Comité sectoriel de la Sécurité sociale et de la Santé
Section « Sécurité sociale »

CSSS/09/121

AVIS N° 09/22 DU 6 OCTOBRE 2009 CONCERNANT LA DEMANDE DE L'OZ ONAFHANKELIJK ZIEKENFONDS AFIN D'OBTENIR UNE RECONNAISSANCE MINISTÉRIELLE POUR UN SYSTÈME D'ARCHIVAGE ÉLECTRONIQUE EN APPLICATION DE L'ARRÊTÉ ROYAL DU 22 MARS 1993 RELATIF A LA FORCE PROBANTE

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 l'OZ Onafhankelijk Ziekenfonds du 21 août 2009;

Vu le rapport d'auditorat de la Banque-carrefour du 30 septembre 2009;

Vu le rapport présenté par Yves Roger.

A. CONTEXTE ET OBJET DE LA DEMANDE

1.1. En date du 21 août 2009, l'OZ Onafhankelijk Ziekenfonds[1] a introduit une demande d'agréation auprès du comité sectoriel de la sécurité sociale et de la santé.

La présente demande vise à obtenir une agréation ministérielle pour ses procédures dans le cadre de l'application de l'arrêté royal du 22 mars 1993 relatif à la force probante, en matière de sécurité sociale, des informations enregistrées, conservées ou reproduites par des institutions de sécurité sociale.

[1] L 'Union nationale des Mutualités Libres regroupe sept mutualités: Euromut Mutualité Libre, Partenamut Mutualité Libre, Mutualité Libre Securex, la Mutualité Professionnelle et Libre de la Région wallonne, la Freie Krankenkasse, Partena Ziekenfonds & Partners et **l'OZ Onafhankelijk Ziekenfonds**.

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 22 mars 1993.

Ces conditions ont été examinées point par point dans le dossier de l'***OZ***.

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 l'***OZ*** sur le contenu du dossier 'force probante' qui est nécessaire à son approbation (8 29avril 2008);
- ✓ la transmission par l'institution d'une première version de son dossier au service de sécurité de l'information de la Banque Carrefour de la sécurité sociale (3 février 2009);
- ✓ une réunion de travail du 25 mars 2009 a été consacrée à l'analyse critique du dossier;
- ✓ la transmission par l'institution d'une nouvelle version de son dossier au service de sécurité de l'information de la Banque Carrefour de la sécurité sociale (24 avril 2009);
- ✓ 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;
- ✓ une visite (audit) du service sécurité de l'information de la Banque Carrefour au site de l' ***OZ*** où une démonstration a été organisée ainsi qu'une séance de questions / réponses (18 juin et 1 juillet 2009);
- ✓ divers échanges de mails en vue d'une analyse critique du dossier et d'une précision de plusieurs détails;
- ✓ la rédaction par l'***OZ*** d'un dossier à l'attention du comité sectoriel de la sécurité sociale et de la santé.

La proposition décrit la procédure avec précision.

2.1. Le dossier introduit par l***'OZ*** comprend une description des procédures mises en place pour l'enregistrement et la conservation avec soin des données au travers d'un système d'archivage électronique 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 l'***OZ*** 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 22 mars 1993.

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 l'***OZ*** 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. L'***OZ*** a notamment installé les mesures suivantes:

- ✓ des mesures efficaces ont été prises afin de garantir la continuité de la prestation de service et la reconstruction en cas d'incident majeur (notamment une infrastructure SAN redondante) ;
- ✓ 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 physique repose sur différentes méthodes en fonction du système d'information visé et des activités confiées aux utilisateurs; les droits d'accès sont déterminés selon la méthode RBAC (role based access control);
- ✓ la connexion au système d'information est possible via des postes de travail sécurisées au sein de l'institution et via un accès sécurisé à distance (VPN et certificat) dans le cadre du télétravail ;
- ✓ 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 ***OZ*** release management process. Les procédures et exemples de documentation utilisées en release management étaient mises à notre disposition lors de l'audit de la Banque Carrefour de la Sécurité Sociale;
- ✓ en tant qu'organisme du réseau secondaire articulé autour de la Banque Carrefour de la sécurité sociale, l'OZ respecte les normes minimales de sécurité.

Pendant la visite des lieux, toute la documentation utile (manuels, disaster recovery plan, VPN security policy, …) pouvait être consultée.

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. L'***OZ*** 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.

Par ces motifs,

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

émet un avis favorable.

Yves ROGER
Président