Comité sectoriel de la sécurité sociale et de la santé
Section « Sécurité sociale »

CSSS/12/350

AVIS N° 12/120 DU 4 DÉCEMBRE 2012 CONCERNANT LA DEMANDE DE LA CAISSE D'ASSURANCES SOCIALES XERIUS AFIN D'OBTENIR UNE RECONNAISSANCE MINISTÉRIELLE POUR UN SYSTÈME D'ARCHIVAGE ÉLECTRONIQUE EN APPLICATION DE 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

Vu la loi du 15 janvier 1990 relative à l'institution et l'organisation d'une Banque-carrefour de la sécurité sociale, notamment l'article 15, alinéa 2;

Vu la demande de la caisse d'assurances sociale XERIUS du 8 octobre 2012;

Vu le rapport d'auditorat de la Banque-carrefour du 27 novembre 2012;

Vu le rapport présenté par Yves Roger.

A. CONTEXTE ET OBJET DE LA DEMANDE

1.1. En date du 8 octobre 2012, la caisse d'assurances sociales XERIUS (ci-après en abrégé XERIUS) introduisait une demande auprès du Comité sectoriel de la sécurité sociale.

La présente demande vise à obtenir une agréation ministérielle pour ses procédures de digitalisaton et d'archivage dans le cadre de l'application de 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.

B. EXAMEN DE LA DEMANDE

2. L'évaluation des procédures qui ont été introduites en vue de l'obtention de l'agréation ministérielle est scindée en fonction des conditions techniques de l'article 3 de l'arrêté royal du 28 novembre 1995.

Ces conditions ont été examinées point par point dans le dossier de XERIUS.

Le rapport d'auditorat est le résultat d'une démarche en collaboration avec les responsables et les techniciens internes et externes de l'institution concernée. Cette démarche s'est déroulée en plusieurs étapes, à savoir:

- une réunion d'information à la Banque Carrefour de la sécurité sociale afin d'informer XERIUS sur le contenu du dossier 'force probante' qui est nécessaire à son approbation (14 novembre 2011);
- la rédaction par XERIUS d'un dossier à l'attention du Comité sectoriel de la sécurité sociale et de la santé (12 juillet 2012);
- une visite (audit) du service sécurité de l'information de la Banque Carrefour au site de XERIUS où une démonstration a été organisée ainsi qu'une séance de questions / réponses avec les acteurs concernés (9 août 2012);
- la rédaction par le service de sécurité de la Banque Carrefour d'une série de questions complémentaires sur divers aspects du processus mis en place;
- divers échanges de mails en vue d'une analyse critique du dossier et d'une précision de plusieurs détails;
- la rédaction par XERIUS d'une version révisée du dossier à l'attention du Comité sectoriel de la sécurité sociale et de la santé (12 octobre 2012).

XERIUS Caisse d'Assurances Sociales (anciennement Caisse d'assurances sociales VEV) a déjà obtenu une reconnaissance ministérielle en date du 2 mars 1998 dans le cadre de l'arrêté royal du 28 novembre 1995 relatif à la force probante des informations numériques en tant qu'organisme coopérant en matière de sécurité sociale. Ces procédures approuvées et le matériel et logiciel (Corsa) employés ont été entièrement renouvelés en 2012. En remplacement du système Corsa, XERIUS a développé un nouveau « Document Management System » (DMS). Le dossier numérique de chaque client a été amélioré et converti vers ce système DMS. Le DMS est un logiciel développé par XERIUS qui a recours à l'infrastructure IT du secrétariat social SD Worx.

L'ensemble de la base de données Corsa a été transféré vers DMS et depuis le 27 février 2012 toutes les nouvelles communications entrantes et sortantes sont enregistrées dans DMS.

Le dossier soumis et le rapport d'auditorat y afférent portent uniquement sur les procédures de numérisation du flux de documents entrant et sortant.

Vous trouverez en annexe de ce rapport un document contenant les remarques qui ont été formulées par le service Sécurité de l'information de la Banque Carrefour. XERIUS a intégré ces commentaires dans la nouvelle version du dossier.

La proposition décrit la procédure avec précision.

2.1. Le dossier introduit par XERIUS comprend une description des procédures mises en place pour l'enregistrement et la conservation avec soin des données au travers de la solution XERIUS DMS et la reproduction de celles-ci sur un support lisible.

Le dossier présenté décrit précisément les mécanismes, les contrôles et les intervenants dans le processus mis en place.

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

2.2. Le dossier présenté par XERIUS nous a conduit à vérifier que la solution décrite de gestion électronique des documents garantit bien les règles énoncées dans le §2 de l'article 3 de l'arrêté royal du 28 novembre 1995.

Pour ce faire, nous avons été particulièrement attentifs aux aspects suivants:

- ✓ aux composants des solutions techniques (architecture technique et logiciels);
- ✓ au circuit de traitement et de scannage des supports concernés;
- ✓ au point de contrôle automatique et manuel selon les étapes du processus;
- ✓ à la transmission des documents électroniques dans le système de document management;
- ✓ aux formats des fichiers et à leur conformité avec les standards d'archivage garantissant la pérennité des données enregistrées;
- ✓ à la gestion des incidents, des erreurs et aux mécanismes de reprise ou de rejet éventuel de l'information;
- ✓ aux instructions d'utilisation de la solution;
- ✓ au déroulement du processus de scannage: le traitement d'une page blanche au cours du scannage, le traitement de documents dont la taille est inférieure / supérieure à un A4, … ;
- ✓ à la prévision de contrats de maintenance pour les logiciels et les hardware installés;
- ✓ à la présence d'une section de support interne;
- ✓ aux mesures / contrôles garantissant qu'aucune modification n'a été réalisée dans les informations enregistrées;
- ✓ au contrôle de la qualité et de la quantité.

Les informations sont enregistrées systématiquement

2.3. Le dossier de XERIUS décrit les procédures concernant:

- ✓ l'indexation des documents;
- ✓ l'impossibilité de modifier ou de perdre des documents scannés ou de les enregistrer plusieurs fois;
- ✓ le mode d'enregistrement et le mécanisme de validité des index;
- ✓ la reconstruction des index;
- ✓ la limitation d'accès aux index ;
- ✓ l'exécution d'un contrôle de qualité et de quantité lors du scannage des documents.

Ces différents aspects ont pu être contrôlés lors de la démonstration.

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

2.4. XERIUS a notamment installé les mesures suivantes:

- ✓ l'infrastructure (e.a. serveurs, banque de données et SAN) est redondante et repartie dans deux salles informatiques distantes de plusieurs kilomètres, ce qui permet de garantir la continuité de la prestation de service et la reconstruction en cas d'incident majeur;
- ✓ le système de sauvegarde 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 sauvegarde global de l'organisme;
- ✓ des mesures efficaces en matière de disaster recovery ont été prises et testées ;
- ✓ 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 l'incendie, les eaux excédentaires, les problèmes d'acclimatement et d'électricité;
- ✓ un système de badges géré à un niveau central est utilisé pour le contrôle d'accès physique;
- ✓ la période de rétention et de conservation des supports est définie;
- ✓ la protection d'accès logique repose sur des méthodes (MS Active Directory) pour lesquelles les droits d'accès sont déterminés au moyen de RBAC (role based access control);
- ✓ la connexion au système d'information est possible via des postes de travail sécurisés au sein de l'institution et via un accès sécurisé à distance (VPN) et l'accès est uniquement accordée via le standard IT security policy de XERIUS;
- ✓ la maintenance des applications et des logiciels concernés est garantie par une politique qui remédie aux faiblesses éventuelles dans la solution mise en place. Les tests, l'acceptation et la release de nouvelles versions d'un

composant de la solution se font conformément au standard XERIUS release management procès ;
- ✓ en tant qu'organisme du réseau secondaire articulé autour de la Banque Carrefour de la sécurité sociale, XERIUS doit respecter les normes minimales de sécurité.

Pendant la visite des lieux, toute la documentation utile (plans en matière de disaster recovery, architecture, manuels, politiques de sécurité, …) était disponible pour consultation.

En ce qui concerne la 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.

2.5. XERIUS a équipé son système de:

- ✓ divers loggings informatisés et de fichiers de suivi permettant de conserver les évènements des différents composants à chaque stade du processus mis en place; l'accès à ces informations suit un processus sécurisé et organisé; les loggings sont intégrés dans les procédures de sauvegarde standard de l'institution;
- ✓ au niveau de la base de données, il y a lieu de faire en sorte que, lors de la migration prévue vers une version supérieure de SQL Server, les possibilités d'audit pour l'administrateur des utilisateurs puissent être exploitées.

Par ces motifs,

la section sécurité sociale du comité sectoriel de la sécurité sociale et de la santé

émet un avis favorable. Le dossier introduit par XERIUS semble satisfaire aux conditions techniques de l'article 3 de l'arrêté royal du 28 novembre 1995.

Yves ROGER
Président