

Informatieveiligheidscomité Kamer sociale zekerheid en gezondheid
--

IVC/KSZG/26/198

BERAADSLAGING NR. 26/114 VAN 2 JUNI 2026 BETREFFENDE DE AANVRAAG VAN DE RIJKSDIENST VOOR SOCIALE ZEKERHEID (RSZ) VOOR HET VERKRIJGEN VAN EEN MINISTERIËLE ERKENNING VAN HET ELEKTRONISCH ARCHIVERINGSSYSTEEM MET TOEPASSING VAN HET KONINKLIJK BESLUIT VAN 7 DECEMBER 2016 OVER DE BEWIJSKRACHT VAN DE GEGEVENS DIE DOOR DE INSTELLINGEN VAN SOCIALE ZEKERHEID WORDEN VERWERKT

Gelet op de wet van 15 januari 1990 *houdende oprichting en organisatie van een Kruispuntbank van de Sociale Zekerheid*;

Gelet op de aanvraag van de Rijksdienst voor Sociale Zekerheid (RSZ);

Gelet op het auditoraatsrapport van de Kruispuntbank van de Sociale Zekerheid.

A. CONTEXT EN ONDERWERP VAN DE AANVRAAG

1. Dit verzoek behelst een aanvulling van het gunstig advies nr. 16/035 van 7 juni 2016 van het sectoraal comité van de sociale zekerheid en van de gezondheid, eerder al aangevuld bij de beraadslaging nr. 20/036 van 4 februari 2020 van het informatieveiligheidscomité. De reden voor het nieuw verzoek is tweeledig: enerzijds de migratie van alle documenten van het oud documentbeheersysteem EDE naar het nieuw documentbeheersysteem DocMan, anderzijds het gebruik van een nieuwe digitale tool (Digital Mailroom) voor het scannen en verwerken van documenten, waaronder de classificatie van de inkomende post sinds maart 2025.

B. BEHANDELING VAN DE AANVRAAG

2. *Onderzoek van het dossier op basis van de technische voorwaarden van het koninklijk besluit van 7 december 2016*

De evaluatie van de procedures die werden ingediend voor het verkrijgen van de ministeriële erkenning is opgesplitst volgens de diverse technische voorwaarden van het koninklijk besluit van 7 december 2016 *over de bewijskracht van de gegevens die door de instellingen van sociale zekerheid worden verwerkt*. Er is afdoende aangetoond dat het voorgestelde systeem voldoet aan die voorwaarden.

2.1. *Het voorstel omschrijft de procedure nauwkeurig.*

Het dossier biedt een uitgebreide en gedetailleerde weergave van het gehele functionele, technische en organisatorische proces rond enerzijds het scannen en het digitaal verwerken van binnenkomende post bij de RSZ (via de tool Digital Mailroom) en anderzijds het beheren, beveiligen, archiveren en traceren van documenten binnen het systeem (Document Repository).

DocMan is het nieuw documentbeheersysteem van de RSZ, dat in de plaats van EDE komt. Het Document Repository is een serviceplatform voor het bewaren, beheren en raadplegen van documenten en metadata, geïntegreerd met Archiving-as-a-Service (AaaS), de elektronische archivering van documenten.

Archiving-as-a-Service (AaaS) biedt sinds 2016 een generieke elektronische archiveringsservice met bewijskracht aan Belgische overheidsinstellingen, ontworpen om authenticiteit, integriteit, toegankelijkheid en leesbaarheid van digitale objecten te garanderen. Het scannen en verwerken van documenten gebeurt door de Digital Mailroom.

Enkele voorbeelden van de gedetailleerde procedurebeschrijvingen zijn:

- **ontvangst van de binnenkomende post:** voorbereiding en sortering, scannen, kwaliteitscontrole, (voor)indexering, tijdelijke opslag, overdracht naar documentbeheersysteem. In de toekomst zullen alle documenten via Digital Mailroom verlopen. De post wordt centraal ontvangen, gesorteerd, gecontroleerd, gescand en uiteindelijk omgezet in PDF/A met optische tekenherkenning (OCR) en opgeslagen.
- **upload en validatie van documenten:** documenten komen binnen via directe upload of scanning en worden vooraf geïndexeerd (pre-indexering), om duplicaties te vermijden en om bewerkingen te reguleren (geen wijziging van finale documenten). Het document beschrijft het authenticeren via een token, hoe de validatie van binnenkomende documenten en metadata plaatsvindt en hoe het document wordt opgeslagen in de Fast Storage Service en metadata in de Metadata Indexer Service.
- **de scanning via Digital Mailroom** gebeurt volgens een strikt procedureel en gecontroleerd proces. De scan- en indexatieprocessen vinden plaats in een beveiligde scanningscel. Hierbij worden metadata zoals naam, aantal documenten, aantal pagina's, aankomstdatum van de post, type behandeling, en data van betrokken agents ingevoerd. Na scanning vindt een kwaliteitscontrole plaats met correctiemogelijkheden.
- **archivering:** het asynchrone proces van het verzenden van documenten naar Archiving-as-a-Service (AaaS) wordt stap voor stap uitgelegd.
- **authenticiteit en integriteit:** er worden processen beschreven voor het controleren van hashwaarden bij upload en verzending naar het archief, evenals de bescherming en opslag van metadata.

- **toegangsbeheer:** het document geeft een gedetailleerd overzicht van de rechten en rollen (owner, reader, messenger) en hoe de toegangscontrole via de Access Manager Service verloopt.
- **auditing en logging:** het traceren van activiteiten via logs in Access List Service is ook uitgebreid beschreven.

Het document volgt een vaste structuur die conform is aan de door de regelgeving gestelde vereisten (conform artikel 14 van het koninklijk besluit van 7 december 2016). Elk hoofdstuk behandelt een specifiek aspect van de procedures, wat bijdraagt aan de volledigheid en nauwkeurigheid.

2.2. *De aangewende technologie waarborgt een getrouwe, duurzame en volledige weergave van de informatie.*

Het document waarborgt dat de aangewende technologie een getrouwe, duurzame en volledige weergave van de informatie garandeert, door verschillende maatregelen en processen die expliciet beschreven worden.

1. getrouwe weergave (authenticiteit en integriteit):

- Document Repository controleert bij het uploaden de integriteit van documenten door de hashwaarden te vergelijken die aangeleverd worden met hashwaarden die intern opnieuw berekend worden. Indien er een mismatch is, wordt het document geweigerd en verwijderd.
- ook bij het verzenden naar de archiefservice (AaaS) vindt opnieuw een integriteitscontrole plaats.
- ook de authenticiteit en imputabiliteit van gebeurtenissen wordt gegarandeerd door het gebruik van tokens gegenereerd via het IAM (OAuth) systeem van het Portaal van de Sociale Zekerheid, waarmee de identiteit van de applicatie of gebruiker betrouwbaar wordt vastgesteld.

2. duurzame opslag:

- Document Repository maakt gebruik van de Archiving-as-a-Service (AaaS) voor de langdurige archivering van documenten, waarbij het document in één entiteit (inhoud en metadata) wordt bewaard.
- het dossier beschrijft ook het waarborgen van de bescherming van metadata en documenten via beveiligde opslag en toegangsbeheer, wat bijdraagt aan het behoud van volledige en betrouwbare data gedurende de tijd.

3. **volledige weergave:**

- zowel de inhoud van het document als alle gerelateerde metadata (business, validatie, toegang, technische metadata, stakeholders) worden bewaard en gemanaged, wat zorgt voor een volledige context van het document.
- detailinformatie en processen omtrent tracing van alle acties op documenten zijn aanwezig (log tracking via Access List Service), zodat de volledige levenscyclus van elk document kan worden gereconstrueerd.
- gedetailleerde rechten- en toegangsbeheermechanismen verzekeren dat alleen bevoegde actoren bepaalde gegevens kunnen wijzigen of raadplegen, wat de consistentie en volledigheid van de informatie beschermt.

4. **infrastructuur en beveiliging:**

- het document vermeldt ook bescherming op infrastructuurniveau, zowel fysiek (datacenter, servers) als logisch (configuratie, change management), wat de betrouwbaarheid en beschikbaarheid van de opgeslagen informatie ondersteunt.

Samenvattend toont het dossier aan dat de gebruikte technologieën en procedures expliciet gericht zijn op het garanderen van een getrouwe, duurzame en volledige bewaring en weergave van documenten en bijbehorende metadata binnen het Document Repository systeem, conform de geldende wettelijke normen en best practices.

2.3. ***De informatie wordt systematisch en zonder weglatingen geregistreerd.***

De informatie wordt systematisch en zonder weglatingen geregistreerd binnen het Document Repository systeem, zoals blijkt uit het dossier:

1. **volledige registratie van documenten en metadata:**

- bij het uploaden wordt niet alleen het document zelf geregistreerd, maar ook verschillende soorten metadata: zakelijke metadata, validatie-metadata, toegangsmethoden, technische metadata en stakeholders worden allemaal verzameld en opgeslagen.
- Document Repository weigert uploads als verplichte metadata ontbreken (bijvoorbeeld een leeg of ontbrekend metadata .json-bestand), wat ervoor zorgt dat geen onvolledige informatie wordt geregistreerd.

2. **traceerbaarheid en logging van alle acties:**

- alle acties op documenten worden gelogd in het Access List Service (ALS), inclusief upload, toegang, wijziging, en archiefacties.
- elke actie wordt vastgelegd met een uniek transaction_id, tijdstip, informatie over de verzoeker, type actie, betrokken microservice, object_id en een hash van de metadata, dit om een volledige en betrouwbare audit trail te creëren.

3. controle op integriteit en consistentie:

- er zijn processen die regelmatig worden uitgevoerd om documenten en metadata te controleren en om zogenaamde “verweesde” documenten te verwijderen (dit zijn documenten die geen geldige koppeling of referentie meer hebben binnen het systeem, wat betekent dat deze documenten niet langer aan een juiste metadata-entiteit, stakeholder, opslaglocatie of een gerelateerd proces zijn verbonden, dus zonder gebruikscontext), wat wijst op een systematische aanpak van data-integriteit en volledigheid.
- bovendien worden wijzigingen in metadata alleen doorgevoerd indien de applicatie de nodige rechten heeft en indien (indien aanwezig) een externe validatieservice deze wijzigingen controleert.

4. beheer en bescherming van metadata:

- alle metadata worden bewaard in een gestructureerde database (Metadata Indexer Service) en specifieke metadata over stakeholders in een aparte Access Manager Service database, wat zorgt voor volledigheid en gestructureerde registratie van alle relevante informatie.

Hieruit blijkt dat het systeem ontworpen is om alle informatie systematisch, coherent en zonder weglatingen te registreren en vast te leggen en dat het actieve maatregelen neemt om volledigheid en betrouwbaarheid te garanderen.

2.4. *De verwerkte informatie wordt op een zorgvuldige manier bewaard, systematisch gerangschikt en beschermd tegen elke vervalsing.*

De verwerkte informatie in het Document Repository wordt op een zorgvuldige, systematische en beschermde wijze bewaard, gerangschikt en beveiligd tegen vervalsing, zoals volgt uit de beschrijvingen in het dossier:

1. zorgvuldige bewaring en systematische rangschikking:

- documenten zijn gekoppeld aan metadata en locaties en worden beheerd via een gestructureerd datamodel waarin elk document meerdere metadata en opslaglocaties kan hebben.
- er is sprake van een microservices-architectuur waarbij de metadata, documentinhoud en toegangsrechten in verschillende gespecialiseerde services (zoals MIS, FSS, AMS) beheerd worden, wat de systematische organisatie en beheer van documenten en metadata ondersteunt.
- de levenscyclus van documenten wordt beheerd met processen voor upload, archivering, en ook routine-opruiming van tijdelijke caches en inconsistenties om zo de consistentie en orde te waarborgen.

2. bescherming tegen vervalsing (authenticiteit en integriteit):

- er wordt een integriteitscontrole uitgevoerd door gebruik van hashes en algoritmes om te verifiëren of het document sinds het uploaden niet is gewijzigd. Dit gebeurt al bij het uploaden en ook bij het archiveren naar AaaS.
- metadata worden beschermd door beperkingen in bewerkbaarheid (bijvoorbeeld niet wijzigbare archiveringsmetadata eenmaal gearhiveerd) en door berekening en bewaring van hashes van metadata om iedere wijziging te kunnen detecteren. Eventuele wijzigingen zijn gebonden aan toegangsrechten.
- alle toegangen en wijzigingen worden gelogd en traceerbaar gemaakt, wat ook bijdraagt aan de authenticiteit en detectie van pogingen tot vervalsing.
- er worden procedures beschreven voor toegangsbeheer en autorisatie, evenals voor audit-trail en logging om alle gebeurtenissen te registreren en zo de authenticiteit, imputabiliteit en controle over documenten te garanderen.

3. duurzaamheid en duurzaamheid van bewaring:

- de opslag is zodanig ingericht dat documenten duurzaam en vertrouwelijk bewaard kunnen blijven met verantwoord formaatbeheer en integriteitschecks.
- er zijn ook beveiligingen op het niveau van de infrastructuur, inclusief fysieke en logische bescherming van de databanken en servers om het geheel van opslag en verwerking te beveiligen.

Samenvattend: het Document Repository zorgt voor een systematische organisatie en zorgvuldige bewerking van documenten en metadata, met robuuste integriteitscontroles, toegangsbeheer, logging en duurzame bewaarprocessen, waardoor de informatie beschermd wordt tegen vervalsing en betrouwbaar bewaard blijft.

2.5. *Bewaren van de volgende gegevens met betrekking tot de verwerking van de informatie: identiteit van de verantwoordelijke voor de verwerking evenals van diegene die ze heeft uitgevoerd, de aard en het onderwerp van de informatie waarop de verwerking betrekking heeft, de datum en de plaats van de verwerking, de eventuele storingen die zijn vastgesteld tijdens de verwerking.*

Het document beschrijft dat er uitgebreide logging en tracering plaatsvindt met betrekking tot de verwerking van de informatie, waarin verschillende gegevens worden bijgehouden die overeenkomen met de gevraagde elementen:

- **identiteit van de verantwoordelijke en uitvoerder van de verwerking:** het systeem vereist authenticatie via het IAM-service van het Portaal van de Sociale Zekerheid, waarbij een token wordt gebruikt dat de identiteit van de clientapplicatie bevat. Dit maakt authenticiteit en imputabiliteit van de acties mogelijk. Ook worden stakeholders (partijen met rechten op het document) en hun rollen expliciet bijgehouden.

- **aard en onderwerp van de informatie waarop de verwerking betrekking heeft:** documenten zijn gekoppeld aan gedetailleerde metadata (in verschillende types, waaronder business metadata) en deze metadata worden systematisch geregistreerd en beheerd.
- **datum en plaats van de verwerking:** tijdens upload, toegang en bewerking worden tijdstempels vastgelegd. Bij archivering wordt bijvoorbeeld het tijdstip van ontvangst bij AaaS bewaard. Locatiegegevens van documenten (waar ze zijn opgeslagen) worden eveneens bijgehouden.
- **eventuele storingen tijdens de verwerking:** er is een loggingmechanisme dat alle gebeurtenissen registreert, inclusief fouten en uitzonderingen die optreden, en er zijn processen actief voor het opschonen van inconsistenties en fouten, zoals “verweesde” documenten (zie hoger). Er zijn ook uitgebreide beschrijvingen over foutafhandeling in het systeem.

Daarnaast bevat het hoofdstuk over sporen van activiteiten en logging een gedetailleerde beschrijving van de logs die worden bijgehouden, welke alle relevante gegevens omvatten voor de controle en audit van de verwerking.

Het Document Repository registreert en bewaart gegevens over de identiteit van verantwoordelijken en uitvoerders, de aard van de informatie, tijd en plaats van verwerking, en algemene storing/foutenmeldingen, conform de eisen gesteld in het koninklijk besluit van 7 december 2016.

Om deze redenen, verleent

de kamer sociale zekerheid en gezondheid van het informatieveiligheidscomité

een gunstige beraadslaging. Het door de RSZ ingediende dossier voldoet aan de technische voorwaarden van het koninklijk besluit van 7 december 2016 *over de bewijskracht van de gegevens die door de instellingen van sociale zekerheid worden verwerkt*.

Deze beraadslaging treedt in werking op 17 juni 2026.

Michel DENEYER
Voorzitter

De zetel van de kamer sociale zekerheid en gezondheid van het informatieveiligheidscomité is gevestigd in de kantoren van de Kruispuntbank van de Sociale Zekerheid, op volgend adres: Willebroekkaai 38 – 1000 Brussel (tel. 32-2-741 83 11).
