EVALUATION PROPRE DU CONTRÔLE D'UN DOSSIER PAR RAPPORT AUX CONDITIONS TECHNIQUES DE L'ARRÊTÉ ROYAL APPLICABLE

L'arrêté royal applicable est, selon le cas, l'arrêté royal du 22 mars 1993 *relatif à la valeur probante, en matière de sécurité sociale, des informations enregistrées, conservées ou reproduites par des institutions de sécurité sociale*, l'arrêté royal du 28 novembre 1995 *relatif à la force probante, en matière de sécurité sociale des travailleurs indépendants, des informations utilisées par l'Administration et les organismes coopérants en matière de sécurité sociale des travailleurs indépendants* ou l'arrêté royal du 15 mars 1999 *relatif à la valeur probante, en matière de sécurité sociale et de droit du travail, des informations échangées, communiquées, enregistrées, conservées ou reproduites par les services ministériels et les parastataux du Ministère de l'Emploi et du Travail.*

Cadre légal

https://www.ksz-bcss.fgov.be/fr (voir Législation / Force probante)

B. Contenu de l'évaluation propre - Conditions de base

L'accent est mis sur la procédure selon laquelle des informations sont enregistrées, conservées et reproduites sur un support lisible.

1. L'accent est mis d'abord sur la procédure et non sur les données concrètes. Autrement dit : il ne s'agit pas de ce qui est enregistré, mais de la façon dont c'est enregistré.
2. La procédure doit porter à la fois sur l'enregistrement, la conservation et la reproduction lisible des informations. Tandis qu'il est question dans l'AR d'une procédure relative à une ou plusieurs de ces actions, le Comité sectoriel a déclaré d'emblée que ces actions devaient toutes être reprises dans une seule procédure. Une procédure qui porte uniquement sur l'enregistrement de données ne pourra jamais faire l'objet d'une reconnaissance.

L'accent est ensuite mis sur le fait que la procédure et le système d'archivage doivent être opérationnels. L'objet de l'évaluation doit donc effectivement exister; les projets et plans n'entrent pas en ligne de compte pour l'évaluation propre. Une conséquence pratique est qu'il faut investir dans un système avant de pouvoir le soumettre à une évaluation, ce qui entraîne des risques.

Finalement, l'accent est mis sur l'approbation formelle du rapport de l'évaluation propre par le niveau supérieur de la hiérarchie au sein de votre organisation.

C. Contenu de l'évaluation propre - Conditions techniques.

L'évaluation propre doit s'effectuer en fonction des conditions techniques de l'arrêté royal. La Banque Carrefour les a réparties dans 5 domaines explicites. De manière générale, une attention particulière est portée aux divers aspects de sécurité.

1. Le système décrit la procédure avec précision

Description complète et schématique de toutes les procédures relatives à :

→ l'enregistrement et à la conservation des informations sur un support d'information électronique ;

→ la reproduction[1], sur un support d'information, lisible ou non à l'œil nu (p.ex.: écran, papier, copie vers un autre support d'information électronique), des informations enregistrées sur le support électronique.

Il y a lieu de fournir une description détaillée des actions et de l'ordre dans lequel celles-ci se déroulent à partir de la réception des informations jusqu'au moment du dernier traitement.

Un aspect important de la procédure à décrire consiste à désigner les personnes ou catégories de personnel habilitées à exécuter les actions décrites.

Mots-clés : INTÉGRITÉ et TRACABILITÉ

Remarque : "localisation des images / fichiers au cours du workflow"
Dès le moment où les images sont enregistrées pour la 1ère fois par la voie électronique jusqu'au moment où les données électroniques sont enregistrées sur leur support définitif (fonctionnalité "WORM"), il y a lieu d'indiquer clairement à quel endroit se trouvent les images/fichiers (temporaires/intermédiaires), par quel hardware/software les données sont traitées et comment l'intégrité de ces images est assurée (et qui possède quels droits d'accès). Il s'agit d'un aspect crucial dans un dossier de force probante. Il y a lieu d'indiquer clairement dans le workflow **où** se situe l'image (décrire les spécifications et les mesures de sécurité garantissant que l'image ne puisse pas être modifiée).

→ "**où**" – correspond aux indications suivantes: sur quel support d'enregistrement et dans quel format, quel système (fichier) / OS / DB, accessible à quelles applications et quels utilisateurs (admins, utilisateurs ordinaires, ...) ...

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

Reproduction = enregistrement sur support d'information électronique + reproduction des informations enregistrées sur un support lisible ou non à l'œil nu

Pour ce domaine, il faut obligatoirement évaluer au moins les aspects suivants dans l'ordre indiqué :

- **A.** la description de la configuration hardware et software installée (avec ajout d'une représentation schématique) ;
- **B.** le caractère durable du support d'enregistrement utilisé (p.ex. WORM, ...) ;
- **C.** le circuit de traitement et de scannage des supports concernés ;
- **D.** le point de contrôle automatique et manuel selon les étapes du processus ;
- **E.** la transmission des documents électroniques dans le système de gestion de documents ;
- **F.** les formats des fichiers et leur conformité avec les standards d'archivage garantissant la pérennité des données enregistrées ;
- **G.** la gestion des incidents, des erreurs et les mécanismes de reprise ou de rejet éventuel de l'information ;
- **H.** les instructions d'utilisation de la solution ;

[1] Par "reproduction" il y a lieu d'entendre la reproduction sur un support d'information, lisible ou non à l'œil nu. Le fait de copier des informations vers un autre support d'information électronique relève donc également de la reproduction. Une *visualisation* n'est donc pas nécessaire.

I. le déroulement du processus de scannage : le traitement d'une page blanche lors du scannage, le traitement de documents dont le format est supérieur ou inférieur à un A4, ... ;
J. la présence de contrats de maintenance pour les logiciels et les matériels installés ;
K. les chiffres de disponibilité en ce qui concerne le hardware et les logiciels (failure & repair) ;
L. la présence de support pour les utilisateurs ;
M. la présence d'un dispositif de back-up (pour l'ensemble de l'infrastructure) ;
N. les mesures / contrôles garantissant qu'aucune modification n'a été effectuée dans les informations enregistrées ;
O. les mesures relatives à l'archivage et à la consultation à distance (par exemple garantie contre les modifications lors de la transmission des données) ;
P. le contrôle de la qualité et de la quantité.

3. Les informations sont enregistrées systématiquement (= facilité d'effectuer des recherches) et sans lacunes.

Des données d'index doivent être enregistrées avec les informations, permettant de localiser une donnée dans la masse d'informations et de reconstruire l'utilisation des informations. Il y a lieu de décrire la procédure pour l'exécution des contrôles de qualité et de quantité lors de l'enregistrement des informations.

Pour ce domaine, il faut obligatoirement évaluer au moins les aspects suivants dans l'ordre indiqué :

A. comment se déroule l'indexation des documents enregistrés de façon électronique ;
B. les mesures visant à éviter que les documents scannés et indexés soient modifiés / supprimés ou enregistrés plusieurs fois ;
C. l'exécution d'un contrôle de qualité et de quantité lors du scannage de documents (éventuellement rescannage, quid documents recto-verso)
D. le mode d'indexation des documents scannés permettant de retrouver facilement les images enregistrées ;
E. les mesures prises pour éviter l'attribution de données d'index erronées ;
F. la possibilité de reconstitution des données d'index en cas de perte de ces données ;
G. la limitation de l'accès aux données d'index et la protection contre les modifications et les suppressions ;
H. le support sur lequel les données d'index sont enregistrées ;
I. la notification immédiate de problèmes intervenus lors du scannage de documents ;
J. la procédure pour résoudre les problèmes constatés.

Une démonstration doit permettre de vérifier ces divers éléments.

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

Pour ce domaine, il faut obligatoirement évaluer au moins les aspects suivants dans l'ordre indiqué :

A. l'infrastructure (e.a. serveurs, banque de données et file storage) est redondante et répartie sur deux sites géographiquement distincts, permettant de garantir la continuité des services et la reconstruction en cas d'incident majeur ; les documents archivés sont conservés au sein d'une architecture de type "WORM" répartie sur les deux sites [OU des mesures adéquates ont été prises pour garantir la continuité des services et la reconstruction en cas d'incident majeur (e.a. infrastructure SAN redondante)] ;

B. le système de back-up/restore est organisé avec des règles précises d'exécution selon un planning pré-établi, des rotations de supports en fonction du planning; ces procédures sont intégrées dans le système de back-up/restore global de l'organisme;
C. des mesures efficaces en matière de disaster recovery ont été prises et testées ;
D. des mesures efficaces ont été prises en ce qui concerne la protection physique du bâtiment, des appareils et des sauvegardes contre des risques naturels tels que les incendies, les dégâts causés par l'eau, les problèmes de climatisation et d'électricité ;
E. en ce qui concerne le contrôle d'accès physique, il est notamment fait usage d'un système de badges géré à un niveau central ;
F. la période de rétention et de conservation des supports est définie ;
G. la protection d'accès logique repose sur différentes méthodes en fonction du système d'information visé et des activités confiées aux utilisateurs; les droits d'accès sont déterminés via RBAC (role based access control) ;
H. la connexion au système d'information s'effectue via des postes de travail dûment sécurisés au sein de l'institution et via une connexion à distance sécurisée (VPN) dans le cadre du télétravail et l'accès est uniquement accordé sur base de la policy en matière de sécurité IT de votre institution ;
I. les applications et logiciels concernés font l'objet d'une maintenance sur base d'une politique de patches qui colmate les faiblesses éventuelles de la solution implémentée ; les tests, l'acceptation et le release de nouvelles versions d'un composant d'une solution sont conformes au processus de release management standard de votre institution ; les procédures et exemples de documentation relatifs au release management étaient tenus à la disposition pour consultation lors de l'audit de la Banque Carrefour de la sécurité sociale ;
J. en tant qu'organisme du réseau [primaire/secondaire] articulé autour de la Banque Carrefour de la sécurité sociale, votre institution respecte les normes minimales de sécurité.

5. La conservation des données suivantes relatives au traitement de l'information : l'identité du responsable du traitement; l'identité de la personne qui a exécuté le traitement; 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.

Traitement = enregistrement sur support d'information électronique + reproduction des informations enregistrées sur un support lisible ou non à l'œil nu

Pour ce domaine, il y a lieu de mentionner explicitement dans le dossier, pour les deux aspects (enregistrement et reproduction), dans quelle mesure et comment le système installé répond aux critères. Le but de l'enregistrement de données de logging est de pouvoir déterminer, à tout instant, qui a effectué quelle action et quels sont les problèmes qui se sont produits. Il y a lieu de décrire sur quelles actions les données de logging ont trait, comment ces données sont enregistrées et conservées et comment s'effectue la visualisation de ces données. En ce qui concerne la création et la conservation des données de loggings, il est important de démontrer le respect des règles suivantes :

a. les données de logging doivent être conservées aussi longtemps que les informations sur lesquelles elles portent (quel que soit le support d'enregistrement) ;
b. les données de logging doivent être disponibles de manière relativement rapide et doivent permettre de rechercher des données de manière aisée et conviviale ;
c. l'accès logique et physique aux données de logging doit être limité aux personnes habilitées ;

d. les données de logging ne peuvent pas être modifiées ;
e. les fichiers de logging sont intégrés dans les procédures de back-up / restore standard de l'institution.

D. Evaluation propre - en pratique

Les étapes suivantes seront parcourues pour votre propre dossier :

1) Analyse du rapport provisoire de l'évaluation propre en fonction des 5 domaines (documentation en annexe) avec les collaborateurs responsables et la direction ;
2) Soumission du rapport final de l'évaluation propre à l'approbation de l'administrateur général de votre institution, qui l'approuvera formellement en apposant sa signature ;

Une bonne pratique consiste à communiquer le rapport final approuvé de l'évaluation propre à titre d'information au comité de direction de votre institution, de sorte que tous les intéressés soient au courant.

Remarque importante : la BCSS a toujours la possibilité de réaliser des contrôles indépendants de votre évaluation propre.

E. Références

- ISO/TR 13028:2010, Information and documentation - Implementation guidelines for digitization of records http://www.iso.org/iso/catalogue_detail.htm?csnumber=52391
- MoReq2 (Model Requirements for the management of electronic records. Update and extension, 2008); http://www.moreq2.eu
- ISO 15489
  - Information and documentation — Records management — Part 1: General ISO 15489-1, 2016-04-15 http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=62542
  - Information and documentation — Records management — Part 2: Guidelines ISO 15489-1, 2001-09-15 http://www.iso.org/iso/catalogue_detail?csnumber=35845
- ISO/TR 15801:2009, Document management -- Information stored electronically -- Recommendations for trustworthiness and reliability (142 CHF) http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=50499
- ISO/FDIS 14641- Electronic archiving -- Part 1: Specifications concerning the design and the operation of an information system for electronic information preservation; http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=54911
- DoD 5015.2 v3, Electronic Records Management Software Applications Design Criteria (April 25, 2007)
- ISO/IEC 27002:2013, Information technology -- Security techniques -- Code of practice for information security management http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54533

FIN DU DOCUMENT