Comité de sécurité de l'information
Chambre sécurité sociale et santé

CSI/CSSS/26/198

DÉLIBÉRATION N° 26/114 DU 2 JUIN 2026 RELATIVE À LA DEMANDE DE L'OFFICE NATIONAL DE SÉCURITÉ SOCIALE (ONSS) EN VUE DE L'OBTENTION D'UNE RECONNAISSANCE MINISTÉRIELLE POUR LE SYSTÈME D' ARCHIVAGE ÉLECTRONIQUE EN APPLICATION DE L'ARRÊTÉ ROYAL DU 7 DÉCEMBRE 2016 RELATIF À LA FORCE PROBANTE DES DONNÉES TRAITÉES PAR LES INSTITUTIONS DE SÉCURITÉ SOCIALE

Vu la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*;

Vu la demande de l' Office National de Sécurité Sociale (ONSS);

Vu le rapport d'auditorat de la Banque Carrefour de la Sécurité Sociale.

A. CONTEXTE ET OBJET DE LA DEMANDE

1. La présente demande entend compléter l'avis favorable émis en 2016 par le Comité sectoriel de la sécurité sociale et de la santé (section sécurité sociale, avis n° 16/35) et la modification qui a été approuvée en 2020 par le Comité de sécurité de l'information (délibération n° 20/036).

Le motif de cette nouvelle demande est double. D'une part, la migration de tous les documents de l'ancien système de gestion documentaire (EDE) vers le nouveau système (DocMan) et, d'autre part, l'utilisation d'un nouvel outil numérique (Digital Mailroom) pour la numérisation et le traitement de documents, dont la classification du courrier entrant depuis mars 2025.

B. EXAMEN DE LA DEMANDE

2. ***Examen du dossier sur base des conditions techniques de l'arrêté royal du 7 décembre 2016***

L'évaluation des procédures qui ont été introduites en vue de l'obtention de l'agréation ministérielle est scindée en fonction des différentes conditions techniques de l'arrêté royal du 7 décembre 2016.

Il a été prouvé que le présent dossier satisfait aux conditions décrites dans l'arrêté royal du 7 décembre 2016 *relatif à la force probante des données traitées par les institutions de sécurité sociale.*

2.1. *La proposition décrit la procédure avec précision*

Le dossier fournit une description exhaustive et détaillée de l'ensemble du processus fonctionnel, technique et organisationnel concernant, d'une part, la numérisation et le traitement numérique du courrier entrant à l'ONSS (via l'outil Digital Mailroom) et, d'autre part, la gestion, la sécurisation, l'archivage et le suivi des documents au sein du système (Document Repository).

DocMan est le nouveau système de gestion documentaire (remplaçant le système EDE). Le Document Repository est une plateforme de services dédiée au stockage, à la gestion et à la consultation de documents et de métadonnées, intégrée à l'Archiving-as-Service (AaaS), le service d'archivage électronique de documents.

Depuis 2016, l'Archiving-as-a-Service (AaaS) propose aux institutions publiques belges un service d'archivage électronique générique avec valeur probante, conçu pour garantir l'authenticité, l'intégrité, l'accessibilité et la lisibilité des objets numériques. La numérisation et le traitement de documents sont effectués par le Digital Mailroom.

Voici quelques exemples de descriptions détaillées des procédures:

- **réception du courrier entrant**: préparation et triage, numérisation, contrôle de qualité, (pré-)indexation, enregistrement temporaire, transfert vers le système de gestion documentaire. À l'avenir, tous les documents transiteront via le Digital Mailroom. Le courrier est réceptionné, trié, contrôlé et numérisé à un niveau central, avant d'être converti au format PDF/A à l'aide de la reconnaissance optique de caractères (OCR) et d'être enregistré.

- **chargement et validation de documents:** les documents entrent via le chargement direct ou la numérisation et sont indexés au préalable ((pré-)indexation), afin d'éviter des duplications et de régulariser des traitements (pas de modification de documents finaux). Le document décrit l'authentification au moyen d'un jeton, la procédure de validation de documents entrants et de métadonnées ainsi que la procédure d'enregistrement du document dans le Fast Storage Service et des métadonnées dans le Metadata Indexer Service.

- **la numérisation via le Digital Mailroom** s'effectue selon un processus strictement réglementé et contrôlé. Les processus de numérisation et d'indexation ont lieu dans une cellule de scannage sécurisée. Sont introduites à cette occasion des métadonnées telles le nom, le nombre de documents, le nombre de pages, la date d'arrivée du courrier, le type de traitement, et les données des agents concernés. À l'issue de la numérisation, un contrôle de qualité a lieu et des possibilités de correction sont offertes.

- **archivage:** le processus asynchrone d'envoi de documents vers l'Archiving-as-a-Service (AaaS) est expliqué étape par étape.

- **authenticité et intégrité:** les procédures de vérification des valeurs de hachage lors du chargement et de l'envoi vers les archives, ainsi que la protection et l'enregistrement des métadonnées sont décrits.

- **gestion des accès:** le document contient un aperçu détaillé des droits et rôles (owner, reader, messenger) et explique comment s'effectue le contrôle d'accès via le service Access Manager.

- **auditing et logging:** le traçage d'activités via des logs dans l'Access List Service est également décrit en détail.

Le document suit une structure fixe qui est conforme aux conditions légales (conformément à l'article 14 de l'AR du 7 décembre 2016). Chaque chapitre traite un aspect spécifique des procédures, ce qui contribue à l'exhaustivité et à la précision.

2.2. *La technologie utilisée garantit une reproduction fidèle, durable et complète des informations*

Le document précise que la technologie utilisée garantit une reproduction fidèle, durable et complète des informations par plusieurs mesures et processus qui sont décrits de manière explicite.

1. **Reproduction fidèle (authenticité et intégrité):**

   - le Document Repository contrôle, lors du chargement des documents, leur intégrité en comparant les valeurs de hachage fournies avec les valeurs de hachage qui sont à nouveau calculées au niveau interne. En effet, en l'absence de correspondance, le document est refusé et supprimé.
   - lors de l'envoi vers le service des archives (AaaS), un contrôle d'intégrité est à nouveau réalisé.
   - l'authenticité et l'imputabilité d'événements sont également garanties par l'utilisation de jetons générés via le système IAM (OAuth) du Portail de la sécurité sociale, qui permet de déterminer l'identité de l'application ou de l'utilisateur de manière crédible.

2. **Enregistrement durable:**

   - le Document Repository utilise la solution « Archiving-as-a-Service » (AaaS) pour l'archivage des documents à long terme, solution qui permet de conserver le document sous la forme d'une seule entité (contenu et métadonnées).
   - le dossier décrit également les mesures prises pour garantir la protection des métadonnées et des documents grâce à un enregistrement et une gestion des accès sécurisés, ce qui permet de disposer à tout moment de données complètes et fiables.

3. **Reproduction complète:**

- le contenu du document ainsi que toutes les métadonnées associées (métadonnées métier, de validation, d'accès, techniques et relatives aux parties prenantes) sont conservés et gérés, ce qui permet de disposer d'un contexte complet du document.
- des informations détaillées et des processus de traçage de toutes les actions effectuées sur les documents sont disponibles (journal de suivi via Access List Service), ce qui permet de reconstituer l'intégralité du cycle de vie de chaque document.
- des mécanismes détaillés de gestion des droits et des accès garantissent que seuls les acteurs habilités peuvent modifier ou consulter certaines données, ce qui garantit la cohérence et l'exhaustivité des informations.

4. **Infrastructure et protection:**

- le document évoque également la protection au niveau de l'infrastructure, tant physique (centre de données, serveurs) que logique (configuration, gestion des changements), ce qui contribue à la fiabilité et à la disponibilité des informations enregistrées.

En résumé, le dossier démontre que les technologies et procédures utilisées visent explicitement à garantir une conservation et une reproduction fidèles, durables et complètes des documents et des métadonnées associées au sein du système du Document Repository, conformément aux normes légales en vigueur et aux bonnes pratiques.

2.3. *Les informations sont enregistrées systématiquement et sans lacunes*

Il ressort du dossier que les informations sont enregistrées systématiquement et sans lacunes dans le système du Document Repository:

1. **enregistrement complet de documents et de métadonnées:**

- lors du chargement du document, non seulement le document même est enregistré, mais aussi différents types de métadonnées: métadonnées métier, métadonnées de validation, méthodes d'accès, métadonnées techniques et parties prenantes sont recueillis et enregistrés.
- le Document Repository refuse les chargements lorsque des métadonnées obligatoires font défaut (par exemple, un fichier metadata .json vide ou manquant), afin d'éviter l'enregistrement d'informations incomplètes.

2. **traçabilité et journalisation de toutes les actions:**

- toutes les actions effectuées sur les documents sont enregistrées dans l'Access List Service (ALS), y compris les opérations de chargement, d'accès, de modification et d'archivage.
- chaque action est enregistrée avec un transaction_id unique, la date et l'heure, des informations relatives au demandeur, le type d'action, le microservice concerné,

l'object_id et un hachage des métadonnées, afin de créer une piste d'audit complète et fiable.

3. **contrôle de l'intégrité et de la cohérence:**

   - des processus sont régulièrement exécutés pour vérifier les documents et les métadonnées et pour supprimer les documents dits « orphelins » (il s'agit de documents qui n'ont plus de lien ou de référence valide au sein du système, ce qui signifie que ces documents ne sont plus associés à une entité de métadonnées, une partie prenante, un espace de stockage ou un processus connexe approprié, et donc sans contexte d'utilisation), ce qui témoigne d'une approche systématique de l'intégrité et de l'exhaustivité des données.
   - de plus, les modifications apportées aux métadonnées ne sont effectuées que si l'application dispose des droits nécessaires et si (le cas échéant) un service de validation externe vérifie ces modifications.

4. **gestion et protection des métadonnées:**

   - toutes les métadonnées sont conservées dans une base de données structurée (Metadata Indexer Service) et les métadonnées spécifiques aux parties prenantes dans une base de données distincte (Access Manager Service), ce qui garantit l'exhaustivité et l'enregistrement structuré de toutes les informations pertinentes.

Il en découle que le système est conçu pour enregistrer et consigner toutes les informations de manière systématique, cohérente et sans omission, et qu'il prend des mesures actives pour garantir l'exhaustivité et la fiabilité.

2.4. *Les informations traitées sont conservées avec soin, classées systématiquement et protégées contre toute altération*

Les informations traitées dans le Document Repository sont conservées, classées et protégées contre toute falsification, d'une manière rigoureuse, systématique et sécurisée, comme le montrent les descriptions figurant dans le dossier:

1. **conservation rigoureuse et classement systématique:**

   - les documents sont couplés à des métadonnées et à des emplacements, et sont gérés via un modèle de données structuré dans lequel chaque document peut avoir plusieurs métadonnées et espaces de stockage.
   - il s'agit d'une architecture de microservices dans laquelle les métadonnées, le contenu des documents et les droits d'accès sont gérés dans différents services spécialisés (tels que MIS, FSS, AMS), ce qui facilite l'organisation et la gestion systématiques des documents et des métadonnées.
   - le cycle de vie des documents est géré à l'aide de processus de chargement, d'archivage et de suppressions régulières des caches temporaires et des incohérences, afin de garantir la cohérence et l'ordre.

2. **protection contre la falsification (authenticité et intégrité):**

- un contrôle d'intégrité est réalisé au moyen de hachages et d'algorithmes afin de vérifier que le document n'a pas été modifié depuis son chargement. Cela se fait au moment du chargement, ainsi que lors de l'archivage vers AaaS.
- les métadonnées sont protégées par des restrictions en matière de modification (par exemple, les métadonnées d'archivage ne sont plus modifiables une fois archivées) et par le calcul et la conservation des hachages des métadonnées afin de pouvoir détecter toute modification. Les modifications éventuelles dépendent des droits d'accès.
- tous les accès et toutes les modifications sont enregistrés et sont traçables, ce qui contribue également à l'authenticité et à la détection des tentatives de falsification.
- des procédures sont décrites pour la gestion des accès et l'autorisation, ainsi que pour la piste d'audit et la journalisation, afin d'enregistrer tous les événements et de garantir ainsi l'authenticité, l'imputabilité et le contrôle des documents.

3. **durabilité et pérennité de la conservation:**

- le stockage est conçu de manière à ce que les documents puissent être conservés de manière durable et fiable, grâce à une gestion responsable des formats et à des contrôles d'intégrité.
- des mesures de sécurité sont également mises en place au niveau de l'infrastructure, notamment une protection physique et logique des bases de données et des serveurs afin de sécuriser globalement le stockage et le traitement.

En résumé : le Document Repository permet une organisation systématique et un traitement rigoureux des documents et des métadonnées, avec des contrôles d'intégrité robustes, une gestion des accès, une journalisation et des processus de conservation durables, ce qui protège les informations contre la falsification et garantit leur conservation fiable.

2.5. ***Conservation des indications suivantes relatives au traitement des informations: l'identité du responsable du traitement ainsi que de celui qui a exécuté celui-ci, la nature et l'objet des informations auxquelles le traitement se rapporte, la date et le lieu de l'opération, les perturbations éventuelles qui sont constatées lors du traitement***

Le document précise que le traitement des informations fait l'objet d'une journalisation et d'un traçage détaillés, et que différentes données correspondant aux éléments demandés sont conservées:

- **identité du responsable et de l'exécutant du traitement:** le système nécessite une authentification via le service IAM du Portail de la Sécurité sociale, à l'aide d'un jeton contenant l'identité de l'application cliente. Cela permet de garantir l'authenticité et l'imputabilité des actions. De plus, les parties prenantes (les personnes disposant de droits sur le document) et leurs rôles sont explicitement conservés.

- **nature et objet des informations auxquelles le traitement se rapporte:** les documents sont associés à des métadonnées détaillées (de différents types, notamment

des métadonnées métier), et ces métadonnées sont systématiquement enregistrées et gérées.

- **date et lieu du traitement:** le chargement, l'accès et le traitement font l'objet d'un horodatage. Lors de l'archivage, par exemple, la date et l'heure de réception dans AaaS sont conservées. Les données de localisation des documents (l'endroit où ils sont conservés) sont également conservées.

- **incidents éventuels pendant le traitement:** il existe un mécanisme de journalisation qui enregistre tous les événements, y compris les erreurs et les exceptions qui se produisent, et des processus sont en place pour corriger les incohérences et les erreurs, telles que les documents « orphelins » (voir ci-dessus). Le système contient également des descriptions détaillées sur la gestion des erreurs (voir également la procédure Incident and Support Request Management, annexe 7).

En outre, le chapitre consacré aux traces d'activités et à la journalisation contient une description détaillée des enregistrements conservés, lesquels comprennent toutes les données pertinentes pour le contrôle et l'audit du traitement.

Le Document Repository enregistre et conserve les données relatives à l'identité des responsables et des exécutants, à la nature des données, à la date et à l'heure et au lieu du traitement ainsi que des indications générales d'incident/d'erreurs, conformément aux conditions fixées dans l'AR.

Par ces motifs,

la chambre sécurité sociale et santé du comité de sécurité de l'information

rend une délibération positive. Le dossier introduit par l'ONSS satisfait aux conditions techniques de l'arrêté royal du 7 décembre 2016.

La présente délibération entre en vigueur le 17 juin 2026.

Michel DENEYER
Président