

CSSS/06/098

AVIS N° 06/11 DU 18 JUILLET 2006 RELATIF A LA DEMANDE DE L'ONSS (OFFICE NATIONAL DE SECURITE SOCIALE) D'OBTENIR UNE RECONNAISSANCE MINISTERIELLE POUR UN SYSTEME D'ARCHIVAGE ELECTRONIQUE EN APPLICATION DE L'ARRETE ROYAL DU 22 MARS 1993 RELATIF A LA FORCE PROBANTE

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel*, notamment son article 16, § 4 ;

Vu 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*, notamment ses articles 2 à 6 ;

Vu le rapport d'auditorat de la Banque-carrefour du 18 juin 2006 ;

Vu le rapport présenté par Michel Parisse ;

A. CONTEXTE JURIDIQUE ET OBJET DE LA DEMANDE

1. Le 18 mai 2006, l'Office National de Sécurité Sociale a introduit une demande d'avis auprès du Comité Sectoriel de la Sécurité Sociale.
2. Cette demande d'avis porte sur une proposition de procédure d'archivage électronique des courriers entrants sur support papier, qui doit être soumise à l'agrément du Ministre ayant la Prévoyance sociale dans ses attributions, conformément à 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*.

B. EXAMEN DE LA DEMANDE

3. L'article 4, § 1^{er}, de la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (ci-après, « LVP ») dispose ce qui suit :

§ 1. Les données à caractère personnel doivent être :

1° traitées loyalement et licitement;

2° collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités, compte tenu de tous les facteurs pertinents, notamment des prévisions raisonnables de l'intéressé et des dispositions légales et réglementaires applicables (...);

3° adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement;

4° exactes et, si nécessaire, mises à jour (...)

5° conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement (...).

4. L'article 16, § 2, de la même LVP, dispose :

§ 2. Le responsable du traitement ou, le cas échéant, son représentant en Belgique, doit:

1° faire toute diligence pour tenir les données à jour, pour rectifier ou supprimer les données inexactes, incomplètes, ou non pertinentes, ainsi que celles obtenues ou traitées en méconnaissance des articles 4 à 8;

2° veiller à ce que, pour les personnes agissant sous son autorité, l'accès aux données et les possibilités de traitement soient limités à ce dont ces personnes ont besoin pour l'exercice de leurs fonctions ou à ce qui est nécessaire pour les nécessités du service;

3° informer les personnes agissant sous son autorité des dispositions de la présente loi et de ses arrêtés d'exécution, ainsi que de toute prescription pertinente, relative à la protection de la vie privée à l'égard des traitements des données à caractère personnel;

4° s'assurer de la conformité des programmes servant au traitement automatisé des données à caractère personnel avec les termes de la déclaration visée à l'article 17 ainsi que de la régularité de leur application.

§ 3. Toute personne agissant sous l'autorité du responsable du traitement ou celle du sous-traitant, ainsi que le sous-traitant lui-même, qui accède à des données à caractère personnel, ne peut les traiter que sur instruction du responsable du traitement, sauf en cas d'une obligation imposée par ou en vertu d'une loi, d'un décret ou d'une ordonnance.

§ 4. Afin de garantir la sécurité des données à caractère personnel, le responsable du traitement et, le cas échéant, son représentant en Belgique, ainsi que le sous-traitant doivent prendre les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification, l'accès et tout autre traitement non autorisé de données à caractère personnel.

Ces mesures doivent assurer un niveau de protection adéquat, compte tenu, d'une part, de l'état de la technique en la matière et des frais qu'entraîne l'application de ces mesures et, d'autre part, de la nature des données à protéger et des risques potentiels.

Sur avis de la Commission de la protection de la vie privée, le Roi peut édicter des normes appropriées en matière de sécurité informatique pour toutes ou certaines catégories de traitements.

Base légale de la demande d'avis.

5. La base légale de la demande est 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.*

Examen du dossier en fonction des conditions techniques de l'arrêté royal du 22 mars 1993.

6. L'évaluation des procédures introduites pour la reconnaissance est scindée en fonction des conditions techniques de l'article 3 de l'Arrêté royal du 22 mars 1993.
7. Ces conditions ont été passées en revue point par point dans le dossier de l'Office National de Sécurité Sociale.
8. Le rapport de l'auditorat de la Banque carrefour de la sécurité sociale est le résultat d'une démarche en collaboration avec les responsables et les techniciens de l'ONSS.
9. Cette démarche s'est déroulée en plusieurs étapes à savoir :
 - une séance d'information à la Banque carrefour de la sécurité sociale (ci-après, « BCSS ») pour informer l'ONSS du contenu nécessaire à l'approbation du dossier force probante,
 - la transmission par l'institution d'une première version de son dossier au service de sécurité de l'information de la BCSS,
 - la rédaction par le service de sécurité de la BCSS d'une série de questions complémentaires sur divers aspects du processus mis en place,
 - une visite du conseiller en sécurité en information de la BCSS sur le site de l'Office National de Sécurité Sociale où une démonstration a été organisée ainsi qu'une séance de questions / réponses,
 - deux réunions de travail pour une analyse critique du dossier ainsi que divers échanges de courriers électroniques entre le service de sécurité de la BCSS et les responsables techniques de l'ONSS afin de préciser divers détails,
 - la rédaction par l'Office National de Sécurité Sociale d'un dossier à destination du Comité Sectoriel de la Sécurité Sociale.

La proposition décrit la procédure avec précision.

10. Le dossier introduit par l'ONSS comprend une description des procédures mises en place pour l'enregistrement au travers de la solution 'Dossier Electronique de l'Employeur au sein de l'Office National de Sécurité Sociale' et la reproduction de ceux-ci sur un support lisible.
11. 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.

12. Le dossier présenté par l'Office National de Sécurité Sociale a conduit l'auditorat de la BCSS à vérifier que la solution décrite de gestion électronique des documents faisait une correcte application des règles énoncées dans le §2 de l'article 3 de l'Arrêté royal du 22 mars 1993.
13. Une attention particulière a, dans ce cadre, été apportée aux aspects suivants :
- aux composants des solutions techniques (architecture techniques et logiciels),
 - au circuit du traitement et de scannage des supports papier concernés,
 - au point de contrôle automatique et manuel selon les étapes du processus,
 - à la transmission des documents électroniques dans le dossier électronique de l'employeur,
 - aux formats des fichiers et de leurs conformités aux standards d'archivages garantissant la pérennité des données enregistrées,
 - à la gestion des incidents, des erreurs et les mécanismes de reprises ou de rejets éventuels de l'information,
 - aux instructions d'utilisation de la solution,
 - au contrôle de qualité et de quantité.

Les informations sont enregistrées systématiquement.

14. Le dossier de l'Office National de Sécurité Sociale 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 au mécanisme de validité des index,
 - la reconstruction des index,
 - la limitation d'accès aux index.

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

15. L'Office National de Sécurité Sociale a installé, entre autre, les mesures suivantes :
- l'architecture de l'infrastructure est répartie sur plusieurs serveurs dédiés à l'application d'archivage électronique et organisés de manière à favoriser la continuité de service et la reconstruction en cas d'incident majeur,
 - les données nécessaires à l'application sont réparties selon leurs finalités,
 - le système de sauvegarde est décrit avec des règles précises d'exécution selon un planning préétabli, des rotations de supports en fonction du planning ; à terme ces procédures seront intégrées dans le système global des sauvegardes de l'institution,
 - la période de rétention des supports et de conservation des supports est définie,
 - la sécurité d'accès logique repose sur l'utilisation d'une application de gestion de sécurité renforçant le niveau de sécurité d'un poste de travail classique Windows,

- la connexion au système d'information est possible via des postes de travail au sein de l'institution ou à distance en utilisant des protocoles sécurisés autorisés au sein du réseau de la Banque-carrefour de la sécurité sociale.
- en tant qu'institution du réseau primaire de la Banque-carrefour de la sécurité sociale, l'ONSS se doit de respecter les normes minimales de sécurité notamment en matière de plan catastrophe. Suite à un déménagement récent un nouveau plan est en cours d'élaboration. Le suivi de sa mise en place pourra être vérifié lors de l'évaluation du prochain questionnaire sur le respect des normes minimales de sécurité.

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.

16. L'Office National de Sécurité Sociale a équipé son système de :

- divers loggings informatisés et des carnets de suivi permettant de conserver les événements des différents composants à chaque stade du processus mis en place; l'accès à ces informations suit un processus sécurisé,
- les changements dans les applications internes ou dans la maintenance des logiciels suit un processus organisé.

17. Le Comité constate donc, sur base des vérifications effectuées par la BCSS, que le système d'archivage électronique tel que décrit par l'ONSS, semble correspondre aux normes imposées par l'arrêté royal du 22 mars 1993.

Par ces motifs,

le Comité sectoriel de la sécurité sociale

rend un avis positif sur la proposition de procédure d'archivage électronique des courriers entrants sur support papier datée du 3 avril 2006, proposée par l'Office National de Sécurité Sociale.

Michel PARISSE
Président