

<p>Comité de sécurité de l'information Chambre sécurité sociale et santé</p>
--

CSI/CSSS/26/118

DÉLIBÉRATION N° 26/066 DU 7 AVRIL 2026 RELATIVE À LA DEMANDE DE L'INSTITUT NATIONAL D'ASSURANCES SOCIALES POUR TRAVAILLEURS INDÉPENDANTS (INASTI) VISANT À OBTENIR UNE AGRÉATION 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'Institut National d'Assurances Sociales pour Travailleurs Indépendants (INASTI);

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

A. CONTEXTE ET OBJET DE LA DEMANDE

1. La numérisation de documents est un élément essentiel du mode de fonctionnement de l'INASTI, dans le but de garantir la disponibilité rapide, l'intégrité et la force probante juridique des informations reçues. La procédure de traitement des documents entrants s'opère sur deux canaux complémentaires.
 1. Le flux Bpost (flux principal): il s'agit du canal primaire pour la réception centralisée et le traitement des courriers papier adressés à l'INASTI. Bpost est responsable du scanning, de la pré-indexation (c'est-à-dire la reconnaissance, la classification et l'extraction automatiques des métadonnées pertinentes à partir des images numériques des documents) et des contrôles de qualité, comme décrits dans le processus détaillé qui couvre la livraison, le scanning, l'extraction et la validation de données.
 2. Le scanning ad hoc (scanning interne INASTI): il s'agit d'un processus interne complémentaire. Il permet aux services internes de scanner les documents papier reçus localement et de les intégrer directement dans le système Sequoia. Ce flux interne est soumis à un contrôle strict et requiert une double validation obligatoire (scanner/validateur) pour garantir l'intégrité et la conformité, de sorte à ce que les documents obtiennent une force probante juridique équivalente à celle du flux Bpost.

Les deux canaux aboutissent à la même étape finale : l'intégration des documents numériques dans les systèmes de documentation de l'INASTI et leur archivage au sein de Archiving-as-a-Service (AaaS) via Document Repository.

L'ensemble de l'infrastructure de numérisation et les processus y afférents ont été conçus dans un souci de haute disponibilité, de contrôle systématique et de protection contre toute modification, ce qui constitue la base du dossier en matière de force probante. La force probante s'applique à l'ensemble des processus traitant des données, et ce dès la préparation du document jusqu'au moment de son archivage numérique.

La présente demande vient compléter l'avis favorable du Comité sectoriel de la sécurité sociale et de la santé (jadis compétent) de 2009 et la modification approuvée par le CSI en 2019. Le motif de cette modification est double. Premièrement, la migration de l'ensemble des documents d'un système de gestion de documents vers l'autre et ensuite l'utilisation d'un nouveau processus de scanning pour la classification du courrier entrant de l'INASTI.

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'agrément 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 décrit comment les documents papier sont indexés pour le scanning et comment ils sont ensuite traités et archivés. L'indexation de documents au moyen de métadonnées pertinentes permet de simplifier la recherche et la consultation de documents au sein du système d'archivage. Les principaux aspects de la procédure sont les suivants:

1. Préparation de la numérisation: la procédure débute par la préparation des documents pour la numérisation auprès de Bpost. Le courrier est reçu, enregistré et trié. Ensuite a lieu le scanning. Il existe également un flux de numérisation complémentaire pour les services internes de l'INASTI, permettant d'intégrer directement les documents reçus localement. Ce flux a recours aux scanners multifonctionnels internes.

2. Enregistrement des métadonnées: cela a lieu en plusieurs phases et à travers divers systèmes, à la fois auprès du partenaire externe Bpost et dans les systèmes de documentation internes de l'INASTI (Sequoia).

Préalablement au scanning des documents papier chez Bpost, ceux-ci sont enregistrés avec les métadonnées utiles. Les données sont extraites des images numériques du document au moyen d'OCR (optical character recognition), ICR (intelligent character recognition) et OMR (optical mark recognition). Ces métadonnées sont essentielles pour l'indexation et aident à identifier et à retrouver des documents dans le système d'archivage.

Après la transmission par Bpost, les documents sont intégrés dans les systèmes de l'INASTI via un processus batch. Lors de la numérisation interne ad hoc, les métadonnées sont enregistrées pendant le processus de scanning et de validation et enregistrées dans des tables de base de données sécurisées.

3. Scanning et validation: la procédure décrit le scanning et la validation via les deux flux. Les deux processus incluent des étapes de contrôle de qualité et de validation afin de garantir la force probante des documents numériques.

Le scanning auprès de Bpost comprend des étapes de contrôle de qualité et de validation rigoureuses. Pendant le scanning, la qualité de l'image est contrôlée en permanence. Si la qualité ne correspond pas aux exigences, le document est scanné à nouveau. Après le scanning, une reconnaissance de texte automatique est réalisée (OCR/ICR), les métadonnées sont extraites et les documents sont automatiquement classés sur la base du lay-out, des mots-clés, des logos et autres éléments de contenu. Si une classification automatique est impossible, les documents sont traités manuellement via un portail sécurisé, où des opérateurs spécialisés complètent ou corrigent les données. A la fin du processus, un contrôle de qualité aléatoire est effectué afin de garantir l'exactitude et l'exhaustivité du traitement.

La numérisation ad hoc est exécutée localement au sein de l'INASTI avec des scanners multifonctionnels internes et est conçue de sorte à garantir la même force probante juridique que le flux Bpost. Ce processus repose sur un double contrôle (scanner/validateur) Le scanning est effectué par le gestionnaire. Le système génère automatiquement un document PDF avec un identifiant unique et le fichier est ensuite transféré vers Sequoia. Le validateur consulte l'aperçu PDF et le compare à l'original papier pour vérifier l'intégralité, l'orientation, la lisibilité et la précision de l'image numérisée. Le validateur ne peut jamais valider un document qu'il a lui-même scanné. Après la validation, le document est soumis au même processus d'archivage et aux mêmes mesures de sécurité que les documents du flux Bpost.

4. Enregistrement et archivage: suite au traitement, les documents sont enregistrés dans une solution d'archivage sécurisée, qui conserve le statut et les métadonnées de chaque document.

Le stockage et l'archivage des documents (tant ceux en provenance du flux Bpost que ceux en provenance du scanning ad hoc interne) s'effectuent via différents systèmes intégrés au sein de l'INASTI, avec pour destination finale une plateforme d'archivage avec force probante.

Ce processus comprend trois phases: enregistrement temporaire, intégration dans les systèmes de documentation (Sequoia) et archivage définitif dans Archiving-as-a-Service (AaaS) qui est la solution d'archivage centrale et définitive de l'INASTI. Les mêmes

directives de sécurité et de conservation sont applicables à l'archivage de documents, que ces documents proviennent du flux Bpost ou du flux ad hoc.

Les systèmes utilisés pour le stockage et le traitement des documents (dont les bases de données) sont soumis à des procédures de sauvegarde strictes.

5. Monitoring et logging: le système conserve des logs détaillés de toutes les actions qui ont été exécutées pendant le processus d'archivage, en ce compris la personne qui a exécuté les actions et à quel moment. Ceci contribue à la transparence et à la traçabilité du processus.

Chez Bpost, toutes les étapes du processus sont enregistrées dans un système de workflow management, BoxOffice. Outre les informations concernant le scanner à l'aide duquel le document a été scanné, il est également enregistré à quel moment et par quel collaborateur les corrections dans la classification et la validation des données ont été exécutées. Ainsi, l'intégralité du traitement est enregistré et consigné.

Au sein de l'INASTI, le monitoring et le logging du traitement de documents et des systèmes sous-jacents s'effectuent via différents outils et mécanismes spécialisés afin de garantir une traçabilité complète, la détection d'erreurs et la sécurité.

Le logging peut être réparti en deux catégories principales: les loggings applicatifs et système (pour le monitoring fonctionnel et le monitoring des prestations) et les loggings de sécurité (pour la traçabilité des interactions et des accès). Les loggings de sécurité sont une exigence fondamentale de la BCSS visant à enregistrer les événements et les activités au sein du système. Les loggings contiennent des informations essentielles telles que l'appel d'opérations ou de méthodes, l'identité du demandeur et du destinataire, le statut de l'interaction (réussite ou échec). Après leur archivage, ces loggings sont uniquement accessibles au service de sécurité de l'information de l'INASTI.

6. Gestion d'incidents: la procédure contient aussi des directives pour faire face à des incidents ou erreurs éventuels qui se manifestent pendant le traitement, ce qui aide à garantir la qualité et l'intégrité de l'archivage.

La gestion des incidents à l'INASTI est structurée et comprend à la fois des processus pour les services fournis par Bpost et pour les composants IT internes (Document Repository, AaaS et le réseau/l'infrastructure en général).

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

La reproduction fidèle, durable et complète des informations est atteinte à travers divers mécanismes et processus intégrés aux procédures:

1. Contrôle d'intégrité: l'intégrité des données est garantie par l'attribution d'une valeur de hachage unique lors du scanning, le contrôle de validation (validation obligatoire par une deuxième personne qui n'a pas réalisé le scanning), l'enregistrement des métadonnées, les contrôles de qualité (contrôles d'exhaustivité, de la qualité de l'image, du traitement

correct), l'absence de manipulation de données (aucune modification directe dans la base de données de production n'est autorisée; toutes les actions doivent s'effectuer via les applications métier). La suppression physique de données n'est pas autorisée), la conservation de données historiques, le contrôle d'accès et la gestion des incidents. Ces mécanismes coopèrent afin de garantir que les données soient exactes, complètes et fiables.

2. **Enregistrement durable:** les documents sont enregistrés dans une solution d'archivage (AaaS), qui est conçue pour l'archivage à long terme (les documents sont archivés en format PDF/A) et qui garantit la pérennité et la lisibilité des documents. Cela permet de garantir que les données restent accessibles et que les données ne se perdent pas ou ne soient pas endommagées.
3. **Reproduction complète:** pendant le processus d'archivage, toutes les métadonnées pertinentes et les index sont enregistrés dans des bases de données sécurisées, ce qui contribue à une reproduction complète des informations. Toutes les actions (par des utilisateurs, date et heure des actions, historique des validations et remplacements) font l'objet d'un logging complet dans Sequoia. Ceci est essentiel pour la transparence et la traçabilité.

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

L'enregistrement systématique et sans lacunes est réalisé au moyen de divers mécanismes et procédures qui ont été implémentés.

1. **Pré-enregistrement de la documentation:** préalablement au scanning des documents, ils sont enregistrés avec les métadonnées utiles, telles que la date et l'heure du scanning, le scanner utilisé et un numéro de séquence. L'évolution des métadonnées, à savoir le statut d'un envoi postal est entièrement consigné. Ceci garantit que toutes les modifications dans le processus de traitement sont systématiquement consignées, y compris l'utilisateur et le moment exact de l'action.
2. **Enregistrement complet des processus:** pendant le processus d'archivage, toutes les étapes sont documentées, en ce compris la personne qui a scanné les documents, à quel moment, et le statut de chaque document à différents moments dans le processus. Cela comprend aussi la validation des documents scannés.
3. **Validation des informations: contrôle d'intégrité (hash):** lors de la migration des documents existants; l'intégrité est vérifiée sur la base de la valeur de hachage. Si la valeur de hachage, lors du transfert vers Document Repository, ne correspond pas à celle reçue, le document est rejeté avec un message d'erreur et n'est pas accepté. Si la valeur de hachage n'est pas présente, celle-ci est calculée avant que le document ne soit transmis. Ceci garantit que les documents sont transmis sans modification.
4. **Données historiques:** le système conserve un historique détaillé de toutes les interactions avec les documents, par exemple qui les a consultés et à quel moment. Ceci contribue à un enregistrement complet et transparent des informations.

5. **Protection des données:** la technologie garantit que les informations enregistrées ne peuvent pas être modifiées ou supprimées sans l'autorisation adéquate, ce qui aide à garantir la complétude et l'intégrité des données.

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

La conservation méticuleuse, la classification systématique et la protection contre la falsification sont atteints à travers diverses mesures et des processus qui sont intégrés au système d'archivage.

1. **Conservation minutieuse:** les documents sont enregistrés dans une solution d'archivage sécurisée (AaaS) qui a été conçue pour garantir la pérennité et l'archivage à long terme. Cela permet de garantir que les données ne se perdent pas ou ne soient endommagées. Des mesures effectives sont prises pour garantir la continuité de la prestation de service et la reprise en cas d'incident majeur (voir BCP Bpost et DRP de l'INASTI). Par ailleurs, des mesures ont également été prises concernant la protection physique du bâtiment (tant le bâtiment de Bpost que les centres de données de Smals) et des appareils et des protections sont présentes contre les dangers naturels tels un incendie, des dégâts d'eau, des problèmes avec l'air conditionné et les problèmes électriques.

2. **Classification systématique:** les informations sont organisées sur la base de métadonnées prédéfinies (identification, langue, statut, date de réception, références à la division et à la catégorie) et de classifications, ce qui garantit leur accessibilité et la possibilité de faire des recherches. Cela comprend l'enregistrement de métadonnées pertinentes lors du pré-enregistrement de documents, ce qui contribue à un stockage structuré.

3. **Protection contre la falsification:** le système a recours au contrôle d'intégrité sur base du hachage et d'autres mécanismes de protection (p.ex. la limitation de l'accès via des rôles applicatifs et une authentification forte (IAM)). Par ailleurs, toute modification directe dans la base de données est interdite. Toutes les actions doivent s'effectuer via les applications métier (Sequoia). Les fichiers de logging, dans lesquels sont enregistrées les opérations de migration et les informations de hachage, sont exportés quotidiennement et signés au moyen d'un certificat. Ceci permet un contrôle sûr et fiable en cas d'enquête et réduit considérablement le risque de falsification.

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 processus conserve les données pertinentes relatives au traitement des informations, de manière structurée et minutieuse. Cela comprend les aspects suivants:

1. **identité du responsable du traitement et de la personne qui a réalisé le traitement:** le système enregistre qui est responsable du traitement des documents ainsi que la personne qui a scanné et validé les documents. Ce qui garantit une attribution précise des

responsabilités. Le responsable final du traitement est l'INASTI. L'exécutant est repris dans les fichiers journaux.

2. **nature et objet des informations:** les métadonnées enregistrées avec les documents contiennent des informations relatives à la nature et à l'objet des documents. Ceci comprend des classifications telles que la langue, la catégorie, la division et le statut. La nature et l'objet (classification) des documents sont contrôlés et consignés comme élément du SLA avec Bpost (conformité de la classification).
3. **date et lieu du traitement:** le système enregistre la date et l'heure (tant lors du scanning ad hoc qu'auprès de Bpost) du traitement, ainsi que le lieu (par exemple le système ou l'application utilisé), ce qui indique où se situe le document dans le processus. Cela contribue à la traçabilité des données.
4. **Incidents éventuels pendant le traitement:**
 - **Gestion des incidents:**
Pour les incidents concernant les opérations de numérisation effectuées par Bpost, le processus suivant est appliqué: après qu'un incident a été signalé et a obtenu un numéro de ticket unique et un horodatage, l'INASTI reçoit immédiatement une confirmation de Bpost, qui prend les mesures nécessaires pour résoudre l'incident dans les délais convenus et rétablir le fonctionnement normal des services.
 Pour les incidents au niveau du Document Repository et AaaS (archivage), l'INASTI reçoit une communication automatique via Smals.
 - **Monitoring et traitement des incidents d'infrastructure:**
Error logging lors de la migration: lors de la migration de documents, des loggings détaillés sont enregistrés, y compris les messages d'erreur. En cas d'erreur, une procédure de relance ('retry') est appliquée et si celle-ci échoue, le document est placé dans une file d'attente d'erreurs en vue d'une intervention manuelle par les équipes techniques de l'INASTI.
Erreurs d'intégrité: lorsqu'un contrôle d'intégrité échoue lors de la migration (la valeur de hachage ne correspond pas), le Document Repository transmet un message d'erreur spécifique, indiquant une anomalie. Dans ce cas, le document n'est pas accepté par le Document Repository.

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'INASTI satisfait aux conditions techniques de l'arrêté royal du 7 décembre 2016.

La présente délibération entre en vigueur le 22 avril 2026.

Michel DENEYER
Président

Le siège de la chambre sécurité sociale et santé du comité de sécurité de l'information est établi dans les bureaux de la Banque Carrefour de la sécurité sociale, à l'adresse suivante: Quai de Willebroeck 38 - 1000 Bruxelles (tél. 32-2-741 83 11).