phishing, smishing, …), afpersing, stigmatisering, ongelijke behandeling, ...

### Maatregelen

* Standaard is de DigiPost-software geïntegreerd met ACM/IDM. Dit zorgt ervoor dat als de persoon uit dienst treedt of van organisatie verandert, de entiteit dit eenvoudig zelf kan aanpassen. Het is echter aan de entiteit zelf om dit op orde te houden
* Elke organisatie beschikt over een afgescheiden omgeving waardoor een gebruiker steeds enkel toegang heeft tot de berichten die bestemd zijn voor de eigen organisatie.
* De toegang tot de applicatie voor de systeembeheerders verloopt via PAMaas (in afwachting van PAMaas gelden er procedures.)

### Restrisico

Gezien het kan voorkomen dat iemand een andere functie gaat uitvoeren en er vergeten wordt rechten weg te nemen, wordt de kans op gemiddeld geschat. De impact wordt echter laag ingeschat gezien elke VO medewerker gehouden is tot vertrouwelijkheid en de deontologische code dient na te leven.

|  |  |  |
| --- | --- | --- |
| Kans |  | Gemiddeld |
| Impact |  | Laag |
| Risico score: |  | Laag (6) |

## Verkeerde bezorging

### Risico

Vanwege onbewuste fouten in de toekenning aan de geadresseerde (bv. fout in de toepassing, menselijke fout, afzender die foutief adresseert, …) komen ingescande poststukken bij de verkeerde entiteit of persoon terecht. Als gevolg hiervan wordt er kennisgenomen van persoonsgegevens van de betrokkene door een onbevoegde, of kunnen bepaalde rechten en aanspraken van de betrokkene niet of niet tijdig toegekend worden omdat de juiste stukken niet op de juiste plek terecht gekomen zijn.

### Maatregelen

Diverse maatregelen zijn toegepast om deze fouten te voorkomen:

* Binnen het proces in de scankamer is functiescheiding toegepast waardoor altijd minstens twee personen hebben gevalideerd of de poststukken correct zijn verwerkt voor die gescand wordt. Ook na scanning wordt een controle uitgevoerd. (zie hiervoor ook de beschrijving onder titel 6.3. Systematische beschrijving van de verwerkingen (en verwerkingsdoeleinden);
* De basis voor verzending naar postvakken is de koppeling met IDM, binnen de Vlaamse overheid de betrouwbaarste bron voor autorisatie van toegangen;
* Mocht een verkeerde verzending toch plaatsvinden, is dit een verzending binnen de Vlaamse overheid wat betekent dat iedere ontvanger gebonden is aan de verplichtingen uit het Vlaams Personeelsstatuut waarin een discretieplicht opgenomen is[[13]](#footnote-14). Bij Externen die geworven zijn via USG of bij medewerkers die tewerkgesteld worden via Vlaanderen Connect zijn standaard vertrouwelijksheidsbepalingen opgenomen in hun arbeidsovereenkomsten.
* Medewerkers zijn gesensibiliseerd rond de vertrouwelijkheid van de gegevens: niet enkel in het kader van de breder geldende discretieplicht als ambtenaar, maar ook specifiek voor hun rol in het DigiPost team.
* De poststempel van de enveloppe wordt altijd mee ingescand. Indien een betrokkene door tijdsverlies naar aanleiding van verkeerde postbezorging bepaalde aanspraken zou verliezen of niet tijdig zou indienen in een bepaalde procedure, kan aan de hand van het poststempel aangetoond worden dat de fout niet bij de betrokkene ligt.

### Restrisicoscore

Gezien poststukken vaak onvoldoende nauwkeurig geadresseerd zijn is het zeer waarschijnlijk dat er op regelmatige basis poststukken verkeerd toegewezen zullen worden. Om die reden wordt de kans van een foutieve verdeling hoog ingeschat. Echter het is niet omdat dit zich frequent kan voordoen, dat de betrokkene hier ook effectief nadeel van zal ondervinden. Daarom wordt de kans gemiddeld ingeschat. Hoewel alle medewerkers gehouden zijn tot vertrouwelijkheid en tot de deontologische code van de Vlaamse overheid, is het mogelijk dat bepaalde medewerkers regelmatig informatie te zien krijgen de ze niet strikt nodig hebben voor hun werk. Om die reden wordt de impact op gemiddeld geschat.

|  |  |  |
| --- | --- | --- |
| Kans |  | Gemiddeld |
| Impact |  | Gemiddeld |
| Risico score: |  | Gemiddeld (9) |

## Inbreuk na verkeerde bezorging

### Risico

Een foute bezorging kan in bepaalde gevallen gekwalificeerd worden als een inbreuk in verband met persoonsgegevens die gemeld moet worden aan de toezichthoudende autoriteit en in bepaalde gevallen aan de betrokkene zelf. Het is mogelijk dat een verkeerde bezorging onbewust en onbedoeld niet als een inbreuk geregistreerd wordt, wanneer dit wel had moeten gebeuren. Dit is bijvoorbeeld het geval wanneer de DPO van de entiteit in kwestie niet op de hoogte gebracht wordt om hierover een juiste inschatting te maken. Zo lang de foute bezorging geen waarschijnlijk risico voor de betrokkene inhoudt dient er geen melding te gebeuren. Het is echter nodig om toezicht te houden op foutieve bezorgingen om telkens het risico voor de betrokkene te beoordelen.

Er is bijgevolg een risico dat er zich een inbreuk voordoet, maar dat niemand (of toch niet de juiste personen) ervan op de hoogte is. Daardoor kunnen geen mitigerende maatregelen genomen worden om het risico te beperken of om de vertrouwelijkheidsschending te stoppen en zal de inbreuk niet gemeld worden aan de toezichthoudende autoriteit, maar ook niet aan de betrokkene (mocht de inbreuk dat vragen in overeenstemming met art. 34 AVG). Het gevolg is dat de betrokkene niet op de hoogte is en zelf eveneens geen acties kan ondernemen om eventuele nadelige gevolgen te beperken.

### Maatregelen

De belangrijkste maatregel om dit risico te beperken is gelegen in het verstrekken van signalen aan de DPO van een verkeerde bezorging, zodat de DPO zorg kan dragen voor een correcte afhandeling.

Er zijn twee variaties mogelijk wanneer poststukken verkeerd bezorgd zou worden:

* Poststukken komen bij de verkeerde entiteit terecht, die gebruik maakt van de functionaliteit om zelf de poststukken juist door te sturen naar de correcte entiteit
* Poststukken komen bij de verkeerde entiteit terecht en wordt teruggestuurd naar het DigiPost-team waarna handmatig een correcte adressering plaatsvindt

In één van de komende releases wordt een ‘knop’ toegevoegd op het niveau van een poststuk waarmee een gebruiker een melding van een inbreuk kan aangeven aan de DPO. Daarnaast zal er ook een rapportering voorzien worden die duidelijk maakt hoe vaak de hierboven beschreven acties (terugsturen naar DigiPost en doorsturen naar de correcte entiteit) gebruikt worden.

### Restrisicoscore

Gezien er door Het Facilitair Bedrijf een proces wordt voorzien dat mogelijk maakt om de DPO op de hoogte te brengen van foutieve bezorgingen is de kans dat een inbreuk onder de radar blijft laag. De impact wordt als gemiddeld ingeschat, gezien het om een interne vertrouwelijkheidsschending zou gaan.

|  |  |  |
| --- | --- | --- |
| Kans |  | Laag |
| Impact |  | Gemiddeld |
| Risico score: |  | Laag (6) |

## Schending briefgeheim

### Risico

De verwerking van poststukken door Het Facilitair Bedrijf kan mogelijks een schending van het briefgeheim betekenen. Doordat Het Facilitair Bedrijf de poststukken opent, en niet de bestemmeling zelf, is er altijd een kleine kans dat er een impact is op de rechten en vrijheden van de betrokkene. Dit zou als een schending van de vertrouwelijkheid kunnen beschouwd worden met een potentieel gelijkaardige impact als vorige vertrouwelijkheidsrisico’s: identiteitsfraude, financiële fraude (scamming, phishing, smishing, …), afpersing, stigmatisering, ongelijke behandeling, enz.

### Maatregelen

Het Facilitair Bedrijf heeft met betrekking tot de problematiek van het briefgeheim advies gevraagd aan advocatenkantoor Eubelius. In dit advies worden een aantal maatregelen opgelijst die Het Facilitair Bedrijf kan nemen m.b.t. het risico rond schending van het briefgeheim. De volgende maatregelen zijn nu reeds opgenomen door Het Facilitair Bedrijf:

* Alle scanoperatoren ondertekenen een geheimhoudingsverklaring;
* Er wordt een nieuw artikel toegevoegd in het Bestuursdecreet dat de basis biedt aan de scankamer van Het Facilitair Bedrijf voor het openen van poststukken (de tekst hiervan, is na advies van VTC een tweede keer principieel goedkeurd op 17 februari 2023);
* Er worden overeenkomsten gesloten met de entiteiten;
* Er zal transparant gecommuniceerd worden naar (potentiële) afzenders van analoge poststukken over het feit dat de analoge poststukken zullen worden gedigitaliseerd door Het Facilitair Bedrijf (meer info hierover onder 7.2.1. );
* Er worden interne procedures uitgewerkt voor de scankamer (werkinstructies);
* Er worden aanvullende technische en organisatorische maatregelen genomen, zie annex I.

De tekst van het hierboven vermelde nieuwe artikel dat toegevoegd wordt in het Bestuursdecreet is te raadplegen in Annex II.

### Restrisicoscore

Gezien de aanvullende maatregelen die Het Facilitair Bedrijf genomen heeft wordt de kans op een risico voor de betrokkene op zeer laag ingeschat. Bovendien hebben de scanmedewerkers veel poststukken te verwerken en zal er geen tijd zijn om de poststukken door te nemen. Enkel een kleine groep scanmedewerkers zou theoretisch de poststukken kunnen inzien. Gezien de vele afspraken en goede training wordt de impact bijgevolg op gemiddeld geschat.

|  |  |  |
| --- | --- | --- |
| Kans |  | Zeer laag |
| Impact |  | Gemiddeld |
| Risico score: |  | Zeer laag (3) |

## Niet naleven van de afspraken m.b.t. vertrouwelijke poststukken en gemaakte afspraken m.b.t. niet scanbare poststukken

### Risico

Alle poststukken worden ingescand. Ook die poststukken waarvoor andere afspraken gelden.

### Maatregelen:

Het Facilitair Bedrijf maakt met de entiteiten van de Vlaamse overheid afspraken over welke poststukken niet gescand mogen worden. Deze poststukken worden via de pakketautomaten van Bringme verdeeld. Concreet betreft het o.a.

* Enveloppes waarop duidelijk ‘vertrouwelijk’ is vermeld;
* Enveloppes waarop duidelijk ‘geheim’ is vermeld;
* Enveloppes waarop duidelijk ‘medisch geheim’ is vermeld;
* Poststukken die bestemd zijn voor postbusnummers waarvoor afgesproken is dat alle poststukken die op die postbus toekomen niet gescand mogen worden;
  + Deze postbussen zullen bij de verdeling in de scankamer met kleurcodes aangeduid worden in de ‘sorteerkasten’. Op die manier is het voor de medewerkers snel duidelijk welke postbussen nooit geopend en gescand mogen worden
* Meldingen van klokkenluiders:
  + Op VO-niveau wordt er 1 centraal postadres (incl. specifiek busnummer) gecreëerd waarnaar klokkenluiders hun meldingen moeten sturen. Op de enveloppe moeten ze dan ook duidelijk vermelden voor wie (persoon) die melding bestemd is;
  + Alles dat bestemd is voor dat specifieke postadres zal NOOIT ingescand worden en steeds fysiek verdeeld worden door Het Facilitair Bedrijf (via de pakketautomaten) op naam van de bestemmeling;
  + Bovenstaande zal door AGO vastgelegd worden in een algemeen VO-afsprakenkader over klokkenluiders en ook duidelijk gecommuniceerd worden op de (nog op te maken) webpagina m.b.t. de klokkenluidersregeling.
* [specifieke afspraken met uw entiteit dienen hier uitgewerkt te worden]

### Restrisicoscore:

|  |  |  |
| --- | --- | --- |
| Kans |  | Laag |
| Impact |  | Gemiddeld |
| Risico score: |  | Gemiddeld (3) |

## Onethisch gebruik door personen met geoorloofde toegang – verspreiden van informatie

### Risico

Personen met geoorloofde toegang nemen kennis van informatie (bv. door het nemen van foto’s, het lezen van poststukken, het kopiëren van OCR-data …) en verspreiden deze informatie publiek of intern. Als gevolg hiervan wordt er kennis genomen van persoonsgegevens van de betrokkene door een onbevoegde wat kan leiden tot misbruik van gegevens door derden met schade voor de betrokkene tot gevolg. De mogelijke gevolgen voor de betrokkene zijn gelijkaardig aan vorige vertrouwelijkheidsrisico’s: identiteitsfraude, financiële fraude (scamming, phishing, smishing, …), afpersing, stigmatisering, ongelijke behandeling, enz.

### Maatregelen

De volgende maatregelen zijn toegepast om dit risico te beperken:

* Iedere medewerker is gebonden aan de verplichtingen uit het Vlaams Personeelsstatuut waarin een discretieplicht opgenomen is.
* Medewerkers zijn gesensibiliseerd rond de vertrouwelijkheid van de gegevens: niet enkel in het kader van de breder geldende discretieplicht als ambtenaar, maar ook specifiek voor hun rol in het DigiPost team.
* Elke medewerker in de scankamer heeft een vertrouwelijkheidsverklaring getekend in aanvulling op de geldende voorschriften rond discretieplicht.
* Door middel van de toepassing van logging is te achterhalen wie welke gegevens heeft geraadpleegd. Deze maatregel helpt niet alleen misbruik op te sporen, maar heeft ook een afschrikkende werking.

### Restrisicoscore

Hieronder wordt het risico in twee opgesplitst. Enerzijds het risico voor de betrokkene wanneer deze informatie publiek verspreid wordt, anderzijds wanneer deze intern binnen de Vlaamse overheid verspreid wordt. De kans wordt in beide scenario’s hetzelfde ingeschat omdat dezelfde maatregelen voor de medewerkers van de scankamer van toepassing zijn. De impact van een interne verspreiding wordt als iets lager ingeschat gezien elke medewerker van de Vlaamse overheid gehouden is tot vertrouwelijkheid en de deontologische code dient te respecteren.

Publieke verspreiding

|  |  |  |
| --- | --- | --- |
| Kans |  | Laag |
| Impact |  | Hoog |
| Risico score: |  | Gemiddeld (8) |

Interne verspreiding

|  |  |  |
| --- | --- | --- |
| Kans |  | Laag |
| Impact |  | Gemiddeld |
| Risico score: |  | Laag (6) |

## Menselijke fout in de scankamer

### Risico

Er is een risico dat medewerkers van de scankamer, ondanks goede instructies en opleiding, bewust of onbewust een schending van de vertrouwelijkheid of de beschikbaarheid van de informatie veroorzaken. Het is mogelijk dat medewerkers, alle inspanningen ten spijt, onvoldoende geïnformeerd zijn over hoe om te gaan met de verwerking van persoonsgegevens en daardoor een inbreuk veroorzaken. Bijvoorbeeld: poststukken worden (per ongeluk) meegenomen naar huis, worden in een verkeerde doos of container geplaatst, ongecontroleerde vernietigingen die niet via de normale vernietigingsflow lopen, enz.

Daarnaast kan een fout ook tot de onbeschikbaarheid of vernietiging van de poststukken leiden. Bv. een brief wordt als kladpapier gebruikt, poststukken worden (al dan niet bewust) in de gewone papiermand gegooid, poststukken worden maar half of zelfs niet ingescand, enz.

### Maatregelen

* Elke medewerker in de scankamer heeft een aanvullende vertrouwelijkheidsverklaring getekend, en is daarnaast ook gehouden tot vertrouwelijkheid zoals in het Vlaams Personeelsstatuut is opgenomen. De deontologische code is eveneens van toepassing op de medewerkers van de scankamer;
* Wanneer de medewerkers starten in de scankamer krijgen ze elk een duidelijke opleiding over hoe ze moeten omgaan met informatie;
* Binnen het proces in de scankamer is functiescheiding toegepast waardoor altijd minstens twee personen hebben gevalideerd of de poststukken juist zijn verwerkt voor die gescand worden. Bijgevolg zijn ook steeds meerdere medewerkers in de scankamer aanwezig. Het vier-ogenprincipe wordt toegepast;
* De scankamer gebruikt QR-codes om poststukken van elkaar te onderscheiden en om de verdeling te verzorgen;
* Er zijn aparte papiercontainers die specifiek bedoeld zijn om vertrouwelijke informatie te vernietigen. Hiervoor zijn aparte afspraken gemaakt binnen het afvalcontract. Er kunnen bij dit soort vernietigingen certificaten afgeleverd worden door de vernietigingsfirma. Deze certificaten tonen aan dat het papier effectief zodanig vernietigd is dat er geen informatie gerecupereerd kan worden.

### Restrisicoscore

De kans dat dit risico zich voordoet wordt laag ingeschat. De goede opleiding, contractuele maatregelen en vier-ogenprincipe beperkt de kans op een onbewuste fout. Daarnaast zijn moedwillige fouten zeer zeldzaam. De impact op de betrokkene van een vertrouwelijkheidsschending of verlies van informatie kan hoog zijn.

|  |  |  |
| --- | --- | --- |
| Kans |  | Laag |
| Impact |  | Hoog |
| Risico score: |  | Gemiddeld (8) |

## Te late reactie op ontvangen poststukken

### Risico

Het is steeds mogelijk dat de medewerkers die normaal gezien het postvak van hun entiteit moeten opvolgen te lang wachten om poststukken te behandelen. Dit kan een tijdelijke onbeschikbaarheid van informatie met zich meebrengen. Dit kan gebeuren omdat bepaalde poststukken over het hoofd gezien worden, door een lange vakantie of andere afwezigheid. Het risico voor de betrokkene is dat zijn dossier niet (op tijd) behandeld wordt, bepaalde toekenningen niet of later plaatsvinden en bepaalde rechten niet (meer) uitgeoefend kunnen worden.

### Maatregelen

* Eventuele niet behandelde poststukken worden zeer pertinent in beeld gebracht door de DigiPost-software. Het is bijgevolg niet eenvoudig om die per ongeluk over het hoofd te zien.
* De verdelers en admin van elke entiteit zien eveneens de nog niet behandelde poststukken staan en kunnen de nodige acties ondernemen zodat de poststukken wel behandeld worden.
* [aanvullen met maatregelen die de entiteit zelf neemt]

### Restrisicoscore

|  |  |  |
| --- | --- | --- |
| Kans |  | Zeer laag |
| Impact |  | Hoog |
| Risico score: |  | Zeer laag (4) |

# Mening betrokkenen/vertegenwoordigers over de verwerking (verplicht)

Gezien de grote hoeveelheid poststukken die de Vlaamse overheid ontvangt en de diverse groep aan betrokkenen zijn de betrokkenen niet geraadpleegd bij het opstellen van deze GEB. De Vlaamse overheid ontvangt miljoenen poststukken per jaar. Het zou bijgevolg een onredelijke inspanning vragen om alle betrokkenen individueel te contacteren.

Verdere digitalisering van overheidsdienstverlening past binnen de strategie van de Vlaamse regering binnen het programma Vlaamse Veerkracht ( https://www.vlaanderen.be/vlaamse-regering/vlaamse-veerkracht/vlaanderen-digitaal-transformeren). Om die reden is het waarschijnlijk dat verdere digitalisering van de overheid binnen de redelijke verwachtingen van de betrokkenen valt, alsook gezien de algemene tendens daartoe. Daarnaast laat deze dienstverlening, ondanks de verdere digitalisering, ook de mensen die analoog contact willen nemen met de Vlaamse overheid nog steeds toe om op de oude vertrouwde manier contact te nemen.

# Adviezen betreffende de GEB (verplicht)

## Advies functionaris voor gegevensbescherming (FG)

[Vraag advies aan je eigen DPO]

## Voorafgaande raadpleging bij de toezichthouder (verplicht bij hoog restrisico)

[Aan te vullen indien je beslist om een voorafgaande raadpleging te doen bij de toezichthoudende autoriteit.]

## Overzicht van de acties die de verwerkingsverantwoordelijke neemt naaar aanleiding van het advies van de functionaris en de raapleging van de toezichthouder

[Aan te vullen door entiteit indien je na advies DPO en/of een voorafgaande raadpleging nog aanvullende maatregelen hebt genomen.]

# Besluit van de verwerkingsverantwoordelijke (verplicht)

[Besluit van de entiteit]

# Annex I – Technische en organisatorische maatregelen (TOMs)

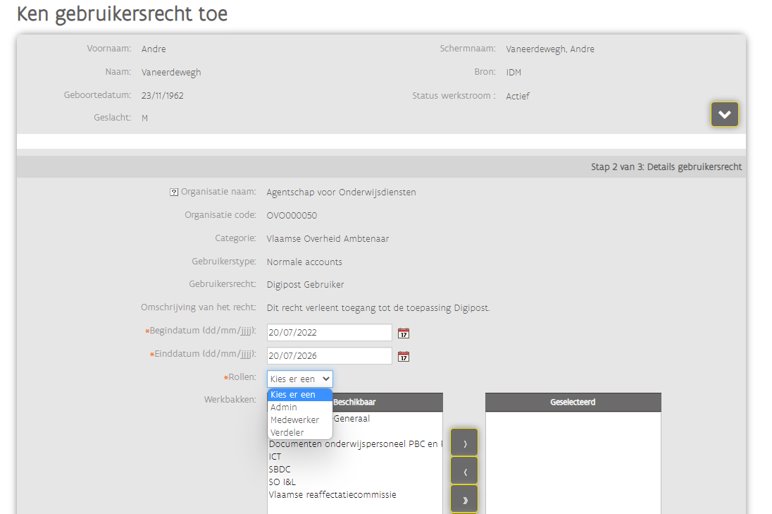
## TOMs op niveau van verwerker Het Facilitair Bedrijf

### Toegang tot het DigiPost platform voor gebruikers

De toegang tot postvakken wordt geregeld met ‘Rollen en Rechten’. Om dit te beheren is de DigiPost-software gekoppeld met toegangs- en gebruikersbeheer van de Vlaamse overheid (ACM/IDM). Het is dus de entiteit zelf die bepaalt wie wat kan zien en doen. Het DigiPost-recht en de rol ‘medewerker’ wordt standaard aan alle personeelsleden van een organisatie toegekend. Hierdoor kan elke gebruiker sowieso privé-post (= poststukken op naam) ontvangen en gebruikmaken van de pakketautomaten.

Inloggen in het DigiPost-platform is zoals hierboven aangegeven enkel mogelijk via ACM/IDM. Dit betekent concreet dat:

* een gebruiker bij het inloggen zich steeds dient te authenticeren via de toegestane multi-factor authenticatiemethodes;
* rollen en toegangen worden beheerd in IDM en kunnen enkel aangepast worden door de lokale beheerders;
* er reeds procedures bestaan voor het actueel houden van gebruikersrechten. Als een medewerker de organisatie verlaat worden sowieso zijn rechten verwijderd in IDM waardoor hij automatisch zijn toegang tot het DigiPost-platform verliest.

Door het feit dat het DigiPost-platform gebruik maakt van een logische toegangsbeveiliging (o.a. mogelijk dankzij de integratie met ACM/IDM) heeft een entiteit enkel en alleen toegang tot die berichten die zich bevinden in hun virtuele postbus. Een personeelslid van een entiteit kan dus nooit berichten zien die niet van zijn entiteit zijn. Men kan enkel die berichten zien die toegewezen zijn aan henzelf of aan postvakken waarop men toegang gekregen heeft. Om een gebruiker toegang te geven tot een postvak, moet het postvak in Gebruikersbeheer (IDM) toegevoegd worden aan die gebruiker.  In IDM wordt een postvak, zoals duidelijk wordt in bijgevoegde screenshot, werkbak genoemd.

Als een gebruiker tot meerdere entiteiten behoort, dient hij bij het inloggen te bepalen voor welke entiteit hij wil inloggen.

Onderstaande tabel geeft per rol een beschrijving weer van wat die rol kan zien en doen.

|  |  |  |
| --- | --- | --- |
| Rolnaam​ | Wat kan de rol doen? | Wat kan de rol zien? |
| Medewerker​ | * Toegang tot de persoonlijke inbox. Daar kan hij:   + Aanvaarden   + Doorsturen   + Afwijzen   + Herscan aanvragen   + Analoge bericht aanvragen * Toegang tot archief en lijst aanvaarde documenten. | * Ziet in de Inbox alle documenten van de postvakken waaraan hij gekoppeld is; * Ziet ook de privé-post. |
| Verdeler​ | * Zelfde als de medewerker; * Toegang tot de rapportering en kan rapporten trekken; * Toegang tot alle poststukken van de algemene verdeelbak van de entiteit. | * Zelfde als de medewerker; * Toegang tot die documenten voor de entiteit die (nog) niet aan een postvak zijn toegekend; * Ziet alle privé-post van medewerkers die niet gelijktijdig aan een postvak is gekoppeld ( en dit tot wanneer de persoon het poststuk aanvaard); * Opvolgfunctie. |
| Admin​  ​ | * Zelfde als de verdeler; * Kan interne postvakken bijmaken; * Kan alle documenten binnen zijn entiteit een andere eigenaar geven; * Toegang tot alle poststukken in alle postvakken van de entiteit. | * Zelfde als de verdeler; * Ziet alle poststukken van alle postvakken; * Ziet welke users aan welk postvak hangen (maar kan dat daar niet aanpassen). |
| DigiPost | * Zelfde als de verdeler; * Toegang tot het ‘DigiPostvak’. Daar kan men:   + Toewijzen   + Verwijderen | * Zelfde als de medewerker; * Ziet alle documenten die niet aan een entiteit zijn gekoppeld.   Deze komen in het ‘DigiPostvak’. |

### Geprivilegieerde toegang tot het platform

Toegang tot de back-end van het systeem is enkel mogelijk zijn via de PAMaas bouwsteen (CyberArc) van de Vlaamse overheid. De PAMaas bouwsteen zal actief zijn vooraleer de oplossing naar alle VO-entiteiten uitgerold wordt. In tussentijd is er een alternatieve oplossing, namelijk dat Cronos (de leverancier van de DigiPost-software) steeds een schriftelijke goedkeuring vraagt aan een ICT-verantwoordelijke van Het Facilitair Bedrijf en de productmanager DigiPost van Het Facilitair Bedrijf.

Meer informatie over de PAMaas bouwsteen is te vinden op: <https://www.vlaanderen.be/digitaal-vlaanderen/beheerderstoegangen-controleren-en-monitoren-pamaas>

### Integratietoegang

Naast de toegang door fysieke gebruikers is er ook toegang door systemen die rechtstreeks communiceren met het DigiPost-platform (bv. doorsturen van de scans via de scansoftware naar het platform).

Alle communicatie door dergelijke systemen verloopt geëncrypteerd via TLS-certificaten voor HTTPS-verbindingen. Daarnaast is een Azure Application Gateway geïnstalleerd die niet gekende inkomende verbindingen blokkeert. Tenslotte zijn er security groups ingesteld, waarbij enkel via vooraf bepaalde poorten communicatie mogelijk is tussen de applicaties, zowel inkomend als uitgaand.

### Encryptie

De volledige omgeving wordt geëncrypteerd. Hierbij wordt/zal worden gebruik gemaakt van de nieuwe KMSaaS bouwsteen van Digitaal Vlaanderen voor Microsoft Azure. Deze bouwsteen zal sleutels genereren voor de Azure Premium Keyvault die Het Facilitair Bedrijf zal opzetten.

De nieuwe KMSaaS voor Azure bouwsteen is een dienstverlening van Digitaal Vlaanderen gebaseerd op technologie van Thales. Digitaal Vlaanderen heeft midden februari 2023 een geslaagde implementatie opgezet op T&I, maar vooraleer men deze bouwsteen naar de productieomgeving wil brengen dienen nog een aantal elementen door hen gefinetuned te worden. Digitaal Vlaanderen communiceert momenteel (eind februari 2023) dat deze bouwsteen midden maart 2023 in productie geplaatst wordt. Digitaal Vlaanderen zal deze bouwsteen ter beoordeling voorleggen aan de VTC . Het Facilitair Bedrijf gaat er vanuit dat de VTC positief zal reageren op het opzet van deze bouwsteen en bijgevolg ook op het gebruik van Het Facilitair Bedrijf van deze bouwsteen.

In het geval de VTC niet positief oordeelt over de KMSaaS bouwsteen van Digitaal Vlaanderen zal Het Facilitair Bedrijf i.k.v. het DigiPost-platform een managed HSM opzetten. Via deze oplossing kan Het Facilitair Bedrijf zelf sleutels genereren in een ‘single tenant’ HSM die gehost wordt door Microsoft en technisch beheerd wordt door Cronos Public Services in opdracht van Het Facilitair Bedrijf. Doordat alle sleutels, ook de noodsleutels, in beheer zijn van Het Facilitair Bedrijf is toegang door Microsoft en Cronos Public Services onmogelijk tenzij met toestemming van Het Facilitair Bedrijf. Voor Het Facilitair Bedrijf is dit echter niet de voorkeursoptie, aangezien de voorkeur gegeven wordt aan het gebruik van de centrale VO veiligheidsbouwstenen.

### Data in motion

Er wordt gebruik gemaakt van Microsoft Azure Confidential Compute op het moment dat de meest ‘kritische’ stappen in het verwerkingsproces gebeuren.

Wat de data in use betreft moet onderscheid gemaakt worden tussen 2 verschillende ‘luiken’ binnen het DigiPost-platform:

1. Een Capture luik
   1. Het Capture luik is het gedeelte van het DigiPost-platform dat data uit de berichten extraheert (bv. interpretatie van de QR-codes die gebruikt worden voor de verdeling van de poststukken). Voor de volledige functionele verwijzing, zie *hoofdstuk 7.3 Systematische beschrijving van de verwerkingen* van de SjabloonGEB.
   2. Technisch draait dit luik op een virtuele machine (VM) die ondergebracht wordt op een Microsoft Azure Confidential Compute omgeving. Dit betekent concreet dat Microsoft onmogelijk toegang kan krijgen tot de informatie die aanwezig is op dit luik.
2. Distributie luik
   1. Het distributieluik is het gedeelte van het DigiPost-platform dat de berichten ter beschikking stelt aan de eindgebruikers.
   2. Technisch maakt dit luik gebruik van Microsoft Azure Functions. Dit betekent concreet dat als een gebruiker een bericht bekijkt er een function start die dat specifieke bericht ter beschikking stelt aan die specifieke gebruiker. Elk bericht dat bekeken wordt, wordt dus ter beschikking gesteld via een aparte function aan één enkele gebruiker. Het aantal actieve functions, en bijgevolg bekijkbare berichten, is dus gelijk aan het aantal gebruikers die een bericht bekijken.

### Andere maatregelen

Diverse andere maatregelen zijn van toepassing die niet specifiek toe te wijzen zijn aan een risico maar algemene maatregelen betreffen die bijdragen aan de bescherming van gegevens:

* Het Facilitair Bedrijf heeft een DPO, de subverwerker (CPS) ook
* Met klanten (aangesloten entiteiten) wordt steeds een toetredings- en verwerkersovereenkomst afgesloten.
* De betrokken medewerkers bij HFB zijn opgeleid en gesensibiliseerd over de AVG en informatieveiligheid.
* Maatregelen ter beveiliging van de fysieke locatie, zowel scankamer als servers.
* Het Facilitair Bedrijf houdt zich aan het informatieclassificatieraamwerk van de VO;
* Het Facilitair Bedrijf voorziet transparante communicatie naar potentiële afzenders van analoge poststukken;
* Er is een uitgewerkt BCM-plan;
* Het gebruik van de API’s is gebonden aan duidelijke gebruiksvoorwaarden voor de integrerende partijen. Deze voorwaarden zijn te raadplegen op: <https://www.vlaanderen.be/informatiemanagement/informatie-digitaliseren/digitalisering-inkomende-post/digipost-webservices>

### Logging en monitoring

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.

## Aanvullende TOMs op niveau van subverwerker Cronos Public Services / FlinQ / Arxus

De diensten worden afgenomen op basis van het ICT-raamovereenkomst voor ICT-exploitatie- en ontwikkelingsdiensten[[14]](#footnote-15). Hoofdstuk 6.8.3 dwingt de noodzakelijke onderdelen in het kader van een verwerkersovereenkomst af. Hoofdstuk 6.8.3.2 benoemt specifiek de technische en organisatorische maatregelen die een verwerker dient te nemen. Deze maatregelen zijn ook van toepassing op Cronos Public Services (CPS) en haar onderaannemers zoals bv. FlinQ.

CPS onderbouwt het nakomen van deze verplichtingen o.a. door het verkregen ISO27001 certificaat[[15]](#footnote-16).

### Pentesting

Voor de validatie van bovenvermelde aspecten werd een pentest uitgevoerd. Het officiële rapport hiervan is beschikbaar voor Het Facilitair Bedrijf. Cronos geeft de garantie dat kritische bevindingen onmiddellijk verholpen worden en dat alle hoge risico’s door hen verholpen worden binnen de 30 dagen nadat ze op de hoogte gebracht via het officiële rapport.

## TOMs op niveau van subverwerker Bringme

Bringme verwerkt enkel professionele contactgegevens die vallen onder informatieklasse 2. In lijn daarmee zijn bepaalde maatregelen genomen.

Toegangscontrole om te voorkomen dat onbevoegden toegang krijgen tot of gebruik kunnen maken van de gegevensverwerkingssystemen waarin de gegevens worden verwerkt of gebruikt.

Toewijzing van rechten en rollen voor gebruik van bijzondere gebieden van gegevensverwerkingssystemen zodat personen die toestemming hebben om het gegevensverwerkingssysteem te gebruiken, uitsluitend toegang hebben tot de gegevens binnen het gebied dat hen is toegewezen

* Bringme neemt passende voorzorgsmaatregelen om te garanderen dat de gegevens worden beschermd tegen accidentele vernietiging of verlies. Ook tijdens de overdracht van gegevens of het transport van gegevensdragers wordt erop toegezien dat gegevens niet door onbevoegden worden gelezen, gekopieerd, gewijzigd of gewist;
* Inputcontrole en logging;
* Afzonderlijke verwerking voor verschillende doeleinden in een afgescheiden omgeving.

# Annex II – Ontwerptekst aanpassing Bestuursdecreet

## Artikels in het Wijzigingsdecreet i.k.v. DigiPost

**Art. 102.** Aan titel III, hoofdstuk 3, afdeling 5, van hetzelfde decreet wordt een onderafdeling 5 toegevoegd, die luidt als volgt:

“Onderafdeling 5. Scanning van bestuursdocumenten”.

**Art. 103.** In hetzelfde decreet wordt in onderafdeling 5, toegevoegd bij artikel 99, een artikel 89/1 ingevoegd, dat luidt als volgt:

“Art. III.89/1. §1. Dit artikel is van toepassing op de volgende instanties:

1° de overheidsinstanties, vermeld in artikel III.79, §1, 1° tot en met 4°;

2° de kabinetten van de leden van de Vlaamse Regering.

§2. De door de Vlaamse Regering aan te wijzen entiteit, bevoegd voor het facilitair management en documentbeheer, hierna de entiteit te noemen, kan, op verzoek van een instantie als vermeld in paragraaf 1, instaan voor de scanning en, in voorkomend geval, de vervanging van de volgende bestuursdocumenten door elektronische kopieën, met toepassing van artikel II.25 van het Bestuursdecreet van 7 december 2018:

1° de bestuursdocumenten die de instantie in kwestie via analoge weg ontvangt;

2° de bestuursdocumenten die de instantie in kwestie beheert overeenkomstig onderafdeling 2.

De entiteit kan, op verzoek van een instantie als vermeld in paragraaf 1, instaan voor het openen en doorsturen van elektronische berichten die geadresseerd zijn aan bepaalde elektronische adressen van de instantie in kwestie.

Bij de uitvoering van de opdrachten, vermeld in het eerste en tweede lid, is de entiteit gemachtigd om:

1° de berichten die geadresseerd zijn aan een andere instantie of aan een personeelslid van die instantie, te openen;

2° met toepassing van de regelgeving over de bescherming van natuurlijke personen bij de verwerking van persoonsgegevens bestuursdocumenten die persoonsgegevens bevatten, te verwerken.

De personeelsleden van de entiteit zijn bij de uitvoering van de opdrachten, vermeld in het eerste en tweede lid, gebonden aan een geheimhoudingsverplichting.

De entiteit treedt voor de opdrachten, vermeld in het eerste, tweede en derde lid, op als verwerker als vermeld in artikel 4, 8), van de algemene verordening gegevensbescherming ten behoeve van de instanties.

De Vlaamse Regering kan de instanties, vermeld in paragraaf 1, verplichten om gebruik te maken van de dienstverlening van de entiteit.”.

## Memorie van Toelichting bij hogervermelde artikels

**Artikel 102**

Via dit artikel wordt in titel III, hoofdstuk 3, afdeling 5, van het Bestuursdecreet een onderafdeling 5 toegevoegd, die luidt als volgt: “Onderafdeling 5. Scanning van bestuursdocumenten”.

**Artikel 103**

Paragraaf 1 bepaalt het toepassingsgebied van dit artikel, nl. de overheidsinstanties, vermeld in artikel III.79, §1, 1° tot en met 4°, van het Bestuursdecreet en de kabinetten van de leden van de Vlaamse Regering.

Paragraaf 2 legt vast dat de door de Vlaamse Regering aan te duiden entiteit, bevoegd voor het facilitair management en documentbeheer, op verzoek van een instantie kan instaan voor de scanning en in voorkomend geval de vervanging van bestuursdocumenten door elektronische kopieën, met toepassing van artikel II.25 van het Bestuursdecreet van 7 december 2018, nl. van bestuursdocumenten die de instantie in kwestie via analoge weg ontvangt of bestuursdocumenten die de instantie in kwestie beheert.

Na scanning zal de entiteit de analoge berichten (geautomatiseerd) doorsturen naar de bestemmelingen via virtuele postbussen.

De entiteit staat daarnaast, op verzoek van een instantie, in voor het openen en doorsturen van elektronische berichten die geadresseerd zijn aan bepaalde elektronische adressen van de instantie in kwestie. Dit is ingegeven doordat er op heden sprake is van een nood aan efficiëntie en effectiviteit op het vlak van

* de verdeling en klassering van inkomende digitale berichten die aan instanties op generieke e-mailadressen worden toegestuurd;
* De verdeling en klassering van inkomende berichten die aan instanties worden toegestuurd via de federale eBox.

In de praktijk openen en verdelen medewerkers van de instanties momenteel zelf de inkomende digitale poststukken en versturen zij deze daarna naar het juiste team, de verantwoordelijke medewerker, enz.

Deze werkwijze vormt eerst en vooral een administratieve last voor de instanties aangezien zij het volledige beheer van de inkomende digitale post moeten waarnemen. De Vlaamse overheid wenst die complexiteit en administratieve lasten zoveel mogelijk weg te nemen bij de instanties zelf. Ten tweede is de huidige werkwijze privacy-invasief, aangezien in de praktijk verschillende medewerkers van verschillende instanties digitale poststukken dienen te openen en te verdelen die niet voor hen bestemd zijn. Een minder privacy-invasieve werkwijze is beschikbaar door de verdeling en klassering van de digitale berichten te centraliseren waarbij de digitale berichten onmiddellijk (a.d.h.v. software) aan de juiste dienst/behandelaar kunnen worden toegewezen.

De software die gebruikt wordt voor het doorsturen en verdelen van ingescande analoge berichten zorgt zowel voor een privacy-conforme als een efficiënte oplossing om digitale berichten eenvoudig bij de bestemmeling te krijgen. Daarom wordt hier ook de opening gecreëerd om deze software (beheerd door de in paragraaf 2 vermelde entiteit) ook daarvoor te gebruiken.

Bij de uitvoering van de opdrachten is de entiteit gemachtigd om berichten die geadresseerd zijn aan een andere instantie of aan een personeelslid van die instantie, te openen en conform de algemene verordening gegevensbescherming, bestuursdocumenten die persoonsgegevens bevatten, te verwerken.

De entiteit treedt met betrekking tot de voornoemde opdrachten op als verwerker als vermeld in artikel 4, 8), van de algemene verordening gegevensbescherming ten behoeve van de instanties.

Het laatste lid van paragraaf twee geeft de Vlaamse Regering de mogelijkheid om, omwille van efficiëntieredenen, het gebruik van de diensten van de entiteit te verplichten.

Het voorgestelde artikel III.89/1 vormt een decretale uitzondering op het recht op privéleven en briefgeheim (zoals onder meer vervat in artikel 8 EVRM juncto artikel 22 GW) en op het telecomgeheim (zoals vervat in artikel 124 en 125 Wet Elektronische Communicatie en artikel 259bis en artikel 314bis Sw.). Deze inmenging in het recht op het brief- en telecomgeheim, die tevens verband houdt met het recht op privéleven van afzenders en bestemmelingen van inkomende elektronische en analoge berichten is verantwoord, rekening houdend met het feit dat de inmenging via huidige wijziging:

* voldoet aan het wettigheidsbeginsel, vermits zij in een voorzienbare en toegankelijke decretale bepaling wordt opgenomen;
* een legitiem doel nastreeft. De voorziene inmenging is (onder meer) gericht op de efficiëntere werking van de overheid (door een vermindering van de administratieve lasten), en beoogt dus het economisch welzijn van het land te bevorderen (bv. door een kostendaling van de overheidsdienstverlening door schaalgrootte en “insourcing”). De voorziene inmenging draagt bovendien bij aan de bescherming van de rechten en vrijheden van personen, in de mate dat de beoogde efficiëntere dienstverlening ervoor zorgt dat:
  1. burgers sneller antwoord krijgen op (bepaalde) verstuurde brieven aangezien het bericht sneller bij de bevoegde dienst/medewerker terecht komt;
  2. flexibiliteit langs overheidszijde wordt gegarandeerd (ook bij piekmomenten);
  3. betere aansluiting wordt gezocht bij nieuwe hybride werkvormen;
* noodzakelijk is in een democratische samenleving, en meer bepaald beantwoordt aan een dwingende maatschappelijke noodzaak:
  + pertinentie: er mag redelijkerwijze worden aangenomen dat de voorziene inmenging nuttig, relevant en toereikend is om het beoogde doel op het vlak van een efficiëntere werking van de overheid te bereiken.
  + proportioneel: er bestaat een redelijke verhouding tussen de aantasting van het recht op briefgeheim enerzijds en de nagestreefde legitieme doelstelling(en) anderzijds. Er dient te worden benadrukt dat de voorziene inmenging, vanuit haar aard, beperkt is qua omvang, nu deze regeling enkel betrekking heeft op berichten toegestuurd aan instanties in de zin van paragraaf 1 en hun medewerkers. Daarenboven zijn er door de Vlaamse Regering op het vlak van de vervanging van de analoge bestuursdocumenten verschillende procedurele vereisten ingevoerd die belangrijke waarborgen vormen tegen willekeurige inmengingen in het privéleven van de betrokkenen, d.w.z. niet alleen de instanties, zoals vermeld in paragraaf 1 en hun medewerkers, maar ook de afzenders van de analoge poststukken. Zo zou de aangewezen instantie bijvoorbeeld op basis van die vereisten de vertrouwelijkheid van de persoonsgegevens in de elektronische kopieën van de analoge bestuursdocumenten moeten garanderen. De door de Vlaamse Regering aangewezen entiteit die gemachtigd zal worden om voor rekening van de instanties, vermeld in paragraaf 1, de analoge bestuursdocumenten per analoge post toegestuurd aan deze instanties en hun medewerkers te openen, in te scannen en aan de bestemmeling(en) te bezorgen, zal bovendien de noodzakelijke waarborgen moeten bieden opdat de rechten en vrijheden van de afzender en de bestemmeling van de in analoge post gewaarborgd zijn. Tot slot vormt het een proportionele inmenging aangezien veelvuldige schendingen van het recht op brief- en telecomgeheim door instanties kunnen vermeden worden door het proces te centraliseren.
  + subsidiariteit: er zijn geen minder “zware” middelen die het beoogde doel kunnen bereiken.

# Annex III – Foto’s inrichting scankamer

|  |  |
| --- | --- |
| *Verdeelkast*  Gemaakte foto | *Inrichting scankamer*  Afbeelding met tekst, vloer, binnen, muur  Automatisch gegenereerde beschrijving |
| *Niet-digitaliseerbare poststukken (Estafette)*  Afbeelding met tekst, vloer, binnen  Automatisch gegenereerde beschrijving | *Opstelling A4/A3 scanners (Kodak i4250)*  Gemaakte foto |
| *Suprascan Quartz A0*  Afbeelding met muur, binnen, vloer, bureau  Automatisch gegenereerde beschrijving | *A0 doorvoerscanner*  Afbeelding met tekst, vloer, binnen  Automatisch gegenereerde beschrijving |

1. <https://overheid.vlaanderen.be/raamcontracten/pakketautomaten> [↑](#footnote-ref-2)
2. Meer info over deze afleverlocaties is te vinden op: <https://www.vlaanderen.be/informatiemanagement/informatie-digitaliseren/digitalisering-inkomende-post/aflevermethodes-digipost> [↑](#footnote-ref-3)
3. Deze actie is 90 dagen beschikbaar omdat het analoge poststuk 90 dagen bewaard wordt. [↑](#footnote-ref-4)
4. Deze actie is 90 dagen beschikbaar omdat het analoge poststuk 90 dagen bewaard wordt. [↑](#footnote-ref-5)
5. Artikel 4 van het Besluit van de Vlaamse Regering van 11 juni 2004 tot oprichting van het intern verzelfstandigd agentschap ["agentschap Facilitair Bedrijf" (verv. BVR 4 juli 2014, art. 7, I: 28 juli 2014)].  [↑](#footnote-ref-6)
6. <https://overheid.vlaanderen.be/onze-organisatie/het-facilitair-bedrijf/strategie-beleid> [↑](#footnote-ref-7)
7. Een uitgebreide beschrijving van de aspecten die relevant zijn voor substitutie zijn te vinden in de Substitutieprocedure die uitgeschreven is voor DigiPost. [↑](#footnote-ref-8)
8. Om een deel van het proces visueel te kunnen voorstellen zijn er foto’s van de scankamer opgenomen in *Annex V*. [↑](#footnote-ref-9)
9. De procedure van Het Facilitair Bedrijf is gebaseerd op: <https://www.vlaanderen.be/informatiemanagement/selecteren-en-vernietigen/informatie-vernietigen> [↑](#footnote-ref-10)
10. Na een informeel overleg tussen VTC en Het Facilitair Bedrijf op 13 september is deze termijn van 90 dagen teruggebracht naar 14 dagen. [↑](#footnote-ref-11)
11. Deze tekst wordt wel als aparte laag in het document, in casu PDF, geplaatst. Dit betekent dat er geen aparte tekstfile beschikbaar is. [↑](#footnote-ref-12)
12. <https://assets.vlaanderen.be/image/upload/v1669378806/202207_-_substitutieprocedure_def_zhc91u.pdf> [↑](#footnote-ref-13)
13. <https://overheid.vlaanderen.be/int_vertrouwelijke_behandeling> [↑](#footnote-ref-14)
14. <https://assets.vlaanderen.be/image/upload/v1636999209/Basiscontract_-_ICT-contracten_2022_-_Finaal_bestek_nfnb54.pdf> [↑](#footnote-ref-15)
15. <https://cronos-public-services.be/data-groeit-sneller-dan-je-denkt-en-data-is-overal/> [↑](#footnote-ref-16)